ORDRE DES PSYCHOÉDUCATEURS ET PSYCHOÉDUCATRICES DU QUÉBEC

Une présence qui fait la différence

FEUILLET

26 MARS 2020

Tenue et gestion de dossiers numériques:
Les essentiels en situation d'urgence sanitaire et sociale

L'Ordre des psychoéducateurs et psychoéducatrices du Québec produit ce feuillet dans le contexte de la pandémie de la COVID-19 afin d'outiller ses membres dans la mise en place de mesures de facilitant la tenue et la gestion de dossiers numériques.

Principes généraux

Les circonstances vous amènent à effectuer votre tenue de dossier en version numérique?

Voici quelques règles à ne pas oublier afin que votre pratique demeure conforme à votre déontologie professionnelle.

La norme en tenue de dossiers des psychoéducateurs précise que le dossier est un fichier où sont consignées les données recueillies dans le cadre d'une intervention avec un client et que celui-ci peut être sur un support papier ou sur un support numérique.

Il est important de s'assurer de respecter la norme de même que toutes vos obligations sur le plan de 1) la confidentialité et l'intégrité des renseignements versés au dossier, 2) l'accès à l'information aux personnes autorisées uniquement, et 3) l'apposition de votre signature.

1. Confidentialité et intégrité des renseignements

En tout temps, la confidentialité des renseignements contenus au dossier numérique doit être assurée, de même que leur intégrité, c'est-à-dire qu'ils ne pourront être altérés.

L'accès au dossier sur support numérique est de deux ordres : l'accès physique à l'outil technologique où est conservé le dossier (ex. : ordinateur portable, serveur) et l'accès virtuel à ce dossier par une source externe

Dans tous les cas, des règles de base s'appliquent :

- Prévoir un mécanisme d'accès à ses dossiers, approprié à sa situation :
  - profil d'accès (code d'utilisateur et mot de passe efficace) à l'outil technologique, qu'il s'agisse d'un ordinateur fixe ou mobile (portable, tablette, téléphone intelligent, etc.), ainsi que pour accéder à une application mobile ou un logiciel;
  - utilisation d'un mot de passe pour accéder au dossier.
- Adopter des comportements préventifs :
  - s'assurer que les informations qui s'affichent à l'écran ne peuvent être vues par toute autre personne pouvant se trouver à l'intérieur de la pièce où l'outil technologique se trouve, ni même de l'extérieur de celle-ci (par exemple, par la fenêtre);
  - prévoir un mécanisme de mise en veille dont le réaffichage nécessite l'entrée d'un mot de passe sécuritaire;
  - s'assurer que le pare-feu et le système antivirus de l'outil technologique soient adéquats et mis à jour régulièrement;
  - s'assurer de la mise à jour des logiciels et des systèmes d'exploitation;
  - effectuer une copie de sauvegarde régulière sur un disque externe, une clé USB, etc. Ces copies seront évidemment protégées par mot de passe ou bien elles seront chiffrées (encryptées), ou gardées sous clé dans un endroit distinct de l'équipement informatique d'où elles proviennent.

Dans ce feuillet

2) Accès à l'information aux personnes autorisées uniquement

- Mettre en place une méthode de repérage efficace des renseignements afin de répondre de manière diligente à une demande d'accès par la personne, en conformité avec le code de déontologie des psychoéducateurs et psychoéducatrices (art. 28)
- Rendre ces renseignements disponibles aux personnes autorisées uniquement, en conformité avec le code de déontologie (art. 28)

3) Apposition de votre signature

- automatique par l'application utilisée (certaines applications le permettent);
- inscrite de manière numérique à la suite de la note au dossier (les initiales peuvent suffire).

Partage d'équipement informatique avec d'autres personnes

Afin que ce partage ne compromette pas la protection des renseignements de nature confidentielle, il est nécessaire :

- d'avoir son propre profil sécurisé par mot de passe efficace;
- de prévoir un mécanisme de mise en veille rapide avec mot de passe pour réactiver;
- de fermer sa session de travail lorsque la tâche est terminée.

Le partage d'équipement informatique dans le cadre de travail d'équipes cliniques (clinique privée, organisme communautaire, services multidisciplinaires dans les réseaux scolaire et de la santé et des services sociaux)

- s'assurer que le dossier du psychoéducateur, ou la section du dossier qui lui est réservée n'est accessible que par lui (profil d'accès avec nom d'utilisateur et mot de passe), par les personnes autorisées par la loi ou par le client lors du consentement;
- dans le cas d'accès à distance :
    - s'assurer d'utiliser une connexion RPV sécurisée (réseau privé virtuel; plus souvent appelé VPN ou Virtual Private Network);
    - s'il est utilisé, sécuriser le réseau sans fil (wifi) en s'assurant, par exemple, d'avoir modifié le code administrateur et le mot de passe d'origine.

Utilisation d'applications mobiles et de supports amovibles

L'utilisation des applications mobiles et des supports mobiles (portable, tablette, téléphone intelligent, etc.) nécessite d'agir avec la même rigueur afin de prévenir la divulgation d'information confidentielle à une personne non-autorisée, soit en s'assurant que l'accès à ces supports et applications mobiles soit limité par un mot de passe efficace.

Utilisation de l'infonuagique

L'utilisation de l'infonuagique comporte des risques et implique de prendre des mesures de sécurité semblables à celles requises pour la transmission d'information ou encore l'intervention à distance.

Plus particulièrement, il est nécessaire de :

- s'assurer de connaitre le modèle d'infonuagique[1] dans lequel on effectue sa tenue de dossiers;
- vérifier les termes du contrat d'hébergement des données de la plateforme ou de l'application utilisées;
- choisir un hébergement au Canada sous contrôle canadien;
- utiliser un mot de passe efficace;
- s'assurer du chiffrement des données «de bout en bout» (les données sont encryptée au départ, à l'arrivée, et leur transmission l'est également);
- conserver une copie de sauvegarde des données;
- informer le client de cette utilisation de l'infonuagique, des risques associés, et obtenir son accord.

Transmission d'information

Pour l'utilisation des courriels :

- obtenir l'autorisation pour cette utilisation auprès de la personne à laquelle on donne des services;
- informer cette personne des avantages et des risques liés à cette utilisation (mauvais destinataire, interception par un tiers non désirée);
- prendre des actions préventives afin de s'assurer que l'envoi s'effectue de manière sécuritaire :
  - les informations confidentielles et les renseignements personnels sont contenus dans un document sécurisé par un de ces moyens:
    - par mot de passe
    - par chiffrement
  - le mot de passe ou la clé de chiffrement sont fournis au destinataire par un autre moyen de communication;
  - le document est préférablement en format PDF non-modifiable;
  - dans le cas d'un envoi en réponse à un courriel reçu, le psychoéducateur s'assure de bien choisir la fonction «répondre» plutôt que celle de «répondre à tous»;
- déposer les courriels au dossier;
- documenter au dossier les actions préventives effectuées (identifiées plus haut), relatives à la transmission d'information par courriel;
- déposer au dossier les informations liées à la transmission par courriel:
  - mode de transmission convenu;
  - moyens pris pour assurer la confidentialité.

Nous contacter

N'hésitez pas à communiquer avec nous par courriel pour obtenir des informations supplémentaires

Ordre des psychoéducateurs et psychoéducatrices du Québec

info@ordrepsed.qc.ca

Visitez notre site web : www.ordrepsed.qc.ca

[1]La connexion à distance à une structure informatique permet, en plus du stockage, l'échange d'information à distance. Ces structures peuvent être diverses : l'infonuagique peut se déployer en un réseau interne à une organisation (infonuagique privé interne), un réseau externe à une organisation réservé à cette dernière (infonuagique externe privé), un réseau d'une organisation ouvert au public (infonuagique public), un réseau partagé à l'intérieur d'un regroupement d'organismes (infonuagique communautaire), et des réseaux combinant un ou plusieurs modèles d'organisation de réseau (infonuagique hybride).