Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-36
	Direction responsable : Direction des ressources informationnelles
	Adoptée par le comité de direction le : 5 juillet 2018 Révisée le : 9 janvier 2024
	Approuvée par le conseil d'administration le :
	Entrée en vigueur le : 10 janvier 2024

TITRE : Politique de gestion des identités et des accès des actifs informationnels

CONSULTATIONS	☐ Cadres :
☐ Conseil des infirmières et infirmiers :	☐ Autres :
☐ Conseil multidisciplinaire :	
☐ Conseil des médecins, dentistes et pharmaciens :	

1. FONDEMENTS

La politique de gestion des identités et des accès des actifs informationnels du Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale (CIUSSS de la Capitale-Nationale) découle de la Politique provinciale de sécurité de l'information du ministère de la Santé et des Services sociaux (MSSS). Cette politique découle elle-même de la Loi modifiant la loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du Gouvernement (LQ 2021, c 22), ci-après LGGRI, de la Directive gouvernementale sur la sécurité de l'information (Décret 1514-2021 du 8 décembre 2021) ainsi que du cadre gouvernemental de gestion de la sécurité de l'information du MSSS. Cette politique est également en complément à la Politique relative à la tenue du dossier de l'usager et la protection des renseignements personnels (PO-22) du CIUSSS de la Capitale-Nationale concernant les accès au dossier de l'usager.

2. PRINCIPES

Le CIUSSS de la Capitale-Nationale détient, dans le cadre de sa mission, des renseignements personnels et confidentiels dont le degré de sensibilité et de criticité, en termes de disponibilité, d'intégrité et de confidentialité, peut être élevé. Cette information doit donc être préservée, tout au long de son cycle de vie, de toute divulgation, de tout accès et de toute utilisation non autorisée.

La présente politique fait partie d'un ensemble de documents d'encadrement, permettant au CIUSSS de la Capitale-Nationale d'assurer pleinement la protection des informations qu'il détient, dans le cadre de l'exercice de sa mission.

3. OBJECTIFS

La présente politique édicte des lignes directrices qui visent à encadrer les conditions dans lesquelles l'accès aux actifs informationnels du CIUSSS de la Capitale-Nationale est permis. Elle aborde, notamment, les modalités d'identification et d'authentification des utilisateurs, ainsi que les niveaux d'autorisation requis aux ressources.

Elle définit également les responsabilités des principaux intervenants.

4. CHAMP D'APPLICATION

La présente politique s'applique à :

- L'information numérique que détient le CIUSSS de la Capitale-Nationale dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers;
- L'information numérique confiée au CIUSSS de la Capitale-Nationale en vertu d'une entente et qui est identifiée comme devant faire l'objet d'un contrôle d'accès;
- L'infrastructure technologique du CIUSSS de la Capitale-Nationale;
- Toute personne physique ou morale qui, à titre d'employé, de médecin, de consultant, de stagiaire, de partenaire ou de fournisseur, a un accès, sur place ou à distance, à l'information numérique, hébergée sur site ou en infonuagique, dont la sécurité est assurée par le CIUSSS de la Capitale-Nationale.

5. DÉFINITIONS

Pour la présente politique, les termes et expressions qui suivent signifient :

- **Actif informationnel :** Actif informationnel au sens de la Loi concernant le partage de certains renseignements de santé, soit, une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé.

  Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

- **Authentification :** Acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif.

- **Confidentialité :** Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées.

- **Cycle de vie de l'information :** L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'établissement.

- **Détenteur :** Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est notamment de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité de son unité administrative.

- **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

- **Gestion intégrée des risques de sécurité :** Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques de sécurité à tous les niveaux hiérarchiques de l'organisation.

- **Habilitation :** Attribution des droits d'accès d'un utilisateur à des données et/ou à des applications spécifiques.

- **Identification** : L'identification est un processus de vérification permettant d'identifier, de façon unique, un utilisateur. Un tel processus peut permettre d'établir l'identité dont un utilisateur se réclame afin d'avoir accès à un actif informationnel.

- **Intégrité :** Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

- **Irrévocabilité :** Propriété d'un acte d'être définitif et qui est explicitement attribué à la personne qui l'a posé ou au dispositif avec lequel cet acte a été accompli.

- **Preuve de l'identité essentielle** : un permis de conduire, une carte d'assurance maladie, une preuve de citoyenneté canadienne ou tout autre document officiel émanant d'une autorité étatique, une source considérée fiable, établissant son identité (prénom, nom) et sa date de naissance avec photo.

- **Preuve de l'identité contextuelle** : une preuve, autre qu'une preuve de l'identité essentielle, mentionnant un attribut de l'identité considéré pertinent pour l'identification. Par exemple, son unité administrative, le nom de son gestionnaire et le besoin nécessitant l'accès.

- **Principe du moindre privilège :** Le principe du moindre privilège stipule qu'il ne faut octroyer aux utilisateurs que les privilèges strictement nécessaires à la réalisation de leur travail.

- **Principe de séparation des tâches :** Principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible sont réparties entre plusieurs entités (personnes, processus, etc.) afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité. Il vise à limiter les possibilités d'abus et d'infraction par une seule personne.

- **Renseignements personnels :** Sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier. Le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne.

- **Réseau :** Ensemble des organismes qui relèvent du Dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la LGGRI.

- **Risque de sécurité de l'information :** Probabilité que survienne un événement préjudiciable, plus ou moins prévisible, qui peut affecter la réalisation des objectifs de l'établissement ou du Réseau.

- **Utilisateur :** Toute personne physique ou morale, groupe ou entité administrative qui entend utiliser ou autrement bénéficier d'un ou de plusieurs actifs informationnels sous la responsabilité de l'établissement. Notamment, les stagiaires, les résidents, les externes, les chercheurs, les médecins, le personnel et les tiers tels que les fournisseurs et les partenaires, etc.

6. MODALITÉS

- Lors de l'identification d'un utilisateur, une preuve de l'identité essentielle et une preuve de l'identité contextuelle en provenance d'une telle personne peuvent lui être exigées ainsi qu'à son gestionnaire en fonction du niveau d'assurance déterminé pour l'accès à un actif informationnel;
- Le niveau d'assurance déterminé pour un actif informationnel dépend de l'information contenue au sein du registre d'autorité[1], qui inclut le niveau de disponibilité, d'intégrité et de confidentialité pour chaque actif, ainsi que de l'évaluation des risques associée;
- La vérification de l'identité d'un utilisateur peut être effectuée sur place ou à distance, en employant tout moyen qui permet de voir et d'entendre l'utilisateur faisant l'objet d'une telle vérification;
- Tout utilisateur devant accéder à des actifs informationnels du CIUSSS de la Capitale-Nationale et pour lesquels une traçabilité des activités est requise, se voit attribuer un code d'accès composé d'un identifiant unique associé à un authentifiant, qui est généralement un mot de passe, mais qui peut être également un jeton physique ou une caractéristique biométrique dans certains cas;
- Chaque code d'accès ne doit être attribué qu'à une seule personne à des fins d'imputabilité et de traçabilité;
- Toute demande d'accès à un actif informationnel doit comporter les informations requises et respecter les délais requis spécifiés dans les procédures de demande d'accès de tous types (accès au réseau, accès internet particulier, accès à une application, accès à un répertoire, accès aux services sans fil, accès à distance, accès à un système clinique, etc.);
- Les comptes d'accès au réseau et les comptes utilisateurs des applications dits « génériques » ne sont pas permis, à moins d'en justifier l'utilisation auprès de l'équipe de sécurité de l'information du CIUSSS de la Capitale-Nationale qui en définira les modalités d'utilisation;

[1] Se référer à la Politique relative à la sécurité de l'information (PO-13).

- En cas de partage ou de fraude portant sur un identifiant d'accès, ou un mot de passe utilisateur, le détenteur de l'identifiant concerné devra promptement veiller à demander la suspension de l'identité et procéder à une déclaration d'incident de sécurité de l'information ;
- Il est formellement interdit, par le biais de mécanismes quelconques, de manière délibérée ou consentie, d'utiliser, d'usurper ou de tenter d'usurper l'identité conférée à autrui;
- L'authentification aux services externes qui permet d'accéder aux données sensibles doit être protégée par un dispositif d'authentification multifacteur (MFA) et une mesure de protection anti-robot dans la page d'authentification dans le but de prévenir tout accès automatisé frauduleux;
- Les détenteurs des actifs informationnels sont imputables de la gestion des identités et des accès aux actifs qui sont sous leur tutelle en s'appuyant sur les pilotes en charge des tâches d'administration;
- La gestion du mot de passe doit respecter les principes suivants :
    1. Tout mot de passe émis par le CIUSSS de la Capitale-Nationale doit être temporaire (expiration définie dans le temps dès la création);
    2. L'utilisateur doit lui-même choisir son mot de passe;
    3. L'utilisateur doit pouvoir utiliser les services et accéder aux actifs informationnels du CIUSSS de la Capitale-Nationale sans avoir à fournir son mot de passe de façon verbale ou lisible à l'écran ou sur un actif;
    4. Des mécanismes doivent être mis en place, pour :
        - Imposer l'utilisation d'un mot de passe respectant les règles de complexité définies pour les différents actifs informationnels;
        - Faire expirer un mot de passe après un délai déterminé ou lorsque survient un changement chez des utilisateurs disposant du mot de passe d'un compte partagé;
        - Rendre impossible la réutilisation des derniers mots de passe;
        - Respecter les modalités de gestion relatives à la saisie infructueuse du mot de passe et à sa modification en cas de perte ou d'oubli.
- Le principe du « moindre privilège » doit être appliqué dans la définition des accès accordés à un utilisateur du CIUSSS de la Capitale-Nationale;
- Le principe de « séparation des tâches » doit être appliqué dans la définition des accès accordés à un utilisateur du CIUSSS de la Capitale-Nationale;
- La présente politique est une politique de gestion des accès « fermée », ainsi, tout ce qui n'est pas expressément autorisé est interdit;
- La gestion des droits d'accès basée sur les rôles où l'appartenance à un groupe est privilégiée;
- L'octroi, l'utilisation ainsi que les justificatifs d'attribution des privilèges d'accès « comptes à hauts privilèges » doivent être encadrés et contrôlés rigoureusement par de la journalisation;
- Le départ, le transfert et la mutation d'un utilisateur ainsi que tout autre changement relatif à ses tâches et ses fonctions doit conduire systématiquement à la révision de ses droits d'accès;
- Les codes d'accès doivent être désactivés lors du départ de l'utilisateur associé et ses privilèges d'accès doivent être révoqués;
- Les règles d'autorisation et de restriction des accès à distance doivent être clairement définies et approuvées par les détenteurs de l'information;
- Les accès attribués pour chaque actif informationnel doivent être revus périodiquement par les détenteurs des actifs informationnels. Les droits, leurs modifications et leurs violations doivent être répertoriés;

- Tous les utilisateurs d'un actif informationnel acceptent la mise en place ou l'utilisation des journaux d'activités permettant de détecter des menaces ainsi que de détecter et de retracer toute activité et tout accès non autorisé ou nécessaire aux tâches de l'utilisateur;
- Un registre de gestion des accès centralisé est utilisé pour appliquer le processus de gestion des accès. Le registre est mis à jour en fonction des règles définies pour la révision des accès;
- Le niveau d'assurance pour chaque actif informationnel permet de déterminer les profils d'accès adéquat;
- Des règles sont définies pour la révision des accès en tenant compte des changements relatifs au profil d'accès, de la situation personnelle de l'utilisateur (maladie, congé prolongé, etc.), de son statut professionnel ou tout autre élément demandé par le CSIO;
- Un audit des mécanismes de contrôle de gestion des accès doit être effectué en se référant au rapport de revue des droits d'accès fourni par les détenteurs des actifs informationnels.

7. RESPONSABILITÉS

Dans le cadre de la mise en œuvre du processus de gestion des identités des accès, les principales responsabilités assignées par la présente politique sont :

7.1 LE COMITÉ DE DIRECTION DE L'ÉTABLISSEMENT

- Approuve la présente politique et s'assure de sa diffusion;
- S'assure de la mise en place du processus de gestion des identités et des accès à l'information;
- Apprécie les indicateurs de gestion et émet des recommandations au CSIO et aux détenteurs le cas échéant;

7.2 LE DIRECTEUR DES RESSOURCES INFORMATIONNELLES

- Met en place les solutions technologiques répondant aux exigences de la politique de gestion des identités et des accès et intègre dans les ententes et contrats les clauses garantissant le respect des exigences de sécurité de l'information, dont celles se rapportant à la gestion des identités et des accès;
- Met en place les outils de surveillance et de journalisation des accès requis.
- Met en place les mesures de protection techniques contre les accès non autorisés.

7.3 LE DIRECTEUR DES RESSOURCES HUMAINES ET DES COMMUNICATIONS (DRHC)

- Met en œuvre les processus nécessaires pour obtenir une preuve de l'identité essentielle lors du recrutement de ressources humaines ou l'octroi de contrat de main-d'œuvre indépendante;
- S'assure de faire connaître les mutations et les départs au directeur des ressources informationnelles et aux détenteurs afin que les accès soient révisés ou révoqués.

7.4 LE CHEF DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNELLE (CSIO)

- Fait appliquer la politique de gestion des identités et des accès ainsi que les procédures afférentes;
- S'assure qu'un audit des mécanismes de contrôles de gestion des accès est effectué périodiquement par les détenteurs;
- Élabore et met à jour toute la documentation nécessaire à la mise en place du processus de gestion des identités et des accès en respectant les modalités précitées et s'assure de son application auprès des détenteurs;

- Réalise une reddition de comptes des indicateurs de gestion de la présente politique et les présente au comité de direction;
- S'assure que la reddition de compte permet d'améliorer les exigences de sécurité concernant les contrôles d'identité et d'accès.

7.5 LE CHEF ADJOINT DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNELLE (CSIO ADJOINT)

- Participe à l'élaboration des indicateurs de gestion et des différents documents nécessaires à la mise en place des processus de gestion des identités et des accès;
- Coordonne et soutient les activités internes et externes d'audit des mécanismes de contrôles de gestion des identités et des accès qui sont effectués périodiquement
- Soutient le CSIO dans l'élaboration de ses tâches par des conseils, par le suivi et le contrôle de l'application des exigences de sécurité et par l'accompagnement des détenteurs.

7.6 LE COORDONNATEUR ORGANISATIONNEL DES MESURES DE SÉCURITÉ DE L'INFORMATION (COMSI)

- Contribue à la mise en place des activités opérationnelles de sécurité de l'information nécessaire à la gestion opérationnelle de la sécurité dans l'établissement;
- Contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées;
- Supporte le CSIO et le CSIO adjoint pour le volet technique de la sécurité dans le respect des exigences de sécurité définies dans les règles particulières;
- S'assure de la production des rapports des processus de sécurité de l'information et les transmet au chef adjoint de la sécurité de l'information organisationnelle et au chef de la sécurité de l'information organisationnelle, avec son appréciation et des justifications, au besoin.

7.7 GESTIONNAIRE

- Participe ou réalise, dans le cas de situation exceptionnelle, au processus permettant d'obtenir une preuve de l'identité essentielle et une preuve de l'identité contextuelle lors du recrutement de ressources humaines ou l'embauche de main-d'œuvre indépendante dans son unité administrative;
- Définit les habilitations et les critères d'habilitations associés aux fonctions (emplois) relevant de son autorité;
- S'assure de la conformité, en tout temps, des accès autorisés au principe du privilège minimum et des qualifications de son personnel aux critères d'habilitation associés aux fonctions;
- Autorise, s'assure de fournir les preuves de l'identité contextuelle et justifie tout besoin d'accès à l'information ne faisant pas partie des habilitations normales prévues pour le poste occupé par l'employé;
- Assure le suivi des autorisations d'accès octroyées aux utilisateurs relevant de son autorité depuis leur arrivée jusqu'à leur départ de son unité administrative;
- Ajuste dans les délais recommandés, tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès réellement octroyées.

7.8 DÉTENTEUR DE L'INFORMATION

- Définit les profils d'accès supportés par les applications relevant de son autorité et s'assure de la conformité des mécanismes d'accès aux exigences de sécurité émises par le CSIO;
- Définit clairement les règles d'autorisation et de restriction des accès à distance relevant de son autorité;
- Définit les accès à l'information sur la base du principe du moindre privilège et du principe de séparation de tâches.

- Accorde les accès aux actifs informationnels sous sa responsabilité;
- Valide les rapports périodiques des autorisations d'accès attribuées;
- Ajuste dans les délais recommandés, tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès octroyées;
- Met en place un audit de contrôle de gestion des accès et s'assure qu'il est effectué périodiquement;
- Transmet à chaque année au CSIO adjoint, les données permettant d'établir les indicateurs de gestion de la présente politique.

7.9 L'UTILISATEUR

- S'engage à ne pas partager son code d'accès et à ne pas utiliser le code d'accès d'une autre personne;
- N'utilise l'information à laquelle il a accès que pour des tâches qui lui sont assignées;
- Est responsable des accès qui lui sont octroyés et imputable des actions exécutées par ses identifiants et authentifiants (codes d'accès);
- S'engage formellement au respect des exigences de la présente politique;

8. REDDITION DE COMPTES

Pour une appréciation des modalités de la présente politique et pour atténuer les risques relatifs à la gestion des identités et des accès, une reddition de comptes est présentée au comité de direction suivant une périodicité d'une fois par année au minimum.

Dans le cadre de la reddition de comptes de la gestion des identités et des accès, les indicateurs de gestion occupent une place essentielle. L'analyse de ces indicateurs permet au CSIO de dégager des tendances et de déterminer les opportunités d'amélioration qui sont présentées au comité de direction pour décision. La liste d'indicateurs de gestion minimalement exigée est :

N°	Indicateur	• Cible / ○ Application	Explication
1	Délai moyen de révocation des accès	• 1 semaine : vert • 1 semaine et plus : jaune • 2 semaines et plus : rouge ○ Première année d'application de la politique : Code R03 seulement ○ Deuxième année : Avec tous les actifs critiques ○ À partir de la troisième : Avec tous les actifs	Les accès accordés à un utilisateur doivent être révoqués dès la cessation des activités de ce dernier. Plus le délai est long, plus la probabilité d'utilisation des accès à mauvais escient est grande. Cet indicateur contribue à l'évaluation de la performance des activités de révocation des accès et permet d'envisager des pistes d'amélioration en fonction de la situation.
2	Nombre de comptes modifiés à la suite de la revue des accès sur les actifs critiques	Nombre de comptes non conformes vérifiés *aux 3 mois* : • 0 compte non conforme : vert • 1 compte non conforme : jaune • 1 compte et plus non conforme : rouge ○ Première année : Cet indicateur ne sera pas comptabilisé ○ À partir de la deuxième année et pour les années suivantes, cet indicateur sera calculé avec tous les actifs critiques	Il contribue à repérer la présence d'écarts ou de lacunes dans la complétion ou le traitement des demandes de modifications des accès par rapport au délai préconisé. Un pourcentage élevé est un indicateur de non-conformité des responsables aux pratiques organisationnelles de gestion des identités et des accès. Plus ce pourcentage est élevé, plus il démontre la pertinence de faire une revue périodique des accès.
3	Nombre de comptes non conformes avec privilèges d'administration du domaine	Nombre de comptes non conformes vérifiés *aux 3 mois* : • 0 compte non conforme : vert • 1 compte non conforme : jaune • 1 compte et plus non conforme : rouge ○ Indicateur comptabilisé dès la première année	Les comptes disposant d'accès privilégiés sont très recherchés par les pirates informatiques, car ils permettent l'accès et la gestion de l'ensemble des ressources informationnelles. Cet indicateur permet de déterminer le nombre de comptes avec des privilèges d'administration du domaine pour ensuite les analyser et, si le besoin n'est pas justifié, de rectifier la situation. Un registre des personnes, groupes de personnes et entités technologiques autorisées à utiliser ces identifiants doit être constitué et continuellement mis à jour.
4	Nombre de comptes génériques	Nombre de comptes non conformes	L'octroi d'accès privilégiés à des comptes

	non conforme avec privilèges	vérifiés *aux 3 mois* : 0 compte non conforme : vert 1 compte non conforme : jaune 1 compte et plus non conforme : rouge ○ Indicateur comptabilisé à partir de la deuxième année	génériques n'est pas recommandé, car il est difficile d'assurer la traçabilité ou l'imputabilité des actions posées à partir de ce type de comptes. La connaissance du nombre de comptes génériques ayant des accès privilégiés dans l'organisation contribue à l'évaluation du niveau de risques liés à cette pratique et d'en atténuer la gravité par des actions correctives ou par des mesures de sécurité compensatoires si cela est jugé nécessaire.
5	Nombre d'accès non conforme à la suite d'un audit de journalisation des accès	Nombre d'accès non conformes vérifiés tous les 3 mois • 0 accès non conforme : vert • 1 accès non conforme : jaune • 1 accès et plus non conforme : rouge ○ Indicateur comptabilisé dès la première année	L'audit de journalisation des accès implique la surveillance et le contrôle des activités d'accès aux systèmes, aux applications et aux données. Cela permet de garder une trace de qui a accédé à quoi, quand, et quelles actions ont été effectuées. Un pourcentage élevé d'accès non conformes suivant un audit implique des accès effectués sans respect du principe du moindre privilège, des accès non autorisés, des problèmes graves de confidentialité des données ou des erreurs dans la gestion des droits d'accès. En surveillant régulièrement cet indicateur, le CIUSSS de la Capitale-Nationale peut identifier la source des problèmes, prendre des mesures correctives, renforcer la sécurité des données médicales et administratives et garantir la conformité aux réglementations de protection des renseignements personnels.

9. SANCTIONS

Manquements à la présente politique

Considérant l'impact des conséquences liées à un manquement en matière d'accès à des actifs informationnels, en cas du non-respect de la présente politique, des mesures administratives ou disciplinaires s'appliqueront.

10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la suite de son approbation par le comité de direction du 5 juillet 2018 et a été révisée le 9 janvier 2024.

ANNEXE 1

Cadre légal et administratif

La présente politique s'inscrit principalement dans un contexte régit par :

- La Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LQ 2021, chapitre 22);
- La Loi concernant le cadre juridique des technologies et l'information, R.L.R.Q., c. C-1.1;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, R.L.R.Q., c. A-2.1;
- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c. 25;
- Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives, 2023, c. 5;
- La Loi sur la protection des renseignements personnels dans le secteur privé;
- La Loi sur la protection des renseignements personnels et les documents électroniques;
- La Loi sur le droit d'auteur, L.R.C, 1985, c. C-42;
- La loi sur les services de santé et les services sociaux, R.L.R.Q., C. S-4.2;
- La loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales;
- La loi sur les services de santé et les services sociaux pour les autochtones cris, R.L.R.Q., c. S-5;
- La loi sur les services préhospitaliers d'urgence, R.L.R.Q., c. S-6.2;
- La Loi sur la Régie de l'assurance maladie du Québec, R.L.R.Q., c. R-5;
- La Loi sur l'assurance maladie, R.L.R.Q., c. A-29, section VII;
- La Loi médicale, R.L.R.Q., c. M-9;
- La Loi sur la pharmacie, R.L.R.Q., c. P-10;
- La Loi sur la santé publique, R.L.R.Q., c. S-2.2;
- La Loi sur la protection de la jeunesse, R.L.R.Q., c. P-34.1;
- La Loi sur le curateur public, R.L.R.Q., c. C-81;
- La Loi sur la santé et la sécurité au travail, R.L.R.Q., c. S-2.1;
- La Loi sur les accidents de travail et les maladies professionnelles, R.L.R.Q., c. A-3.001;
- La Loi sur les coroners, R.L.R.Q., chapitre C-68.01;
- Le Code des professions, R.L.R.Q., c. C-26, articles 60.4 et 60.6 et 87;
- Code de déontologie des membres de l'Ordre professionnel des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec, C-26, r.28 ;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnel, c. A-2.1, r. 02;
- La Charte des droits et libertés de la personne, R.L.R.Q., c. C-12;
- Le Code civil du Québec, R.L.R.Q., c CCQ-1991;
- La Loi sur les archives, R.L.R.Q., c. A-21.1;
- La Loi sur l'administration publique, R.L.R.Q., c. A-6.01;
- La Loi sur la fonction publique, R.L.R.Q., c. F-3.1.1;
- La Loi canadienne sur les droits de la personne, L.R.C., 1985, c. H-6;
- Le Code criminel, L.R.C, 1985, c. C-46;
- Les Règles relatives à la planification et à la gestion des ressources informationnelles;
- Les Règles relatives à l'assurance de l'identité numérique;
- La directive gouvernementale sur la sécurité de l'information, décret 1514-2021.