Organisation du Monde du Travail
Thérapie Complémentaire

Questions et réponses fréquentes pour les thérapeutes sur le DROIT RÉVISÉ DE LA PROTECTION DES DONNÉES

1. Registre des activités de traitement

Tous les Thérapeutes Complémentaires doivent-ils tenir un registre des activités de traitement?

Les données de santé étant considérées comme particulièrement sensibles, il est vivement recommandé aux thérapeutes de tenir un tel registre.

Que doit contenir ce registre?

Pour un cabinet courant, il suffit de dresser une liste des données collectées par telle ou telle personne et dans quel but, et de préciser si ces données sont transmises à d'autres personnes. Normalement, il devrait s'agir du dossier du patient, de l'agenda (surtout s'il est en ligne) et de la facturation (voir à ce sujet le modèle sur le site web de l'OrTra TC). Pour toutes les données qui ne sont pas enregistrées par écrit ou sur son propre disque dur, mais dans le cloud d'un fournisseur (tarif 590, etc.), le/la thérapeute doit s'assurer que les directives de la LPD sont respectées.

2. Personne responsable en matière de la protection des données

Doit-il y avoir obligatoirement une personne responsable en matière de la protection des données?

Il est toujours question dans la loi de la «personne responsable des données». Une telle personne donc exister pour tous les fichiers, qui en assume la (co)responsabilité et sert d'interlocutrice (le cas échéant, également pour les autorités et les tribunaux). En tant que thérapeute exerçant dans un cabinet individuel, vous êtes vous-même le/la responsable de la protection des données.

Que signifie «connaissances professionnelles nécessaires»?

Il n'existe aucune exigence légale en la matière. Il ressort des circonstances que la personne est informée du droit révisé de la protection des données ainsi que des mesures nécessaires, et qu'elle s'est penchée sur la question.

3. Mesures techniques et organisationnelles pour la sécurité des données

Que faut-il modifier sur son propre site web?

Une déclaration de protection des données devrait être mise en ligne sur le site web du cabinet et être facile à trouver. On trouve sur le site de l'OrTra TC un modèle simple de déclaration pour les thérapeutes, tandis que de nombreuses variantes plus détaillées, souvent mises à disposition gratuitement, sont disponibles sur Internet. Chaque thérapeute est lui/elle-même responsable de la formulation d'une déclaration de protection des données adaptée aux conditions qui sont les siennes.

Dans notre cabinet de groupe, nous avons accès aux données de tous les clients des thérapeutes et des spécialistes qui travaillent chez nous, faut-il procéder à des adaptations spécifiques?

Dans un cabinet de groupe également, les droits d'accès doivent être limités aux données des clients pris en charge par le cabinet.

A quoi faut-il faire attention pour les données stockées électroniquement?

La sécurité des données doit être garantie, par exemple, par des pare-feu et des restrictions d'accès (protection par mot de passe pour le PC/ordinateur portable). Des alternatives pour le transfert de données dans des pays tiers non sûrs doivent être examinées: par exemple choisir si possible d'autres fournisseurs pour les logiciels ou les applications, changer de site pour le serveur/cloud (déposer les données à l'étranger en changeant de fournisseur de stockage en Suisse).

Puis-je envoyer des données personnelles par e-mail?

Si les données personnelles sont envoyées par e-mail, il faut utiliser un système qui procède au cryptage (p. ex. HIN) ou obtenir l'accord de la personne concernée pour que la transmission puisse se faire sans cryptage.

Les dossiers médicaux peuvent-ils continuer à être tenus sur papier?

Si les dossiers médicaux sont classés physiquement, ils doivent être stockés dans un endroit sûr qui les protège contre les accès non autorisés, le vol ou les dommages physiques (p. ex. dans une armoire fermée à clé, un coffre-fort ou un local fermant à clé). Si plusieurs personnes travaillent dans le cabinet, il faut limiter l'accès aux dossiers médicaux en ne donnant la clé du lieu de conservation qu'à certaines d'entre elles.

Comment informer mes collaborateurs?

Pour les employés, des formations, notamment continues, doivent être organisées afin de les sensibiliser à la protection des données. Mais il est également possible d'introduire des directives/règlements sur la protection des données, le cas échéant en faisant appel à des prestataires externes (p. ex. hébergeur, webmaster, etc.). Pour l'engagement de collaborateurs et de collaboratrices, on fera référence à une déclaration de protection des données dans le contrat de travail ou le règlement du personnel.

4. Droit d'accès/devoir d'information

Comment les thérapeutes doivent-ils informer leurs clients?

La nLPD ne précise pas comment les personnes concernées doivent être informées. Dans la pratique, une déclaration de protection des données est chose courante, mais une information dans les conditions générales, un formulaire de consentement ou une information orale (p. ex. annonce sur bande magnétique) suffisent également. La simple indication d'une personne de contact pour d'autres questions est en revanche insuffisante.
Le fait que les personnes concernées consultent effectivement la déclaration de protection des données ne joue aucun rôle.
Celui qui n'a pas de site web doit remettre la déclaration de protection des données (par exemple avec l'information destinée aux patients) ou l'afficher ou la mettre à disposition dans un endroit bien visible du cabinet.

Les clients* de la Thérapie Complémentaire doivent-ils remplir et signer une déclaration de consentement?

Dans la mesure où les principes du traitement des données sont respectés (art. 6 LPD) et qu'il n'y a pas de déclaration expresse de volonté contre un traitement de données, les données personnelles peuvent être traitées. Par conséquent, aucune déclaration de consentement n'est nécessaire.

Quand la transmission à des tiers est-elle autorisée?

Une telle transmission est autorisée pour autant que le traitement des données soit légal, qu'il respecte les principes de la protection des données et que les personnes concernées soient informées de la transmission en question (voir la déclaration de protection des données).

Les factures, rapports, etc. peuvent-ils être envoyés par e-mail aux clients/assureurs maladie?

On prendre dans ce cas des mesures techniques afin d'éviter que des tiers non autorisés puissent consulter les données. Cela peut se faire par exemple par un cryptage (par ex. avec HIN-Mail). Pour les données personnelles sensibles, on demandera toujours l'accord explicite de la personne concernée ou, mieux encore, cette dernière se chargera elle-même du transfert.

Quand faut-il annoncer au PFPDT les violations de la sécurité des données?

Il y a violation lorsque la confidentialité, l'intégrité ou la disponibilité de données personnelles est compromise, c'est-à-dire lorsque des données personnelles sont effacées, perdues, modifiées ou divulguées ou rendues accessibles à des personnes non autorisées. Toutefois, seules les violations qui présentent un risque élevé de conséquences négatives pour les personnes concernées doivent être notifiées. C'est le cas, par exemple, lorsque des dossiers de patients sont enregistrés sur une clé USB non cryptée et que cette clé est perdue.

Que dois-je faire si j'envoie un mail au mauvais destinataire ou si je perds une clé contenant des données?

On évaluera au cas par cas s'il faut communiquer la chose au PFPDT. Si, par exemple, un courriel contenant des données personnelles est envoyé par erreur à une personne digne de confiance et connue de l'expéditeur, le risque n'est pas élevé. En revanche, si une clé contenant des données de collaborateurs et leurs données salariales est perdue, une notification est nécessaire.

5. Portabilité des données

Le dossier de mes clients est tenu sur papier, comment puis-je satisfaire à l'exigence d'une restitution au format électronique?

Si les documents ne sont pas classés sous forme électronique et ne sont disponibles que sous forme physique, ils doivent être scannés et restitués au format PDF. Il est donc important de rassembler et d'organiser tous les documents concernant un client.

6. Effacement des données

Combien de temps les données des clients peuvent-elles être conservées?

Conformément aux délais de prescription du Code des obligations et aux dispositions de certains cantons, on peut en général partir d'un délai de conservation de 20 ans.

Seules les données électroniques doivent être effacées?

Non, cela vaut également pour les données des patients, telles que les dossiers médicaux, qui sont conservées sur papier.

La présente fiche d'information et ses annexes ont été rédigées de manière aussi précise et complète que possible, en fonction de l'état actuel des connaissances. Néanmoins, aucune garantie juridique ne peut être donnée à ce sujet.

Soleure, le 14.02.2024