Fiche d'information

Protection des données en psychothérapie

Entrée en vigueur en Suisse depuis le 1er septembre 2023, la nouvelle loi sur la protection des données (LPD) vise à renforcer la protection des personnes dans leurs droits fondamentaux quant au traitement de leurs données. À cette fin, des directives spécifiques ont également été mises en place pour protéger les patients contre les abus dans le domaine de la santé. L'un des principaux objectifs de la LPD est de renforcer l'autodétermination des patients sur l'utilisation de leurs données. Les psychothérapeutes doivent désormais faire preuve de plus de transparence envers leurs patients et clients.

Les cabinets de psychothérapie devront désormais tenir compte des modifications suivantes:

1. Déclaration de protection des données

Les patients et clients doivent être informés de manière transparente sur la manière dont leurs données personnelles sont traitées. Cela s'applique non seulement au traitement des données au sein du cabinet de psychothérapie, mais également à la transmission à des tiers.
À cet effet, vous pouvez équiper votre site web d'une bannière de cookies, permettant aux visiteurs d'accepter ou de refuser la collecte de leurs données. Veillez à créer une déclaration de protection des données ou à mettre à jour celle qui existe déjà.
Déclaration de protection des données

2. Responsable de la protection des données

Le cabinet est pleinement responsable de la protection des données, et il incombe donc au psychothérapeute de mettre en œuvre les mesures nécessaires pour la garantir. Si vous externalisez certains traitements de données (comme la gestion des données ou la comptabilité), vous demeurez entièrement responsable du respect des réglementations en matière de protection des données. Vous devez vous assurer que le sous-traitant respecte les instructions et directives que vous lui avez données. Il est impératif de formaliser le traitement des données par contrat, lequel doit inclure les clauses relatives à la protection des données, conformément à l'article 9 de la nLPD.
Externalisation (sous-traitance)

3. Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles (MTO) sont des actions de sécurité à mettre en place pour garantir la protection des données personnelles, comme le prévoit le règlement général sur la protection des données. Leur mise en œuvre incombe au responsable du traitement des données.

•Les mesures techniques concernent les aspects techniques du système d'information, tels que l'anonymisation, le cryptage et l'authentification.

• Les mesures organisationnelles impliquent des aspects plus globaux et se rapportent plutôt à l'environnement du système, aux personnes qui l'utilisent et au type d'utilisation (tels que la gestion des accès, les autorisations, la tenue d'un registre des activités de traitement, etc.).

L'efficacité de la protection des données repose sur l'association de ces deux types de mesures, qui seules permettent de prévenir non seulement la destruction ou la perte de données, mais aussi les erreurs, les falsifications, les accès non autorisés, etc. Elles doivent être appliquées tout au long du cycle de vie des données et à chaque niveau du système d'information.[1]

[1] https://www.edoeb.admin.ch/fr/securite-de-linformation

4. Formulaire patientèle / déclaration de consentement

Lors du premier rendez-vous avec le patient, faites-lui confirmer, par la signature d'une déclaration de consentement (formulaire patientèle), qu'il accepte l'accès à ses données et leur traitement ainsi que leur transmission à des tiers conformément aux informations destinées à la patientèle figurant à la page suivante de la déclaration de consentement (formulaire patientèle).

Formulaire patientèle/déclaration de consentement

5. Convention de confidentialité

Les psychothérapeutes et leurs auxiliaires sont soumis au secret professionnel conformément à l'article 321 du Code pénal. Par auxiliaires, on entend toutes les personnes qui assistent directement ou indirectement les professionnels. Si des tiers sont chargés du traitement des données sous quelque forme que ce soit, un accord de confidentialité doit être conclu avec eux.

Convention de confidentialité

6. Demandes de renseignements et de remises de données

Conformément à la LPD et aux lois cantonales sur la santé, tout patient capable de discernement a le droit de demander une copie de son dossier médical. Est considéré comme capable de discernement toute personne en mesure d'agir de manière raisonnable. Les informations concernant des tiers présentes dans le dossier médical, qui pourraient porter atteinte à leurs intérêts, doivent être caviardées de façon irréversible dans la copie.

Le psychothérapeute peut communiquer des informations à des tiers si le patient a donné son consentement, si une loi le prévoit ou si une autorité cantonale a autorisé la levée du secret.

Dans tous les cas, il faut garantir le maintien de la confidentialité des données.

Les personnes concernées ont le droit (art. 28 nLPD) de recevoir leurs données personnelles dans un format électronique courant, si le cabinet travaille de manière automatisée, ou de faire transmettre les données à des tiers. La remise ou la transmission doit être gratuite. (Le Conseil fédéral peut prévoir des exceptions, notamment lorsque les coûts sont disproportionnés).

Demandes de renseignements

7. Registre des activités de traitement

Si des psychothérapeutes traitent des "données personnelles sensibles à grande échelle", ils sont tenus de tenir un registre des activités de traitement.

Registre des activités de traitement

8. Conservation et archivage

La conservation des données personnelles des psychothérapeutes est fixée à 10 ans au niveau fédéral. Les données professionnelles doivent être conservées aussi longtemps que les délais de conservation légaux le prévoient. Il convient toutefois de vérifier si d'autres dispositions légales cantonales doivent être prises en compte.

La protection et la sécurité des données doivent être garanties pendant la durée de conservation. Cela signifie que les dossiers médicaux doivent être conservés de manière appropriée et que les personnes non autorisées ne doivent pas y avoir accès. L'objectif de la conservation est de permettre la traçabilité d'un traitement thérapeutique.

En cas de cessation ou de transfert d'une activité commerciale, il est essentiel d'identifier la partie avec laquelle le contrat de traitement a été conclu. Si celui-ci a été signé avec un cabinet de groupe (SA, Sàrl, association, etc.), l'obligation de conservation incombe au cabinet. En revanche, si le contrat a été conclu directement avec un psychothérapeute, l'obligation de conservation repose sur ce dernier.

En cas de transfert du cabinet à un successeur, le consentement des patients concernés doit être obtenu pour la transmission de leur dossier médical.

8.1 Suppression des données

En vertu du principe de proportionnalité, les traitements de données doivent être limités à ce qui est strictement nécessaire pour atteindre les objectifs visés. Les délais de conservation légaux restent applicables.
Les psychothérapeutes sont tenus de conserver les dossiers des patients en toute sécurité pendant au moins 20 ans.[2]
En cas de demande d'effacement des données par un patient, celui-ci doit être informé des raisons, si la suppression a été effectuée ou si elle est impossible. Si une obligation légale de conservation s'applique, la demande de suppression ne pourra pas être satisfaite.
Conservation et archivage

9. Procédures en cas de violation de la protection des données

Selon la loi sur la protection des données, une violation de la sécurité des données est considérée comme avérée lorsque des données personnelles sont perdues, effacées, détruites ou modifiées de manière involontaire ou illégale, ou lorsqu'elles sont divulguées ou rendues accessibles à des personnes non autorisées. Cela peut se produire à la suite de la perte d'un support de données (ordinateur portable, iPod, smartphone, CD, clé USB, etc.), à la destruction des données par un phénomène naturel tel qu'une inondation ou un incendie, ou encore à des attaques telles que le phishing, les cambriolages, le vol de données de santé (cyberattaque), une défaillance technique, etc.
En cas d'action ou d'omission intentionnelle, des amendes d'un montant pouvant atteindre CHF 250'000 peuvent être infligées pour violation de la nLPD, conformément aux sanctions renforcées prévues par les articles 60 à 66 de la nLPD. Dans ce cas, la personne physique responsable de la violation au sein de l'entreprise ou du cabinet en assume la responsabilité. En revanche, la négligence n'entraîne pas de sanctions.

9.1 Obligation de notification

Une obligation de notification s'applique lorsque la violation de la sécurité des données présente un risque important pour la personne concernée, menaçant vraisemblablement ses droits fondamentaux ou sa personnalité. Dans ce cas, cette violation doit être signalée au Préposé fédéral à la protection des données et à la transparence (PFPDT).[3]
Il est recommandé de préparer, à titre préventif, une liste de contrôle incluant les éléments clés d'une violation de sécurité des données, ainsi que les étapes essentielles du processus de notification obligatoire. De plus, les patients doivent être informés des données personnelles les concernant et de la manière dont elles sont traitées.
Liste de contrôle violations de la protection des données

Il suffit de cliquer sur les liens fournis dans cette fiche pour obtenir de plus amples informations. Vous trouverez aussi des informations complémentaires et des listes de contrôle en matière de protection des données sur les sites Internet de la FMH et de la Caisse des Médecins.

[2] https://www.edoeb.admin.ch/fr/consultation-conservation-et-effacement-des-donnees-des-patients
[3] https://haerting.ch/wissen/strafbestimmungen_des_neuen_datenschutzgesetzes/ (en allemand ou anglais)