capter les numéros, pour ensuite espionner l'appareil. Les dispositifs Stingray les plus évolués permettent de copier toute l'information en provenance du téléphone.

Pensez-y à deux fois avant d'utiliser des textos par téléphone intelligent pour communiquer avec les clients. Il est préférable de recourir à une appli ou à un service qui garantit le cryptage des données. Soyez conscient de ce qui vous entoure et faites preuve de prudence chaque fois que vous êtes en situation de communiquer de l'information confidentielle au moyen d'un appareil mobile.

Conseils au sujet du Wi-Fi

- Si vous utilisez le Wi-Fi dans votre lieu d'affaires, assurez-vous qu'il est sécurisé;
- N'utilisez pas le Wi-Fi public pour des renseignements confidentiels, car les services publics sans fil ne sont pas sécurisés, même lorsqu'ils sont protégés par mot de passe;
- Songez à la possibilité d'utiliser vos propres données cellulaires dans des lieux publics;
- Utilisez un réseau privé virtuel (RPV) (qui est conçu pour fournir un tunnel sécurisé et crypté pour la transmission des données);
- Soyez à l'affût des Wi-Fi « de mystification » Par exemple, si vous vous trouvez dans un resto Starbucks , il se peut que vous soyez en présence de 3 réseaux Wi-Fi : Starbucks, Starbucks Toronto et le Starbucks local. Informez-en le gérant de l'établissement et déterminez lequel est le vrai Wi-Fi. Un Wi-Fi de mystification vous fournira un accès Internet tout en vous dérobant vos informations de connexion à tous les sites que vous visiterez;
- Assurez-vous que votre connexion Wi-Fi à domicile est sécurisée;
- Si vous avez une connexion Wi-Fi, ne permettez pas que des invités puissent s'y brancher, car vous risqueriez que des virus s'y propagent;
- Si plusieurs ordinateurs sont branchés à votre réseau Wi-Fi et que vous autorisez le partage des fichiers entre les appareils, alors si vous laissez quelqu'un se brancher à votre réseau, vous pourriez exposer les données qui se trouvent dans ces dossiers. Il est facile de configurer un réseau Wi-Fi distinct à l'usage des invités.

ANNEXE B – Liste de contrôle pour le recours à la technologie en supervision clinique

Voici certaines des modalités de prestation de la supervision clinique :

- Téléphone (ligne fixe, cellulaire ou intelligent);
- Enregistrement numérique/vidéo à partager avec le superviseur
- Vidéoconférence
- Messagerie texte ou clavardage
- Courriel
- Supervision en direct par vidéoconférence d'une séance en personne ou d'une séance en réalité virtuelle

Choisissez la technologie qui répond le mieux aux besoins de vos supervisés et évaluez :

- La disponibilité
- Les prix abordables
- La fiabilité
- La protection des renseignements personnels
- La sécurité
- L'effet de la technologie sur l'alliance de travail

Le consentement éclairé du supervisé et du client doit inclure :

- La façon dont on préservera la confidentialité de l'information
- La façon de communiquer en cas de défaillance technique
- Les limites de la technologie/modalité
- Les risques potentiels de la technologie/modalité
- Les avantages potentiels de la technologie/modalité
- Le plan d'urgence en cas de situation de crise chez le client
- La politique sur les médias sociaux

Les points à discuter avec votre supervisé :

- Signer et respecter une entente de supervision clinique
- Les défis que pose le recours à la technologie et leurs effets possibles sur la communication
    - Par exemple, les silences lorsqu'on utilise le téléphone ou la vidéo. Convenir de part et d'autre de ce qui devrait être considéré comme étant un délai acceptable en silence avant d'entreprendre la conversation.
- Réduction des sources de distraction et des tâches multiples non pertinentes durant la période de supervision
- À quel moment importe-t-il de recourir à une rencontre en personne ou à une conversation téléphonique pour discuter d'information confidentielle?
- La politique sur les médias sociaux
- La responsabilité du maintien de la confidentialité et des pauses de sécurité à la fois pour le superviseur et le supervisé
- Possible prise en compte des heures supplémentaires pour la supervision

Connaissances et habiletés du superviseur concernant l'utilisation de la technologie en supervision clinique :

- Aptitudes de base concernant l'utilisation et le dépannage de la technologie
- Le superviseur doit se tenir au fait des divers types de technologie et de leurs usages possibles
- Doit démontrer et promouvoir les bonnes pratiques chez le supervisé en vue de protéger la vie privée et la confidentialité du client.
- Le superviseur doit savoir comment minimiser le risque associé au transfert et à l'entreposage des données sensibles
- Doit évaluer dans quelle mesure le supervisé est apte à recevoir de la supervision à distance et s'assurer que ce dernier sait bien trier les clients
- Fournir des lectures et des lignes directrices sur le professionnalisme, la protection des renseignements personnels/la sécurité et l'éthique en matière de technologie
- Doit pouvoir démontrer son habileté à transposer les pratiques exemplaires de supervision clinique dans un format fondé sur la technologie
- Doit pouvoir justifier le choix de la plateforme technologique
- Se préparer et s'exercer à utiliser la technologie et se familiariser avec les configurations technologiques visant à protéger les renseignements personnels
- Comprendre les effets possibles de la désinhibition sur les supervisés et sur lui-même
- Se tenir au courant des lois et de la déontologie professionnelle de l'association à laquelle appartient le supervisé
- Développer sa compréhension des implications de la technologie sur lui-même en tant que superviseur
- Se renseigner sur la responsabilité du fait d'autrui

Si vous souhaitez recevoir des services de supervision, vous ne devriez vous adresser qu'à des personnes qui ont de l'expérience et de la formation en matière de travail en ligne. Il peut s'avérer utile de recevoir la supervision selon la même modalité que celle dans laquelle vous travaillez.

<u>De bons conseils pratiques pour le recours à diverses technologies à des fins de supervision clinique :</u>

Quelle que soit la modalité utilisée, ne discutez jamais de renseignements personnels sur la santé à moins que la technologie ne soit sécurisée, protégée par mot de passe et que vous l'estimiez conforme aux lois applicables en matière de protection des renseignements personnels.

Téléphone (ligne fixe, cellulaire ou intelligent)

- Effectuez les appels dans un bureau privé et fermé
- Utilisez des écouteurs pour améliorer la qualité sonore
- Évitez d'utiliser des connexions Wi-Fi publiques ou non sécurisées pour vos appels sur téléphone mobile

Vidéoconférences

- Dotez-vous d'un plan de communication de relève en cas de défaillance technique
- Assurez la protection des renseignements personnels
- Limitez les distractions

Enregistrement numérique vidéo ou audio

- Assurez-vous que des protocoles de sécurité sont en place lorsqu'il s'agit d'enregistrer, de transmettre, d'archiver et de supprimer des contenus
- La caméra ne doit filmer que la conseillère ou le conseiller

Courriel

- Cryptez tous les courriels
- Faites attention au ton de l'écrit et apprenez des façons de compenser l'absence d'indices visuels

Partage de fichiers

- Contrôlez attentivement toute forme d'entreposage dans le nuage quant à la conformité aux lois sur la protection des renseignements personnels
- Assurez-vous que les dispositifs d'envoi et de réception sont également conformes
- Utilisez un logiciel de cryptage pour partager les fichiers
- Utilisez des mots de passe et les paramètres les plus sévères de protection de la vie privée
- Le partage d'écran peut s'avérer utile

Messagerie texte/clavardage

- Établissez clairement avec le supervisé à quel moment il conviendrait de recourir aux textos ou au clavardage
- À n'utiliser que pour des conversations simples et non confidentielles
- Exercez-vous à y recourir par mesure de clarté et de brièveté