Respect de la confidentialité et sécurité informationnelle

Les principes en matière de confidentialité et de protection des renseignements personnels s'appliquent en tout temps dans le cadre de votre travail, et ce, quel que soit le lieu où vous l'effectuez (dans une installation du CIUSSS de l'Estrie – CHUS, comme à votre domicile).

En effet, comme télétravailleur, vous avez la responsabilité de vous aménager un environnement propice au travail, notamment en respect des normes de confidentialité et de sécurité de l'information de l'organisation.

Sécurité de l'information

L'utilisation d'outils de télésanté et de télétravail ne fait pas exception lorsqu'il est question de la sécurité de l'information. À cet effet, il est important de respecter les mêmes règles de sécurité que lorsque vous êtes au bureau. Une liste de principes à respecter est présentée dans cette fiche.

Règles générales

- Se conformer à la Politique de la sécurité de l'information ainsi qu'aux directives et mesures de sécurité publiées par l'établissement (voir la section plus bas « Documents de référence »).
- Respecter les clauses qu'on trouve dans le formulaire Engagement à la confidentialité, à la sécurité de l'information et au maintien d'un sain climat de travail, signé lors de l'embauche.
- Éviter de sauvegarder localement des documents confidentiels sur l'ordinateur; le cas échéant, s'assurer de les retirer aussitôt qu'ils n'y sont plus utiles.
- Éviter de brancher un périphérique amovible, source potentielle d'infection (ex. : clé USB, CD, DVD) sur un équipement fourni par l'établissement.
  - Si des informations sensibles doivent tout de même être copiées sur ces médias, assurez-vous qu'elles sont encryptées et protégées.
- Assurer la confidentialité lors des échanges électroniques.
  - Dans Outlook, utiliser le chiffrement si des informations confidentielles doivent être partagées par courriel.
  - Dans Teams, éviter de partager des informations confidentielles ou nominatives par écrit.
- Pendant vos heures de travail et avec le matériel fourni par l'employeur, utiliser Internet de façon appropriée et pour des fins professionnelles seulement.
- S'assurer d'être vigilant en tout temps, notamment lors de la navigation sur Internet (sites web suspects) et lors de la réception de courriels (hameçonnage).

Outils de collaboration

- Toujours utiliser des solutions de conférence Web approuvées par l'équipe de sécurité de l'information de l'établissement. En ce moment, Teams est la solution à privilégier. Les abonnements Zoom Télésanté et Reacts acquis par l'établissement sont aussi permis s'ils répondent à un ou des besoins particuliers auxquels Teams ne peut répondre.
- Ne pas utiliser les abonnements gratuits d'application de visioconférence ou de partage de document, tels que Zoom ou Google drive.
- Être vigilant lors de l'utilisation des fonctions avancées des outils de visioconférence, particulièrement le partage de document ou d'écran, incluant le contrôle à distance. Ces fonctions présentent des enjeux qui augmentent de manière considérable le risque lié à la confidentialité et la fuite d'information.
  - Il est fortement conseillé de partager uniquement l'application souhaitée et non l'écran complet.
  - Si vous utilisez le partage du contrôle à distance, assurez-vous de bien connaitre les raccourcis clavier pour pouvoir faire cesser le partage à tout moment.
  - N'utilisez que les plateformes de partage de document approuvées par l'établissement.
- L'enregistrement (audio, vidéo ou de photos) lors d'une séance de visioconférence à l'aide de Teams, Zoom ou React pour les activités de télésanté, inclut souvent des informations à caractère confidentiel. Veuillez éviter de partager les enregistrements des séances de visioconférence. Seuls les participants à la rencontre devraient pouvoir consulter l'enregistrement.
  - Pour en connaitre davantage sur l'enregistrement de vos réunions Teams, veuillez visionner la capsule « Comment enregistrer une réunion Teams et où retrouver cet enregistrement » sur Mon portail O365.

Réseau Wi-Fi

Le télétravail s'opère principalement sur votre connexion Wi-Fi personnelle. Il est donc primordial de bien la sécuriser pour éviter toute intrusion sur votre réseau, qui pourrait être utilisé pour attaquer l'organisation. Assurez-vous de la sécurité du routeur :

- Protocole de sécurité WPA2/WPA3 et de chiffrement AES.
- Mot de passe robuste pour accéder à la configuration du routeur.
- Mot de passe robuste pour accéder au réseau Wi-Fi.

Utilisation du jeton de téléaccès

- Le jeton de téléaccès ne doit être utilisé qu'avec un équipement fourni par l'organisation (à l'exception de certains médecins ciblés autorisés selon des modalités très précises).
- Vous devez prendre les mesures de sécurité requises pour éviter qu'une tierce personne utilise votre jeton, soit :
  - ne jamais partager votre NIP ou vos questions et réponses secrètes avec quiconque.
  - conserver votre NIP dans un endroit très sûr.

Protection des renseignements confidentiels

Lorsque vous vous trouvez en contexte de télétravail, vous devez appliquer les mêmes règles qu'au bureau. Il est donc primordial de prendre le temps nécessaire pour évaluer votre environnement de travail ainsi que les mesures prises afin de respecter la confidentialité et la protection des renseignements confidentiels en vue de répondre aux normes de l'établissement et de votre ordre professionnel s'il y a lieu.

Aménagement sécuritaire et confidentiel de votre espace de travail

- Les équipements prêtés par l'établissement ne doivent être utilisés qu'à des fins professionnelles. Ces équipements (ordinateur, téléphone ou autres périphériques) ainsi que logiciels ou accès à des systèmes d'information ne peuvent être partagés avec personne.
- L'écran et le bureau sont aménagés de façon à être à l'abri des regards.
- Toutes les communications de nature confidentielle ou clinique (concernant un usager ou avec un usager) doivent demeurer privées. Notamment, vous devez :
  - Travailler dans une pièce fermée ou avec la possibilité de vous retirer.
  - Utiliser un casque d'écoute.
  - Etc.
- Au début d'une rencontre à distance avec un usager, il est recommandé de confirmer à l'usager la confidentialité de la séance et de lui indiquer votre lieu de pratique (domicile ou établissement).
- Il est judicieux d'inviter l'usager à lui aussi participer à la rencontre dans un environnement confidentiel qui favorise une qualité sonore et visuelle optimale.
  - Vous pouvez le référer au portail du Réseau québécois de la télésanté pour plus d'information.

Conservation d'informations confidentielles

- Tous les documents papier contenant des informations confidentielles doivent être sécurisés, pour la durée qui aura été établie de leur conservation à votre domicile, notamment par l'utilisation de moyens sécuritaires, par exemple :
  - Un tiroir de classeur barré.
  - Une valise ou un porte-document verrouillé.
  - Une porte pouvant se fermer et se verrouiller pour protéger la pièce où vous travaillez.
- Toute documentation de nature clinique devant être classée au dossier de l'usager dans une installation de l'établissement doit être acheminée à ce dossier sur une base hebdomadaire. Il est interdit de constituer des dossiers parallèles.
- Aucun dossier d'usager, gardé dans les murs de l'établissement, ne peut être apporté à votre domicile.

Destruction des informations confidentielles

- Vous devez vous assurer que les documents et informations dont vous disposez soient détruits de façon sécuritaire. Quelques pratiques possibles :
  - Ne pas jeter des documents contenant des informations confidentielles à la maison; les conserver de façon sécuritaire et les rapporter dans une installation de l'établissement pour destruction selon le processus en place.
  - Si vous avez accès à une déchiqueteuse de documents à votre domicile, utilisez-la comme vous le feriez au bureau.

Signalement de toute situation à risque

Signalez au Centre de services de la Direction des ressources informationnelles et technologiques (DRIT) toute situation susceptible de compromettre la sécurité des actifs informationnels auxquels vous avez accès.

- De l'interne : poste 15555.
- De l'externe : 1 819 829-0084 (poste 15555).

Avisez immédiatement votre supérieur immédiat si vous constatez une problématique de confidentialité, que ce soit en lien avec une situation spécifique impliquant un usager ou de façon plus générale, avec votre environnement de travail.

À consulter

- Dans l'intranet du CIUSSS de l'Estrie – CHUS :
  - Boîte à outils | Sécurité de l'information
  - Politique de la sécurité de l'information
  - Avis de sécurité Échange d'informations confidentielles par courriel avec Outlook 365
  - Avis de sécurité Enregistrement d'une rencontre Microsoft Teams
  - Avis de sécurité Utilisation des outils de conférences Web
  - Directive sur l'utilisation des systèmes électroniques
  - La directive clinico-administrative « Tenue de dossier des usagers et sécurité de l'information dans un contexte de télétravail »
- Formation sur la confidentialité et la sécurité de l'information (ENA – Création d'un accès gratuit lors de la première visite)
- Comment enregistrer une réunion Teams et où retrouver cet enregistrement (Mon portail O365)

Des questions?

N'hésitez pas à en parler avec votre gestionnaire.
Vous pouvez également soumettre vos questions à teletravail-telesante.ciussse-chus@ssss.gouv.qc.ca.