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

Regolamento per il trattamento dei dati KPT

(Secondo gli artt. 5 e 6 OPDa e l'art. 84b LAMal)

Indice

1 Situazione di partenza

La KPT Cassa malati SA e la KPT Assicurazioni SA elaborano dati personali (particolarmente sensibili). L'elaborazione dei 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. 5 e dell'art. 6 dell'ordinanza sulla protezione dei dati (OPDa), la KPT Cassa malati SA, in veste di organo federale responsabile, e la KPT Assicurazioni SA, in veste di responsabile privato per l'elaborazione automatizzata dei propri dati personali, hanno il dovere di redigere un regolamento per il trattamento dei dati. Ai sensi dell'art. 84b della legge federale sull'assicurazione malattie (LAMal) il regolamento va sottoposto per la valutazione all'IFPDT e deve essere accessibile pubblicamente.

2 Contenuto

Il regolamento per il trattamento dei dati contiene in particolare informazioni sull'organizzazione interna, la procedura di elaborazione e di controllo dei dati nonché sulle misure adottate per garantire la sicurezza dei dati.

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

La KPT Cassa malati SA e la KPT Assicurazioni SA (di seguito KPT) gestiscono congiuntamente i sistemi informatici in qualità di organo responsabile.

3.2 Origine dei dati, finalità del trattamento, inoltro dei dati

Nella dichiarazione sulla protezione dei dati, la KPT fornisce informazioni trasparenti su come, per quali scopi e su quali basi giuridiche raccoglie ed elabora i dati personali e a chi li divulga. Inoltre, le persone interessate devono essere informate sui loro diritti (diritto all'informazione, alla correzione e alla divulgazione dei dati).

3.3 Fornitori di servizi esterni / Interfacce

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 disciplinati nei rispettivi contratti e Service Level Agreement (SLA). Inoltre, i partner IT sono per lo più certificati secondo diverse norme ISO (ad es. ISO 9001: sistema di gestione della qualità, e ISO/IEC 27001: sistema di gestione della sicurezza delle informazioni).

Nell'ambito dell'attuazione e dell'elaborazione dell'assicurazione malattie e infortuni nel settore dell'assicurazione obbligatoria delle cure medico-sanitarie ai sensi della LAMal e dell'assicurazione complementare delle cure medico-sanitarie ai sensi della LCA, diverse interfacce consentono il contatto diretto con gli assicurati, i fornitori di servizi esterni (ad es. banche, partner di regresso, autorità) e i fornitori di prestazioni (ad es. partner HMO, partner di servizi di telemedicina). La protezione dei dati e la relativa sicurezza sono garantite da una forte autenticazione e da moderne tecnologie di crittografia e trasmissione.

4 Organigramma dell'organo responsabile della gestione del sistema

5 Responsabilità

Il Comitato direttivo della KPT 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 dei dati

La gestione dei sistemi informatici è documentata in forma adeguata.

Il trattamento dei dati è definito da regolamenti, direttive e manuali e documentato nello strumento centrale di gestione dei processi e nel repertorio delle attività di trattamento. I documenti vengono regolarmente aggiornati dalle unità organizzative responsabili.

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 eseguiti e documentati dal project management secondo la governance di progetto.

7 Procedure di controllo e misure tecniche e organizzative previste dall'art. 3 OPDa

7.1 Generale

Le misure di sicurezza tecnica e organizzativa dei dati della KPT si basano su standard stabiliti a livello internazionale come ISO/IEC 27001 e NIST (National Institute of Standards and Technology). Oltre alle varie certificazioni ISO, i partner di outsourcing IT dispongono di una relazione ISAE 3402 in cui il sistema di controllo interno viene verificato e documentato da revisori indipendenti.

7.2 Controllo degli ingressi

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.

Negli uffici della KPT è concesso accedere solo per scopi di servizio. È vietato far entrare persone sconosciute all'interno dell'edificio. I badge e i cartellini per visitatori devono essere indossati in modo ben visibile 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.

7.3 Controllo dell'accesso

Per l'accesso ai sistemi informatici, la KPT dispone di un'infrastruttura di sicurezza a più livelli. Tutti i collaboratori dispongono di un login per l'utilizzo di tali sistemi.

I diritti di accesso sono regolati mediante un sistema di autorizzazione degli accessi basato sui ruoli e precisati in piani di autorizzazione e nella matrice di accesso.

Con la definizione e l'applicazione di piani di autorizzazione adeguati, l'accesso ai dati personali viene limitato in base al principio «need to know». In particolare si stabilisce anche se i collaboratori necessitano solo di un'autorizzazione alla ricerca o anche di un'autorizzazione alla mutazione. In questo modo si impedisce la consultazione, modifica o cancellazione dei dati da parte di persone non autorizzate.

Le autorizzazioni vengono concesse o ritirate automaticamente ai collaboratori in base al loro profilo (organizzazione, funzione, livello dirigenziale).

Le richieste di autorizzazione aggiuntive e manuali vengono sottoposte a una procedura di autorizzazione a 2 o 3 fasi. Le autorizzazioni non più necessarie vengono ritirate attraverso un processo definito.

Inoltre, per tutte le autorizzazioni vengono effettuate attestazioni periodiche. Le richieste di autorizzazione devono essere approvate dal rispettivo superiore e dal titolare dell'autorizzazione. Le autorizzazioni vengono ritirate ai collaboratori quando non sono più necessarie per i compiti assegnati.

I collaboratori della KPT non hanno accesso ai dati MCD (Minimal Clinical Dataset) ricevuti dal Servizio di ricezione dei dati indipendente della KPT e da esso elaborati automaticamente. Se le fatture vengono trasferite dal Servizio di ricezione dei per la revisione, i collaboratori responsabili della revisione del caso hanno accesso alle fatture e al MCD associato fino alla chiusura del caso. L'accesso al MCD viene bloccato quando il caso viene chiuso.

7.4 Controllo delle registrazioni (protocollo)

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.

7.5 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 nei sistemi informatici 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. Ulteriori precisazioni sulla limitazione dell'accesso sono riportate al punto 7.3 del presente regolamento.

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

Determinate modifiche eseguite dai collaboratori possono essere tracciate nei sistemi (cfr. punto 7.4).

7.6 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).

7.7 Controllo della comunicazione

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

7.8 Controllo degli utenti

Si veda il punto 7.3

8 Protocollazione ai sensi dell'art. 4 OPDa

Oltre a controllare l'accesso ai sistemi informatici, il trattamento automatizzato viene registrato in modo da poter determinare a posteriori se i dati sono stati trattati per gli scopi per cui sono stati raccolti o divulgati. La protocollazione viene effettuata in applicazione dell'art. 4 dell'OPDa. I protocolli sono conservati a prova di revisione per almeno 12 mesi. Sono accessibili solo agli organi e alle persone incaricate di verificare l'applicazione delle disposizioni in materia di protezione dei dati o di mantenere o ripristinare la riservatezza, l'integrità, la disponibilità e la tracciabilità dei dati e possono essere utilizzati solo a tale scopo. I fornitori esterni di servizi informatici dispongono di norme proprie per la registrazione dei dati.

9 Formazione degli utenti

Gli utenti dei sistemi informatici 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 informatiche. Inoltre la KPT forma i collaboratori in materia di protezione dei dati con un modulo di e-learning.

Gli utenti del hanno a disposizione ausili specifici per ogni campo dell'intero sistema sotto forma di manuali d'uso e di documenti relativi alle disposizioni in materia di protezione dei dati.

10 Versione / Modifiche

Le presenti norme di elaborazione non costituiscono parte integrante di alcun contratto con le persone assicurate o con altri terzi. Esse possono essere modificate in qualsiasi momento. La versione pubblicata su questo sito web è quella più aggiornata.