

1- RESPECTER LES MÊMES OBLIGATIONS QU'EN PRESENTIEL

Appliquer et se conformer :

- Aux politiques et procédures du CISSS ;
- Aux lois et règlements en vigueur concernant les champs de pratique et les activités réservées ;
- Aux standards et normes de pratique (prestation de services sécuritaire et appuyée sur les données scientifiques pertinentes) ;
- Aux obligations déontologiques (responsabilités professionnelles).

2- OBTENIR UN CONSENTEMENT VERBAL LIBRE, ECLAIRE ET CONTINU

Expliquer à l'utilisateur et s'assurer qu'il comprend :

- La nature et les résultats attendus du soin ou service proposé ;
- Les moyens technologiques utilisés ;
- Les risques, limites et avantages de la modalité ;
- Les risques liés à la protection des renseignements personnels associés aux communications électroniques ;
- Les solutions alternatives possibles.

S'assurer de l'âge légal et de l'aptitude à donner son consentement (demander le consentement des parents ou du représentant légal si requis).

*Le consentement écrit est non obligatoire en contexte de pandémie.

3- ASSURER LA CONFIDENTIALITE ET LA PROTECTION DE LA VIE PRIVEE

- Utiliser les plateformes et logiciels approuvés par le MSSS et l'établissement (Zoom, Teams, Reacts, IRIS);
- Assurer la sécurité de la connexion avec l'utilisateur (ex. : mot de passe, numéro de rencontre unique, salle d'attente virtuelle, etc.);
- Utiliser un environnement physique qui permette d'assurer la confidentialité et la discrétion ;
- Utiliser un casque d'écoute avec microphone si possible ;
- Vérifier l'identité de l'utilisateur et le lieu où il se trouve ;
- Si un tiers est présent (ex. : proche aidant, technicien en informatique), obtenir le consentement de l'utilisateur. Le tiers doit s'identifier et est tenu à la confidentialité ;
- Informer l'utilisateur que les rencontres ne peuvent pas être enregistrées ;
- Aviser l'utilisateur dans les meilleurs délais de tout manquement à l'obligation de confidentialité.

4- RESPECTER LA DOUBLE IDENTIFICATION

- Confirmer l'identité de l'utilisateur à l'aide d'au moins deux identifiants propres à la personne (par exemple le nom et la date de naissance). Il est recommandé de demander à l'utilisateur de présenter sa carte d'assurance maladie à la caméra.

5- ÉTABLIR UN PLAN D'URGENCE

- Convenir avec l'utilisateur d'une stratégie pour communiquer avec lui en cas de problèmes technologiques (ex. : demander un numéro de téléphone) ;
- Identifier avec l'utilisateur les ressources à contacter en cas d'urgence ou d'événements indésirables ;
- Au besoin, selon la situation et les caractéristiques de l'utilisateur, prévoir la présence d'une tierce personne dont le rôle sera précisé au préalable;
- Ne jamais raccrocher, rester connecté avec l'utilisateur afin de le rassurer et savoir ce qui se passe pour en informer les secours au besoin.

6- EFFECTUER LA TENUE DE DOSSIER

- Préciser que l'intervention a été réalisée à distance et indiquer le moyen technologique utilisé ;
- Faire état du consentement libre et éclairé obtenu de l'utilisateur ;
- Documenter la double identification de l'utilisateur et la participation d'une tierce personne, si applicable ;
- Documenter les moyens mis en place pour assurer la confidentialité ;
- Documenter le protocole d'urgence convenu avec l'utilisateur pour assurer sa sécurité ;
- Documenter toute ordonnance ou demande de consultation transmises ;
- Verser la note au dossier de l'utilisateur le plus rapidement possible, qu'elle soit numérique ou papier.