Regolamento per il trattamento dei dati

Indice

1. Premessa

La CONCORDIA Assicurazione svizzera malattie e infortuni SA è il detentore della collezione di dati automatizzata secondo la legge federale sull'assicurazione malattie (LAMal). La collezione di dati è utilizzata per lo svolgimento delle operazioni relative all'assicurazione malattie e infortuni nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie ai sensi della LAMal.

Il presente regolamento per il trattamento dei dati è valido anche per il servizio di ricezione dei dati indipendente ai sensi dell'art. 59a OAMal, gestito internamente presso la CONCORDIA.

2. Documentazione delle unità organizzative interessate dal sistema

La CONCORDIA Assicurazione svizzera malattie e infortuni SA è il gestore del sistema e, in quanto detentore della collezione di dati automatizzata, ne costituisce l'organo responsabile.

3. Descrizione delle interfacce

3.1 Interfacce con i fruitori e i fornitori esterni di dati

Basandosi sull'art. 84 LAMal, la CONCORDIA ha esternalizzato alcuni servizi nell'ambito dell'elaborazione di documenti e di soluzioni per invii postali, che alle volte richiedono il trattamento di dati personali, a partner di outsourcing esterni. In ogni contratto di collaborazione è definito che il trattamento dei dati deve avvenire nel rispetto della protezione e della sicurezza dei dati stessi. I partner IT sono in parte certificati secono diverse norme ISO (in particolare le certificazioni del sistema di gestione della qualità ISO 9001:2008 e del sistema di gestione della sicurezza delle informazioni ISO/IEC 27001).

La CONCORDIA, quale detentore della collezione di dati, resta comunque responsabile della protezione dei dati anche per gli ambiti affidati all'esterno (art. 22 OLPD).

Nel quadro dello svolgimento delle operazioni relative all'assicurazione malattie e infortuni nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie secondo la LAMal, la CONCORDIA gestisce delle interfacce con i fruitori e i fornitori di dati che descriviamo qui di seguito.

Destinatario/Fornitore	**Scopo**	**Dati particolarmente sensibili**	**Attivazione**
Banche	Traffico dei pagamenti	No	Automatica
Istituzioni/Tribunali	Art. 82 LAMal, Art. 84a LAMal	Sì	Manuale
Tipografia esterna	Rivista per la clientela	No	Automatica
Società di servizi finanziari	Bank Master	No	Automatica
Istituzioni comuni LAMal	Compensazione dei rischi, giorni di degenza ospedaliera	No	Manuale
Partner HMO	Art. 84a LAMal	Sì	Manuale
Servizi di raffronto Internet	Offerte calcolate	No	Automatica
Cantoni	RIP, art. 64 LAMal	Sì	Automatica
Fornitori di prestazioni	Art. 84a LAMal, art. 59 OAMal	Sì	Automatica / Manuale

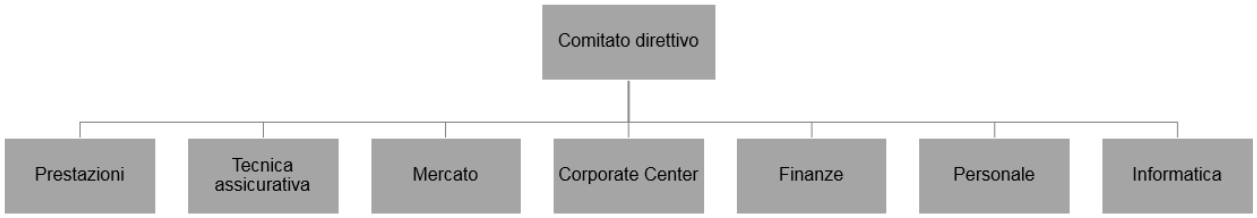
Destinatario/Fornitore	Scopo	Dati particolarmente sensibili	Attivazione
MediData	Piattaforma di scambio di documenti elettronici	Sì	Automatica
Partner servizi di telemedicina	Assistenza sanitaria	Sì	Manuale
santésuisse	Informazioni, RCC; pool di dati	No	Automatica
Sedex	RIP	Sì	Automatica
Assicuratori sociali	Art. 84a LAMal	Sì	Manuale
SwissPost Solutions	Visualizzazione delle ricevute di pagamento	No	Manuale
VEKA	Tessera d'assicurato (art. 42a LAMal, OTeA)	Sì	Automatica
Assicurati	Informazioni, corrispondenza, conteggi delle prestazioni	Sì	Automatica / Manuale
RCCo	Informazioni	No	Manuale

3.2 Provenienza dei dati

I dati provengono da fornitori di prestazioni, assicurati, altre assicurazioni sociali, istituzioni e società di servizi finanziari.

4. Organigramma del gestore della collezione di dati

Organigramma della CONCORDIA Assicurazione svizzera malattie e infortuni SA



5. Responsabilità

Il Comitato direttivo della CONCORDIA Assicurazione svizzera malattie e infortuni SA in quanto detentore della collezione di dati è responsabile della sicurezza dei dati e dell'adempimento delle prescrizioni in materia di protezione dei dati.

Le questioni inerenti alla protezione e alla sicurezza dei dati sono affidate agli incaricati per la protezione dei dati, la sicurezza delle informazioni e la sicurezza fisica. Gli incaricati consigliano il Comitato direttivo, allestiscono le linee guida e sono integrati nei processi di sorveglianza.

6. Documentazione sulla programmazione, realizzazione e gestione della collezione di dati

La gestione della collezione di dati è descritta in specifici manuali operativi. La programmazione e realizzazione tecnica sono illustrate in documenti di progetto. La documentazione tecnica dei componenti del sistema è esposta nei manuali operativi dell'informatica.

7. Notifica della collezione di dati presso l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) d'intesa con l’incaricata della protezione dei dati (DSB)

Conformemente all'art. 11a cpv. 5 lett. e LPD, la CONCORDIA Assicurazione svizzera malattie e infortuni SA ha designato un responsabile della protezione dei dati che controlli autonomamente se le disposizioni interne in materia di protezione dei dati siano rispettate e tiene un inventario delle collezioni. Ciò solleva la CONCORDIA dall'obbligo di notificare la collezione di dati presso l'IFPDT ai sensi dell'art. 11a cpv. 2 LPD.

La CONCORDIA adempie l'obbligo di presentazione all'IFPDT ai sensi dell'art. 84b LAMal.

8. Documentazione dei processi che interessano le collezioni di dati

I processi di trattamento dei dati per le singole collezioni sono descritti in documenti interni.

9. Provenienza dei dati

Vedi l'elenco riportato al capitolo 3.

10. Scopi della trasmissione regolare di dati

Vedi l'elenco riportato al capitolo 3.

11. Procedure di controllo e in particolare misure tecnico-organizzative ai sensi dell'art. 20 OLPD

Sono state implementate misure tecnico-organizzative per garantire la riservatezza, l'integrità e l'accessibilità dei dati.

11.1 Controllo dell'entrata nelle installazioni

Per evitare che persone non autorizzate possano introdursi negli immobili aziendali della CONCORDIA, l'accesso è possibile solo ai collaboratori della CONCORDIA in possesso di un badge o di una chiave.

L'accesso agli immobili aziendali della CONCORDIA è regolamentato nelle disposizioni «Accesso agli immobili aziendali della CONCORDIA» e «Zutritts- und Schliessorganisation» (Dispositivi di accesso e chiusura, disponibile in tedesco).

Per l'accesso ai locali dell'informatica esiste una direttiva a parte «Zutrittsrechte bei der Informatik» (Diritti d'accesso per l'informatica, disponibile in tedesco).

11.2 Controllo dei supporti di dati

Mediante l'adozione di misure tecnico-organizzative, la CONCORDIA assicura che nessuna persona non autorizzata possa leggere, copiare, modificare o eliminare dei dati; che nessuna immissione non autorizzata possa essere effettuata nel sistema di memorizzazione e che non sia possibile visionare, modificare o cancellare dati personali memorizzati senza debita autorizzazione.

Alcune modifiche eseguite dai collaboratori possono essere rintracciate nei sistemi.

Mediante diverse direttive e regolamenti i collaboratori sono istruiti sul trattamento corretto dei dati. Di importanza centrale è la direttiva «Uso di hardware, software e dati elettronici».

Lo smaltimento dei supporti di dati viene effettuato dall'unità aziendale Informatica secondo un processo stabilito.

11.3 Controllo del trasporto

Con appropriati provvedimenti tecnico-organizzativi la CONCORDIA garantisce che nel comunicare dati personali nonché durante il trasporto di supporti di dati, nessuna persona non autorizzata possa leggere, copiare, modificare o cancellare i dati (ad esempio mediante cifratura dei dati o direttive sull'uso delle e-mail).

11.4 Controllo della comunicazione

I destinatari di dati personali sono verificati manualmente o con il supporto di strumenti tecnici.

11.5 Controllo della memoria

Vedi 11.2

11.6 Controllo dell’utilizzazione

La CONCORDIA dispone di un sistema di sicurezza a più livelli adeguato alle necessità di protezione dei dati. Gli utenti devono identificarsi per poter accedere ai sistemi di informazione.

11.7 Controllo dell'accesso ai dati

Le autorizzazioni per accedere ai dati sono assegnate in base al cosiddetto principio «Need to know», ovvero sono attribuiti solo i diritti necessari per lo svolgimento della propria funzione. L'assegnazione avviene in base a profili di autorizzazione. La gestione degli utenti e dei diritti è regolamentata da processi ben definiti, con il supporto di strumenti tecnici.

I diritti assegnati sono verificati periodicamente durante i processi di controllo interni.

11.8 Controllo dell'introduzione (verbalizzazione)

Nel sistema di informazione centrale i dati personali inseriti sono salvati con cronologia. In caso di abuso o di sospetto di abuso è possibile analizzarli. I collaboratori sono informati di questa prassi tramite il regolamento «Uso di hardware, software e dati elettronici».

12. Descrizione dei campi di dati e unità organizzative munite di accesso

Nel quadro del processo di notifica della collezione di dati, in regolamenti sul trattamento dei dati separati viene offerta una descrizione dei campi di dati e illustrato il sistema delle autorizzazioni.

13. Natura e portata dell'accesso degli utenti alla collezione di dati

Ogni collaboratore può accedere ai dati che gli occorrono per lo svolgimento delle proprie mansioni.

Nel sistema delle autorizzazioni si descrivono le modalità di accesso, quali profili di autorizzazione (ruoli) sono abilitati allo svolgimento di quali funzioni e a quale «data room» è possibile accedere. Inoltre viene definito e approvato chi è autorizzato a richiedere questi ruoli e chi deve autorizzare la loro attribuzione.

I collaboratori della CONCORDIA non hanno accesso ai dati MCD (minimal clinical dataset) che pervengono al servizio di ricezione dei dati indipendente e che quest'ultimo elabora in modo automatizzato. Se il servizio di ricezione dei dati seleziona delle fatture da verificare, i collaboratori incaricati dell'esame del caso possono accedere alle fatture e ai relativi dati MCD fino alla conclusione di tale verifica.

14. Procedure di trattamento dei dati, in particolare di rettifica, blocco, anonimizzazione (pseudonimizzazione), salvataggio, conservazione, archiviazione o distruzione di dati

Le procedure per il trattamento dei dati sono descritte in direttive, regolamenti e manuali specifici (vedi anche i capitoli 13 - 15).

Gli utenti di una collezione di dati sono regolarmente istruiti in merito ai processi tecnici e alla protezione dei dati.

15. Configurazione dei mezzi informatici

Gli strumenti informatici (hardware e software) in uso presso la CONCORDIA sono conformi agli standard internazionali del settore. Essi sono sottoposti a un processo regolamentato di gestione del ciclo di vita.

La configurazione dei mezzi informatici è illustrata nei manuali operativi e all'occorrenza aggiornata.

16. Procedura per l'esercizio del diritto di accesso

Le richieste di accesso ai sensi dell'art. 8 LPD devono essere presentate all'incaricata aziendale della protezione dei dati:

CONCORDIA Assicurazione svizzera
malattie e infortuni SA
Incaricata della protezione dei dati
Bundesplatz 15
6002 Lucerna