Policy per la sicurezza dei sistemi d'informazione della EGK-Cassa della salute

Destinatari: - Direzione della EGK-Cassa della salute
- tutti i collaboratori della EGK-Cassa della salute

Pubblicata su: http://www.egk.ch/egk/

Informazioni importanti sul documento	
Autore responsabile:	Kilian Schmidlin
Nome file:	Policy per la sicurezza dei sistemi d'informazione della EGK-Cassa della salute
Numero versione:	2.0
Numero del documento:	1.3.02-i
Numero di pagine:	6
Livello di riservatezza:	V1 - pubblico
Data di creazione:	25 settembre 2014
Data di approvazione:	20 ottobre 2014
Data dell'ultima modifica:	14 ottobre 2020
Stato di elaborazione:	Approvato
Data dell'ultima approvazione:	19 ottobre 2020
Approvato da:	Direzione

Documenti integrativi/documentazione applicabile			
Titolo del documento	*Versione*	*Data*	*Autore responsabile*
Regolamento per il trattamento della collezione di dati	3.2	26.10.2020	Kilian Schmidlin
Dichiarazione sulla protezione dei dati per i servizi online	1.0	01.05.2020	Stefanie Omlin
Regolamento sui mezzi informatici	2.0	19.08.2019	Andrea Grolimund
Modello BCM	3.0	12.10.2020	Patrick Tanner Alice Grolimund Kilian Schmidlin
Modello per la sicurezza dei dati	1.4	25.10.2019	Patrick Tanner
Direttiva per la classificazione di dati / informazioni / documenti	2.0	12.10.2020	Kilian Schmidlin

I. Sommario

II. Abbreviazioni

BCM	Business Continuity Management (italiano: gestione della continuità operativa)
SRD	Servizio di ricezione dei dati
DRG	Diagnosis Related Groups (italiano: raggruppamenti omogenei di diagnosi per fatture relative a degenze ospedaliere)
DSG	Legge sulla protezione dei dati
DWH	Data Warehouse
EDÖB	Incaricato federale della protezione dei dati e della trasparenza
FINMA	Autorità federale di vigilanza sui mercati finanziari
ICT	Information and communications technology (italiano: tecnologia dell'informazione e della comunicazione)
KVG	Legge sull'assicurazione malattie
MCD	Minimal clinical dataset (italiano: set di dati medici)
OCR	Optical character recognition (italiano: riconoscimento ottico dei caratteri)
SHP	Swiss Health Platform (applicazione principale di EGK/Centris AG)
TARPSY	Tariffa per psichiatria stazionaria (raggruppamenti di casi giornalieri in funzione della diagnosi)
VVG	Legge sul contratto d'assicurazione

1 Ambito di applicazione

La denominazione sociale EGK-Cassa della salute, di seguito «EGK», comprende la Fondazione EGK-Cassa della salute e le seguenti società anonime ad essa affiliate: EGK Assicurazioni di base SA (assicuratore nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie secondo LAMal), EGK Assicurazioni private SA (assicuratore nell'ambito delle assicurazioni complementari secondo LCA) ed EGK Services SA. La presente policy per la sicurezza dei sistemi d'informazione della EGK è valida per tutte le società del gruppo EGK.

2 Scopo

Nel rispetto dei propri valori la EGK-Cassa della salute protegge e rispetta la sfera privata dei propri clienti. A tal fine gestiamo con attenzione i dati che ci vengono forniti per il trattamento. In questo modo rispettiamo le principali norme di legge e osserviamo le disposizioni corrispondenti del codice di comportamento, dei regolamenti dell'EGK, dei contratti e di tutte le norme riguardanti la sicurezza dei dati e delle informazioni. Questi principi forniscono la cornice di riferimento della nostra policy per la sicurezza dei sistemi d'informazione.

Le informazioni e i dati, soprattutto i dati personali e relativi alla salute degli assicurati, rivestono un'importanza centrale ai fini dell'adempimento del nostro mandato legale secondo la LAMal nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie (assicurazione base) nonché ai fini dell'esecuzione in conformità al contratto delle assicurazioni complementari secondo la LAMal. Le nostre misure di sicurezza e di protezione dei dati sono volte a impedire per quanto possibile eventi dannosi o almeno a contenere la loro frequenza e portata entro limiti ragionevoli e sostenibili.

3 Obiettivi di sicurezza della EGK

- Garantire la continuità dei processi aziendali centrali.

- Ottenere un'elevata sicurezza, stabilità, continuità e qualità nel trattamento dei dati e delle informazioni e nella fornitura di servizi in conformità alle disposizioni di legge e ai principi di proporzionalità e di economicità.
- Impedire danni d'immagine o finanziari alla EGK derivanti dalla perdita di dati o informazioni oppure dall'acquisizione di dati e informazioni da parte di terzi non autorizzati.
- Sensibilizzare i collaboratori di tutti i livelli in qualsiasi reparto aziendale in merito all'importanza della sicurezza e della protezione dei dati.

4 Strategia di outsourcing informatico

La EGK attua una strategia di outsourcing parziale dei servizi informatici tramite un'esternalizzazione mirata e la delega dei servizi di progettazione e gestione. Tra questi è compresa anche l'applicazione assicurativa principale che viene gestita dalla Centris AG di Soletta. Tale società è un provider professionale certificato del settore che gestisce la piattaforma SHP (Swiss Health Platform) per più assicuratori malattia. Nei processi elettronici relativi alle fatture di tipo DRG / TARPSY, la Centris AG funge da servizio certificato di ricezione dei dati (SRD) della EGK in quanto è registrata e riconosciuta come SRD dall'Incaricato federale della protezione dei dati e della trasparenza (IFPDT). Fanno parte dell'ambiente SHP in particolare i sistemi Syrius ASE, il modulo workflow di Syrius, il modulo di offerta e proposta di Syrius, SUMEX II, DWH, il sistema di archiviazione FileNet, la Digital Insurance Platform (DIP) e il mass printing.

La EGK si avvale inoltre dei servizi informatici della Econis AG che gestisce nell'ambito di un Managed Service l'infrastruttura e il funzionamento di base del centro di calcolo. Nel Managed Service è compresa la gestione dell'hardware per quanto concerne l'archiviazione sul server e l'accesso remoto. Il reparto ICT della EGK detiene invece il controllo a partire dai sistemi operativi dell'infrastruttura virtuale e di quella della banca dati in uso (hardware e OS del server) per i sistemi periferici della EGK.

L'infrastruttura di rete e i servizi di telefonia sono acquistati dalla Swisscom.

La EGK conta su altri importanti partner di outsourcing a cui esternalizza il trattamento dei dati, come Swiss Post Solutions (SPS), controllata di Swiss Post, per la fornitura dei servizi di scansione e Cent Systems AG per il servizio di acquisizione dati (digitalizzazione dati).

5 Principi

5.1 Norme, leggi e contratti

- Il trattamento dei dati e delle informazioni deve avvenire sempre in conformità alle disposizioni di legge, contrattuali e interne.
- In relazione ai dati e alle informazioni sensibili degli assicurati devono essere osservati i principi di diritto specifici enunciati nella Legge federale sulla protezione dei dati (LPD) e nella Legge federale sull'assicurazione malattie (LAMal).
- Ai sensi dell'art. 84b LAMal è prevista l'elaborazione di un regolamento per il trattamento dei dati accessibile al pubblico.
- La continuità dell'attività deve essere garantita anche in caso di eventi e situazioni straordinarie e devono essere rispettati gli standard minimi riconosciuti dalla FINMA per le compagnie di assicurazione (BCM).
- Dati, informazioni e documenti sono conservati secondo le modalità previste dalla legge; nei casi dubbi si applica un periodo di conservazione di almeno 10 anni.

5.2 Finalità della protezione IT

- In ogni momento deve essere garantita la disponibilità, l'integrità nonché il trattamento confidenziale e conforme alle norme sulla privacy di dati e informazioni relativi ad assicurati, collaboratori e partner. Vigono quindi i principi descritti di seguito.

5.2.1 Riservatezza

- In caso di trasmissione a terzi, le modalità di utilizzo, trattamento e impiego di tali dati e informazioni devono essere convenute per contratto. I dati trasmessi devono essere resi anonimi oppure inviati tramite supporti dati e canali cifrati.

- Nelle comunicazioni e-mail individuali devono essere utilizzati dei sistemi di crittografia quando si trasmettono dati personali.

- I collaboratori sono formati e aggiornati regolarmente in merito alla protezione dei dati e alla sicurezza delle informazioni. Si deve garantire che essi conoscano e applichino il regolamento sul trattamento dei dati valido per il loro reparto.

- I dati e le informazioni devono essere suddivisi in categorie secondo la Direttiva per la classificazione di dati / informazioni / documenti e protetti di conseguenza. I livelli di classificazione sono indipendenti dall'applicazione che contiene i dati e le informazioni.

5.2.2 Disponibilità

- Si deve elaborare un modello per la sicurezza dei dati che fissa le condizioni quadro per le misure tecniche e organizzative relative alla sicurezza dei dati.

- I sistemi devono essere aggiornati regolarmente con update di sicurezza.

- Le modifiche alle applicazioni devono avvenire sulla base di un processo di change-management definito.

- Le collezioni di dati personali devono essere gestite in una directory di elaborazione dei dati da cui è possibile risalire al luogo di conservazione dei dati e al loro termine per la cancellazione.

5.2.3 Integrità

- Le informazioni devono essere protette per mezzo di chiavi crittografiche con una data di scadenza prevista di massimo due anni.

- Tramite un sistema di autorizzazioni basato su ruoli si deve garantire che i collaboratori abbiano accesso solo a quei dati e quelle informazioni di cui necessitano per lo svolgimento dei loro compiti.

- Meccanismi di protezione devono garantire che soltanto i collaboratori autorizzati abbiano la possibilità di installare autonomamente dei file eseguibili.

6 Responsabilità

Il responsabile del reparto ICT della EGK è responsabile della sicurezza dei dati e dei sistemi d'informazione, nonché della disponibilità e dell'integrità dei dati. Tutti i servizi offerti dall'EGK sono soggetti a queste disposizioni relative alla policy per la sicurezza dei sistemi di informazione e alle prescrizioni di legge sulla segretezza e protezione dei dati.

I fornitori di servizi di outsourcing possono utilizzare e trattare i dati esclusivamente nello stesso ambito in cui è consentito all'EGK e sono tenuti a rispettare le stesse prescrizioni sulla segretezza e la protezione dei dati dell'EGK.

I responsabili di reparto e i quadri dirigenziali dei diversi reparti sono responsabili dell'applicazione della sicurezza dei dati e delle informazioni nel rispettivo ambito di competenza.

Ai collaboratori viene richiesto di comunicare alla direzione di reparto competente, al responsabile ICT e al responsabile aziendale della protezione dei dati qualsiasi problema inerente alla protezione dei dati o alla sicurezza riscontrato o sospettato.

L'uso dei servizi e-mail e social media rientra nella sfera di responsabilità dell'utente.

7 Procedure per la gestione di deroghe ed eccezioni

Eventuali richieste per eccezioni e deroghe alla presente policy per la sicurezza dei sistemi d'informazione devono essere esaminate e approvate dalla Direzione.

8 Entrata in vigore / Verifica

Il presente documento sulla policy per la sicurezza dei sistemi d'informazione entra in vigore il 20.10.2014. Il documento è sottoposto a una verifica annuale ai fini del suo eventuale aggiornamento e necessario adeguamento. Le modifiche apportate hanno effetto dalla data in cui sono approvate dalla Direzione.

9 Cronologia delle modifiche

Cronologia delle modifiche				
Numero versione	*Stato di elaborazione*	*Data*	*Autore modifica*	*Modifica / commento*
0.1	Stesura iniziale	25.09.2014	K. Schmidlin	
1.0	Approvato	20.10.2014	K. Schmidlin	
1.1	Approvato	03.10.2016	K. Schmidlin	- Adeguamento al nuovo ambiente di sistema SHP
1.2	Approvato	25.09.2017	K. Schmidlin	- Integrazione BCM - div. piccoli adeguamenti
1.3	Approvato	01.10.2018	P. Tanner	- Modifiche al capitolo 4 - Nuovi capitoli 5.1, 5.2 e 7 - modifiche redaz. minori
1.4	Approvato	28.10.2019	K. Schmidlin	- modifiche redaz. Adeguamenti e aggiornamenti
2.0	Approvato	19.10.2020	K. Schmidlin	- Adeguamento all'ambiente di sistema SHP (CBPM non più in uso) e aggiornamenti, integrazioni e modifiche redazionali