Lignes directrices concernant le recours aux technologies en counseling et psychothérapie

Projet de la Section technologies et solutions innovatrices

Dawn Schell, Expert-conseil pour le projet

CANADIAN COUNSELLING AND PSYCHOTHERAPY ASSOCIATION
L'ASSOCIATION CANADIENNE DE COUNSELING ET DE PSYCHOTHÉRAPIE

Mars 2019

Table des matières

Reconnaissance des lignes directrices existantes et des sources, ainsi que des collaborateurs

Nous tenons à souligner le travail accompli par divers organismes qui ont servi d'inspiration pour la conception des présentes lignes directrices.

American Psychological Association
American Telemedicine Association
Association of Social Work Boards
British Association of Counselling and Psychotherapy
British Columbia Association of Clinical Counsellors (BCACC)
Association canadienne de counseling et de psychothérapie
Société canadienne de psychologie
College of Psychologists of British Columbia
International Society for Mental Health Online
Online Therapy Institute
Association de psychologie de l'Ontario
Worldwide Therapy Online

Nous voulons également souligner les contributions suivantes :

L'équipe chargée du Projet des lignes directrices :

Linda Rombough, Chef de projet
Dawn Schell, Expert-conseil pour le projet
Dan Mitchell
Sherry Law
Lawrence Murphy

Le CA de la Section technologies et solutions innovatrices :

Dan Mitchell	Sherry Law
Shawn Smith	Constance Lynn Hummel
Lawrence Murphy	Linda Rombough
Dawn Schell	Micheala Slipp
Elise Meertens	Michel Turcotte, représentant du CA de l'ACCP

Les panélistes lors de la téléconférence :

Kris Klein, Partenaire, nNovation LLP @k_klein
Andrew See, M. Sc. Professionnel des TI
Iain Nicol, Chef - Clinical Information Systems, Mental Health and Substance Use, Fraser Health
D, ancien client de counseling en ligne et professionnel des TI

Commentaires sur les Lignes directrices :

Ben Cutler, chef de direction, Hushmail
Natasha Caverley, Présidente sortante, ACCP
Blythe Shepard, Enseignante, Université de Lethbridge
Elise Meertens
Micheala Slipp

Avis de non-responsabilité

L'INFORMATION FOURNIE DANS LES PRÉSENTES EST OFFERTE À TITRE INFORMATIF SEULEMENT ET « TELLE QUELLE », NE CONSTITUANT DONC PAS UN AVIS JURIDIQUE. L'ACCP NE SE PORTE PAS GARANTE, DE FAÇON EXPLICITE OU IMPLICITE, DES INTERPRÉTATIONS DÉCOULANT DE TEXTES LÉGISLATIFS OU AUTRES, EN CE QUI CONCERNE L'INFORMATION FOURNIE DANS LES PRÉSENTES ET SE DÉSISTE DE TOUTES REPRÉSENTATIONS, GARANTIES ET CONDITIONS EN OUTRE, L'ACCP NE FAIT AUCUNE DÉCLARATION ET NE DONNE AUCUNE GARANTIE, CAUTION OU CONDITION À L'EFFET QUE L'INFORMATION FOURNIE DANS LES PRÉSENTES EST EXACTE, COMPLÈTE OU À JOUR. TOUTES LES DÉCLARATIONS, GARANTIES, CAUTIONS ET CONDITIONS SONT DÉCLINÉES PAR LA PRÉSENTE DANS TOUTE LA MESURE PERMISE PAR LA LÉGISLATION APPLICABLE.

EN AUCUN CAS, L'ACCP NE SAURAIT ÊTRE TENUE RESPONSABLE DE TOUTES PERTES OU TOUS DOMMAGES DE QUELQUE NATURE QUE CE SOIT (DIRECTS, INDIRECTS, CONSÉCUTIFS OU AUTRES) DÉCOULANT D'UN CONTRAT, D'UN DÉLIT CIVIL OU AUTREMENT, EN LIEN AVEC VOTRE UTILISATION (OU VOTRE INCAPACITÉ À UTILISER) L'INFORMATION FOURNIE DANS LES PRÉSENTES.

Préambule

Au cours des dernières années, on a assisté à des progrès technologiques fulgurants et à un recours croissant à la technologie en counseling et en psychothérapie. De nouveaux cas d'utilisation de la technologie en counseling et en psychothérapie font régulièrement leur apparition. Les praticiennes et praticiens doivent faire preuve de vigilance et de résilience lorsqu'il s'agit de manœuvrer parmi les risques et les possibilités associés à cet environnement numérique. Il n'est pas toujours évident de savoir appliquer le *Code de déontologie de l'ACCP* et les *Normes d'exercice*[1] aux nouveaux appareils, aux nouveaux systèmes d'exploitation, aux nouveaux logiciels ou aux nouvelles versions d'applications.

Les conseillères, conseillers et psychothérapeutes ne perçoivent pas tous le recours à la technologie de la même manière. Certains praticiens sont des enthousiastes de la toile qui adoptent spontanément toute nouvelle forme de technologie. D'autres se montrent plus hésitants, et même rébarbatifs, à tout recours à la technologie. Peu importe la manière dont nous percevons ces technologies dans nos pratiques et dans quelle mesure nous les utilisons, nous devons apprendre comment y avoir recours intelligemment.

Les présentes Lignes directrices contiennent des suggestions concrètes sur la façon d'utiliser la technologie judicieusement, tout en protégeant nos clients et nous-mêmes. L'objectif est d'appuyer et d'affirmer la pratique professionnelle dans notre monde envahi par la technologie, en proposant des outils nous permettant de devenir des praticiennes et praticiens résilients. Car après tout, « Internet est là pour rester, et il nous faut changer et nous adapter, développer de la résilience en tant que praticiens dans notre relation avec le monde numérique ».[2]

Qu'entend-on par « recours à la technologie »?

Les présentes Lignes directrices portent sur toute utilisation d'une « technologie numérique ou électronique pour fournir de l'information au public, des services aux clients, pour communiquer avec les clients ou à leur sujet, gérer de l'information confidentielle et des dossiers de cas et pour stocker des renseignements sur les clients et y avoir accès ».[3]

---

[1] Les renvois à des passages particuliers du *Code de déontologie et aux Normes d'exercice de l'ACCP* sont notés par le numéro d'ordre et le titre. Par exemple, A3 Limites de la compétence.

[2] Weitz, P. Éd. (2014) Psychotherapy 2.0: Where Psychotherapy and Technology Meet. Karnac Books, Londres, R.-U. p. 12

[3] Normes de pratique en matière de technologie 2016 du BC College of Social Workers http://www.bccollegeofsocialworkers.ca/wp-content/uploads/2016/10/BCCSW-Technology-Standards.pdf

Ce terme de recours à la technologie désigne, entre autres :

- Le téléphone (ligne fixe, cellulaire ou intelligent);
- Le courriel;
- La messagerie texte;
- Le dialogue en ligne (temps réel) ou clavardage;
- La discussion électronique asynchrone;
- La webcaméra/téléconférence;
- La réalité virtuelle/avatar;
- L'évaluation et les tests en ligne;
- Les applications;
- Les technologies portables;
- Les médias sociaux;
- Les programmes en ligne de traitement de santé mentale assisté par thérapeute (p. ex. TAO Connect);
- Les logiciels de gestion du bureau, y compris les options de réservations en ligne.

Il se peut que les Lignes directrices contiennent des termes qui ne vous sont pas familiers. Nous avons inclus à la fin du document un lexique des termes les plus usités.

Qu'entend-on par le terme « Lignes directrices »?

Ces Lignes directrices sont des *recommandations* conçues pour aider les conseillers et psychothérapeutes à prendre des décisions éclairées quant au recours à la technologie. Bien que *l'utilisation des Lignes directrices soit sur une base volontaire*, il est recommandé aux professionnels qui aspirent à devenir des praticiens résilients de suivre les Lignes directrices en tant qu'outil essentiel.

Les sections pertinentes du *Code de déontologie de l'ACCP*

Voici une liste des sections du *Code de déontologie de l'ACCP*[4] qui sont pertinentes à la discussion du recours à la technologie en counseling et en psychothérapie.

A1. Responsabilité générale
A3. Limites de compétence
A11. Prolongement des responsabilités en matière déontologique
B2. Confidentialité
B4. Droits des clients et consentement éclairé
B6. Tenue des dossiers
B7. Accès aux dossiers
B16. Utilisation de l'ordinateur et d'autres technologies électroniques
B17. Prestation des services à distance, médias sociaux et technologies électroniques
D5. Recours à la technologie pour l'administration de tests et d'évaluations

[4] https://www.ccpa-accp.ca/wp-content/uploads/2014/11/CodeofEthics_fr.pdf

Les lois sur la protection des renseignements personnels au Canada

Le Canada s'est doté de lois sur la protection des renseignements personnels qui régissent quels sont les renseignements qui peuvent être collectés et quels sont ceux qui peuvent être stockés. Toute personne qui a recours à la technologie pour l'un ou l'autre aspect de sa pratique du counseling ou de la psychothérapie doit tenir compte des lois canadiennes, provinciales et territoriales applicables à la protection des renseignements personnels[5] et/ou des renseignements personnels sur la santé[6].

Les praticiennes et praticiens doivent apprendre les lois, bien les comprendre, savoir ce qui est permis par la loi, connaître ses responsabilités et la façon de les appliquer dans la pratique au quotidien. Cela ne veut pas dire qu'il faille devenir des avocats en plus d'être des conseillers ou psychothérapeutes. Par contre, cela signifie que nous devons avoir acquis une compréhension de base de ces lois en particulier et sur la façon dont elles interviennent dans notre profession et dans son exercice.

Le Canada dispose de deux lois sur la protection des renseignements personnels et de la vie privée, soit la *Loi sur la protection des renseignements personnels*, qui régit les pratiques de traitement des renseignements personnels des institutions fédérales et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale sur la protection des renseignements personnels qui régit les organismes du secteur privé.[7]

> La LPRPDE est la loi canadienne qui régit **la façon dont les secteurs privés collectent, utilisent et divulguent les renseignements personnels** dans le cours de leurs activités commerciales. Toutes les organisations qui exercent des activités commerciales au Canada (sauf quelques exceptions) sont tenues de se conformer à cette Loi et il leur incombe de surveiller leur propre conformité. **Lorsqu'elles stockent leurs données en ligne** (résidence des données), les entreprises **doivent savoir où celles-ci sont stockées, qui y a accès ou qui pourrait y avoir accès et pourquoi cette Loi justifie de les conserver au Canada maintenant et à l'avenir**.[8]

Les organisations ont la responsabilité de protéger les renseignements personnels en **s'assurant de la mise en place de mécanismes de sécurité fiables, qui sont adaptés au niveau de confidentialité de l'information.**

---

[5]Les renseignements personnels désignent toute information au sujet d'une personne identifiable.

[6] Les renseignements personnels sur la santé désignent de l'information consignée au sujet d'une personne identifiable et qui porte sur la santé de cette personne ou sur la prestation de services de santé auprès de celle-ci.

[7] https://www.priv.gc.ca/fr/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[8]http://www.servercloudcanada.com/2016/07/canadian-privacy-laws-pipeda-core-principles-cloud/ (Les caractères gras sont de l'auteur)

Plus le niveau de confidentialité de l'information est élevé, plus la sécurité doit être solide. L'information à laquelle nous avons accès au sujet des personnes dans le cadre du counseling et de la psychothérapie est considérée comme étant extrêmement confidentielle; nous devons donc mettre en place les mécanismes de sécurité les plus solides qui soient.

Chaque province et territoire dispose de sa propre loi régissant le secteur public, donc applicable aux organismes gouvernementaux de la province ou du territoire. Pour le secteur privé, certaines provinces et certains territoires ont mis en place des lois de protection des renseignements personnels qui s'appliquent en lieu et place de la LPRPDE. On compte aussi un grand nombre de lois provinciales et territoriales contenant des dispositions relatives aux renseignements personnels recueillis par des professionnels (terme qui peut englober les conseillers et les psychothérapeutes).[9]

Heureusement, le Commissariat à la protection de la vie privée du Canada propose des guides relatifs aux lois fédérales, provinciales et territoriales sur la protection des renseignements personnels et peut vous aider à trouver l'organisme qu'il faut contacter en cas de problèmes liés à la protection des renseignements personnels. [10]

Comme nous l'avons déjà précisé, « peu importe où sont stockées vos données, en définitive, chaque loi fédérale, provinciale/territoriale est très claire : **dès qu'une organisation recueille des données confidentielles**, elle est **responsable à 100 % de les protéger et de les sécuriser**, et il incombe à chaque organisation individuelle de bien comprendre les règles. »[11]

Protection des données

Que vous adoptiez ou non la prestation directe en ligne de services de counseling ou de psychothérapie, il est probable que vous utilisiez la technologie auprès de vos clients ou pour les desservir. Les lois sur la protection des renseignements personnels et notre *Code de déontologie (B2. Confidentialité)* nous obligent à garantir la confidentialité et la protection des renseignements des clients. Pour leur part, nos clients s'attendent eux aussi qu'en tant que fournisseurs de services, nous nous occupions de ces détails. Autrement dit, nous devons concevoir des plans pour protéger toute information que nous recueillons ou que nous stockons. Nous devons assurer la cybersécurité[12]. Il n'est pas nécessaire de vous transformer en informaticien analyste pour vous sentir à l'aise de fournir un niveau éthique de confidentialité et de protection des renseignements personnels.

[9] https://www.priv.gc.ca/fr/privacy-topics/privacy-laws-in-canada/02_05_d_15/
[10] https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/
[11] http://www.servercloudcanada.com/2015/09/canadian-privacy-laws-canadian-cloud-primer-canadian-businesses/
[12] www.pensezcybersecurite.gc.ca/index-fr.aspx

Si vous n'êtes pas certain que la protection des données concerne votre pratique et la technologie que vous utilisez, veuillez passer en revue la section des Lignes directrices qui s'intitule « Qu'entend-on par recours à la technologie? ».

Les mesures de sécurité de base

Hushmail, fournisseur de courriels sécurisés par cryptage, souligne que votre compte de courriel constitue une mine de renseignements pour toute personne en mesure d'y avoir accès. Bien des services emploient le courriel pour acheminer les liens de réinitialisation de mot de passe. Si une personne parvient à pénétrer dans votre compte de courriel, elle peut facilement utiliser votre adresse courriel pour déclencher des réinitialisations du mot de passe de vos comptes en ligne. Pour éviter que cela ne se produise, il faut doter votre compte de courriel d'un mot de passe robuste. Certains services prévoient d'ailleurs une vérification en 2 étapes.

Des mots de passe robustes

Le fait de doter tous vos appareils technologiques de robustes mots de passe (p. ex. téléphones, portables, tablettes, ordinateurs) constitue une mesure de sécurité. On trouve de nombreux et excellents conseils sur la façon de configurer des mots de passe robustes.

- Utilisez comme mots de passe des locutions composées de mots aléatoires. À ce propos, Hushmail indique qu'une locution mot de passe créée à partir de quelques mots choisis au hasard est facile à mémoriser et très robuste. Cela s'avère supérieur aux mots de passe complexes et difficiles à mémoriser;
- Mélangez les caractères (p. ex. $m1the93#90s);
- Utilisez un mot de passe différent pour chaque site web ou chaque application où vous vous inscrivez;
- Songez à utiliser un gestionnaire de mots de passe (p. ex. 1Password);
- Modifiez vos mots de passe ou vos locutions mots de passe au moins tous les trois mois.

La vérification en 2 étapes

Certains services ont recours à la vérification en deux étapes pour accorder l'accès à un compte. Par exemple, il se peut qu'un service vous demande votre mot de passe, puis vous pose une question de sécurité (p. ex. le nom de fille de votre mère). D'autres choisiront plutôt d'acheminer un code vers votre téléphone afin que vous le saisissiez après avoir entré votre mot de passe. Bien que peu usité dans les logiciels de courriel, ce système est souvent utilisé lorsque vous vous connectez à une banque depuis un ordinateur que vous n'utilisez pas habituellement.

La protection contre l'hameçonnage

Il est important de bien comprendre les risques associés aux courriels d'hameçonnage. Il s'agit de courriels que vous recevez et qui semblent provenir de votre banque ou d'un autre service ou d'une autre personne. Ils semblent parfois provenir d'une personne que vous connaissez. D'autres fois, ils semblent sortis de nulle part (p. ex. un courriel de UPS vous indiquant que la livraison de votre colis sera retardée). En règle générale, on vous demande de cliquer sur un lien dans le courriel ou de télécharger une pièce jointe. Si vous

téléchargez un fichier, vous courez le risque d'infecter votre ordinateur ou de devenir victime d'un logiciel rançonneur. Si vous vous rendez dans un site web et fournissez vos renseignements personnels, votre compte bancaire pourrait être vidé et votre identité, volée. Parmi les autres problèmes, citons le risque que tous les renseignements sur la clientèle qui se trouvent enregistrés dans votre système informatique soient utilisés pour d'autres tentatives d'hameçonnage.

Reportez-vous à l'Annexe A pour en savoir plus sur la façon de protéger vos données contre l'hameçonnage et l'hameçonnage ciblé.

La sécurité Wi-Fi

Que vous utilisiez le Wi-Fi à la maison, au travail ou dans un contexte public, il importe de savoir quelles sont les mesures à prendre pour garantir la sécurité et protéger vos appareils et tous les renseignements sur la clientèle qu'ils contiennent.

Reportez-vous à l'Annexe A pour de plus amples conseils sur la façon d'assurer la sécurité de tout dispositif Wi-Fi que vous pourriez utiliser.

Garantir la sécurité de base

La sécurité de base comporte quatre étapes principales :

- Assurez-vous de disposer de versions à jour de logiciels antivirus et antiprogrammes malveillants;
- Assurez-vous que vos navigateurs et systèmes d'exploitation sont mis à jour lorsque des mises à jour sont disponibles. Cela garantit que les failles de sécurité connues ne peuvent pas être exploitées;
- Activez le cryptage du disque;
- Procédez au cryptage des dispositifs de stockage amovibles (p. ex. les clés USB).

La fin de vie du matériel

Lorsqu'il n'est plus utilisé, le matériel informatique contient encore beaucoup d'information. Lorsqu'ils contiennent de l'information confidentielle, les ordinateurs et tablettes ne doivent pas être simplement recyclés. Si votre matériel fonctionne encore lorsque vous décidez de vous en départir, vous devriez en retirer le disque dur. Le fait d'effacer les fichiers ne permet pas de les retirer du disque dur. Le fait d'écraser les fichiers permet seulement d'empêcher certains pirates d'y avoir accès. Même le fait de reformater le disque ne permet pas de faire disparaître entièrement les données, car un pirate habile pourra les récupérer. Avant de recycler le téléphone, stockez toutes les données sur une carte SIM. Puis, à moins que vous vouliez transférer la carte sur un nouveau téléphone, vous devriez détruire la carte.

La sécurité physique

Les dispositifs mobiles sont petits, portables et il est très facile pour un tiers d'y jeter un coup d'œil. Ils sont faciles à voler ou à perdre. Diverses recommandations visent à aider à garantir la sécurité physique de vos appareils.

- Lorsque vous ne les utilisez pas, mettez physiquement vos appareils sous clé;
- Tous les appareils doivent être protégés par des mots de passe, que vous ne partagerez avec personne d'autre;
- Ne laissez jamais vos appareils sans surveillance;
- Ne conservez dans vos appareils que le minimum de données sur la clientèle (p. ex. si un client vous fait parvenir un message texte, supprimez ce dernier de façon sécurisée);
- Servez-vous d'une application de suppression des données, afin que si vos appareils sont volés, vous puissiez en purger les données;
- Dans le cas d'un iPhone, activez la fonction *Localiser mon iPhone*; il s'agit d'un service iCloud. Vous pouvez verrouiller votre appareil à distance et le purger. Cela fonctionne dans le cas des iPhones, iPads et des ordinateurs Mac;
- Si vous conservez une liste imprimée de vos mots de passe, gardez-la sous clé;
- Si vous devez imprimer des données sur un client (p. ex. ses coordonnées en cas d'urgence), conservez le document sous clé.

Plus vous vous montrerez enthousiaste et confiant au sujet des outils de sécurité que vous utilisez, plus les clients le seront eux aussi. Il faut donc s'entraîner. Exercez-vous à utiliser les technologies avec des membres de votre famille et des amis. Demandez conseil à d'autres utilisateurs de la technologie. Soyez sans crainte. Renseignez-vous.

La gestion et la conservation des dossiers

Les conditions d'utilisation

- Lisez les clauses en petits caractères. Pour faire des mises à jour, vous devez accepter les nouvelles Conditions d'utilisation, qui font partie de la démarche de mise à jour. Lisez les conditions d'utilisation. Portez une attention particulière à ce qui suit :
  - Toutes les politiques de protection des renseignements personnels applicables aux ressources que vous comptez utiliser (parce que vous ne pouvez pas promettre plus que ce qui y est promis);
  - De nouvelles façons de protéger les données;
  - La politique de sauvegarde et la possibilité que les données soient éventuellement supprimées, et selon quelle échéance.
- Confirmez le lieu où se trouvent les serveurs : les dossiers devraient être entreposés au Canada;
- Confirmez les exigences des agences et des institutions : certaines agences et institutions exigent que les données soient entreposées à l'intérieur de la même province ou du même territoire que le lieu physique où vous vous trouvez;
- Assurez-vous que l'usage commercial est permis;
- Accordez une attention particulière à la relecture des Conditions d'utilisation si l'entreprise change de propriétaire.

Les sauvegardes

- Apprenez à connaître vos logiciels! Bon nombre de services offrent une sauvegarde automatique de tout ce qui se trouve sur votre ordinateur/appareil mobile (p. ex. iCloud, DropBox). Assurez-vous que les dossiers de counseling et de psychothérapie ne sont pas sauvegardés automatiquement vers un tiers non concerné;
- Si vous avez évalué une plateforme en particulier et que vous envisagez de l'utiliser, confirmez la politique de sauvegarde qui la régit. Informez-vous de ce qu'il advient des données si vous cessez d'utiliser la plateforme. Sont-elles entreposées même si vous ne payez pas ou si vous ne l'utilisez plus? Pendant combien de temps?
- Existe-t-il des lois ou règlements en particulier sur votre territoire ou au sein de votre organisation qui vous obligent à conserver indéfiniment certains types de dossiers? Si c'est le cas, comment ceux-ci seront-ils conservés tandis que d'autres dossiers seront supprimés?
- Déterminez à quel endroit les données sont entreposées. Les dossiers quittent-ils le Canada?
- Déterminez si les sauvegardes sont cryptées et, le cas échéant, qui est en mesure de les décrypter.
- Certains systèmes s'annoncent comme étant de type « Zero Knowledge », ce qui signifie qu'ils sont incapables de décrypter vos données. C'est une caractéristique souhaitable, car cela garantit la confidentialité. Mais cela signifie également que vous devez prendre encore plus de précautions pour ne pas perdre le mot de passe servant au décryptage.

Choisir une technologie ou une modalité

Il existe une foule de modalités de prestation du counseling et de la psychothérapie en ligne[13]. Dans plusieurs de ces modalités, il faut être en mesure de démontrer une certaine capacité à travailler sans indices visuels. Il faut aussi trouver des façons durables de se maintenir à jour par rapport aux tendances et à la recherche de pointe. La formation peut vous rendre plus confiant dans le recours à la technologie, vous aider à mieux comprendre les enjeux éthiques, de protection des renseignements personnels et de sécurité, tout en vous fournissant une rétroaction au sujet de votre présence en ligne. Selon le type de formation, cela peut aussi permettre de mieux évaluer quelle technologie est la plus appropriée à des fins données.

[13] Pour consulter une liste de modalités, veuillez vous reporter à la section intitulée « Qu'entend-on par recours à la technologie? »

Vous pouvez avoir recours à l'une ou l'autre ou à toutes ces modalités pour communiquer avec les clients, de façon complémentaire à votre travail auprès d'eux ou encore pour leur offrir un service direct. Comme le signale Suler (2011) :

> Ces diverses modalités se distinguent parfois de façon évidente, mais parfois plus subtilement, ce qui fait d'ailleurs que chaque contexte psychologique est unique; le praticien en ligne devrait en tenir compte lorsqu'il doit choisir un outil de communication pour travailler auprès d'un client en particulier. Il convient de prendre en compte divers aspects particuliers des relations textuelles aux fins du travail clinique en ligne : les habiletés de lecture et d'écriture façonnent la communication; les indices visuels et sonores sont réduits au minimum; un sens subjectif de l'espace interpersonnel vient remplacer l'importance de l'espace géographique; les gens peuvent converser avec presque n'importe qui en ligne et avec plusieurs partenaires à la fois; et les conversations peuvent être sauvegardées et réexaminées ultérieurement. Plusieurs de ces facteurs provoquent la désinhibition sociale. Les praticiennes et praticiens en ligne peuvent vouloir se spécialiser dans un type particulier de support textuel, tout en reconnaissant ses avantages et inconvénients par rapport à d'autres.[14]

Comment évaluer quelle modalité et/ou quelle plateforme technologique utiliser?

Avant de choisir une technologie à utiliser dans la pratique professionnelle, examinez soigneusement les **capacités relationnelles** et les **risques à la protection des renseignements personnels** qui sont inhérents à la modalité ou à la plateforme en cause.

Les capacités relationnelles

En quoi cette technologie répond-elle aux besoins cliniques? Qu'est-ce qui justifie d'utiliser cette technologie ou cette modalité auprès de ce client en particulier?

- En quoi le recours à cette technologie aura-t-il une incidence sur la relation client-conseiller/psychothérapeute?
- Comment parviendrez-vous à atténuer toute incidence négative?
- Effectuez une recherche sur les données probantes concernant la technologie (p. ex. l'outil de recherche spécialisé Google Scholar) et sur les évaluations de la technologie ou de la modalité.
- Faites l'essai de la technologie afin de déterminer sa convivialité, son mode de fonctionnement et si elle est à la hauteur de ses prétentions.

Les risques liés à la protection des renseignements personnels

Songez à effectuer votre propre étude d'impact sur la vie privée (ÉIVP) pour chacune des technologies dont vous faites usage. Lisez attentivement les politiques sur la protection des renseignements personnels des différentes plateformes ou modalités technologiques.

[14] Suler, J. (2011). The Psychology of Text Relationships. Dans Speyer, C. (Éd.). *Online Counseling (deuxième édition)*, (p. 21- 53). Londres : R.-U., Elsevier.

Voici quelques questions d'ÉIVP qu'il convient d'aborder :

- Quels renseignements personnels seront recueillis? (p. ex. noms des clients, coordonnées, numéros d'assurance sociale) Et à quelles fins?
- Qui aura accès aux renseignements personnels recueillis? Ces renseignements personnels seront-ils partagés?
    - Avec un clinicien, un assistant administratif, un technicien, équipe clinique? Que savez-vous des concepteurs de la plateforme technologique? Ont-ils accès aux données que vous recueillez?
    - Examinez les obligations contractuelles et assurez-vous que celles en place protègent bien la clientèle contre les accès ou l'utilisation non autorisés.
- De quelle façon les renseignements personnels seront-ils utilisés? (p. ex. serviront-ils à des fins d'identification ou à déterminer les offres de services?)
- Où les données sont-elles entreposées?
    - Le détenteur de la technologie a-t-il un serveur au Canada ou bien entrepose-t-il les données dans le nuage? Quelles sont les lois de protection des renseignements personnels en vigueur dans ma province ou mon territoire?
    - *Dans les références des Lignes directrices, vous trouverez la liste des sites web concernant les lois fédérales et provinciales sur la protection des renseignements personnels.*
- De quelle façon les données sont-elles transmises? Sont-elles cryptées?
- La technologie exige-t-elle une protection par mot de passe? L'authentification à deux facteurs est-elle disponible?
- Votre matériel est-il situé dans un lieu sécurisé?
- Le système auquel vous songez est-il situé dans un lieu sécurisé?
- Pouvez-vous désactiver certaines fonctions de collecte de données?
- Si des données sont enregistrées auprès de tierces parties (p. ex. fournisseur de cellulaire, fournisseur d'infonuagique), est-ce que ces enregistrements sont supprimés lorsque vous les rayez de votre appareil (p. ex. ordinateur portable, cellulaire)?
- Des atteintes à la vie privée et à la sécurité peuvent toujours survenir. Concevez un plan de gestion de ces atteintes au cas où elles se produiraient. Qui devrez-vous contacter et à quel moment? Quels risques cela pose-t-il aux individus ou au groupe? Quels sont les dommages possibles s'il survient une telle atteinte? Comment peut-on atténuer ces risques?

Il peut parfois s'avérer utile de recourir à une liste de contrôle pour définir les risques. Roy Huggins de la société Person Centered Tech propose une « liste de contrôle pratique » lorsqu'il s'agit de choisir une technologie. [15]

[15] https://personcenteredtech.com/2017/05/26/practice-checklist-practice-tech-choices/

Prestation compétente de services en ligne de counseling et de psychothérapie

La technologie étant omniprésente dans nos vies, il semble facile de supposer qu'il suffit de transposer notre travail en ligne. L'International Society for Mental Health Online (ISMHO) insiste sur l'importance de la compétence dans le domaine des services en ligne, et bien d'autres organisations de praticiens incitent les conseillères, conseillers et psychothérapeutes à faire preuve de maîtrise et de compétence en suivant une formation spécialisée sur le travail en ligne.[16] Le counseling et la psychothérapie en personne sont fort différents du travail en ligne. Chacune des modalités de prestation en ligne comporte des caractéristiques uniques qui peuvent avoir une incidence sur la relation thérapeutique et qui commandent des considérations diverses concernant la protection des renseignements personnels et la sécurité. En tant que membres de l'ACCP, nous sommes tenus de n'exercer que dans les domaines dans lesquels nous avons reçu une formation adéquate (A3. Limites de la compétence). La formation sur le travail en ligne est indispensable.

Notre rôle de professionnel nous oblige à bien nous renseigner sur la manière dont fonctionnent les technologies auxquelles nous avons recours et sur le mode d'utilisation des appareils. **Avoir acquis les habiletés de base en informatique et savoir crypter les messages, voilà qui est indispensable à ce type de travail.** Il faut savoir bien utiliser la technologie.

Les compétences technologiques de base

Voici quelques-unes des compétences de base liées à l'utilisation de la technologie :

- **Cryptage** – savoir accéder aux services de cryptage servant à l'entreposage des dossiers et à la livraison des communications
- **Systèmes de sauvegarde** – savoir entreposer les dossiers et les données en toute sécurité sur votre propre système ou par l'intermédiaire d'un système sécurisé et crypté
- **Protection par mot de passe** – savoir créer des mots de passe robustes et en utiliser des différents pour chaque site web ou service auquel vous avez recours; songer à modifier vos mots de passe régulièrement
- **Coupe-feu** – connaître le rôle du coupe-feu
- **Protection antivirus** – savoir protéger votre système contre les virus
- **Matériel** – comprendre la plateforme de base sous laquelle tourne votre ordinateur
- **Logiciel** – savoir télécharger et exploiter du logiciel et pouvoir assister les clients dans cette tâche
- **Tiers fournisseur de services** – savoir où sont entreposées les données, leur utilisation et qui peut y accéder
- **Internet** – une compréhension de base de son fonctionnement

[16] Il existe de nombreux programmes reconnus au Canada, aux É.-U. et au R.-U. qui offrent de la formation sur le recours à la technologie en counseling et psychothérapie.

L'utilisation compétente de diverses modalités

La British Association of Counselling & Psychotherapy a établi une liste des compétences applicables au counseling à distance (par téléphone ou par internet).[17] On y affirme que la connaissance fondamentale pour l'utilisation de toutes les formes de technologie en counseling est en fait la **connaissance des processus psychologiques impliqués dans l'offre de services en ligne de counseling et de psychothérapie**.

Lorsque vous utilisez des modalités par échanges textuels (p. ex. le courriel, le texto, le clavardage), vous devez :

- Comprendre en quoi le texte peut aider;
- Évaluer dans quelle mesure cela convient au counseling ou à la psychothérapie en ligne;
- Définir et gérer le risque inhérent au counseling ou à la psychothérapie en ligne;
- Définir les limites;
- Sans doute l'un des aspects les plus importants concerne le fait de savoir gérer l'impact de la désinhibition.

Pour chacune des modalités, voici une liste des considérations de base :

Téléphone (cellulaire ou intelligent)

- Sécurité de la connexion téléphonique;
- Votre lieu géographique et celui du client;
- Le minimum d'interruptions (ou leur élimination complète);
- Le timbre et le ton de la voix;
- La nécessité de signes vocaux plus fréquents pour indiquer que vous êtes à l'écoute;
- Une fois l'appel terminé, suppression sécurisée du numéro de téléphone du client;
- Assurez-vous de ne pas être à la portée d'un dispositif de surveillance Stingray;
- Si vous travaillez pour une agence, n'utilisez que les appareils téléphoniques de celle-ci. Évitez d'utiliser un cellulaire personnel.

Courriel

Utilisez une adresse de courriel distincte et sécurisée pour les clients.

Tous les courriels utilisés pour communiquer avec les clients doivent être cryptés. Voici ce qu'en dit Roy Huggins de Personcenteredtech.com : « le cryptage, c'est le cyber équivalent des murs d'insonorisation, des portes closes et du déplacement des machines bruyantes dans le corridor (traduction libre) ».[18] C'est un puissant outil, mais ça ne reste qu'un outil. Vous devez l'utiliser et l'entretenir correctement.

---

[17] https://www.bacp.co.uk/media/2045/bacp-competences-for-telephone-ecounselling.pdf

[18] https://personcenteredtech.com/2016/10/16/even-though-right-hipaa-unencrypted-emails-case-using-secure-email-texting-clients/

Voici les possibilités à considérer :

- Vous pouvez crypter ou protéger par mot de passe un document que vous adressez à un client;
- Vous pouvez crypter ou protéger par mot de passe le courriel lui-même;
- Vous pouvez choisir d'utiliser un système de courriel crypté et sécurisé (p. ex. Hushmail ou Privacemail) pour communiquer avec vos clients ou pour leur fournir des services de counseling ou de psychothérapie.

En tant que conseillères, conseillers et psychothérapeutes, nous devons rendre les options sécurisées disponibles de manière raisonnable. Il se peut que les clients affirment accepter les communications non cryptées, mais c'est peut-être parce qu'ils ne comprennent pas tout à fait les implications de la protection des renseignements personnels.

Messagerie texte

- Assurez-vous d'utiliser une option de messagerie texte sécurisée;
- Établissez clairement à quelles fins vous utiliserez la messagerie texte – Les changements de rendez-vous? Les rappels? Les inscriptions?
- Comment votre client perçoit-il le recours au texto sur le plan de la relation?
- La rapidité de communication est un élément crucial de la messagerie texte, mais cela peut facilement créer des malentendus si un échange prend plus de temps que l'anticipait le client;
- Apprenez à décoder le sens des émoticons et des abréviations;
- Apprenez le jargon en usage dans la messagerie texte.

Dialogue en ligne ou clavardage (temps réel)

- Exige une approche différente, empreinte de patience;
- Fermez toutes les autres applications;
- Éliminez les interruptions;
- La plupart des considérations citées ci-dessus pour la messagerie texte s'appliquent ici aussi;
- Prenez en compte votre propre vitesse de frappe au clavier et celle du client.

Counseling par échanges textuels asynchrones

- Utilisez un système crypté;
- Utilisez des techniques de présence pour compenser l'absence d'indices visuels et pour améliorer l'impression de vivre la séance sur le moment;
- Portez une attention particulière au temps que vous consacrez à une séance;
- Il faut une certaine habileté pour traduire en mots les interventions de counseling/psychothérapie.

Webcam/Vidéo

- Utilisez une plateforme cryptée sécurisée;
- Il faut prendre en compte la bande passante, l'éclairage, l'habillement, le décor, etc.;
- Notez la qualité du casque d'écoute, la fiabilité du son (signal audio);
- Tenez compte du dispositif du client (capacité, compatibilité);
- Une foule d'autres facteurs à prendre en compte, notamment qui d'autre pourra entendre la conversation, quelle autre personne pourrait se trouver déjà dans la pièce ou y entrer;
- Une foule de considérations éthiques : par exemple, permettrez-vous aux clients d'enregistrer les séances? Si oui, peuvent-ils en publier certains extraits sur Internet?

Réalité virtuelle/Avatars ebcam/Vidéo

- Les progrès de la technologie de réalité virtuelle (RV) ont permis aux praticiennes et praticiens d'y recourir de façons de plus en plus efficaces pour traiter divers problèmes (p. ex. les phobies, l'ESPT). La RV et les avatars comportent certains avantages comparativement au fait de reproduire les expériences dans la vie réelle, notamment la possibilité de contrôler l'environnement. Nous devons mieux comprendre l'*incidence de ces environnements de RV à la fois sur le client et sur le praticien*;
- Ces deux domaines exigent que l'on comprenne leurs modes de fonctionnement et que l'on acquière une **formation spécialisée** sur leurs applications thérapeutiques;
- Prévoyez du temps pour vous exercer à devenir à l'aise avec cette technologie;
- Choisissez le niveau de communication approprié et songez à recourir à une fonction de clavardage privé;
- Élaborez un plan pour la prise en charge des urgences qui pourraient survenir durant une séance de counseling/psychothérapie virtuelle.

Évaluation et tests en ligne

- Étudiez la sécurité de l'outil d'évaluation;
- Où les données sont-elles entreposées; et
- Les données peuvent-elles être utilisées par des tiers et, si oui, de quelle façon?

Applications (Appli)

Les applications sont rapidement en train de devenir une composante essentielle des soins de santé globale. Comme dans le cas des autres modalités de prestation, le facteur sécurité est important, tout comme la finalité de la communication (c.-à-d. Est-elle entreposée? Où et par qui? Pendant combien de temps?). Bien des applications sont utilisées comme suit en counseling et en psychothérapie :[19]

- Psychopédagogie;
- Filtrage et rétroaction;
- Prise de décisions, résolution de problèmes et établissement d'objectifs;
- Autosurveillance et suivi des progrès du traitement (y compris l'adhésion à la médication);
- Les travaux à domicile (devoirs);
- L'acquisition de nouvelles compétences;
- L'autogestion;
- La recherche d'aide;

Pourquoi suggérez-vous une appli? Votre client utilise-t-il l'appli pour vous faire un compte rendu ou pour partager un suivi?

Technologies portables

- Étudiez le fonctionnement du système et son impact potentiel sur le client
- Quelle démarche doit effectuer le client pour partager l'information que vous avez recueillie?
- À qui appartiennent les données? À votre client? Ou à la compagnie?

Programmes de traitement de santé mentale en ligne assistés par un thérapeute

- Il faut être familier avec le traitement;
- Savoir utiliser les techniques de présence dans un tel environnement (selon le programme en cause);
- Bien comprendre l'impact sur le client et la façon d'évaluer si le tout est bien adapté.

Deux considérations importantes :
D'abord, nous n'avons aucune prise sur les situations vécues par les clients et il peut s'avérer impossible de détecter certains problèmes auxquels ils sont confrontés. Nous ne contrôlons pas le lieu où les clients choisissent de se trouver, ni qui les accompagne, quelles distractions peuvent être présentes, leur degré de sécurité personnelle, etc.

Deuxièmement, nous devons consacrer du temps à nous demander dans quelle mesure les clients sont concernés par les technologies et en quoi cela les influence. Comprenons-nous bien les univers en ligne dans lesquels ils pourraient s'engager (p. ex. jouer à Second life, la pratique de jeux)? Réfléchir à quel degré de connaissances technologiques les clients s'attendent de votre part.

[19] Hides, L. (2014). Are SMARTapps the future of youth mental health? *InPsych* Juin 2014

Vérification de l'identité du client

La question suivante se pose souvent : comment puis-je m'assurer que le client ou la cliente est vraiment la personne qu'il ou elle prétend être en ligne? Il faut prendre des mesures raisonnables pour s'assurer que la personne se présente avec exactitude. On recommande d'en faire une exigence dans le formulaire de consentement, de même qu'exiger que les clients fournissent des coordonnées complètes.

Selon votre contexte de travail (p. ex. en clinique comparativement au cabinet privé), il existe diverses façons de vérifier l'identité du client. Dans les contextes de grandes organisations, il est parfois possible d'utiliser un numéro de client à des fins de vérification. Par exemple, dans le contexte d'une université, les étudiants possèdent un numéro d'identification de l'étudiant que l'on peut employer ou encore dans le cadre d'un Programme d'aide aux employés, on peut parfois exiger que l'employé fournisse son numéro d'employé. Dans des contextes de plus petites organisations, on peut choisir d'établir un mot de passe ou un code pour chaque client, ce qui permet au praticien de vérifier l'identité de ce dernier. On peut aussi adresser un message au client dans un premier temps afin de confirmer qu'il s'agit de la bonne personne avant de lui adresser de l'information personnelle ou confidentielle.

Par souci d'équilibre, nous devons aussi réfléchir à nos activités en personne. Comme le souligne Weitz : « Nous ne procédons pas à une vérification d'identité dans le cadre d'une thérapie en personne, nous ne mettons pas en doute l'identité des clients et ce sont ces derniers qui nous fournissent l'image d'eux-mêmes qu'ils veulent bien nous projeter. Et en fait, est-ce si important? Le client se présente en thérapie pour travailler sur un ou plusieurs problèmes en particulier, et si nous sommes capables de travailler sur ceux-ci de façon satisfaisante, alors le reste est probablement sans importance. (Traduction libre) »[20]

Il y a lieu de se préoccuper lorsqu'un client commence tout à coup à se comporter différemment ou s'il partage quelque chose qui ne semble plus du tout correspondre à nos engagements antérieurs à son égard. Les clients peuvent partager leurs mots de passe avec des tiers ou encore une autre personne peut être présente dans la pièce au cours d'une séance vidéo. Évidemment, de telles situations peuvent aussi survenir dans le cadre d'une thérapie en personne. Quelqu'un pourrait avoir menacé le client et lui avoir ordonné de nous mentir en personne. Que ce soit en ligne ou en personne, il est crucial de rester vigilant et de faire appel à notre intuition de clinicien.

Gestion du risque

Que vous travailliez en cabinet privé ou pour une agence ou une institution ou dans tout autre contexte dans lequel les conseillers et psychothérapeutes sont appelés à évoluer, vous aurez besoin de posséder une compréhension de base de la gestion du risque. Il nous incombe en effet de garantir à nos clients la protection des renseignements personnels et la confidentialité (B2. Confidentialité); il en va de même pour toutes les données que nous recueillons sur eux dans le cadre de la démarche de counseling et de psychothérapie.

[20] Weitz, p. 164

« Le **risque** désigne la possibilité que survienne quelque chose de préjudiciable ou de non souhaitable.

La **gestion du risque** désigne les procédures qu'une personne ou une organisation met en place pour se protéger et pour protéger ses clients.

Rappel : personne ne peut éliminer totalement les risques! Il vous incombe de démontrer que vous avez reconnu les risques et que vous avez pris des précautions raisonnables pour empêcher qu'ils ne causent des dommages à vos clients, à la propriété ou à la réputation. (Traduction libre) » [21]

On peut définir la gestion du risque en fonction de quelques étapes simples :

- La détermination des **éléments d'actif** de votre organisation;
- Les **impacts** sur l'organisation qu'auraient le vol, le bris ou autre mise à mal des éléments d'actif;
- La détermination des **menaces** pesant sur chaque élément d'actif;
- Les mesures que l'on peut prendre systématiquement pour **atténuer**, surveiller et maîtriser l'impact d'un malheureux événement touchant les actifs.

Au terme de votre analyse de gestion du risque, vous aurez dégagé une série de décisions sur la façon dont vous planifiez de protéger vos actifs. Cela fera partie de votre politique de sécurité. Celle-ci documente des aspects tels que la façon de classer vos éléments d'actif et les politiques que vous adoptez pour atténuer le risque qui leur est associé ou du moins le maîtriser. Le fait de documenter une politique de sécurité constitue une excellente pratique, car vous pouvez ainsi regrouper en un même endroit les décisions prises et auxquelles vous pourrez vous reporter ultérieurement.

La gestion du risque vous permet de décider du niveau de risque que vous êtes prêt à assumer. Ces principes s'appliquent aussi bien à ceux et celles qui travaillent en cabinet privé qu'au sein de grandes organisations. Plus l'organisation est grande, plus l'analyse est complexe. Et, bien évidemment, pour élaborer les politiques et les procédures, il faut tenir compte des sections précédentes du présent document, qui portent sur les lois de protection des renseignements personnels.

Détermination de vos éléments d'actif

Il faut d'abord dresser l'inventaire de vos actifs. Il peut s'agir de **biens matériels ou de données numérisées, comme des renseignements personnels et des bases de données sur la clientèle.** Dressez la liste complète de tout ce qui peut être perdu, volé ou endommagé. En comprenant mieux en quoi consistent vos actifs et où ils se trouvent, vous serez plus en mesure de décider ce que vous devez protéger et quelles sont vos lacunes, de sorte que vous saurez quels aspects de votre sécurité doivent, le cas échéant, être renforcis.

[21] https://www.queensu.ca/alumni/sites/default/files/risk_management_guide.pdf

Vous pouvez également classer vos actifs numériques afin de mieux les protéger. Par exemple, certaines de vos données pourraient consister en des notes très confidentielles au sujet des clients, tandis que d'autres données, comme des dossiers comptables, pourraient se révéler moins sensibles. En classant les notes sur les clients dans la catégorie **information confidentielle de client**, tandis que les dossiers de comptabilité tomberaient dans la catégorie **confidentiel**, vous serez en mesure d'élaborer des politiques précises sur la façon d'entreposer, d'utiliser et de protéger ces données.

Imaginer les impacts

La prochaine étape consiste à souligner les conséquences d'un incident (p. ex. le vol d'un ordinateur, le piratage de votre système informatique). Si tout à coup vous n'aviez plus accès à vos données ou que celles-ci avaient été volées, quelles en seraient les conséquences? En quoi vos clients en seraient-ils touchés? Combien de revenus pourriez-vous perdre ou est-ce que les impacts porteraient davantage sur la nature embarrassante de la situation ou le tort fait à votre réputation? Combien faudrait-il de temps pour reconstruire ou serait-ce même envisageable? En parvenant à mieux comprendre les impacts relatifs de certaines pertes d'éléments d'actif, vous serez plus en mesure d'établir vos priorités en matière d'investissement pour sécuriser vos systèmes informatiques.

Déterminer les menaces

Étudiez les différentes situations qui pourraient mal tourner et dressez la liste de toutes les *menaces potentielles* à tous les éléments d'actif de votre entreprise. Par exemple, votre système pourrait-il être victime de piratage? Quelles sont les failles dans la façon dont vous ou vos collègues concevez l'accès à vos systèmes et à vos données? Avez-vous reçu suffisamment de formation pour pouvoir détecter les courriels d'hameçonnage? Vos politiques sont-elles bien comprises par tous les membres de votre organisation ou de votre cabinet? Sauvegardez-vous vos données pour les protéger d'une perte éventuelle?

Atténuez vos risques

Une fois que vous avez déterminé vos éléments d'actif, que vous avez imaginé les impacts qu'ils peuvent subir et défini ce qui les menace, vous pouvez commencer à prioriser les menaces les plus susceptibles de survenir. Vous pouvez alors décider dans quel ordre vous allez aborder les risques. Vous avez la possibilité de les régler en adoptant des politiques et des pratiques précises. Ce sont ces décisions qui forment alors la base de votre politique de sécurité.

Exemple :

> Au terme de votre évaluation des risques, vous pourriez décider de recourir au cryptage complet des disques sur tous vos ordinateurs, en raison des risques de vol. Le cryptage complet du disque dur assure que les données qui s'y trouvent sont illisibles, sauf pour le détenteur d'un nom d'utilisateur et d'un mot de passe reconnus par l'ordinateur. Cette décision ferait dorénavant partie de votre politique de sécurité.

En suivant les étapes décrites ci-dessus, vous avez pu :

- **Déterminer les actifs** – Vos ordinateurs sont classés parmi les éléments d'actif matériel, et les données confidentielles sur les clients contenues sur les disques durs sont elles aussi classées parmi les actifs;
- **Imaginer les impacts** – Premièrement, la perte matérielle de vos ordinateurs représenterait un coût financier qui inclut le coût de remplacement du matériel et celui associé au temps de reconfiguration des appareils substituts. Deuxièmement, les données contenues dans l'ordinateur sont les données confidentielles que vous détenez sur vos clients. Elles sont sauvegardées et ne sont donc pas exposées à une perte pure et simple. Cependant, votre cabinet et vos clients seront touchés dans une mesure qui est difficile à évaluer si ces données tombent entre les mains d'un tiers non autorisé. C'est cet impact qui est le plus préoccupant.
- **Déterminer les menaces** – Bien qu'il existe d'autres types de menaces à prendre en compte, c'est le vol qui, en l'occurrence, constitue la menace principale susceptible de toucher aussi bien l'ordinateur matériel que les données qu'il contient;
- **Atténuer la menace** – Vous pouvez vous en remettre à l'assurance afin d'atténuer la perte financière associée à celle des ordinateurs ou encore décider que le risque associé à cette perte financière est acceptable. Mais dans le cas de la pire des menaces, soit le fait que les données tombent entre des mains malfaisantes, c'est le recours au cryptage complet des disques qui permet de réduire l'impact sur votre pratique. C'est pourquoi ce recours constitue l'action à prendre de façon prioritaire.

Territoire de compétence

L'une des questions qui reviennent sans doute le plus souvent au sujet du counseling à distance concerne le territoire de compétence. Lorsque des conseillères, conseillers ou psychothérapeutes se demandent : « puis-je offrir des services de counseling ou de psychothérapie à une personne qui habite une autre province, un autre territoire ou même un autre pays? », la réponse dépend souvent de la position adoptée par les organismes de réglementation et du lieu dans lequel ces derniers considèrent que s'effectue cette prestation de services.

Ici, au Canada, la réglementation de la profession de counseling et de psychothérapie est en pleine évolution. Dans le cas du counseling en personne, la loi qui s'applique est déterminée par le lieu où se déroule le travail. Si vous et votre client vous trouvez en C.-B., alors ce sont les lois de cette province qui s'appliquent. Lorsque le travail s'effectue en ligne, le conseiller/psychothérapeute et le client peuvent se trouver dans des lieux géographiques différents et régis par des lois et des règlements différents en matière de

counseling et de psychothérapie. Cela peut entraîner de l'incertitude quant aux lois qui s'appliquent.[22]

Selon certains organismes de réglementation, le counseling se déroule **à l'endroit où se trouve le client au moment de la prestation du service**. Autrement dit, ce sont les règlements en vigueur où se trouve le client qui ont préséance. Par exemple, si votre cliente se trouve en Ontario (même si ce n'est que pour une brève visite) et que vous êtes en C.-B., alors ce sont les règlements de l'OPAO qui s'appliquent.

Selon d'autres organismes de réglementation, les règlements applicables dépendent à la fois du lieu où se trouve le client **et** du lieu où se trouve le conseiller au moment de la prestation du service.

Là où une réglementation est en vigueur (comme c'est le cas dans certaines provinces du Canada), il se peut que vous deviez adhérer à l'ordre professionnel concerné pour avoir le droit de pratiquer en ligne dans ladite province.

Voici une pratique exemplaire proposée par l'American Counselling Association :

> Les conseillères et conseillers qui ont recours au counseling à distance, à la technologie et aux médias sociaux dans le cadre de leur pratique comprennent qu'elles ou ils peuvent être assujettis aux lois et règlements en vigueur aussi bien là où exerce la praticienne ou le praticien que là où habite la cliente ou le client. Les conseillères et conseillers doivent s'assurer que leurs clients sont au courant des droits et obligations juridiques qui régissent l'exercice du counseling de part et d'autre des frontières provinciales, territoriales ou internationales.[23]

On peut réduire certains risques en demandant au client de signer un formulaire de consentement précisant que s'il devait entreprendre un recours devant les tribunaux, ce serait dans la province où se trouve la conseillère ou le conseiller.
Vous aurez donc avantage à communiquer avec l'association à laquelle vous appartenez en demandant quelle est sa position sur le sujet.

Assurance

La plupart des compagnies d'assurance couvrent ce qu'il est parfois convenu d'appeler les « services assistés par la technologie ». Dans certains cas, votre politique en vigueur couvrira ces activités, tandis que d'autres fournisseurs vous obligeront à acheter un avenant pour obtenir cette couverture.

---

[22] Document de réflexion présenté dans le site web de l'ACCP- https://www.ccpa-accp.ca/wp-content/uploads/2018/07/E-counselling.docx.pdf

[23] https://www.counseling.org/Resources/aca-code-of-ethics.pdf

Sachez que cette couverture peut s'avérer nécessaire même si vous ne pratiquez pas la psychothérapie en ligne à plein temps. Le simple fait d'avoir un site web par lequel les gens peuvent s'informer à votre sujet ou se connecter, ou d'utiliser un cellulaire pour adresser des messages texte aux clients ou le courriel pour fixer les heures de rendez-vous, voilà autant d'exemples du recours à la technologie pour améliorer les services. En fait, le téléphone n'est-il pas un appareil issu de la technologie? S'il survient un incident et que la technologie est en cause, de même que votre responsabilité, alors vous ne pouvez pas vous attendre à ce que votre fournisseur d'assurance vous couvre si vous ne lui aviez pas divulgué la nature de la technologie en cause afin d'obtenir une couverture appropriée.

Si vous avez l'intention d'offrir des services de counseling en ligne, assurez-vous que votre assurance responsabilité couvre le counseling à distance, quelle que soit la modalité de prestation que vous prévoyez utiliser. Par ailleurs, vérifiez si votre assurance vous couvre en en ce qui concerne la cybersécurité et la responsabilité en matière de protection des renseignements personnels. Dans certains cas, vous pourriez avoir avantage à vous renseigner au sujet d'une couverture qui irait au-delà de la simple responsabilité professionnelle.

Vérifiez auprès de votre assureur et informez-le des activités que vous pratiquez, des lieux depuis lesquels vous fournissez ces activités et des lieux où se trouvent vos clients au moment de la prestation de services.

La supervision clinique

Bien que les lignes directrices applicables à la supervision clinique soient semblables à celles qui régissent d'autres domaines du travail en ligne, la supervision clinique fondée sur la technologie comporte certains avantages non négligeables. L'un d'entre eux concerne un meilleur accès à de la supervision de qualité, peu importe le lieu, notamment auprès de superviseurs possédant une expertise particulière; cet accès aurait pu autrement se révéler problématique.

Évidemment, le recours à la technologie ne change en rien les lignes directrices pour une supervision éthique, mais il faut alors prendre en considération de nouveaux aspects ayant trait à la confidentialité du client, au consentement éclairé et à la relation de supervision.

Voici les principales questions qui se posent :

- La supervision de la thérapie en ligne s'effectue-t-elle aussi en ligne? Selon quelle modalité?
- La supervision du travail en personne s'effectue-t-elle en ligne? Ou vice-versa?

Vous trouverez de plus amples renseignements dans l'Annexe B – Liste de contrôle pour le recours à la technologie en supervision clinique.

Le consentement éclairé

On trouve dans le *Code de déontologie de l'ACCP* des indications claires sur ce qu'il faut inclure dans un Consentement éclairé (B4. Droits des clients et consentement éclairé / C5. Consentement éclairé)

Que devez-vous ajouter à votre formulaire de consentement éclairé à l'intention des clients lorsque vous travaillez en ligne? Il importe d'inclure ce qui suit :

- Des indications claires sur la façon dont vous travaillez en ligne;
- Des indications claires concernant votre disponibilité
- La possibilité que surviennent des problèmes techniques;
- Assurez-vous de disposer de procédures d'urgence et de sauvegarde des communications, surtout si vous prévoyez avoir recours à des modalités en temps réel;
- Tout comme pour le counseling ou la psychothérapie en personne, des problèmes de communication peuvent survenir. Expliquez aux clients comment gérer tout problème de communication ou les malentendus qu'ils pourraient éprouver;
- Assurez-vous d'expliquer clairement à quel moment vous êtes disponible et à quel moment vous ne l'êtes pas. Expliquez aux clients de quelle façon vous communiquerez entre les séances, s'il y a lieu;
- Assurez-vous que les clients comprennent bien l'importance de la confidentialité des communications entre vous (p. ex. éviter les copies conformes ou les transferts à des tiers);
- Demandez-vous s'il y a lieu de restreindre le copier-coller de votre travail (p. ex. si vous vous sentiriez à l'aise qu'un client copie-colle vos commentaires pour en faire son nouveau statut Facebook);
- Insérez une section dans laquelle les clients s'engagent à ne pas se présenter sous une fausse identité.

Les lois sur la protection des renseignements personnels interviennent également dans le consentement éclairé. Tout comme pour le counseling et la psychothérapie en personne, les clients doivent recevoir suffisamment d'information pour être en mesure de bien comprendre ce à quoi ils consentent. Ils doivent savoir :

- Quelle est l'information recueillie;
- Pourquoi l'information est recueillie;
- À quelles fins l'information sera utilisée;
- Qui aura accès à l'information;
- De quelle façon l'information sera protégée;
- Combien de temps l'information sera conservée;
- Si les personnes peuvent se retirer;

- Si l'information sera partagée avec des tiers;
  - Quels genres de tierces parties;
  - Ce que les tiers feront de l'information;
  - Si les tiers se trouvent à l'étranger et s'il est possible que d'autres lois y soient en vigueur. [24]

Les médias sociaux

Les médias sociaux comportent un certain nombre de problèmes pour les conseillers et psychothérapeutes. La protection des renseignements personnels représente un tel problème, aussi bien pour vous que pour vos clients. Le degré de dévoilement de soi, l'établissement des limites et leur maintien sont autant de considérations importantes.

Le fait de devenir « amis » ou de « suivre » les clients ou que ceux-ci deviennent vos amis ou vous suivent peut compromettre le respect des limites entre la vie personnelle et la vie professionnelle. Cela peut aussi donner lieu à un manquement à l'obligation de confidentialité à l'égard des clients. Les clients et les cliniciens peuvent s'engager dans des comportements de publication en ligne inappropriés ou dans des discussions en ligne qui peuvent avoir une incidence sur la relation thérapeutique.

En devenant un ami Facebook, le client peut aussi voir tout ce que vous affichez en ligne dans d'autres fils de discussion et sur les murs d'autres personnes. Et il peut également solliciter vos amis ou vos proches pour qu'ils deviennent ses amis. Selon les paramètres de sécurité que vous aurez établis, les clients pourraient même être en mesure de « fouiner » auprès de ces personnes.

Rappelez-vous que le contenu personnel est aussi public. Au fait, n'oubliez pas que tout ce que vous adressez aux clients, que ce soit publiquement ou en privé, peut devenir public si ces derniers le choisissent.

Les clients effectueront des recherches en ligne à votre sujet. Déterminez ce que les clients potentiels sont susceptibles de trouver à votre sujet s'ils effectuent une recherche. Réfléchissez à ce que cela pourrait avoir comme répercussions sur le counseling et la psychothérapie. Cela reflète ce que vous êtes disposé à afficher publiquement en ligne.

Compte tenu de tous ces défis, il est souhaitable d'établir une politique sur les médias sociaux qui permet à vos clients de connaître votre position sur le sujet.[25] Indiquez clairement les médias sociaux que vous utilisez, et à quelles fins pour vous-même également. De plus, il importe d'analyser les répercussions qu'ont sur notre vie

[24] https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/

[25] La Dre Keely Kolmes, qui donne des cours sur l'éthique des médias sociaux, propose dans son site web des exemples tirés de sa politique sur les médias sociaux en vigueur dans son cabinet. http://drkkolmes.com/social-media-policy/

professionnelle en ligne les types de décisions que nous prenons au sujet de notre vie privée en ligne.

Il est probable que les clients effectueront des recherches en ligne à notre sujet, mais devrions-nous en effectuer à leur sujet? L'une des façons de protéger la vie privée de nos clients consiste à nous poser les questions suivantes avant d'effectuer une recherche en ligne pour obtenir de l'information à leur sujet :

- Pourquoi est-ce que je veux mener cette recherche?
- Ma recherche pourrait-elle favoriser ou compromettre le traitement?
- Devrais-je obtenir le consentement éclairé du client avant de procéder à une recherche?
- Devrais-je partager les résultats de la recherche avec le client?
- Devrais-je consigner les résultats de ma recherche dans le dossier du client?
- Comment puis-je assurer le suivi de mes motivations et de l'évolution constante des risques et avantages associés à la recherche? [26]

Les conseils de la Dre Keely Kolmes[27] et autres au sujet des médias

- Utilisez un nom et une page distincts pour les usages personnels et professionnels, tout en étant conscient que cela n'empêche pas nécessairement votre moi personnel d'être découvert;
- Pour vos échanges sur les médias sociaux, utilisez une adresse courriel différente de l'adresse cryptée servant à communiquer avec vos clients;
- Voici quelques questions que vous devez vous poser avant de publier en ligne (blogues/commentaires/wikis/tweets, etc.) :
    - Quels sont les avantages/inconvénients associés à la publication de cette information en ligne?
    - Est-il possible que des clients passés, actuels ou à venir puissent être touchés de façon significative et négative?
    - En quoi ce dévoilement influence-t-il ma relation avec les clients?
    - Le dévoilement compromet-il ma crédibilité ou la confiance du public à l'égard du counseling? [28]
- Restreignez vos tweets/publications en ligne/etc. aux sujets suivants : psychopédagogie, nouvelles dans le domaine de la santé ou travaux de vos collègues;

---

[26] Clinton et. coll. (2010) *Patient-targeted googling: the ethics of searching online for patient information.* Harvard Rev. Psychiatry (mars-avril) : 18(2): 103-12 doi:10.3109/10673221003683861.

[27] http://drkkolmes.com/clinician-articles/

[28] Gabbard et coll. (2011). Professional Boundaries in the Era of the Internet. *Academic Psychiatry 35* (3) :168-74.

- Évitez les rôles multiples; le fait de ne pas vous connecter aux médias sociaux de vos clients constitue un moyen facile et rapide de ne pas vous empêtrer dans des situations à rôles multiples;
- Ne demandez pas aux clients de vous fournir des témoignages ou une évaluation;
- Obtenez un consentement éclairé avant d'effectuer une recherche Google sur vos clients.

Formation sur le recours aux technologies en counseling et psychothérapie

Il existe de nombreux programmes reconnus au Canada, aux É.-U. et au R.-U. qui offrent de la formation sur le recours à la technologie en counseling et psychothérapie. Si vous songez à suivre une formation complémentaire dans ce domaine, voici quelques éléments à considérer lors de votre choix de cours.

Qui donne le cours et quelle est son expérience dans le domaine? L'enseignant est-il également actif dans la recherche?

Le cours aborde-t-il : les aspects éthiques, techniques et pratiques comme le degré de compatibilité pour le client et pour la modalité, la sauvegarde des communications et la planification en situation de crise?

Le cours aborde-t-il les différences entre les relations thérapeutiques en personne et en ligne?

Lexique

Application de suppression de données
Application qui vous permet de supprimer en toute sécurité les données et les documents stockés sur n'importe quel de vos appareils. La suppression peut s'effectuer sur place ou à distance, dans le cas d'un appareil perdu ou volé.

Applications
(Parfois abrégé sous le terme « appli » en français.) Désigne un logiciel capable de tourner sous un navigateur web ou même de façon autonome sur votre ordinateur, téléphone, tablette ou autre dispositif électronique. Les applications peuvent ou non être connectées à Internet.

Authentification à deux facteurs
L'authentification à deux facteurs (A2F), souvent appelée vérification en deux étapes, est un procédé de sécurité par lequel l'utilisateur fournit deux facteurs d'authentification aux fins de vérification de son identité. Ce procédé se distingue de l'authentification à un seul facteur, qui consiste pour l'utilisateur à ne fournir qu'un seul élément de vérification d'identité, habituellement un mot de passe.

Avatar
Image électronique représentant un utilisateur d'ordinateur et manipulée par celui-ci dans un espace virtuel (comme dans un jeu d'ordinateur ou un site de magasinage en ligne) et qui interagit avec d'autres objets dans l'espace.

Bitcoin
Type de monnaie électronique pour laquelle on utilise des techniques de cryptage afin de régir la production d'unités de monnaie et pour vérifier le transfert de fonds, le tout fonctionnant indépendamment d'une banque centrale.

Communications synchrones
Interactions entre le client et le conseiller ou psychothérapeute qui se déroulent au même moment dans le temps.

Counseling par échanges textuels
Le recours à une modalité de prestation du counseling s'effectuant exclusivement par texte.

Counseling par échanges textuels asynchrones
Cette modalité de prestation du counseling désigne un mode de communication par texte; le client et le conseiller/psychothérapeute n'ont pas besoin d'être à l'ordinateur en même temps, ce qui suppose un délai dans le déroulement des interactions.

Counseling par vidéo
Service de counseling synchrone dans lequel le client et le conseiller ou psychothérapeute communiquent au moyen d'une webcaméra, d'une ligne fixe et d'un logiciel Internet crypté,

ce dispositif permettant aux deux parties de pouvoir se voir et s'entendre, de partager et de créer des documents en temps réel.

Coupe-feu

Système de sécurité d'un réseau qui permet de surveiller et de contrôler le trafic entrant et sortant du réseau en fonction de règles de sécurité préétablies. Un **coupe-feu** sert généralement à ériger une barrière entre un réseau interne fiable et un réseau externe non fiable, comme le réseau Internet.

Cryptage

Le cryptage des données permet de traduire celles-ci sous une autre forme ou dans un autre code, afin que seules les personnes ayant accès à une clé secrète (autrefois appelée la clé de déchiffrement) ou à un mot de passe puissent les lire.

Cryptomonnaie

La cryptomonnaie est un type de monnaie numérique qui utilise le cryptage pour garantir la sécurité et pour empêcher la contrefaçon. On utilise souvent des clés publiques et privées pour transférer la cryptomonnaie entre les personnes.

Désinhibition

Lorsqu'elles interviennent en ligne ou qu'elles utilisent d'autres médias, les personnes peuvent adopter un comportement différent de celui qui guide leurs interactions dans des situations qui se déroulent en personne. Elles peuvent alors dévoiler de l'information plus rapidement que lorsqu'elles se trouvent dans des situations en personne. Elles peuvent aussi perdre leurs inhibitions dans leur façon d'exprimer leurs émotions (p. ex. se montrer plus insensibles ou plus en colère). Ces différences de comportement peuvent être influencées par les caractéristiques suivantes de l'environnement en ligne :

- Le sentiment d'anonymat et d'invisibilité
- Le fait de ne pas voir (donc de ne pas éprouver) les réactions d'autrui aux propos tenus, d'éprouver l'absence d'autorité externe dans le contexte des échanges en ligne ou dans d'autres médias
- Ne pas percevoir autrui comme étant « réel »

Dialogue en ligne ou clavardage (temps réel)

Il s'agit de la transmission en temps réel de messages texte de l'expéditeur au destinataire. Les messages de dialogue en ligne (ou de clavardage) sont habituellement assez courts afin que les autres participants puissent y répondre rapidement.

Étude d'impact sur la vie privée (ÉIVP)
Analyse du mode de collecte, d'utilisation, de partage et de maintenance des renseignements personnels identifiables d'une personne ou d'un groupe de personnes. Procédé servant à évaluer et à gérer les impacts sur la vie privée et à garantir la conformité aux règles et responsabilités en matière de protection des renseignements personnels. Vous trouverez des modèles d'ÉIVP dans les sites web provinciaux et du fédéral.

Fossé numérique
Désigne l'écart observable entre les populations et les régions qui ont accès à la technologie moderne d'information et de communication comparativement à celles qui n'y ont qu'un accès restreint. Cela concerne notamment le téléphone, la télévision, les ordinateurs et Internet.

Hameçonnage
Pratique frauduleuse par laquelle on dérobe des données privées sur des sites web ou par courriel; le tout est conçu pour ressembler à la démarche d'une tierce partie fiable. En règle générale, les escroqueries par hameçonnage se caractérisent par l'envoi d'un courriel informant l'utilisateur d'un problème survenu à sa banque ou dans un autre type de compte.

Hameçonnage ciblé
Un courriel d'hameçonnage ciblé (certains parlent de harponnage) est similaire à un courriel d'hameçonnage, sauf qu'il est ciblé sur une personne ou une organisation en particulier. Par exemple, cela peut consister en un courriel adressé à toutes les personnes d'une université en leur demandant de cliquer sur un lien dans lequel il leur sera demandé de fournir leurs informations de connexion.

Infonuagique
L'infonuagique est un terme qui désigne l'espace en ligne que vous pouvez utiliser pour entreposer vos données. L'illustration la plus simple de l'entreposage dans le nuage est le fait que des utilisateurs puissent télécharger des fichiers et des dossiers de leurs ordinateurs ou appareils mobiles vers un serveur Internet. Les fichiers ainsi téléchargés servent de copie de sauvegarde au cas où les fichiers d'origine devaient être endommagés ou perdus. Le recours à un serveur infonuagique permet à l'utilisateur de télécharger des fichiers vers d'autres appareils s'il y a lieu. Les fichiers sont alors protégés par cryptage et leur utilisateur y accède au moyen d'un identifiant de connexion et d'un mot de passe. Les fichiers sont accessibles à l'utilisateur en tout temps, pourvu que ce dernier ait une connexion Internet pour les visualiser et les récupérer.

Logiciel
L'élément du système informatique qui se compose de données ou d'instructions à l'ordinateur.

Logiciel malveillant

Logiciel malveillant est un terme générique qui désigne toute forme de logiciel conçu avec une intention malveillante. Cette *intention malveillante* vise souvent à dérober vos renseignements personnels ou à créer une porte dissimulée vers votre ordinateur afin que quelqu'un puisse y avoir accès sans votre autorisation. Cependant, on peut considérer comme étant malveillant tout logiciel qui accomplit *quelque chose* dont il ne vous avait pas prévenu.

Logiciel rançonneur

Le logiciel rançonneur est un type de logiciel malveillant qui consiste à crypter les fichiers sur un dispositif altéré et à les garder en otages jusqu'à ce que l'utilisateur verse une rançon à la personne qui exploite le logiciel malveillant.

Matériel

Il s'agit des éléments physiques ou composants d'un ordinateur, comme l'écran, le clavier, le dispositif de stockage des données, la carte graphique, la carte audio et la carte mère. Le matériel reçoit les directives du logiciel pour exécuter des commandes et des instructions.

Mégadonnées

« Les mégadonnées désignent la nouvelle science qui vise à comprendre et à prédire le comportement humain à partir de l'étude de grands volumes de données non structurées. On utilise aussi l'expression « analyse prédictive » pour désigner les mégadonnées. Par exemple, procéder à l'analyse de messages Twitter, de fils de nouvelles Facebook, de recherches sur eBay, de télépointeurs GPS et de machines ATM.

Messagerie texte

L'action qui consiste à rédiger et à envoyer des messages électroniques, généralement composés de caractères alphanumériques, et qui sont échangés entre deux ou plusieurs utilisateurs de téléphones mobiles, de tablettes, d'ordinateurs de table ou portables ou autres appareils. Les messages texte peuvent être envoyés par réseau cellulaire ou par connexion Internet.

Mystification

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.

Politique de sauvegarde

Échéancier fixe et pré**défini** en vertu duquel l'information des applications commerciales, comme Oracle, Microsoft SQL, les bases de données des serveurs de courriel et des fichiers d'utilisateurs sont copiés vers un disque et/ou une bande magnétique afin de s'assurer que les données seront récupérables s'il survenait une suppression accidentelle, une altération des données ou une forme de panne du système. Mais ce terme peut aussi désigner les procédures et les règles qu'emploie une organisation pour garantir que les sauvegardes s'effectuent en quantités et en types appropriés, notamment que l'on teste à une fréquence

adéquate le processus de restauration du système de production d'origine à partir des copies sauvegardées.

Programmes de traitement de santé mentale en ligne assistés par un thérapeute

Modèle de prestation de services de santé mentale qui conjugue le recours à des ressources interactives fondées sur le web et de brèves séances hebdomadaires en ligne avec une conseillère ou un conseiller.

Protection par mot de passe

Procédé de sécurité qui sert à préserver l'information accessible par ordinateur que l'on doit protéger contre certains utilisateurs. La protection par mot de passe permet de ne donner accès à certaines données qu'aux personnes détentrices d'un mot de passe autorisé.

Réalité augmentée

Vue directe ou indirecte en temps réel d'un environnement physique en contexte réel dont les éléments sont « augmentés » par des données sensorielles du monde réel ou générées par ordinateur. La réalité augmentée améliore la perception que l'on a de la réalité.

Réalité virtuelle

Simulation informatisée d'une image ou d'un environnement en trois dimensions avec lequel il est possible d'interagir de manière apparemment réelle ou physique pour une personne dotée d'un équipement électronique spécial, comme un casque muni d'un écran ou des gants munis de capteurs.

Renseignements personnels

Toute information au sujet d'une personne identifiable, à l'exception des coordonnées professionnelles (p. ex. le titre d'une personne, le numéro de téléphone d'affaires, l'adresse d'affaires, le courriel ou le numéro de télécopieur d'entreprise).

Renseignements personnels sur la santé

L'information consignée au sujet d'une personne identifiable et qui porte sur la santé de cette personne ou sur la prestation des services de santé qu'elle reçoit.

Réseau privé virtuel

Le terme réseau privé virtuel (RPV) désigne une technologie qui crée une connexion sécurisée et cryptée à même un autre réseau moins sécurisé, comme Internet. La technologie de RPV fut mise au point pour permettre aux utilisateurs à distance et aux succursales d'entreprise d'avoir accès en toute sécurité aux applications et autres ressources de l'entreprise. Pour garantir la sécurité des données, on les fait transiter par des tunnels sécurisés, et les utilisateurs du RPV doivent recourir à des méthodes d'authentification (notamment des mots de passe, l'accès à l'anneau à jeton et autres méthodes d'identification) qui déterminent l'accès au RPV.

Services de tierce partie
Une tierce partie (ou un tiers) est une entité qui intervient d'une manière quelconque dans une interaction se déroulant principalement entre deux autres entités. Le tiers peut ou non faire officiellement partie de l'échange entre les deux entités principales; il peut ou non intervenir de façon transparente et/ou légale.

Systèmes de sauvegarde
Processus par lequel l'état, les fichiers et les données d'un **système** informatique sont dupliqués en vue de servir comme **copie de sauvegarde** ou données substitutives au cas où les données du **système** d'origine deviendraient corrompues, supprimées ou perdues.

Techniques de présence
Techniques thérapeutiques fondées sur le texte qui permettent aux psychothérapeutes et aux conseillers de compenser l'absence du ton de la voix ou des éléments non verbaux dans le cadre d'un counseling par échanges textuels asynchrones.

Technologies portables
Catégorie de dispositifs technologiques que le consommateur peut enfiler comme un vêtement et qui comporte souvent le repérage d'information relative à la santé et à la condition physique.

ANNEXE A – Mesures détaillées de protection des données

Conseils au sujet de l'hameçonnage et de l'hameçonnage ciblé

Les conseils suivants vous permettront de réduire la menace :

- Si vous recevez un courriel comportant une pièce jointe et que l'on vous demande d'ouvrir celle-ci, assurez-vous que l'adresse du courriel est bien celle de la personne qui prétend être l'expéditeur. Cliquez sur le nom de l'expéditeur et examinez l'adresse courriel;
- Si vous avez le moindre doute, évitez d'ouvrir ou de télécharger le fichier. Communiquez avec la personne présentée comme étant l'expéditeur et demandez-lui si elle vous a adressé ce courriel;
- Les institutions bancaires ne font pas d'envois comportant des pièces jointes. Les entreprises n'envoient pas des factures tombées du ciel. Prenez toujours le temps de réfléchir à ce qui se présente à vous. Avez-vous commandé quelque chose auprès de cette entreprise dernièrement?
- Souvent, dans les courriels d'hameçonnage, les liens auront une apparence officielle du genre votrebanque.com/connexion. Mais ce lien vous mène vers un autre site web. Vérifiez toujours l'URL du site dans lequel vous vous retrouvez après avoir cliqué sur le lien. Par exemple, s'il se lit comme suit : http://www.voleurs.com/rbc/login, ce n'est pas le site de la Banque royale du Canada;
- Si vous n'êtes pas certain de la fiabilité d'un courriel, faites comme s'il n'était pas fiable. Évitez de cliquer sur le lien. Communiquez avec les responsables de l'institution et demandez-leur s'ils vous ont adressé des courriels;
- Les entreprises canadiennes et de partout dans le monde sont au courant des cas d'hameçonnage. Elles s'abstiennent donc d'adresser des courriels vous demandant de fournir vos informations de connexion. L'entreprise, l'agence ou l'institution avec laquelle vous faites affaire ne vous adressera pas de courriel vous demandant de lui fournir vos codes d'accès ni vos informations de connexion. Si vous recevez un courriel de ce genre, méfiez-vous.

Dispositifs de surveillance Stingray et intercepteurs IMSI[29]

Les progrès technologiques sont un peu comme une course aux armements. Les méchants développent de nouveaux virus, tandis que les bons développent de nouvelles façons d'intercepter et de neutraliser ces virus. On découvre une nouvelle faille par laquelle les malveillants peuvent s'infiltrer pour dérober vos renseignements personnels. Les bons finissent par boucher cette faille.

Parmi les récentes avancées en matière de vol de renseignements, citons le dispositif appelé Stingray. Tous les cellulaires sont dotés d'un numéro d'identité (l'IMSI) qu'ils envoient vers la tour de téléphonie cellulaire afin de pouvoir communiquer par son intermédiaire. Les dispositifs Stingray peuvent mimer le comportement d'une tour et

[29] Pour des exemples, voir, https://privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions

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