KPT, Casella postale, CH-3001 Berna
kpt.ch

Regolamento per il trattamento dei dati nel sistema di informazione KPT

(Secondo l’art. 21 OLPD e l’art. 84b LAMal)

Versione 4.0 in vigore dal 1. gennaio 2022

Indice

1 Situazione di partenza

La KPT Cassa malati SA detiene la collezione di dati automatizzata «**sistema d'informazione KPT**», notificata all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), che contiene dati personali degni di particolare protezione e di profili della personalità. La collezione di dati ha come obiettivo l'attuazione e la gestione dell'assicurazione malattie e infortuni nel ramo dell'assicurazione obbligatoria delle cure medico-sanitarie e delle assicurazioni malattie complementari ai sensi della LCA.

In applicazione dell'art. 11 e dell'art. 21 dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD), per la collezione dei dati deve essere emanato un regolamento per il trattamento dei dati. Ai sensi dell'art. 84b della legge federale sull'assicurazione malattie il regolamento va sottoposto per valutazione all'IFPDT e deve essere reso pubblico.

2 Contenuto

Il presente regolamento per il trattamento dei dati descrive in particolare le procedure di trattamento e di controllo dei dati nonché la gestione del «sistema di informazione KPT». Inoltre, il regolamento contiene le informazioni necessarie per la notifica delle collezioni (art. 16 OLPD), nonché le indicazioni relative all'organo responsabile della protezione e della sicurezza dei dati, la provenienza dei dati, gli scopi per i quali i dati sono comunicati regolarmente, le procedure di controllo e in particolare le misure tecniche e organizzative previste dall'art. 20 OLPD, la descrizione dei campi di dati e delle unità organizzative che vi hanno accesso, il modo d'accesso degli utenti alla collezione di dati nonché l'estensione dell'accesso, le procedure di trattamento dei dati, segnatamente le procedure di rettificazione, di blocco, di anonimizzazione, di salvaguardia, di conservazione, di archiviazione e di distruzione dei dati, la configurazione dei mezzi informatici, la procedura di esercizio del diritto di accesso.

Il presente regolamento per il trattamento dei dati si applica anche al servizio indipendente di ricezione dei dati secondo l'art. 59a OAMal, che viene gestito internamente alla KPT.

3 Sistema di documentazione

3.1 Unità organizzative interessate

Quale detentrice della collezione di dati automatizzata «sistema di informazione KPT», la KPT Cassa malati SA gestisce il sistema e ne è l'organo responsabile.

3.2 Descrizione delle interfacce

In base all'art. 84 LAMal, la KPT ha esternalizzato alcuni servizi, che parzialmente includono anche il trattamento di dati personali, a partner di outsourcing per la gestione IT nonché a partner per l'elaborazione di documenti e soluzioni postali. La sicurezza e il trattamento dei dati in conformità alle norme in materia di protezione dei dati sono stati disciplinati nei rispettivi contratti e Service Level Agreement (SLA). Inoltre, i partner IT sono per lo più certificati secondo diverse norme ISO (in particolare ISO 9001: sistema di gestione della qualità, e ISO/IEC 27001: sistema di gestione della sicurezza delle informazioni).

Quale detentrice della collezione di dati, la KPT rimane responsabile per l'osservanza della protezione dei dati per i settori esternalizzati (art. 22 OLPD).

Nell'ambito dell'attuazione e della gestione dell'assicurazione malattie e infortuni nel ramo dell'assicurazione obbligatoria delle cure medico-sanitarie secondo la LAMal, la KPT gestisce delle interfacce con fornitori e acquirenti di dati, come descritto di seguito.

Destinatario/fornitore	Scopo	Dati personali degni di particolare protezione	Attivazione invio
Banche / fornitori di servizi finanziari	Operazioni di pagamento	No	Automatica / manuale
Autorità / tribunali	Art. 82 LAMal Art. 84a LAMal	Sì	Manuale
Piattaforma di scambio dei dati	Elaborazione delle prestazioni LAMal	Sì	Automatica
Tipografia esterna	Rivista per i clienti	No	Automatica
Istituzione comune LAMal	Compensazione del rischio	No	Manuale
Partner HMO	Gatekeeping, adempimento contratto	Sì	Automatica
Cantoni	Riduzione individuale dei premi	Sì	Manuale
Fornitori di prestazioni	Art. 84a LAMal	Sì	Automatica / manuale
Partner servizio di telemedicina	Assistenza sanitaria	Sì	Automatica
Partner per regresso	Regresso	Sì	Automatica
Santésuisse	Informazioni, RCC, pool di dati	No	Automatica
Assicuratori sociali	Art. 84a LAMal	Sì	Manuale
TeA	Tessera d'assicurato (art. 42a LAMal; OTeA)	Sì	Automatica
Assicurati	Informazione	Sì	Automatica / manuale
RCC (Registro centrale delle convenzioni)	Informazione	No	Manuale

3.3 Provenienza dei dati

I dati provengono dai fornitori di prestazioni, dagli assicurati, da altre assicurazioni sociali, dalle autorità e da fornitori di servizi finanziari.

3.4 Destinatari dei dati

La destinataria dei dati è la KPT Cassa Malati SA. I documenti con indirizzo personale (principalmente documenti per la direzione e il medico di fiducia) sono recapitati direttamente ai collaboratori KPT interessati. Gli altri documenti (lettere, moduli e fatture) vengono digitalizzati, strutturati e transcodificati dal partner per l'elaborazione dei documenti (partner di outsourcing) e inseriti nel «sistema di informazione KPT» ovvero nel workflow.

Nell'ambito della fatturazione nel ramo stazionario, tipo DRG, il fornitore di prestazioni inoltra sistematicamente insieme alla fattura i set di dati con le indicazioni amministrative e mediche secondo l'articolo 59, capoverso 1, OAMal, al servizio indipendente di ricezione dei dati della KPT secondo l'art. 59a OAMal.

I processi per i singoli trattamenti di dati sono definiti nei relativi documenti interni.

3.5 Scopi per i quali i dati sono comunicati regolarmente

Lo scopo della trasmissione dei dati è in ogni caso l'attuazione dell'assicurazione obbligatoria delle cure medico-sanitarie in applicazione della legge federale sull'assicurazione malattie (LAMal). Informazioni più dettagliate sono consultabili nella descrizione delle interfacce (punto 3.2).

3.6 Estensione della trasmissione di dati

La descrizione delle interfacce (punto 3.2) illustra quali dati vengono trasmessi a quali destinatari. I dati vengono trasmessi esclusivamente per le finalità seguenti:

- assistenza amministrativa e giudiziaria secondo l'art. 32 cpv. 2 LPGA e art. 82 LAMal;
- informazione e consulenza secondo l'art. 27 LPGA;
- consultazione degli atti secondo l'art. 47 LPGA;
- nel quadro della comunicazione di dati ai sensi dell'art. 84a LAMal.

Altre trasmissioni di dati hanno luogo in singoli casi solo con il consenso della persona assicurata. Inoltre, la trasmissione dei dati viene effettuata solo nel rispetto dei principi enunciati negli articoli 4 e seguenti della legge federale sulla protezione dei dati (LPD), in particolare solo in osservanza ai principi di finalità e di proporzionalità.

4 Organigramma dell'organo responsabile della gestione del sistema

5 Responsabilità

Il Comitato direttore della KPT Cassa malati SA, quale detentore della collezione di dati, è responsabile della protezione e della sicurezza dei dati. Le questioni relative alla protezione e alla sicurezza dei dati sono di pertinenza delle funzioni di governance (Protezione dei dati, Corporate security, Compliance e GICR). Le funzioni di governance forniscono consulenza al Comitato direttore, elaborano direttive e sono coinvolte nei processi di controllo.

6 Documentazione della pianificazione, realizzazione e gestione della collezione di dati

La gestione della collezione di dati è documentata in forma adeguata.

La documentazione tecnica dei componenti del sistema viene effettuata in appositi manuali operativi.

La pianificazione e la realizzazione di aggiornamenti (ciclo di vita) e ulteriori sviluppi vengono eseguite e documentate dal project management secondo il sistema HERMES.

7 Notifica della collezione di dati all'IFPDT (art. 16 OLPD)

Ai sensi dell'art. 11a, cpv. 5, lett. e LPD, la KPT Cassa malati SA ha designato un responsabile della protezione dei dati che controlla autonomamente se le disposizioni interne in materia di protezione dei dati sono rispettate e tiene un inventario delle collezioni. Di conseguenza la KPT è esonerata dall'obbligo di notificare la collezione dei dati all'IFPDT.

8 Documentazione dei processi del sistema di informazione KPT

I processi di trattamento dei dati del «sistema di informazione KPT» sono documentati nel tool centrale di gestione dei processi e sono consultabili per tutti i collaboratori KPT.

9 Procedure di controllo e misure tecniche e organizzative previste dall'art. 20 OLPD

9.1 Controllo dell'entrata nelle installazioni

Per impedire l'entrata negli edifici della KPT da parte di persone non autorizzate, l'ingresso è possibile solo per i collaboratori KPT che sono in possesso di un badge o di una chiave.

Agli uffici della KPT è concesso accedere solo per scopi di servizio. È vietato ammettere persone sconosciute all'interno dell'edificio. In caso di dubbio le persone devono identificarsi.

I visitatori, che devono identificarsi e registrarsi alla reception, vengono accolti alla reception da una persona di contatto della KPT e possono muoversi all'interno dell'edificio solo se accompagnati. L'ingresso nell'edificio è disciplinato nelle direttive interne.

9.2 Controllo dell'accesso

Per l'accesso al «sistema di informazione KPT», la KPT dispone di un'infrastruttura di sicurezza a più livelli. Tutti i collaboratori dispongono di un login per l'utilizzo del sistema.

I diritti di accesso sono regolati mediante un sistema di autorizzazione degli accessi basato sui ruoli e precisati in pianti di autorizzazione e nella matrice di accesso (art. 21, cpv. 2, lett. e OLPD).

Con la definizione e l'applicazione di piani di autorizzazione adeguati, l'accesso alle collezioni di dati viene limitato in base al principio «need to know» (adempimento dei compiti secondo l'art. 84 LAMal). In questo modo si impedisce la consultazione, modifica o cancellazione dei dati da parte di persone non autorizzate.

I collaboratori che dispongono di diritti di accesso per l'adempimento dei loro compiti hanno l'obbligo, sancito da appositi documenti normativi, di trattare i dati in modo corretto.

9.3 Controllo dell'introduzione (protocollazione)

Tutti gli ingressi e accessi sono protocollati in modo tracciabile.

La KPT registra sistematicamente le principali attività effettuate dagli utenti. Per verificare il rispetto del regolamento di utilizzo la KPT analizza i protocolli in forma anonima.

In caso di abuso accertato o sospetto di abuso, viene effettuata un'analisi nominale dei protocolli. In caso di abuso comprovato vengono applicate le sanzioni del caso. I collaboratori KPT sono informati in merito a questa procedura.

9.4 Controllo dei supporti dati / controllo di memoria

La KPT adotta inoltre misure adeguate per assicurare che nessuna persona non autorizzata possa leggere, copiare, modificare o cancellare i dati presenti nel «sistema di informazione KPT» nonché per impedire che i dati personali siano inseriti, consultati, modificati o cancellati senza autorizzazione.

Ad esempio, come descritto in precedenza, il controllo dell'entrata nelle installazioni assicura che persone esterne non autorizzate non possano entrare negli edifici della KPT, il che permette quindi di impedire un trattamento dei dati da parte di esterni non autorizzati. Per impedire un trattamento dei dati non autorizzato da parte di collaboratori della KPT, con adeguate misure tecniche la KPT limita o impedisce l'accesso ai dati che non sono necessari ai collaboratori per l'adempimento dei compiti loro affidati conformemente alla legge sull'assicurazione malattie (art. 84 LAMal). Ulteriori precisazioni sulla limitazione dell'accesso sono riportate al punto 11 del presente regolamento.

Inoltre l'obbligo dei collaboratori al trattamento corretto dei dati è sancito in vari regolamenti e direttive. Ad esempio, i regolamenti sulla protezione dei dati spiegano ai collaboratori come trattare correttamente i dati.

Determinate modifiche eseguite dai collaboratori possono essere tracciate nei sistemi (cfr. punto 9.3).

9.5 Controllo del trasporto

La KPT adotta misure tecniche e organizzative adeguate per assicurare che, al momento della trasmissione dei dati personali (ad es. e-mail) o al momento del trasporto di supporti di dati, persone non autorizzate non possano visionare o manipolare i dati (ad es. mediante cifratura, e-mail HIN o direttive sulla posta elettronica).

9.6 Controllo di comunicazione

I destinatari dei dati personali vengono verificati manualmente o con l'ausilio di strumenti tecnici.

9.7 Controllo degli utenti

Si veda il punto 9.2

10 Descrizione dei campi di dati e delle unità organizzative che vi hanno accesso (art. 21, cpv. 2, lett. e OLPD)

I diritti di accesso al «sistema di informazione KPT» sono regolati mediante un sistema di autorizzazione degli accessi basato sui ruoli. In una matrice di accesso sono specificati i vari ruoli con i rispettivi tipi di accesso al «sistema di informazione KPT».

11 Modo di accesso degli utenti alla collezione di dati nonché estensione dell'accesso (art. 21, cpv. 2, lett. f OLPD)

L'accesso al «sistema di informazione KPT» è concesso solo ai collaboratori che ne hanno effettivamente bisogno. Ai collaboratori viene attribuito un profilo utente (cfr. sopra punto 9.2) e viene concesso quindi un diritto di accesso che non può essere ceduto a terzi. In particolare si stabilisce anche se i collaboratori hanno bisogno soltanto di un diritto di consultazione o anche di un diritto di modifica.

I collaboratori KPT non hanno alcun accesso ai dati MCD che pervengono al servizio indipendente di ricezione dei dati della KPT e vengono trattati in modo automatizzato da quest'ultimo. Qualora le fatture vengano deviate dal servizio di ricezione alla KPT per la verifica, i collaboratori incaricati dell'esame del caso ricevono accesso alle fatture e ai relativi MCD fino alla chiusura del caso. L'accesso ai dati MCD viene bloccato con la chiusura del caso.

Le richieste di autorizzazione devono essere approvate dai rispettivi superiori e dal titolare dell'autorizzazione. Le autorizzazioni devono essere revocate ai collaboratori se non sono più necessarie per l'adempimento dei compiti assegnati.

12 Formazione degli utenti della collezione di dati

Gli utenti del «sistema di informazione KPT» ricevono una formazione con diverse modalità in ambito giuridico, in materia di protezione dei dati, e in ambito tecnico sulle varie applicazioni di sistema. Tutti i collaboratori neoassunti della KPT devono ad esempio seguire una formazione in materia di protezione dei dati. È prevista anche una formazione sulle applicazioni del «sistema di informazione KPT». Inoltre la KPT forma i collaboratori in materia di protezione dei dati con un modulo di e-learning.

Gli utenti del «sistema di informazione KPT» hanno a disposizione ausili specifici per ogni campo dell'intero sistema sotto forma di manuali d'uso e di regolamenti sulla protezione dei dati.

13 Procedure di trattamento dei dati, segnatamente procedure di rettificazione, di blocco, di anonimizzazione, di salvaguardia, di conservazione, di archiviazione e di distruzione dei dati (art. 21, cpv. 2, lett. g OLPD)

Ogni modifica eseguita da un collaboratore KPT viene registrata tecnicamente (cfr. sopra punto 9.3). Per garantire la tracciabilità del trattamento dei dati, è sempre visibile sia lo stato precedente che quello successivo alla modifica.

Le procedure di trattamento dei dati sono documentate in direttive, regolamenti e manuali specifici.

14 Configurazione dei mezzi informatici (art. 21, cpv. 2, lett. h OLPD)

I software e hardware utilizzati dalla KPT d'intesa con i partner di outsourcing corrispondono agli standard internazionali e vengono controllati periodicamente da revisori indipendenti (ISAE 3402; ISO 27001).

I documenti della configurazione degli strumenti informatici utilizzati per il «sistema di informazione KPT» vengono conservati dal settore IT nonché dai partner di outsourcing e aggiornati all'occorrenza.

15 Procedura di esercizio del diritto di accesso (art. 21, cpv. 2, lett. i OLPD)

Le richieste di accesso ovvero di informazioni secondo l'art. 8 LPD vanno indirizzate al responsabile aziendale della protezione dei dati:

KPT
Protezione dei dati
Wankdorfallee 3
3014 Berna
datenschutz@kpt.ch

16 Pubblicazione

Secondo l'art. 84b LAMal il presente regolamento viene pubblicato su internet sul sito kpt.ch.