Centre intégré de santé et de services sociaux des Laurentides
Québec

Directive

Titre	**Directive sur l'utilisation sécuritaire du courriel et de la messagerie instantanée pour la transmission de renseignements confidentiels**	
N°	DIR 2022 DQEPE 054	
En vigueur le	2023-05-05	
Révisée le	Ne s'applique pas	
Validation	2022-11-19	Comité de sécurité de l'information et Directeurs
Approbation	2022-12-16	Comité de direction
Diffusion	2023-05-05	Dépôt sur l'intranet du CISSS
Responsable de l'application	Direction de la qualité, de l'évaluation, de la performance et de l'éthique	
Application et personnes concernées	Toute personne contribuant à la mission du CISSS des Laurentides et toute autre personne qui exerce ou développe sa profession au sein de l'établissement	
Remplace	Tous les documents précédemment émis à ce sujet	
Document(s) initiateur(s)	Mise en œuvre de la règle particulière sur la sécurité organisationnelle, MSSS-GUI02 Politique de sécurité de l'information du CISSS des Laurentides	
Document(s)en découlant	Politique et procédure sur l'encadrement des appareils mobiles (DRILLL) Capsule de sensibilisation à la Directive Aide-mémoire - Directive sur l'utilisation sécuritaire du courriel et de la messagerie instantanée pour la transmission de renseignements confidentiels (DQEPE) Formulaire d'engagement des intervenants au respect de la directive (DQEPE) Consentement de l'usager – Utilisation des TIC pour échanger des renseignements confidentiels le concernant (DQEPE)	

Table des matières

1. Préambule

Les technologies de l'information et de la communication (TIC) font maintenant partie des mécanismes utilisés dans le cadre des activités de l'organisation. Le ministère de la Santé et des Services sociaux (MSSS) reconnaît et encadre l'utilisation des TIC par les établissements. Cependant, il laisse à la discrétion de chaque organisation de définir les règles spécifiques pour assurer l'utilisation sécuritaire de ce type d'outils.

En plus de représenter des moyens de communication rapides et efficaces, les TIC sont susceptibles d'améliorer la qualité des services aux citoyens, d'accroître la productivité et d'améliorer notre efficacité tant au niveau des suivis que de la diffusion « ciblée » de l'information. Cependant, chaque médaille a son revers puisque ces moyens de communication, aussi efficaces qu'ils soient, peuvent comporter des risques importants si non utilisés adéquatement.

Cette directive vise à informer, sensibiliser et réduire les risques reliés à l'utilisation des TIC.

L'annexe 5 contient les liens web permettant d'accéder rapidement à tous les documents afférents à la présente directive.

2. Objectifs

Le but est d'énoncer les attentes minimales à respecter lors de la transmission de courriels et messagerie instantanée contenant des informations confidentielles, et ce, en conformité avec les lois, directives et exigences ministérielles.

De façon plus spécifique, elle vise à :

- Établir les responsabilités des usagers, gestionnaires, employés, médecins et collaborateurs dans l'utilisation de modes de communication jugés plus à risque ;
- Définir les moyens de protection à mettre en place afin de rendre à un niveau acceptable les risques encourus lors de l'utilisation de courriels et de messages instantanés ;
- Assurer l'intégrité de l'information en normalisant la tenue de dossier et la gestion des documents.

Ainsi, la directive énonce les attentes et règles minimales à respecter par tous les services. Le cas échéant, il sera de la responsabilité des directions de définir de manière plus précise ou sévère, les pratiques particulières dans leur domaine. En établissant celle-ci afin que la gestion des risques soit acceptable, le directeur en assume ainsi la pleine responsabilité par son imputabilité.

3. Domaine d'application

La présente directive s'applique à toutes les personnes qui transmettent de l'information électronique à l'aide des courriels et de la messagerie instantanée, dans le cadre des activités du CISSS des Laurentides.

3.1. Personnes visées

Les personnes visées et responsables d'appliquer la présente directive peuvent être des membres du personnel, médecins, membres du CMDP, résidents en médecine, dentistes, pharmaciens, sages-femmes, membres du conseil d'administration, personnes travaillant pour le CISSS sur une base contractuelle (main-d'œuvre indépendante [MOI]), entreprises liées par contrat, fournisseurs, stagiaires, bénévoles, usagers et leurs familles, visiteurs, etc.

Afin de faciliter la rédaction et la lecture du texte, le terme « intervenant » sera utilisé. Le terme « intervenant » regroupe toutes les personnes qui transigent de l'information confidentielle dans le cadre de la mission et, tel que précisé au paragraphe précédent, il ne s'agit pas exclusivement d'employés.

3.2. Portée et définitions

Les technologies de l'information et de la communication (TIC) comprennent tous les équipements, systèmes, applications ou services qui servent à l'entreposage, à la manipulation, à la gestion, au déplacement, à l'affichage, à la communication, aux échanges, à la transmission et la réception des informations.

La présente directive vise plus particulièrement la communication principalement à l'aide de deux types d'outils :

Service de messagerie électronique (SMÉ) : Le courriel est un message créé, envoyé ou reçu par un système de messagerie électronique comprenant toutes les pièces jointes au message ainsi que les données de transmission ou de réception (nom de l'expéditeur et du destinataire, objet, date, heure) tant à l'interne qu'à l'externe. En anglais, nous utilisons « Email » pour parler de courriel et « *Electronic mail* » pour courrier électronique.

Application de messagerie instantanée : La messagerie instantanée est un dialogue en ligne, actif qui permet d'échanger des messages textuels ou des fichiers en temps réel dans un dialogue interactif. Nous utilisons également les expressions suivantes : « chat », « chatter », clavardage, bavardage, texto ou communément appelé « *SMS* pour *short message service* » en anglais, etc.

3.3. Les communications visées

Cette utilisation peut être réalisée autant à l'interne qu'à l'externe, dans le cadre de l'emploi exercé, l'exercice de sa fonction, une formation ou une activité bénévole entre **les intervenants** dispensant les soins et services dans le cadre de la mission du CISSS des Laurentides, **les collaborateurs externes** (autres CISSS, fournisseurs, etc.) et **les usagers**.

4. Principes directeurs

Les principes de la directive ont été élaborés en fonction des meilleures pratiques connues, des lois, des règlements et des directives du ministère de la Santé et des Services sociaux (MSSS).

4.1. Fondements légaux

Le CISSS doit s'assurer que le personnel qui utilise les technologies de l'information dans le cadre de sa mission respecte les dispositions des lois ci-dessous relatives à la collecte, l'utilisation, la communication, la conservation et, selon le cas, l'archivage ou la destruction d'un renseignement confidentiel.

Il est important de souligner que cette directive répond aux exigences de l'article 34 de la Loi concernant le cadre juridique des technologies de l'information.

Cette loi prévoit que : « lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication. La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuves, le cas échéant » (Éditeur officiel du Québec, 2019a).

Ainsi, la présente directive fait état des moyens à respecter lors de la transmission de renseignements confidentiels et pourra être produite en preuve, le cas échéant (Annexe 1 : Fondements légaux et autres).

4.2. Responsabilité et imputabilité

Le CISSS est responsable de mettre à la disposition des intervenants, des appareils[1] et des outils[2] technologiques sécuritaires en établissant des balises d'utilisation.

Les documents d'encadrement des pratiques sont disponibles et de la sensibilisation est offerte en continu afin que les intervenants soient habiletés à communiquer et agir de manière sécuritaire.

Les intervenants appelés à utiliser le courriel et la messagerie instantanée pour échanger des renseignements confidentiels doivent prendre connaissance de la présente directive et s'engager à respecter les balises d'utilisation établies à l'aide du formulaire prévu à cet effet.

Les gestionnaires intègrent cette démarche dans le cadre de l'orientation et l'intégration de leur personnel et utilisent l'environnement numérique d'apprentissage (ENA) pour obtenir cet engagement[3]. Pour les secteurs externes (fournisseurs, maison d'enseignement, etc.), le formulaire est aussi disponible sur le site Internet de l'organisation.

Les intervenants doivent faire preuve de jugement et tenir compte de leurs obligations déontologiques avant de décider de transmettre et d'échanger des données confidentielles par courriel ou messagerie instantanée. Ils doivent prendre toutes les précautions pour minimiser les risques d'utilisation qui y sont associés.

[1] Cellulaire, ordinateur, tablette, etc.
[2] Outlook du MSSS, Teams du MSSS, etc.
[3] Voir annexe 5.

Pour assurer l'harmonisation et la sécurité des pratiques, en cas de doute, les intervenants doivent se référer à leur supérieur immédiat.

Il est important de préciser que l'usager est le seul « propriétaire » de l'information contenue à son dossier et, pour cette raison, il est en droit (sauf en cas d'exceptions prévues à la loi) de décider par quels moyens les informations le concernant peuvent être transmises. Dans ce contexte, l'intervenant doit l'informer de la procédure utilisée lors de l'utilisation du courriel et de la messagerie instantanée.

Finalement, ces deux outils d'information ont un caractère formel et chaque intervenant doit afficher un comportement exemplaire tant sur le plan de la qualité des contenus que sur le plan de la courtoisie.

4.3. Propriété du courriel et de la messagerie instantanée

Le courriel et la messagerie instantanée, utilisés dans le cadre des activités du CISSS des Laurentides, sont considérés comme étant des documents au sens de la Loi sur les archives. Par conséquent, ces derniers appartiennent à l'établissement.

Lors de situations exceptionnelles (plaintes, enquêtes, etc.), l'organisation pourrait entreprendre les démarches pour inspecter, consulter et conserver les communications reçues et transmises. Dans de telles situations, la personne visée pourrait être contrainte de donner accès à l'appareil utilisé, lorsque demandé, qu'il soit personnel ou fourni par le CISSS.

4.4. Utilisation des informations échangées

Les informations et pièces jointes transmises à l'aide du courriel ou d'un message instantané doivent être utilisées qu'uniquement pour l'objectif visé par ladite communication. Ainsi, une photo échangée par messagerie instantanée à un collègue pour obtenir son avis ne pourra être utilisée ultérieurement dans le cadre d'une formation.

5. Exigences en matière d'utilisation du courriel et de la messagerie instantanée

Cette section présente les conduites à adopter et cette directive énonce les attentes et règles minimales à respecter par tous les services.

Le cas échéant, il sera de la responsabilité des directions de définir de manière plus précise ou sévère, les pratiques particulières dans leur domaine. Cette stratégie permet l'harmonisation des pratiques pour un même secteur d'activité (ou direction) et ce, en fonction des besoins et risques spécifiques. Le directeur concerné peut ainsi connaître ses risques et prendre une décision éclairée (gestion des risques acceptables dont il endosse la responsabilité.

5.1. Identifier les communications avec renseignements confidentiels

Pour protéger les renseignements confidentiels et minimiser les risques entourant l'utilisation des TIC, tous les intervenants doivent d'abord reconnaître ce qu'est un renseignement confidentiel.

Il y a deux types d'informations confidentielles : l'information à caractère personnel et l'information de nature stratégique.

Information à caractère personnel :

Elle porte sur une personne physique et permet de l'identifier directement ou indirectement. Sauf lors d'exception, elle ne peut être communiquée sans le consentement de la personne concernée, voici quelques exemples :

- Information d'identification : numéro d'assurance maladie, date de naissance, etc. ;
- Information relative au travail : appréciation annuelle, avis disciplinaire, etc. ;
- Information de santé : évaluation médicale, médicaments prescrits, photographies, etc. ;
- Information financière : renseignements liés aux cartes de crédit, renseignements liés à la paie, etc.

Information de nature stratégique :

Cette information n'est pas nominative. Elle a un caractère stratégique pour l'organisation, ce qui la rend confidentielle. Ce type d'information exige que sa diffusion soit protégée et limitée aux seules personnes autorisées :

- Information de planification : stratégie de recrutement, éléments permettant de produire les états financiers, plans stratégiques, etc.
- Information pouvant constituer une menace à la sécurité du CISSS : renseignements relatifs à un incident de sécurité, clés de chiffrement et mots de passe d'accès aux applications administratives et clientèles, information liée à l'architecture du réseau informatique, etc.
- Information de gestion interne (avant une annonce officielle) : réorganisation de service, abolition ou création de poste, enquête interne, etc.
- Information de nature scientifique : données relatives à des études et travaux de recherches non publiés, données relatives aux participants à ces études, etc.
- Information juridique : toute information faisant l'objet de plaintes, poursuites, contentieux et enquêtes.

Considérant les différentes règles encadrant la transmission des renseignements personnels et stratégiques à des tiers, nous demeurons soumis en tout temps aux différentes lois applicables.

5.2. Identifier les risques de bris de confidentialité

Tous les intervenants faisant l'usage du courriel ou de la messagerie instantanée pour transmettre des renseignements confidentiels, dans le cadre de leurs fonctions, doivent connaître les risques associés à ces technologies, voir l'Annexe 2 : Risques potentiels associés à l'utilisation des technologies de communication).

Les risques liés à la communication à l'aide du courriel et de la messagerie instantanée entre l'intervenant et l'usager sont plus élevés que lors des échanges entre les intervenants.

Voici quelques éléments qui réduisent les risques de communication entre intervenants : Appareils et outils sécuritaires et autorisés par l'organisation ; communication à l'intérieur du réseau du MSSS (sécuritaire) ; Etc.

Avec ce qui précède, l'intervenant doit offrir une vigilance substantielle lors de ses échanges avec l'usager.

5.3. Situations non recommandées

Dans le cadre des activités, l'utilisation des deux types d'information n'est pas toujours le moyen le plus approprié pour assurer un service de qualité. Dans certaines situations, ces moyens de communication ne sont pas recommandés et l'utilisation des moyens traditionnels tels que la rencontre en présentiel, la communication téléphonique, la rencontre virtuelle, etc., seront demandées.

5.3.1. Critères de choix

Comme mentionné précédemment, voici quelques critères à utiliser dans le choix du moyen de communication approprié selon la situation et l'usager. La liste présentée ci-dessous est non exhaustive et doit faire l'objet d'une réflexion rigoureuse.

La **notion d'urgence.** Qu'il s'agisse d'un échange entre intervenants, entre un intervenant et un usager, son proche aidant ou son représentant légal, les communications comportant une notion d'urgence exigent une attention particulière.

Les intervenants doivent se référer aux pratiques convenues dans leur secteur d'activité.

De manière générale, le courriel ou le message instantané n'est pas un moyen de communication approprié dans les situations suivantes (le jugement est à préconiser) :

- Communication pour une situation d'urgence (médicale, sociale ou autre) qui nécessite une attention et une réponse immédiate ;
- Intervention en situation de crise : risque suicidaire, violence conjugale, risque d'homicide, etc. ;
- Transmission d'informations concernant un changement de dernière minute pour un rendez-vous.

La nature des informations à communiquer. L'utilisation du courriel ou de la messagerie instantanée n'est pas recommandée lorsque :

- L'intervenant doit s'assurer auprès de son interlocuteur que l'information a été comprise et interprétée adéquatement ;
- La communication peut générer une grande charge émotionnelle ;
- Les échanges sont de nature hautement confidentielle et sont à risque de préjudices importants pour la personne s'il survient un bris de confidentialité.

Voici à titre d'exemple, quelques situations où l'utilisation du courriel et du message texte est non recommandée dans les échanges :

- Communication d'un nouveau diagnostic ou d'un nouveau traitement ;
- Présentation d'un rapport d'évaluation et ses conclusions ;
- Annonce d'un pronostic défavorable ;
- Présentation et discussion entourant un plan d'intervention ;
- Discussion et conclusion concernant une insatisfaction envers les services fournis.

5.4. Consentement à utiliser les TIC pour échanger des renseignements confidentiels concernant un usager

L'usager est le seul « propriétaire » de l'information contenue à son dossier et, pour cette raison, il est en droit (sauf en cas d'exceptions prévues à la loi) de décider par quels moyens (en personne, verbalement, par téléphone, par courriel, par message instantané, etc.) les informations le concernant peuvent être transmises.

Lors de l'utilisation des TIC, en cohérence avec la présence de nombreux risques, le CISSS des Laurentides se doit d'obtenir le consentement de l'usager autant pour les échanges entre intervenants que celles entre les intervenants et l'usager.

Comme prévu à la loi, l'usager ou le représentant légal peut consentir à ce que les échanges soient réalisés en présence d'un proche aidant.

Cette démarche ne se substitue pas aux obligations de l'intervenant en matière de consentement aux soins, consentement à échanger de l'information, consentement à divulguer ou communiquer de l'information et finalement au processus de demande d'accès à l'information.

5.4.1. Démarche à réaliser pour obtenir le consentement de l'usager pour l'utilisation des TIC

Voici la démarche à réaliser auprès de l'usager :

1) Obtenir le consentement de l'usager (ou son représentant) avant de transmettre des renseignements confidentiels par message instantané ou courriel. Ainsi, le premier courriel ne contient que ce qui est obligatoire dans la démarche ci-dessous.
2) Choisir un des 3 types de modalités pour obtenir le consentement :
   - Par communication téléphonique – consentement verbal ;
   - En personne et signé par l'usager (ou son représentant) ;
   - Par courriel et la réponse de l'usager (ou son représentant) est considérée comme une signature électronique.

Peu importe, le type de consentement choisit :

3) Utiliser le gabarit[4] *Consentement de l'usager – Utilisation des TIC pour échanger des renseignements confidentiels le concernant*.

IMPORTANT : Les sections en bleu dans le formulaire doivent être complétées par l'intervenant.

L'intervenant doit :

- Pour le consentement en personne, imprimer le gabarit et permettre à l'usager (ou son représentant) de bien lire ;
- Pour le consentement par communication téléphonique, utiliser le gabarit pour guider sa démarche et fournir toutes les informations à l'usager (ou son représentant) ;

[4] Voir annexe 5.

- Par courriel, inclure le texte du gabarit dans le corps du courriel et l'acheminer à l'usager (ou son représentant).

4) S'assurer de donner toutes les informations nécessaires à la prise de décision de l'usager et que le consentement est *libre et éclairé.*
5) Offrir à l'usager (ou son représentant) le support nécessaire afin de s'assurer de sa compréhension.
6) Recueillir les précisions fournies par l'usager (ou son représentant) :
   - Consentir aux échanges d'information le concernant à l'aide des TIC (courriel et message instantané) entre lui, un intervenant ou un service de l'organisation.
   - Informer par écrit l'organisation de tous les sujets qu'il ne souhaite pas qui sont abordés à l'aide de ces moyens.
   - Refuser tous les types d'échanges avec des TIC entre les intervenants ou lui.
7) Documenter au dossier de l'usager la démarche et les détails de ce qui précède. Nous vous référons aux exemples placés à l'Annexe 3 : Exemples - Libellé dossier usager.

5.5. Les appareils et outils autorisés

Le CISSS des Laurentides est responsable de la protection des renseignements personnels sous sa gouverne, peu importe si l'appareil ou l'outil utilisé est sous la gouverne du MSSS ou dans un environnement technologique externe au CISSS.

Les intervenants doivent se référer et respecter les directives émises quant à l'utilisation des appareils (ordinateur, portable, cellulaire, tablette, etc.) et des outils (application, système d'information, outil de messagerie, etc.) sécuritaires dans le cadre de leur fonction.

5.6. Qualité du contenu des échanges

Voici quelques éléments permettant d'optimiser les échanges :

- Poser clairement les questions à l'intervenant ou à l'usager et transmettre toutes les informations requises afin de recevoir une réponse pertinente ;
- Demander un accusé de réception ;
- Demander à l'intervenant ou à l'usager un échéancier raisonnable pour donner sa réponse.

5.7. Identification de la personne concernée par le renseignement confidentiel

La pratique sécuritaire veut éviter d'identifier l'usager ou la personne mise en cause dans l'échange courriel ou le message instantané. Ainsi, en cas d'erreur (ex. : courriel envoyé à un mauvais destinataire), l'absence d'information nominative sur la personne mise en cause, minimise les impacts sur le plan de la confidentialité. Cette mesure constitue ainsi une mesure de protection.

Comment y arriver ? Faire référence au numéro d'usager, numéro de dossier ou numéro d'employé au lieu de préciser le nom. Il est possible de référer l'interlocuteur à une note laissée au dossier (système d'information) en précisant par exemple : « cela concerne l'usager que nous avons en commun » ou bien « celui que tu m'as demandé de contacter ».

Cette mesure peut avoir ses limites dans le cadre de certaines activités qui, par exemple, exigent l'identification de l'usager ou de la personne mise en cause afin d'assurer la qualité des soins et des services de ce dernier. Dans ces situations exceptionnelles, le CISSS des Laurentides considère que le risque d'erreur (médicale, clinique, sociale ou autre) prévaut sur les risques de bris de confidentialité. Ainsi, l'identification de l'usager est requise afin d'éviter une erreur et doit respecter les critères de la double identification. L'application des autres mesures édictées dans la présente directive permet de réduire les risques.

5.8. Communiquer avec la bonne personne

Afin d'éviter un bris de confidentialité dû à une erreur de destinataire, il est requis de prendre les précautions nécessaires pour s'assurer que l'information soit transmise à la bonne personne (numéro de téléphone ou adresse courriel exacte).

Lors d'une première communication avec un intervenant, un médecin, un usager ou toute autre personne en relation avec le CISSS, il est prudent d'établir un premier contact qui ne contient aucun renseignement confidentiel.

De plus, il est recommandé d'adresser le message à un seul destinataire et ainsi d'éviter les envois de renseignements confidentiels à un groupe de personnes.

5.9. Tenue de dossier et gestion documentaire

Comme prévu dans les lois, règlements et politiques internes[5], les intervenants du CISSS des Laurentides doivent utiliser les outils qui sont mis à leur disposition pour l'entreposage des informations. Nous vous référons aux exemples placés à l'Annexe 3 : Exemples - Libellé dossier usager.

5.9.1. Note au dossier de l'établissement

Rappelons que la boîte de courriels et les outils de messagerie instantanée ne sont pas des lieux reconnus et approuvés pour la conservation des documents officiels et d'archives.

Les activités effectuées à l'aide de ces moyens de communication électroniques doivent être résumées et consignées dans une note au dossier de l'établissement. Ensuite, elles doivent être effacées rapidement et de manière définitive des appareils et outils utilisés.

Dans le contexte où la personne concernée consent à l'échange d'information à l'aide des TIC et que ce consentement est écris (obtenu par courriel), il n'est pas nécessaire de répéter toutes les informations contenues dans l'échange dans la note au dossier. L'information pertinente à inscrire dans le dossier est le fait que le consentement a été obtenu et qu'il a été versé au dossier (verser le courriel au dossier). Dans le cas d'un consentement verbal, la note consignée au dossier doit être plus complète et décrire exactement ce à quoi l'usager a consenti.

Lorsque l'intervenant reçoit des informations dans le cadre des activités par le biais de courriel ou de message instantané, il rédige la note au dossier en indiquant la date, le nom et le prénom de l'expéditeur et un résumé des informations échangées comme il le ferait pour un appel téléphonique.

[5] LSSSS, Loi sur les technologies de l'information, Politique de gestion documentaire, Politique de la sécurité de l'information, etc.

5.9.2. Courriel ou message instantané versé au dossier

En plus de la note au dossier, il peut être pertinent de conserver le courriel ou le message original lorsque ce dernier a une valeur juridique, clinique ou financière (ex. : messages contenant des injures ou des menaces, consentement à des soins, divulgation d'un abus, etc.). Il est important de noter au dossier, à titre de référence, les documents qui ont été versés au dossier.

5.10. Gestion des incidents et des bris de confidentialité

Les personnes concernées par la présente directive doivent signaler, sans délai, une situation susceptible d'affecter la sécurité des informations.

En cas d'un **possible incident en lien avec la sécurité de l'information**, veuillez communiquer avec le centre de service informatique en utilisant le portail libre-service ou par téléphone 450-432-2777, poste : 77777.

Lors d'un **potentiel bris de confidentialité**, veuillez communiquer avec le supérieur immédiat et un(e) des archivistes de votre installation.

De plus, si la situation **implique un bris à la confidentialité de l'usager**, il est obligatoire de respecter le processus de la gestion des risques en remplissant un formulaire de déclaration AH-223 sur l'Intranet.

Pour tout **questionnement ou demande de support concernant la télésanté**, veuillez contacter l'équipe de soutien télésanté au numéro 450-473-6811 poste : 44321, par courriel ou consulter la page Télésanté sur l'Intranet.

6. Mesures applicables en cas de non-observance

En cas de non-conformité de cette directive, toute autre instance ayant l'autorité peut prendre les mesures correctives appropriées pour remédier aux problèmes ou peut imposer toutes autres mesures jugées appropriées.

7. Mécanisme de suivi

Cette directive sera validée dans le cadre des activités régulières d'audit, pour assurer sa qualité et sa performance en lien avec son contenu (qualité et amélioration du processus) et avec son application concrète (respect des règles et des rôles et responsabilités).

8. Rôles et responsabilités

8.1. Président-directeur général :

- Approuve et prends les moyens nécessaires à la mise en œuvre de la directive ;
- Assure les actions requises lorsqu'un intervenant ne respecte pas les consignes émises et met en péril la protection des renseignements confidentiels de l'organisation.

8.2. Direction de la qualité, de l'évaluation, de la performance et de l'éthique :

- Rédige et mets à jour la présente directive ;
- Accompagne et supporte les directions dans l'amélioration de leurs pratiques et dans les incidents ;
- Informe le PDG de toute situation exceptionnelle qui pourrait mettre en péril la sécurité de l'information de l'organisme ;
- Veille à l'application de la directive.

8.3. Direction des ressources informationnelles Lanaudière-Laurentides-Laval – Chef de la sécurité de l'information organisationnelle (CSIO) pour le CISSS des Laurentides :

- Rends disponible la liste des appareils et outils technologiques sécuritaires pour l'échange de renseignements confidentiels ;
- Mets à jour, en continu, la liste ci-dessus pour assurer l'amélioration continue des pratiques ;
- Reçois et évalue les demandes d'autorisation ou de dérogations quant à l'utilisation des TIC d'un point de vue sécurité technologique ;
- Conseille et accepte la gestion des risques de concert avec le directeur responsable ;
- Prends les décisions en cohérence avec son devoir de protection des renseignements confidentiels.

8.4. Direction des ressources humaines, communications et affaires juridiques (DRHCAJ) :

- Informe tout nouvel employé de ses obligations découlant de la présente directive ;
- S'assure de l'engagement de nouveaux employés à la respecter.

8.5. Directeurs, Gestionnaires et CMDP :

- Respecte les activités sous sa responsabilité selon les balises définies ;
- Valide que ses intervenants soient informés et respectent les mesures de protection émises ;
- Demande aux intervenants sous sa responsabilité de prendre connaissance de la présente directive et s'engager à respecter les balises d'utilisation établies à l'aide du formulaire prévu à cet effet (Annexe 1 : Fondements légaux et autres) ;
- S'assure d'utiliser les appareils et outils sécuritaires pour les échanges TIC ;
- Entérine les pratiques spécifiques développées dans sa direction ;
- Communique avec l'autorité compétente, en cas de problème ou difficulté en lien avec la présente directive ;
- Agis rapidement lors d'incident ou de comportements inappropriés et mets en place les mesures correctives appropriées.

8.6. Intervenant concerné :

- Prend connaissance et se conforme aux consignes de la directive ;
- S'engage à la respecter en complétant le formulaire prévu ;
- Demeure pleinement responsable des actes posés et le cas échéant, engage sa responsabilité professionnelle lors de l'utilisation du courriel et de la messagerie instantanée ;

- Informe son supérieur immédiat de toute violation des mesures de sécurité dont il pourrait être témoin ou de toute anomalie décelée pouvant nuire à la protection des informations, dans le cadre de son travail ;
- Remets, sans délai, les appareils utilisés dans le cadre de ses fonctions à la demande de son employeur.

9. Révision du texte

La présente directive pourra être révisée, en tout temps, selon les besoins. Par défaut, elle sera révisée au minimum tous les cinq ans à partir de sa date d'entrée en vigueur.

10. Références bibliographiques

Nous avons recueilli toutes les références utilisées pour élaborer cette directive que vous pouvez consulter à l'annexe 4 : Références bibliographiques.

11. Demande de renseignements

Pour une interprétation du texte ou pour une demande de renseignements concernant la présente directive, veuillez vous adresser à :

Direction de la qualité, de l'évaluation, de la performance et de l'éthique (DQEPE)
500, boul. des Laurentides, local 011
Saint-Jérôme (Québec) J7Z 4M2

Annexe 1 : Fondements légaux et autres

Le CISSS doit s'assurer que le personnel qui utilise les technologies de l'information dans le cadre de sa mission respecte les dispositions des lois ci-dessous relatives à la collecte, l'utilisation, la communication, la conservation et, selon le cas, l'archivage ou la destruction d'un renseignement confidentiel. Liste non exhaustive qui stipule notamment :

- Charte canadienne des droits et libertés de la personne ;
- Charte des droits et libertés de la personne ;
- Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales ;
- Loi sur les services de santé et de services sociaux (LSSSS) ;
- Loi sur la protection de la jeunesse ;
- Loi sur la santé publique ;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ;
- Loi sur la protection des renseignements personnels et les documents électroniques ;
- Loi sur la protection des renseignements personnels dans le secteur privé ;
- Loi sur les archives ;
- Loi sur le curateur public ;
- Code civil du Québec ;
- Code des professions ;
- Codes de déontologie des différents professionnels ;
- Règlement sur la tenue des dossiers des cabinets bureau des médecins ainsi que des autres effets ;
- Loi sur la gouvernance de la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement ;
- Loi concernant le cadre juridique des technologies de l'information ;
- Lois et règlements encadrant les technologies de l'information ;
- Etc.

Annexe 2 : Risques potentiels associés à l'utilisation des technologies de communication

L'intervenant appelé à utiliser le courriel et le message instantané pour échanger des renseignements confidentiels doit être bien informé des risques afin de pouvoir porter un jugement éclairé pour déterminer si ces moyens sont adéquats pour réaliser l'activité souhaitée.

Les risques pourront également servir de support à l'intervenant en vue d'obtenir leur consentement éclairé de l'usager.

Les risques potentiels sont notamment :

- Il n'est pas possible de sécuriser totalement les renseignements acheminés à l'aide du courriel et du message instantané ;
- Les messages peuvent être interceptés, réacheminés, diffusés, mis en mémoire ou modifiés à l'insu des personnes impliquées ;
- Il est impossible de s'assurer que seul le destinataire pourra lire le message ;
- Les messages peuvent être envoyés par erreur au mauvais destinataire ;
- Les liens et pièces jointes peuvent introduire des logiciels malveillants (virus) ;
- Les informations contenues et envoyées à partir de ou vers des adresses non associées au réseau de la santé peuvent être collectées et vendues à des tiers, selon les conditions du fournisseur de service utilisé ;
- Même si l'expéditeur et le destinataire ont supprimé les messages électroniques, il peut y avoir des copies de sauvegarde sur des systèmes autres (infonuagique « Cloud » ou fournisseurs tels qu'Outlook, Gmail, Hotmail, etc.) pour une durée indéterminée ;
- Le mot de passe d'une boîte courriel ou l'accès au message instantané peut être compromis (volé), donnant ainsi accès à un individu (curieux ou malveillant) à l'ensemble des échanges. L'individu pourra par la suite envoyer des messages et se faire passer pour le détenteur du compte ;
- Une brèche de sécurité, un incident dû à une erreur ou à une intrusion chez le fournisseur de messagerie courriel peut compromettre la confidentialité des communications ;
- L'accessibilité des courriels sur plusieurs appareils (mobiles ou non) hors du réseau multiplie les probabilités d'incident de sécurité (perte, vol, applications-espionnes, etc.) ;
- Un problème réseau ou d'accès à Internet rend indisponible la consultation, la transmission et la réception de courriels ;
- Etc.

Annexe 3 : Exemples - Libellé dossier usager

Exemple de consentement écrit et verbal :

DATE Année Mois Jour	NOTES ET SIGNATURES
2021-08-01	Consentement à l'échange d'information reçu par courriel de la part de Madame Tremblay le 1er août 2021 et versé au dossier
	Signature de l'intervenant
2021-08-02	Discussion téléphonique avec Mme Trembay
	Mme consent verbalement à l'échange d'information par courriel et message texte.
	«Sachez que toutes les informations échangées par courriel et message texte sont confidentielles, mais comme pour toute communication électronique, il existe certains risques quant à la protection des renseignements personnels.Merci de m'indiquer si vous comprenez et êtes d'accord. »
	Signature de l'intervenant

Exemple d'activité réalisée par SMS et courriel :

DATE Année Mois Jour	NOTES ET SIGNATURES
2021-08-01	Message texte de Madame Tremblay reçu le 1er août 2021
	Mme confirme sa présence demain à 11h
	Signature de l'intervenant
2021-08-02	Courriel de la fille de Mme Tremblay reçu le 2 août
	Fille de Mme m'informe que sa mère a oublié notre rendez-vous de ce jour et qu'elle est inquiète pour elle
	Signature de l'intervenant

Annexe 4 : Références bibliographiques

Association canadienne de protection médicale. (2014). *Guide sur les dossiers électroniques.*

Association canadienne de protection médicale. (2016, janvier). *Les communications électroniques et les renseignements personnels* (Publication nº P1304-3-F).

Collège des médecins du Québec. (2017, octobre). *Le médecin et les technologies de l'information et de la communication : les échanges électroniques avec le patient.* http://www.cmq.org/publications-pdf/p-1-2017-10-19-fr-les-echanges-electroniques-avec-le-patient.pdf

Collège des médecins du Québec. (2017, 28 mars). *L'utilisation du téléphone intelligent (texto et courriel) et des médias sociaux.* http://www.cmq.org/nouvelle/fr/utilisation-telephone-intelligent-texto-courriel-medias-sociaux.aspx

Collège des médecins du Québec. (2015, février). *Le médecin, la télémédecine et les technologies de l'information et de la communication*. http://www.cmq.org/publications-pdf/p-1-2015-02-01-fr-medecin-telemedecine-et-tic.pdf

Conseil du trésor. (2017, juin). *Cadre de référence de l'architecture de sécurité de l'information gouvernementale - Architecture d'entreprise gouvernementale 3.3.* https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG_3_3/Cadre_reference_architecture_securite_information.pdf

Conseil du trésor. (2007, juillet). *Cadre stratégique pour l'information et la technologie.* https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12452

Conseil du trésor. (2013, octobre). *Politique sur l'utilisation acceptable des dispositifs et des réseaux.* https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27122

Conseil interprofessionnel du Québec, Ordre professionnel des diététistes du Québec. (2017, juin). *Outil d'aide à la décision - Télépratique et gestion du dossier numérique.* https://opdq.org/wp-content/uploads/2013/07/TELEPRATIQUE-GESTION-DOSSIER-NUMERIQUE.pdf

Éditeur officiel du Québec. (2019a). *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C -1.1). http://legisquebec.gouv.qc.ca/fr/showdoc/cs/C-1.1

Éditeur officiel du Québec. (2019 b). *Loi sur les services de santé et les services sociaux* (L.R.Q., c. S -4.2). http://legisquebec.gouv.qc.ca/fr/showdoc/cs/S-4.2

Éditeur officiel du Québec. (2019 c). *Règlement sur les normes relatives aux ordonnances faites par un médecin* (L.R.Q., c. M -9). http://www.cmq.org/publications-pdf/p-6-2012-01-01-fr-reglement-normes-relatives-aux-ordonnances-faites-par-un-medecin.pdf

Ministère de la Santé et des Services sociaux (MSSS). (2020, mars). *Bulletin COVID-19 – Télésanté #10.* (Publication No. 20-DI-00167-09)

Ministère de la Santé et des Services sociaux (MSSS). (2017, juillet). *Termes et conditions d'utilisation du service de messagerie électronique (SMÉ).*

Ministère de la Santé et des Services sociaux (MSSS). (2008, janvier). *Directive de sécurité - Utilisation éthique des technologies de l'information.* (publication nº MSSS05-005, directive approuvée, version [1,2] du [2008-01-08]). http://extranet.ti.msss.rtss.qc.ca/getdoc/cf73b86c-46be-48b4-907a-779ba1162bc7/MSSS05-005-Directive-sur-l-utilisation-ethique-des.aspx

Ordre professionnel des inhalothérapeutes du Québec. (2017). *Énoncé de position sur l'utilisation du cellulaire et de tout appareil de communication par des inhalothérapeutes sur leur lieu de travail.*https://www.opiq.qc.ca/wp-content/uploads/2017/07/Enonce_PositionCellulaire_VF.pdf

Annexe 5 : Lien web vers les documents

Voici les différents liens vous permettant d'accéder rapidement aux documents.

Lien web vers la page Intranet du CISSS des Laurentides

- Cliquer sur le lien suivant pour ouvrir la page Intranet contenant la directive et les autres documents afférents.

Lien web vers la page Internet du CISSS des Laurentides

- Cliquer sur le lien suivant pour ouvrir la page Internet contenant la directive et les autres documents afférents.

Lien web vers l'environnement numérique d'apprentissage

- Cliquer sur le lien suivant pour ouvrir la page ENA contenant la directive et autres documents afférents.