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

POLITIQUE

H000–POL-06

POLITIQUE DE GOUVERNANCE DES DONNÉES

Émetteur	Direction de la coordination de la mission universitaire
Direction responsable	Présidence-direction générale adjointe
Destinataires	La communauté, partenaires et usagers du CIUSSS de l'Estrie - CHUS
Entrée en vigueur	2024-06-13
Adopté par	Conseil d'administration **Date** 2024-06-13
Signature	*Original signé par :* Jacques Fortier, président du conseil d'administration

Table des matières

1. Mise en contexte

Le CIUSSS de l'Estrie – CHUS est un organisme public qui offre des services de santé et de services sociaux à la population de son territoire de desserte. Ces services s'étendent depuis les services de santé et sociaux de première ligne jusqu'aux services de santé spécialisés de troisième ligne. Le CIUSSS de l'Estrie – CHUS est aussi un établissement universitaire dont la mission est d'offrir des services de santé surspécialisés de quatrième ligne, ainsi que de développer la recherche, l'enseignement et l'évaluation des technologies et des modes d'intervention en santé.

De par la nature de sa mission, le CIUSSS de l'Estrie – CHUS interagit avec des renseignements confidentiels et sensibles. Son objectif : assurer, dans toutes ses activités de gestion de l'information, le respect du droit fondamental à la vie privée de ses usagers et de leurs proches, ainsi que des personnes œuvrant dans l'établissement.

Avec l'entrée en vigueur de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c.25, et de la *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, LQ 2023, c.5, le CIUSSS de l'Estrie – CHUS modernise ses règles et processus de gestion des renseignements personnels et des renseignements de santé et de services sociaux qu'il détient, notamment, par la publication d'une politique de gouvernance des données.

Dans la présente politique, le terme « donnée » est un terme générique qui comprend tout renseignement, toute information collectée, utilisée, communiquée et gérée par le CIUSSS de l'Estrie – CHUS dans le cadre de ses activités cliniques, administratives et universitaires.

2. Objectifs

La présente politique a pour but de présenter les règles qui encadrent la gestion des données dans l'établissement et les instances qui en sont responsables.

Les objectifs intermédiaires de la présente politique sont de :

- Présenter les comités responsables de la gestion des données dans l'établissement ainsi que leur mandat et leurs rôles et responsabilités;
- Préciser les rôles et les responsabilités des membres du personnel impliqués tout au long du cycle de vie des données, incluant les catégories de personnes pouvant utiliser des renseignements de santé ou de services sociaux dans l'exercice de leurs fonctions;
- Présenter les conditions et modalités suivant lesquelles des renseignements peuvent être communiqués à des fins de sécurité publique ou de poursuite liée à une infraction;
- Présenter le calendrier de mise à jour des produits ou services technologiques utilisés par l'établissement;
- Présenter les activités de formation et de sensibilisation que l'établissement offre à son personnel en matière de protection des renseignements;
- Présenter les modalités et conditions encadrant le dépôt d'une plainte par l'usager en cas de manquement aux obligations prévues par la loi, la réglementation applicable ou encore par la présente politique.

3. Définition des termes

- Calendrier de conservation : Document de nature légale qui a une force contraignante et qui puise ses sources dans le cadre juridique. Il identifie et décrit les documents institutionnels utiles et nécessaires au respect des obligations administratives, financières, juridiques ainsi qu'au bon fonctionnement de l'établissement. Il détermine, pour chaque document, le temps que l'on doit le conserver, le support sur lequel il doit être conservé et la manière dont on doit en disposer (s'il doit être conservé ou détruit à la fin de sa vie utile).

- **Chercheur lié** : personne physique dont la profession consiste à faire de la recherche scientifique et qui détient des privilèges de recherche octroyés par le conseil d'administration (CA) du CIUSSS de l'Estrie – CHUS ou des privilèges qui sont reconnus par l'établissement.[1] Ces privilèges sont accordés aux membres du CMDP et aux chercheurs des infrastructures de recherche de l'établissement. Les statuts de chercheurs faisant partie de cette catégorie sont les chercheurs universitaires, les chercheurs cliniciens et les chercheurs d'établissement.
- **Chercheur non lié** : personne physique dont la profession consiste à faire de la recherche scientifique et qui n'a aucun privilège de recherche ni de statut de chercheur au sein de l'établissement. Les statuts de chercheurs faisant partie de cette catégorie sont les chercheurs invités, les chercheurs de collège, les chercheurs externes et les chercheurs d'entreprises privées.

  L'établissement peut toutefois reconnaître les privilèges de recherche octroyés par un autre établissement public du réseau de la santé et des services sociaux (RSSS), par une université ou par un collège du Québec ou ailleurs au Canada, à condition que la personne accepte de se conformer aux exigences fixées à cet effet par l'établissement.
- **Cycle de vie :** l'ensemble des étapes que franchit une donnée : création, collecte, traitement, diffusion, transmission, utilisation, conservation et élimination (suppression et destruction).
- **Détenteur de l'information** : gestionnaire du CIUSSS de l'Estrie – CHUS dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources informationnelles qui la sous-tendent, relevant de la responsabilité de sa direction.[2] Le terme « détenteur d'actif informationnel » est aussi utilisé pour désigner ce rôle. Le terme « pilote de système » est utilisé pour désigner l'employé du détenteur qui agit à titre d'administrateur d'un système d'information déterminé et de son contenu.
- **Documents institutionnels** : Document, en format analogique ou numérique, produit ou reçu par l'établissement pour la réalisation de ses mandats et de sa mission, témoignant ainsi de l'ensemble de ses activités. Les documents institutionnels doivent être soumis au processus de la gestion documentaire.
- **Donnée sensible** : Une donnée qui, par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de respect de la vie privée (LQ2021 c.25, Art. 13 et Art. 110).

  Sont notamment considérées comme sensibles les données suivantes : l'origine raciale, ethnique ou nationale, l'identité ou l'expression de genre, la grossesse, l'orientation sexuelle, l'état civil, l'âge sauf dans la mesure prévue par la loi, la religion, la langue, la condition sociale, le handicap ou l'utilisation d'un moyen pour pallier ce handicap. Est également considéré comme sensible le traitement des données génétiques ou biométriques aux fins d'identifier une personne physique de manière unique ainsi que les données concernant la santé d'une personne physique.
- **Étudiant** : personne inscrite dans un programme de formation reconnu par le ministère de l'Éducation et de l'Enseignement supérieur, qui réalise des activités liées à son programme d'enseignement sous les auspices du CIUSSS de l'Estrie – CHUS et qui dispose d'un accès aux données de l'établissement lorsque cela est nécessaire à l'exercice de ses activités.
- **Incident de confidentialité :** Accès, utilisation ou communication non autorisée par la loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection.
- **Intervenant** : Toute personne qui, dans le cadre de son rôle ou de ses fonctions, doit planifier, coordonner ou dispenser des soins ou des services (incluant les soins et services médicaux) ou intervenir auprès de l'usager ou auprès des employés de l'établissement. Ce terme inclut la notion de professionnel (travailleur social, infirmier, psychoéducateur, etc.), de clinicien, de médecin, de résident, de stagiaire, d'étudiant, de bénévole, de professionnels de recherche et autres.

[1] Voir Politique H000-POL-05 Politique relative à l'attribution et au renouvellement des privilèges de recherche et des statuts de chercheur au CIUSSS de l'Estrie – CHUS.

[2] Inspiré du Guide de catégorisation de l'information, Secrétariat du Conseil du Trésor, Gouvernement du Québec, 2016.

- **Intervenant professionnel :** Intervenant titulaire d'un permis de pratique délivré par un ordre professionnel ou le Collège des médecins du Québec, et inscrit au tableau de cet ordre ou de ce collège. Cette catégorie inclut les résidents en médecine.
- **Intervenant non professionnel :** Intervenant non titulaire d'un permis de pratique délivré par un ordre professionnel ou le Collège des médecins du Québec ni inscrit au tableau de cet ordre ou de collège.
- **Personne concernée** : personne physique à qui se rapportent les renseignements personnels. Il peut s'agir d'un usager de l'établissement, d'un membre de son personnel ou de toute autre personne physique dont l'établissement détient des renseignements personnels.
- **Produit ou service technologique :** Un équipement, une application ou un service requis afin de recueillir, de conserver, d'utiliser ou de communiquer un renseignement personnel ou de santé, tels une banque ou un système d'information, un réseau de télécommunication, une infrastructure technologique, un logiciel ou une composante informatique d'un équipement médical.
- **Renseignement personnel :** Tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.
- **Renseignement de santé et de services sociaux :** Tout renseignement qui permet, même indirectement, d'identifier une personne et qui répond à l'une des caractéristiques suivantes.

  1. Il concerne l'état de santé physique ou mentale de cette personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de la personne ;
  2. Il concerne tout matériel prélevé sur cette personne dans le cadre d'une évaluation ou d'un traitement, incluant le matériel biologique, ainsi que tout implant ou toute orthèse, prothèse ou autre aide suppléant à une incapacité de cette personne ;
  3. Il 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 groupements qui les ont offerts ;
  4. Il a été obtenu dans l'exercice d'une fonction prévue par la Loi sur la santé publique (chapitre S-2.2) ;
  5. Toute autre caractéristique déterminée par règlement du gouvernement.

  De plus, un renseignement permettant l'identification d'une personne tels son nom, sa date de naissance, ses coordonnées ou son numéro d'assurance maladie est un renseignement de santé et de services sociaux lorsqu'il est accolé à un renseignement répondant aux caractéristiques ci-haut mentionnées ou qu'il est recueilli en vue de l'enregistrement, de l'inscription ou de l'admission de la personne concernée dans un établissement ou de sa prise en charge par un autre organisme du secteur de la santé et des services sociaux.

  Malgré le précédent paragraphe, un renseignement qui concerne un membre du personnel d'un organisme du secteur de la santé et des services sociaux ou un professionnel qui y exerce sa profession, y compris un étudiant ou un stagiaire, ou qui concerne un mandataire ou un prestataire de services d'un tel organisme n'est pas un renseignement de santé et de services sociaux lorsqu'il est recueilli à des fins de gestion des ressources humaines.
- **Stagiaire** : étudiant qui est en période de formation pratique, d'apprentissage ou de perfectionnement au CIUSSS de l'Estrie – CHUS et qui dispose d'un accès aux données de l'établissement lorsque cela est nécessaire à l'exercice de ses fonctions.

4. Champs d'application

La présente politique s'applique :

- À l'ensemble des données détenues par le CIUSSS de l'Estrie – CHUS et utilisées dans le cadre de ses activités courantes et dans des cadres autres que ceux pour lesquels les données ont été collectées initialement (utilisation secondaire des données).
- À toutes les personnes œuvrant dans l'organisation et qui ont connaissance de données dans le cadre de leurs fonctions ou de leur implication avec l'organisation.

- À toutes les installations de l'organisation, pour tous les services et programmes qui y sont rattachés.

5. Cadre juridique

Au Québec, plusieurs lois et normes régissent la protection des renseignements personnels, dont notamment :

- Charte des droits et libertés de la personne (RLRQ c. C-12);
- Code civil du Québec (RLRQ c. CCQ-1991);
- Directive gouvernementale sur la sécurité de l'information (2021), découlant de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03, a. 20);
- Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives, (LQ 2023, c. 5);
- 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 sur la protection de la jeunesse (RLRQ, c. P-34.1);
- Loi sur le système de justice pénale pour adolescent (L.C. 2002, ch. 1);
- Loi visant à lutter contre la maltraitance envers les aînés et toute autre personne majeure en situation de vulnérabilité (Chapitre L-6.3);
- Loi sur la protection des personnes dont l'état mental présente un danger pour elles-mêmes ou pour autrui (RLRQ, c. P-38.001);
- Loi visant à favoriser la protection des personnes à l'égard d'une activité impliquant des armes à feu (RLRQ, c. P-38.0001);
- Code des professions (RLRQ, c. C-26);
- Codes de déontologie des différents ordres professionnels;
- Loi sur la santé publique (RLRQ, c. S-2.2);
- Loi sur les archives (RLRQ, c. A-21.1).

6. Structure de gouvernance

6.1 Principes directeurs

Le principe fondamental guidant la gestion des données précise que le processus décisionnel est centralisé à la plus haute instance de gouvernance et l'intendance est distribuée dans les directions impliquées dans la gestion des données à travers l'organisation.

Les orientations en matière de gestion des données concernent notamment la sécurité et protection de l'information, la transparence en matière de décisions et d'actions, l'imputabilité des acteurs impliqués, le respect du cadre légal et réglementaire et le comportement éthique et déontologique face aux données.

La structure de gouvernance respecte les principes directeurs suivants :

- La structure de gouvernance s'intègre à la vision, à la mission et au plan d'organisation de l'établissement;
- La coordination des activités est mobilisée selon un regroupement logique des domaines d'affaires de la gestion des données;
- 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.

6.2 Structure hiérarchique

Les comités impliqués dans la gestion des données se retrouvent dans les trois niveaux de gestion : stratégique, tactique et opérationnel. Pour plus de détails, le lecteur peut consulter le Cadre de gouvernance des données du CIUSSS de l'Estrie – CHUS.

- Au niveau stratégique, on retrouve le Comité directeur de la gestion des données dont les fonctions sont assumées par le Comité stratégique de la mission universitaire;
- Au niveau tactique, on retrouve deux instances : le Comité de coordination de la gestion des données, de la qualité et de l'éthique et le Comité de coordination de la sécurité de l'information, de la gestion des accès et la protection des renseignements personnels;
- Au niveau opérationnel, on retrouve le Comité de gestion et d'assurance qualité des données, le Comité d'éthique de la recherche, le Comité d'évaluation des facteurs relatifs à la vie privée, le Centre DORISE et les détenteurs de l'information.

D'autres personnes assument un rôle important au sein de la gouvernance des données :

- Les responsables de l'accès à l'information et de la protection des renseignements personnels, volet clinique;
- Le responsable de l'accès à l'information et de la protection des renseignements personnels, volet administratif;
- 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;
- Le responsable de la gestion documentaire.

7. Rôles et responsabilités

- Le Président-directeur général (PDG) :
  - Est le premier responsable de la protection des renseignements et de l'accès à l'information que l'établissement détient;
  - Veille à assurer le respect et la mise en œuvre du cadre légal et réglementaire applicable à la protection des renseignements personnels et à la protection des renseignements de santé et de services sociaux;
  - S'assure que sont prises en charge les mesures de sécurité propres à assurer la protection des renseignements collectés, utilisés, communiqués, conservés ou éliminés et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support;
  - Instaure les mesures de protection des renseignements personnels et des renseignements de santé et de services sociaux édictées à cette fin par règlement du gouvernement.
- Les comités de la structure hiérarchique de gouvernance des données
  - La structure fonctionnelle de la gouvernance des données de l'établissement ainsi que les rôles et responsabilités des principaux comités et intervenants en la matière sont définis dans le Cadre de gouvernance des données.

    En bref :

    - Le **Comité directeur de la gestion des données** 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.

- 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 concernant ses responsabilités. Il s'assure de la gestion et du suivi des priorités de développement du Centre de valorisation des données, DORISE.
- Le **Comité de coordination de la sécurité, de l'accès et de la protection des renseignements personnels** assure les responsabilités légales de deux comités exigés par la Loi, soit le Comité sur la sécurité de l'information et le Comité sur l'accès et la protection des renseignements personnels. Il est responsable de l'application opérationnelle et du respect de l'ensemble des règles et exigences encadrant la sécurité de l'information, l'accès aux données et aux documents, ainsi que de la protection des renseignements personnels.
- Le **Comité de gestion et de l'assurance qualité des données** assume le mandat opérationnel d'amélioration continue de la qualité des données.
- Les **détenteurs de l'information** s'assurent que les informations et 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.
- Le **Centre DORISE** est un centre de valorisation des données 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 Comité d'évaluation des facteurs relatifs à la vie privée** est un comité multidisciplinaire conçu spécifiquement pour évaluer les impacts de projets impliquant l'accès, sans obtenir de consentement, à des renseignements personnels ou des renseignements de santé ou de services sociaux, sur la vie privée des personnes concernées par ces derniers. Trois types de projets sont particulièrement ciblés :
  - Les projets de recherche;
  - Les projets d'acquisition, de développement ou de refonte de produits, de systèmes d'information, de services technologiques ou de systèmes de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou l'élimination de renseignements personnels ou de renseignements de santé ou de services sociaux;
  - Les projets impliquant la communication hors Québec, avec ou sans consentement, desdits renseignements.

- **Les responsables de l'accès à l'information et de la protection des renseignements personnels**
  - Sept ressources du CIUSSS de l'Estrie – CHUS assument les fonctions de responsables de l'accès à l'information et de la protection des renseignements personnels. Une ressource couvre l'accès à l'information administrative et la protection des renseignements personnels contenus dans les bases de données et documents administratifs, comprenant tout document ou base de données portant sur les activités administratives de l'établissement et incluant, sans s'y restreindre, les dossiers des employés. Les six autres couvrent l'accès à l'information clinique et la protection des renseignements personnels des usagers et des renseignements de santé et de services sociaux des usagers du CIUSSS de l'Estrie – CHUS. Tous assument les mêmes responsabilités dans leur champ d'application respectif. Ces rôles et responsabilités sont décrits dans le document XXXX-XXX-0X – Rôles et responsabilité du responsable de l'accès à l'information et de la protection des renseignements personnels détenus par le CIUSSS de l'Estrie – CHUS (à venir).

- **Les responsabilités en matière de sécurité de l'information** :
  - La structure fonctionnelle de la sécurité de l'information de l'établissement ainsi que les rôles et responsabilités des principaux intervenants en la matière sont définis dans le Cade de gestion de la sécurité de l'information. Les mécanismes plus spécifiques liés à la gestion des données sont détaillés dans le Cadre de gouvernance des données, section 3 – Assurer la vie privée des personnes;
  - Les mesures de sécurité adoptées afin d'assurer la protection des renseignements détenus par l'établissement, incluant les mécanismes de journalisation, sont détaillées dans le document B001-CDG-0X - Cadre de gestion de la sécurité de l'information (en cours de rédaction).
- **Les responsabilités en matière de gestion intégrée des risques et de gestion des incidents** :
  - L'analyse des risques liés à la collecte, l'accès, l'utilisation, la communication, la conservation ou l'élimination de renseignements détenus par l'établissement fait partie des processus du Système global de gestion intégrée des risques mis en place pour l'ensemble des installations du CIUSSS de l'Estrie – CHUS. Ce système soutient le développement d'une vision d'ensemble des risques organisationnels majeurs, incluant notamment les risques liés à la transformation, les risques cliniques dans le cadre de la prestation des soins et des services aux usagers, les risques administratifs et ceux concernant la présente politique. Plus de détails se trouvent dans le document E000-POL-03 Politique sur la gestion intégrée des risques ainsi que dans le Cadre de gouvernance des données, section 3 – Assurer la vie privée des personnes.
  - L'analyse et le traitement des incidents liés à la collecte, l'accès, l'utilisation, la communication, la conservation ou l'élimination non autorisée des renseignements détenus par l'établissement font partie des processus de gestion de la sécurité de l'information et de la confidentialité des renseignements personnels. Plus de détails sont disponibles dans les documents B001-POL-03 Politique de la sécurité de l'information, K000-POL-01 Politique de confidentialité des renseignements personnels et le Cadre de gouvernance des données, section 3 – Assurer la vie privée des personnes.
  - Les mécanismes d'accès aux données détenues par l'établissement incluant les renseignements personnels et les renseignements de santé ou de services sociaux sont détaillés dans le Cadre de gouvernance des données, section 3 – Assurer la vie privée des personnes ainsi que dans un chapitre du Cadre de gestion de la sécurité de l'information dédié à la gestion des identités et des accès aux données (actuellement en rédaction).
- **Les responsabilités en matière de gestion documentaire** (se référer au document E000-POL-02 – Politique sur la gestion intégrée des documents pour plus d'information) :
  - Appliquer les bonnes méthodes de gestion des documents institutionnels, au regard de leur collecte, classification, diffusion, conservation et destruction;
  - Assurer la bonne marche des opérations, des processus et des techniques de gestion des documents produits, reçus ou utilisés dans le cadre des activités de l'établissement quels que soient leurs supports, et ce, à toutes les étapes du cycle de vie des documents (depuis leur réception/création jusqu'à leur destruction ou à leur versement aux archives);
  - Appliquer les règles de conservation des documents et leurs contenus prescrites dans le calendrier de conservation de l'établissement;
  - Assurer la gestion du calendrier de conservation de l'établissement;
  - Assurer la confidentialité et la protection des informations contenues dans les documents en conformité avec les politiques et règlements de l'établissement.

- **Toute personne œuvrant dans l'établissement qui, dans le cadre de ses fonctions, est autorisée à collecter, consulter, utiliser, communiquer ou éliminer des renseignements personnels ou des renseignements de santé ou de services sociaux, ou d'autres renseignements sensibles, a l'obligation d'en protéger le caractère confidentiel. À cette fin, elle doit :**
  - Signer un engagement à la confidentialité et respecter les règles et conditions qui y sont rattachées;
  - Participer aux activités de formation et de sensibilisation à la protection des renseignements personnels et des renseignements de santé ou de services sociaux qui lui sont offerts;
  - Faire preuve de la plus grande vigilance lorsqu'elle traite des données sensibles détenues par le CIUSSS de l'Estrie – CHUS, incluant des renseignements personnels et des renseignements de santé ou de services sociaux, afin d'en protéger leur caractère confidentiel;
  - Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer;
  - Informer l'établissement dès qu'elle constate ou qu'elle a une raison valable de croire qu'il existe un risque potentiel ou avéré de bris de confidentialité et prendre tous les moyens nécessaires afin de minimiser le préjudice susceptible de découler d'un tel incident.

  Parce que nécessaires à l'exercice de leurs fonctions, certaines catégories de personnes sont autorisées à consulter, utiliser ou communiquer des renseignements personnels ou des renseignements de santé ou de services sociaux détenus par l'établissement. Elles sont soumises aux obligations citées ci-haut. Il s'agit :

  - D'intervenants professionnels ou non professionnels
    - Qui dispensent des soins aux usagers;
    - Qui rendent des services aux usagers (soutien administratif, soutien technique, ressources humaines, soutien juridique, soutien financier, soutien à la qualité des pratiques, protection des renseignements personnels, autres);
  - D'étudiants ou stagiaires supervisés par ces mêmes intervenants et qui œuvrent dans les mêmes directions, départements ou services au sein de l'établissement;

  Les chercheurs liés à l'établissement, qu'ils soient des chercheurs universitaires, des chercheurs cliniciens ou des chercheurs d'établissement peuvent accéder, utiliser ou communiquer des renseignements personnels ou des renseignements de santé et de services sociaux détenus par l'établissement lorsque ces renseignements sont nécessaires à la réalisation d'un projet de recherche et après avoir reçu l'autorisation de la plus haute autorité de l'établissement, à moins que la ou les personnes concernées n'aient refusé l'accès à ces renseignements.

  Les chercheurs non liés à l'établissement, qu'ils soient des chercheurs universitaires, des chercheurs invités, des chercheurs de collège, des chercheurs externes ou des chercheurs d'entreprises privées peuvent accéder, utiliser ou communiquer des renseignements personnels ou des renseignements de santé et de services sociaux détenus par l'établissement lorsque ces renseignements sont nécessaires à la réalisation d'un projet de recherche et après avoir reçu l'autorisation concertée du centre d'accès pour la recherche et de la plus haute autorité de l'établissement, à moins que la ou les personnes concernées n'aient refusé l'accès à ces renseignements.

  Les partenaires du CIUSSS de l'Estrie - CHUS, qu'ils soient des particuliers ou des organismes du réseau public ou du réseau privé, incluant les entreprises, ou encore des organismes gouvernementaux, peuvent consulter, utiliser ou communiquer des renseignements personnels ou des renseignements de santé et de services sociaux détenus par l'établissement lorsque ces renseignements sont nécessaires à la réalisation d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise et après avoir reçu l'autorisation de la plus haute autorité de l'établissement. Cette autorisation n'est valable que si deux conditions sont remplies :

  - Une évaluation des facteurs relatifs à la vie privée a été effectuée et elle démontre, notamment, que les renseignements bénéficieraient d'une protection adéquate au regard des principes de protection des renseignements personnels généralement reconnus;

- Une entente écrite dûment signée entre les parties tient compte notamment des résultats de l'évaluation et des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

Dans le cas d'un particulier ou d'un organisme du secteur privé, l'entente de la deuxième condition peut être remplacée par un mandat écrit ou un contrat écrit et dûment signé entre les parties. Les conditions suivantes doivent être remplies pour obtenir l'autorisation de l'établissement :

- Le mandat ou le contrat doit spécifier que les renseignements ne sont utilisés que dans l'exercice du mandat ou dans l'exécution du contrat;
- Le mandat ou le contrat doit indiquer les mesures que le partenaire doit prendre pour assurer la protection du caractère confidentiel des renseignements consultés, utilisés ou communiqués.

8. Conditions et modalités suivant lesquelles des renseignements peuvent être communiqués à des fins de sécurité publique ou de poursuite des infractions

Le CIUSSS de l'Estrie – CHUS respecte le cadre législatif et réglementaire auquel il est soumis lorsqu'il communique des renseignements qu'il détient dans l'une ou l'autre des situations suivantes :

- Lorsqu'un risque sérieux de mort ou de blessures graves menace la vie d'une personne ou d'un groupe de personnes.
- Lorsque le renseignement est nécessaire à un corps de police pour la planification ou l'exécution d'une intervention adaptée aux caractéristiques d'une personne ou de la situation, dans l'une ou l'autre des situations suivantes : le corps de police vient en aide à l'établissement pour dispenser des services à la personne ou il agit en concertation ou partenariat avec l'établissement dans le cadre de pratiques mixtes d'interventions psychosociales et policières.
- Lorsque le renseignement est nécessaire aux fins d'une poursuite pour une infraction à une loi applicable au Québec.

Quant aux personnes en danger grave d'un passage à l'acte suicidaire, le personnel clinique assure un suivi étroit, conformément au document CREF-SM-001 *Cadre de référence – Suivi étroit auprès des personnes en danger grave d'un passage à l'acte suicidaire – pour la clientèle de 14 ans et plus*. Le personnel s'assure du respect des modalités de divulgation de renseignements confidentiels référées à la section 4 - Cadre juridique et normatif du Cadre de référence. De plus, dans l'objectif de prévenir un acte de violence, dont le suicide, le personnel se réfère à la directive K210-DIR-02 *Divulgation sans autorisation de renseignements confidentiels contenus au dossier de l'usager en vue de prévenir un acte de violence dont le suicide*.

9. Calendrier de mise à jour des produits ou services technologiques utilisés par l'établissement

Les produits et services technologiques utilisés par l'établissement sont inscrits dans un registre. Les modalités de maintien et de mise à jour du registre sont indiquées dans le document XXXX-DIR-0X Directive sur l'élaboration et la gestion du registre des produits et services technologiques (à venir).

10. Activités de formation et de sensibilisation que l'établissement offre à son personnel en matière de protection des renseignements

Dès l'embauche, les nouveaux employés reçoivent une formation sur la confidentialité des renseignements et signent un engagement à la confidentialité. Des capsules de sensibilisation au respect de la confidentialité et sécurité de l'information sont disponibles à la communauté du CIUSSS de l'Estrie - -CHUS. La signature de cette entente est obligatoire pour tout membre du personnel, médecin, étudiant et stagiaire, bénévole et fournisseur de services.

Tous les employés, même ceux qui n'ont pas accès aux dossiers des usagers doivent obligatoirement suivre la formation en cyber sécurité dispensée sur la plateforme ENA (Environnement numérique d'apprentissage). Des informations sur le sujet se trouvent aussi dans l'intranet du CIUSSS de l'Estrie – CHUS : section SÉCURITÉ DE L'INFORMATION.

Des rappels, par voie de notes à l'ensemble de la communauté du CIUSSS de l'Estrie - -CHUS sont effectués concernant les devoirs du personnel envers la confidentialité.

11. Processus de traitement des incidents de confidentialité

L'établissement gère les incidents de confidentialité en conformité avec la directive relative à la gestion des incidents de confidentialité impliquant des renseignements personnels dont il s'est doté.

12. Gestion des accès et journalisation

Chaque utilisateur de données, qu'il s'agisse de renseignements personnels, de renseignements de santé et de services sociaux ou d'autres données sensibles possède un identifiant unique.

L'accès aux systèmes d'information, à partir de l'identifiant unique, est géré sur la base des profils d'emploi des utilisateurs.

Les mécanismes de journalisation mis en place permettent de connaître qui a révisé ou interagi avec quelle information et à quel moment (date, heure, minute).

Les informations de journalisation sont collectées automatiquement et disponibles pour vérifications et audits. La durée de vie de ces informations respecte le calendrier de conservation de l'établissement.

13. Modalités et conditions encadrant le dépôt d'une plainte par l'usager en cas de manquement aux obligations prévues par la loi, la réglementation applicable ou encore par la présente politique

- La personne concernée qui estime que ses droits n'ont pas été respectés ou qui désire signaler tout manquement à la présente politique peut s'adresser à un gestionnaire, à un employé assumant des responsabilités d'encadrement des pratiques cliniques ou administratives, ou à un responsable de l'application de la Loi sur l'accès à l'information et la protection des renseignements personnels ou de la Loi sur les renseignements de santé et de services sociaux.
- Il peut aussi déposer une plainte à la Commissaire aux plaintes de l'établissement en suivant les modalités décrites dans le règlement B000-RGM-02 Règlement sur la procédure d'examen des plaintes.

14. Dispositions finales

14.1 Version antérieure

Il n'existe aucune version antérieure. La présente politique est nouvelle.

14.2 Prochaine révision

La présente politique doit faire l'objet d'une révision au plus tard dans les quatre (4) années suivant son entrée en vigueur.

Annexe A - Historique des versions

Description	Auteur/Responsable	Date / Période
Création	Renald Lemieux, Consultant, DCMU	2023
Consultation	Comité stratégique de la mission universitaire (CSMU)	10 avril 2024
Consultation	Comité des directeurs (CD)	7 mai 2024
Consultation	Comité de la mission universitaire du CA (CMUCA)	30 mai 2024
Adoption	Conseil d'administration (CA)	13 juin 2024