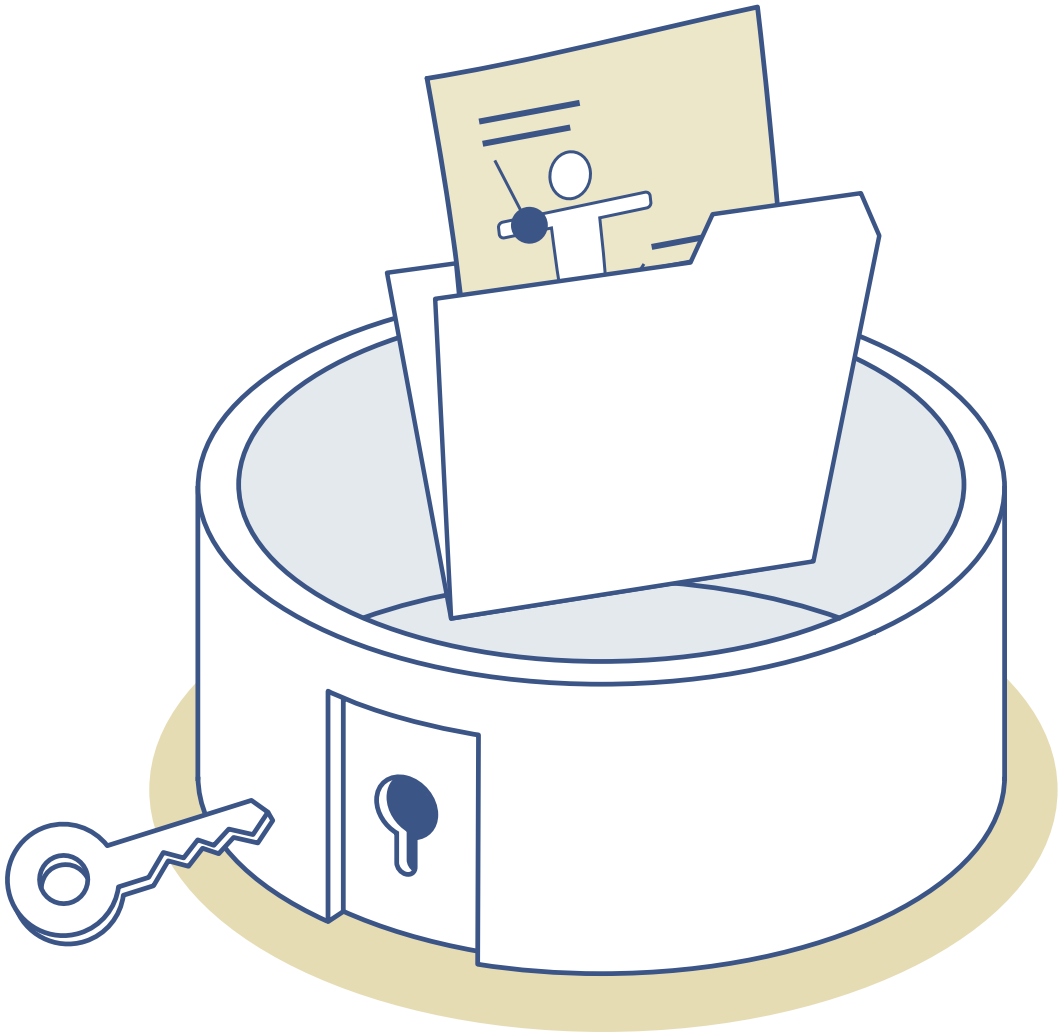
Scheda informativa sulla protezione dei dati



Versione 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Protezione dei dati negli studi medici

Scopo della Legge federale sulla protezione dei dati e della relativa ordinanza è proteggere i diritti fondamentali e della personalità delle persone fisiche i cui dati personali siano oggetto di trattamenti. I medici e i loro collaboratori sono tenuti a trattare i dati personali rispettando tali requisiti di legge.

La presente scheda informativa spiega che cos'è la protezione dei dati, che cosa significa per uno studio medico e quali aspetti è necessario osservare. Per fornire supporto agli studi medici, nelle singole tematiche sono stati inseriti link a modelli, procedure e check-list. In aggiunta al presente documento, sono disponibili anche le FAQ sulla protezione dei dati negli studi medici.

Obiettivi e scopi della protezione dei dati

La protezione dei dati si occupa dell'autodeterminazione informativa, nonché della protezione da trattamenti dei dati abusivi che possano limitare i diritti fondamentali e della personalità delle persone fisiche.

La Legge sulla protezione dei dati ha lo scopo di tutelare tali diritti definendo le direttive per la gestione e il trattamento dei dati personali.

Modifiche introdotte con la nuova legge sulla protezione dei dati

La Legge sulla protezione dei dati (LPD) rivista, che entrerà in vigore il 1° settembre 2023, rafforza in particolare le possibilità di autodeterminazione delle persone interessate in merito ai propri dati, obbligando i responsabili del trattamento ad aumentare la trasparenza e ampliando i diritti delle persone interessate. Per gli studi medici sono rilevanti soprattutto le seguenti modifiche:

— la definizione di dati personali degni di particolare protezione viene ampliata, includendo i dati genetici e biometrici nella misura in cui identifichino in modo univoco una persona fisica. Le condizioni più severe previste per il trattamento dei dati degni di particolare protezione si applicheranno in futuro anche a tali tipi di dati.
— Il registro delle collezioni di dati attualmente in vigore sarà sostituito da un registro delle attività di trattamento di dati. In tal modo l'attenzione non è più focalizzata sulle collezioni di dati, bensì sulle modalità e gli scopi del trattamento di dati personali (cfr. il capitolo «Tenuta di un registro delle attività di trattamento»).
— Ora la legge prescrive che venga effettuata una valutazione d'impatto sulla protezione dei dati laddove sia previsto un trattamento che possa presumibilmente comportare un rischio per i diritti fondamentali e della personalità della persona interessata. Un rischio di questo tipo può sussistere, ad esempio, se vengono trattati dati personali degni di particolare protezione come i dati sanitari oppure se per il trattamento dei dati personali vengono impiegate nuove tecnologie (ad es. prodotti basati su cloud, intelligenza artificiale). Non è invece necessario effettuare una valutazione d'impatto sulla protezione dei dati, se il trattamento viene effettuato sulla base di un obbligo di legge, se i sistemi, i prodotti o i servizi utilizzati sono certificati per il trattamento previsto o se viene rispettato un codice di condotta già sottoposto all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).
— La legge rivista prevede un obbligo di notifica delle violazioni della sicurezza dei dati (cfr. il capitolo «Obbligo di notifica delle violazioni della sicurezza dei dati»).
— Le disposizioni penali contenute nella LPD sono state inasprite (cfr. il capitolo «Disposizioni penali in materia di protezione dei dati»).

Dati personali

Sono considerati dati personali tutti i dati che si riferiscono a una persona e la identificano o contribuiscono alla sua identificazione. Il termine «dati personali» va quindi inteso in senso lato.

La Legge sulla protezione dei dati distingue tra dati personali e dati personali degni di particolare protezione. Tutti i dati personali sono, in linea di principio, degni di protezione. Tuttavia, in relazione al trattamento di dati personali degni di particolare protezione, la legge prescrive requisiti aggiuntivi. Tra i dati personali degni di particolare protezione, la legge cita tra l'altro i dati sanitari, quelli relativi alla sfera intima, nonché i dati concernenti le opinioni e le attività religiose, ideologiche, politiche o sindacali.

I dati personali trattati negli studi medici includono, ad esempio:

— i dati anagrafici e di contatto di pazienti, collaboratori, referenti di fornitori di servizi o di altre strutture sanitarie (ad es. nome, numero di telefono, indirizzo, indirizzo e-mail o anche la data di nascita);
— registrazioni sull'andamento delle cure, descrizioni dei sintomi, diagnosi, prescrizioni, reazioni, risultati di laboratorio, radiografie, medicazioni;
— lo status nei confronti delle assicurazioni sociali;
— i dati sulla sfera intima, come ad esempio lo stato di salute, la vita sessuale e la sfera emotiva;
— i dati sui collaboratori e il loro rapporto di lavoro, ivi inclusi i conteggi salariali e le valutazioni delle prestazioni.

Principi del trattamento

I trattamenti ai sensi della LPD comprendono qualsiasi trattamento di dati personali come, ad esempio, l'acquisizione, la conservazione, l'utilizzo, la rielaborazione, la comunicazione, l'archiviazione e la distruzione di dati, indipendentemente dai mezzi e dalle procedure utilizzati. Per il trattamento di dati personali valgono i seguenti principi:

— il trattamento di dati personali è in linea di principio lecito se vengono rispettate la legislazione vigente e le norme in materia di protezione dei dati.
— In relazione al trattamento di dati personali, i medici hanno nei confronti delle persone interessate (tra cui i pazienti) un obbligo di informazione. I medici sono cioè tenuti a informare i pazienti, in modo comprensibile, riguardo alla raccolta dei dati, al loro trattamento e ai relativi scopi, nonché in merito alle categorie di destinatari ai quali i dati vengono trasmessi.
— Al fine di garantire che i pazienti vengano adeguatamente informati, i medici devono utilizzare appositi moduli che il/la paziente, dopo il colloquio informativo, deve firmare per confermare di avere compreso le informazioni e dare il proprio consenso alla relativa fase del trattamento.
— La raccolta dei dati e lo scopo del trattamento devono avvenire in modo trasparente e in buona fede. Nella misura in cui la raccolta dei dati e lo scopo del trattamento non siano riconoscibili per la persona interessata, è necessario fornire le relative informazioni. In buona fede significa anche che i dati devono essere trattati solo secondo modalità che la persona interessata può attendersi.

Per creare trasparenza, gli studi medici possono, ad esempio, mettere a disposizione un'informativa sulla protezione dei dati o informazioni per i pazienti contenenti spiegazioni sul trattamento dei dati.

Mezzi ausiliari
Cliccando qui è possibile visualizzare un modello di i dichiarazione di consenso.
Cliccando qui è possibile visualizzare un modello di informativa in materia di protezione dei dati.

— Il trattamento dei dati personali deve essere proporzionato. La proporzionalità è data se il trattamento è limitato ai dati effettivamente idonei e necessari per l'esecuzione del compito o il raggiungimento dello scopo dichiarato. Proporzionalità significa inoltre che i dati personali devono essere conservati solo per il tempo effettivamente necessario all'esecuzione del compito o prescritto da un termine di conservazione previsto dalla legge. Se i dati personali non sono più necessari e non sussistono obblighi di conservazione di legge che lo impediscano, devono essere cancellati in modo irrevocabile.

Mezzi ausiliari
Cliccando qui è possibile visualizzare una guida per la conservazione e l'archiviazione, di dati personali.

— Il trattamento deve essere appropriato. L'appropriatezza è data se il trattamento dei dati personali avviene solo per gli scopi definiti e dichiarati al momento della raccolta dei dati.
— Se i dati personali non sono corretti, devono essere corretti o cancellati.

Ad esempio in caso di trasloco o cambio di cassa malati da parte del/della paziente.

Responsabilità all'interno dello studio medico

Responsabile ai sensi della Legge sulla protezione dei dati è in linea di principio lo studio medico, il quale è responsabile del rispetto delle norme in materia di protezione dei dati ed è tenuto in particolare a garantire la tutela dei diritti fondamentali e della personalità dei suoi pazienti e collaboratori.

Se uno studio medico desidera o necessita di assistenza per l'adempimento degli obblighi in materia di protezione dei dati, ha la possibilità di rivolgersi a un consulente interno o esterno. Per gli studi medici di diritto privato, il ricorso a un consulente per la protezione dei dati è facoltativo e non un obbligo di legge.

Il consulente per la protezione dei dati è a disposizione delle persone interessate come referente per tutte le questioni concernenti la protezione dei dati e funge anche da referente per l'IFPDT e per le autorità cantonali competenti. Il consulente fornisce supporto e forma il personale dell'azienda su tutte le questioni relative alla protezione dei dati, partecipando all'adempimento degli obblighi di legge (ad es. gestione di richieste delle persone interessate – obbligo di informare, diritto di informazione, consegna dei dati –, elaborazione di regolamenti interni sulla protezione dei dati ecc.).

Sicurezza dei dati

Per poter garantire la protezione dei diritti fondamentali e della personalità dei pazienti e dei collaboratori, occorre che i dati personali siano protetti da accessi non autorizzati, modifiche e perdite. Lo studio medico deve adottare le relative misure tecniche e organizzative per la protezione dei dati. Le misure tecniche e organizzative da scegliere dipendono in linea di principio dai rischi esistenti. Devono essere pertanto rispettati i requisiti in materia di sicurezza dei dati previsti dall'Ordinanza sulla Legge federale sulla protezione dei dati rivista (OPDa).

Esempi di misure tecniche e organizzative sono le limitazioni dell'accesso ai sistemi e ai dati fisici (ad es. documenti cartacei), le copie di sicurezza dei dati (backup), la formazione del personale, ecc.

Mezzi ausiliari
Come aiuto per l'attuazione della sicurezza dei dati è possibile utilizzare i «Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio», che sono disponibili qui.

Notifica di violazioni della sicurezza dei dati

Sussiste una violazione della sicurezza dei dati se viene compromessa la riservatezza, l'integrità o la disponibilità dei dati personali. Ciò accade, ad esempio, se i dati:

— vanno persi;
— vengono cancellati, distrutti o alterati accidentalmente o senza autorizzazione oppure
— diventano accessibili a persone non autorizzate o tali persone hanno modo di prenderne visione.

Una violazione della sicurezza dei dati può essere causata ad esempio da:

— errore umano;
— atti criminali (hacking);
— malware (infiltrazione di software dannoso);
— perdita o furto di attrezzature (ad es. laptop), supporti di dati (ad es. chiavette USB, dischi rigidi, CD/DVD) o documenti cartacei.

Ai sensi della Legge federale sulla protezione dei dati rivista e della relativa ordinanza, le violazioni della sicurezza dei dati che comportino un rischio elevato per i diritti fondamentali o della personalità delle persone interessate devono essere notificate il più presto possibile all'IFPDT. Nella misura in cui la violazione della sicurezza dei dati non comporti conseguenze per le persone autorizzate o comporti solo conseguenze minime, la notifica non è obbligatoria.

La notifica deve contenere almeno le seguenti informazioni:

— tipo di violazione della sicurezza dei dati (ad es. distruzione dei dati, furto di dati ecc.);
— se note, la data, l'ora e la durata della violazione;
— per quanto possibile, le categorie di dati personali e il quantitativo approssimativo di dati personali interessati;
— per quanto possibile, le categorie di persone interessate e il loro numero approssimativo;
— conseguenze della violazione della sicurezza, ivi inclusi gli eventuali rischi per le persone interessate (ad es. impossibilità di accedere alle cartelle cliniche e quindi trattamento solo parzialmente ricostruibile, con possibili conseguenti rischi per la salute delle persone interessate; pubblicazione delle cartelle cliniche sul «dark Web» con conseguenti rischi di violazioni dei diritti della personalità della persona interessata);
— misure adottate o previste per rimediare al problema o ridurne le conseguenze (ad es. ripristino dei dati da backup in caso di dati digitali);
— nome e dati di contatto di un/una referente.

Se non è possibile comunicare tutte le informazioni allo stesso tempo, le ulteriori informazioni possono essere messe a disposizione dell'IFPDT progressivamente entro un termine ragionevole.

Mezzi ausiliari
Cliccando qui è possibile visualizzare una check-list e una procedura in caso di violazioni protezione dei dati.

Diritto di informazione delle persone interessate

I pazienti hanno il diritto di ottenere, gratuitamente e senza fornire alcuna motivazione, informazioni sui dati che li riguardano e sul loro trattamento, a meno che non sussistano motivi per i quali la comunicazione delle informazioni possa essere rifiutata, limitata o rinviata. Le informazioni in merito all'eventuale trattamento di dati della persona interessata e alle relative modalità devono essere fornite alla persona richiedente entro un termine di 30 giorni.

Mezzi ausiliari
Cliccando qui è possibile visualizzare una guida alla gestione delle richieste di informazioni e consegna di dati personali.

Tenuta di un registro delle attività di trattamento dei dati

Il responsabile di un trattamento di dati che comprenda dati personali degni di particolare protezione in grande quantità (ad es. dati sanitari) o una profilazione ad elevato rischio ha l'obbligo di tenere un registro delle attività di trattamento dei dati. A causa della sensibilità dei dati sanitari, si raccomanda ai medici e agli studi medici di tenere quantomeno un registro delle attività di trattamento con focalizzazione sul trattamento di dati personali degni di particolare protezione (ad es. tenuta e gestione delle cartelle cliniche, gestione dei dati dei pazienti per la fatturazione alle assicurazioni sociali del personale, ecc.).

Il registro deve contenere come minimo le seguenti informazioni:

— persona/funzione responsabile del trattamento;
— descrizione del trattamento e delle sue finalità;
— categorie di dati personali trattati;
— categorie di persone interessate;
— categorie di destinatari, nella misura in cui i dati vengano regolarmente trasmessi a terzi;
— indicazione delle nazioni in cui i dati vengono eventualmente trasmessi, nonché delle garanzie nel caso di paesi terzi che non garantiscano per legge un'adeguata protezione dei dati;
— periodo di conservazione dei dati o, se non noto, criteri per la determinazione della sua durata;
— descrizione delle misure tecniche e organizzative per garantire la sicurezza dei dati;
— origine dei dati, nella misura in cui non siano stati raccolti dalla persona interessata stessa.

Mezzi ausiliari
Cliccando qui è possibile visualizzare un modello di registro delle attività di trattamento dei dati.
Cliccando qui è possibile visualizzare una guida al registro delle attività di trattamento dei dati

Trattamento dei dati da parte di un terzo incaricato

L'articolo 9 della legge sulla protezione dei dati rivista disciplina il trattamento dei dati da parte di un terzo incaricato. Il trattamento su incarico si ha, ad esempio, in caso di esternalizzazione dei sistemi informatici presso un centro di calcolo esterno oppure di esternalizzazione della contabilità salariale.

Mezzi ausiliari

Cliccando qui è possibile visualizzare un modello di accordo per un trattamento di dati su incarico.
Cliccando qui è possibile visualizzare un modello di accordo sulla riservatezza.
Cliccando qui è possibile visualizzare la guida all'utilizzo dell'Accordo sulla riservatezza e dell'Accordo per un trattamento di dati su incarico.

Disposizioni penali in materia di protezione dei dati

Secondo la Legge sulla protezione dei dati rivista, in determinati casi la violazione di obblighi e requisiti in materia di protezione dei dati può comportare la punibilità a livello personale. Alla persona fisica punibile può essere comminata una sanzione pecuniaria fino a CHF 250'000. Il presupposto è che la violazione della protezione dei dati sia stata commessa intenzionalmente, il che significa con consapevolezza e volontà di violare gli obblighi di collaborazione e diligenza.

Colophon
Editrice: FMH Federazione die medici svizzeri
Pubblicazione: marzo 2023
www.fmh.ch