

Domande e risposte frequenti per terapeuti

REVISIONE DELLA NORMATIVA SULLA PROTEZIONE DEI DATI

1. Registro delle attività di trattamento

Tutti i terapeuti complementari devono tenere un registro delle attività di trattamento?

Poiché i dati concernenti la salute sono considerati degni di particolare protezione, si raccomanda vivamente ai terapeuti di tenere un registro.

Che cosa deve contenere un registro delle attività di trattamento?

Per una prassi usuale, è sufficiente avere un elenco contenente i dati che vengono raccolti, la persona che li raccoglie e lo scopo di tale raccolta nonché l'informazione se i dati vengono trasmessi a terzi. Normalmente potrebbe trattarsi della cartella del paziente, dell'agenda (soprattutto se online) e della fatturazione (cfr. in questo contesto il [modello sul sito web dell'OmL TC](#)). Per tutti i dati che non sono memorizzati per iscritto o sul proprio disco rigido, ma nel cloud di un provider (tariffa 590 ecc.), il terapeuta deve garantire il rispetto delle direttive LPD.

2. Persona responsabile in base alla legge sulla protezione dei dati

È assolutamente necessaria una persona responsabile della protezione dei dati?

La legge fa ripetutamente riferimento al «titolare del trattamento». Per tutte le raccolte di dati deve pertanto esistere una persona che si assuma la (co)responsabilità e funga da persona di contatto (anche per le autorità e i tribunali). In qualità di terapeuti in un ambulatorio individuale, siete voi la persona responsabile in base alla legge sulla protezione dei dati.

Che cosa s'intende per «conoscenze tecniche necessarie»?

Non esistono requisiti legali. Dalle circostanze emerge che la persona è a conoscenza della nuova legge sulla protezione dei dati nonché dei provvedimenti necessari e che se n'è occupata.

3. Provvedimenti tecnici e organizzativi per la sicurezza dei dati

Che cosa occorre modificare sul proprio sito web?

Sul sito web dovrebbe figurare un'informativa sulla privacy, facile da trovare. Un semplice [modello di informativa sulla privacy per terapeuti](#) è disponibile sul sito web dell'OmL TC. Versioni più dettagliate sono disponibili su Internet e in molti casi sono gratuite. Ogni terapeuta è responsabile da sé della formulazione di un'informativa sulla privacy commisurata alle proprie condizioni.

Nel nostro poliambulatorio abbiamo accesso ai dati di tutti i clienti dei terapeuti e dei professionisti della salute che lavorano presso di noi, dobbiamo modificare l'accesso?

Anche in un poliambulatorio, i diritti di accesso devono essere limitati ai dati dei clienti che vengono trattati in prima persona.

A che cosa occorre prestare attenzione riguardo ai dati archiviati elettronicamente?

La sicurezza dei dati deve essere garantita, ad esempio, da firewall e restrizioni di accesso (protezione con password per PC/laptop). Devono essere esaminate le alternative per il trasferimento di dati in Paesi terzi non sicuri, ossia, se possibile, occorre scegliere altri fornitori per il software o le applicazioni, cambiare l'ubicazione del server/cloud (passare dall'archiviazione dei dati all'estero a un offerente per l'archiviazione in Svizzera).

Posso inviare dati personali via e-mail?

Se dei dati personali vengono inviati via e-mail, è necessario utilizzare un sistema di crittografia (ad esempio HIN) od ottenere il consenso della persona interessata per la trasmissione non criptata.

Le cartelle cliniche possono continuare a essere conservate su carta?

Se le cartelle cliniche vengono archiviate fisicamente, esse devono essere conservate in un luogo sicuro che le protegga dall'accesso non autorizzato, dal furto o dal danneggiamento fisico (ad esempio, in un armadio chiuso a chiave, una cassaforte o un locale chiuso a chiave). Se nell'ambulatorio lavorano più persone, l'accesso alle cartelle cliniche deve essere limitato e solo determinate persone ricevono la chiave del luogo di conservazione.

Come informo i miei dipendenti?

I dipendenti devono frequentare corsi di formazione/perfezionamento per sensibilizzarli alla protezione dei dati. Ma possono essere introdotti anche direttive/regolamenti sulla protezione dei dati, all'occorrenza con il coinvolgimento di fornitori esterni (ad es. hosting provider, webmaster ecc.). Per quanto riguarda l'impiego di personale, nel contratto di lavoro o nel regolamento del personale occorre rimandare a una rispettiva informativa sulla privacy.

4. Diritto di accesso/obbligo di informazione

Come devono informare i terapisti i loro clienti?

La nLPD non specifica il modo in cui le persone interessate devono essere informate. Nella prassi, è usuale un'informativa sulla privacy, ma basta anche un'informazione nelle CG, un modulo di consenso o un'informazione orale (ad esempio, un annuncio su nastro). Non è, tuttavia, sufficiente la semplice indicazione di una persona di contatto per ulteriori domande.

È irrilevante se le persone interessate consultino o meno l'informativa sulla privacy.

Chi non dispone di un sito web deve consegnare l'informativa sulla privacy (ad esempio insieme alle informazioni sui pazienti) oppure appenderla o esporla in un luogo ben visibile dell'ambulatorio.

È necessario che i pazienti di terapia complementare compilino e firmino una dichiarazione di consenso?

A condizione che siano rispettati i principi del corretto trattamento dei dati (art. 6 LPD) e che non vi sia un esplicito consenso al trattamento dei dati personali. Dichiarazione esplicita di consenso della persona interessata al trattamento dei dati, i dati personali possono essere elaborati. Ciò significa che non è necessaria alcuna dichiarazione di consenso.

Quando è permessa la trasmissione a terzi?

La trasmissione è ammessa se il trattamento dei dati è lecito, conforme ai principi della legge sulla protezione dei dati e se le persone interessate sono informate dell'inoltro (cfr. informativa sulla privacy).

È permesso inviare fatture, rapporti ecc. ai clienti/alle assicurazioni malattie via e-mail?

In questo caso è necessario adottare misure tecniche per garantire che terzi non autorizzati non possano visionare i dati. Ciò è possibile, ad esempio, mediante crittografia (ad esempio con HIN-Mail). In caso di dati personali sensibili, occorre sempre ottenere l'esplicito consenso della persona interessata o, meglio ancora, il trasferimento deve avvenire tramite la persona interessata.

Quando devono essere segnalate all'IFPDT le violazioni della sicurezza dei dati?

Sussiste una violazione al momento in cui la confidenzialità, l'integrità o la disponibilità di dati personali sono compromesse, ossia quando i dati personali vengono cancellati, persi, modificati oppure divulgati o resi accessibili a persone non autorizzate. Vanno tuttavia notificate soltanto le violazioni che causano per le persone interessate un alto rischio di subire conseguenze negative. Un caso del genere si verifica quando, ad esempio, le cartelle dei pazienti sono memorizzate su una chiavetta USB non crittografata e la chiavetta USB viene smarrita.

Cosa devo fare se invio una mail al destinatario sbagliato o se perdo una chiavetta USB con i dati?

È necessario valutare caso per caso se è necessaria una segnalazione all'IFPDT. Ad esempio, se un'e-mail con dati personali viene erroneamente inviata a una persona affidabile e nota al mittente, non sussiste alcun rischio elevato. Se, invece, si perde una chiavetta con i dati dei dipendenti e le indicazioni sul salario, è necessaria una notifica.

5. Portabilità dei dati

Tengo la mia cartella clinica (CC) su carta, come posso soddisfare l'obbligo di consegna in formato elettronico?

Se i documenti non sono archiviati elettronicamente e sono disponibili solo fisicamente, essi devono essere scansionati e consegnati nel formato PDF. Pertanto, è importante che tutti i documenti relativi a un cliente siano raggruppati e in ordine.

6. Cancellazione di dati

Per quanto tempo possono essere conservati i dati dei clienti?

In base ai termini di prescrizione del Codice delle obbligazioni e alle disposizioni dei singoli Cantoni, è generalmente ipotizzabile un periodo di conservazione di 20 anni.

Devono essere cancellati solo i dati elettronici?

No, questo vale anche per i dati dei pazienti, come le cartelle cliniche conservate su carta.

Il presente promemoria e i suoi allegati sono stati allestiti nel modo più accurato e completo possibile sulla base delle conoscenze attuali. Tuttavia, non è possibile fornire alcuna garanzia legale in merito.

© OmL TC (CAMsuisse)

Soletta, 14.02.2024