



Daten-Bearbeitungsreglement

Inhaltsverzeichnis

1. Ausgangslage	3
2. Dokumentation der vom System betroffenen Organisationseinheiten	3
3. Schnittstellenbeschreibung	3
3.1 Schnittstellen zu externen Datenbezugern oder Datenlieferanten	3
3.2 Datenherkunft.....	3
4. Organigramm des verantwortlichen Organs.....	3
5. Verantwortlichkeiten.....	3
6. Dokumentation über die Planung, Realisierung und den Betrieb der Datenbearbeitungen..	4
7. Anmeldung des Verzeichnisses der Bearbeitungstätigkeiten beim EDÖB.....	4
8. Prozessdokumentation welche die Bearbeitungen betreffen	4
9. Die Herkunft der Daten	4
10. Die Zwecke, für welche die Daten regelmässig bekannt gegeben werden	4
11. Die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen	4
11.1 Zugangskontrolle.....	4
11.2 Datenträgerkontrolle	4
11.3 Transportkontrolle	5
11.4 Bekanntgabekontrolle.....	5
11.5 Speicherkontrolle	5
11.6 Benutzerkontrolle	5
11.7 Zugriffskontrolle.....	5
11.8 Eingabekontrolle (Protokollierung).....	5
12. Art und Umfang der Zugriffsberechtigungen.....	5
13. Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung (Pseudonymisierung), Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten	5
14. Die Konfiguration der Informatikmittel	6
15. Verfahren zur Ausübung der Rechte der betroffenen Personen.....	6

1. Ausgangslage

Die CONCORDIA Schweizerische Kranken- und Unfallversicherung AG ist verantwortlich für die Durchführung und Abwicklung der obligatorischen Krankenpflegeversicherung nach KVG..

Das Bearbeitungsreglement gilt auch für die unabhängige Datenannahmestelle gemäss Art. 59a KVV, welche intern bei der CONCORDIA betrieben wird.

2. Dokumentation der vom System betroffenen Organisationseinheiten

Die CONCORDIA Schweizerische Kranken- und Unfallversicherung AG ist das systembetreibende das dafür verantwortliche Organ.

3. Schnittstellenbeschreibung

3.1 Schnittstellen zu externen Datenbezügern oder Datenlieferanten

Einige Dienstleistungen, welche teilweise auch die Bearbeitung von Personendaten umfassen, hat die CONCORDIA gestützt auf Art. 84 KVG an Outsourcingpartner zu Dokumentenbearbeitung und Postlösungen ausgelagert. Die datenschutzkonforme Bearbeitung der Daten wie auch die Datensicherheit wurde in den jeweiligen Zusammenarbeitsverträgen geregelt. Die IT-Partner sind zudem teilweise nach verschiedenen ISO-Normen (insbesondere ISO 9001:2008 Qualitätsmanagementsystem sowie ISO/IEC 27001 Informationssicherheits-Managementssystem) zertifiziert.

Die CONCORDIA bleibt als Verantwortliche weiterhin verantwortlich für die Einhaltung des Datenschutzes für die ausgelagerten Bereiche.

Im Rahmen der Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung gemäss KVG unterhält die CONCORDIA Schnittstellen zu Datenbezügern und Datenlieferanten (z.B. Behörden, Gerichte, andere Versicherer, externe Sachverständige).

3.2 Datenherkunft

Die Daten stammen von Leistungserbringern, Versicherten, anderen Sozialversicherungen, Behörden und Finanzdienstleistern.

4. Organigramm des verantwortlichen Organs

Organigramm der CONCORDIA Kranken- und Unfallversicherung AG



5. Verantwortlichkeiten

Die Geschäftsleitung der CONCORDIA Schweizerische Kranken- und Unfallversicherung AG trägt die Verantwortung für die Einhaltung der Datenschutzvorschriften und die Datensicherheit.

Für die Belange des Datenschutzes und der Datensicherheit gibt es Beauftragte für den Datenschutz, die Informationssicherheit und die physische Sicherheit. Die Beauftragten beraten die Geschäftsleitung, erstellen Leitlinien und sind in die Kontrollprozesse mit eingebunden.

6. Dokumentation über die Planung, Realisierung und den Betrieb der Datenbearbeitungen

Der Betrieb der Datenbearbeitungen ist in spezifischen Betriebshandbüchern festgehalten. Die technische Planung und Realisierung ist in Projektdokumenten dokumentiert. Die technische Dokumentation der Systemkomponenten ist in Betriebshandbüchern der Informatik enthalten.

7. Anmeldung des Verzeichnisses der Bearbeitungstätigkeiten beim EDÖB

Das Verzeichnis der CONCORDIA Schweizerische Kranken- und Unfallversicherung AG wurde am 28.08.2023 im DataReg-Portal des EDÖB angemeldet.

8. Prozessdokumentation welche die Bearbeitungen betreffen

Die Datenbearbeitungsprozesse für die einzelnen Bearbeitungstätigkeiten sind in internen Prozessdokumenten festgehalten.

9. Die Herkunft der Daten

Siehe Kapitel 3.2.

10. Die Zwecke, für welche die Daten regelmässig bekannt gegeben werden

Siehe Kapitel 3.1.

11. Die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen

Es sind angemessene technische und organisatorische Massnahmen implementiert, welche die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gewährleisten.

11.1 Zugangskontrolle

Um sicherzustellen, dass unbefugte Personen keinen Zugang zu den Betriebsliegenschaften der CONCORDIA haben, ist der Zutritt nur den Mitarbeitenden der CONCORDIA, die im Besitz eines Badges oder eines Schlüssels sind, möglich.

Der Zugang zu Betriebsliegenschaften der CONCORDIA ist verschiedenen Weisungen geregelt.

11.2 Datenträgerkontrolle

Die CONCORDIA stellt durch technische und organisatorische Massnahmen sicher, dass keine unbefugten Personen Daten lesen, kopieren, verändern oder entfernen können und keine unbefugte Eingabe in den Speicher sowie die unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten getätigt wird.

Bestimmte, von Mitarbeitenden durchgeführte, Änderungen können in den Systemen zurückverfolgt werden.

Mitarbeitende werden in verschiedenen Weisungen und Reglementen zur korrekten Datenverarbeitung angewiesen.

Die Entsorgung von Datenträgern erfolgt durch die Geschäftseinheit Informatik durch einen geregelten Prozess.

11.3 Transportkontrolle

Die CONCORDIA stellt mittels technischen und organisatorischen Massnahmen sicher, dass bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern keine unbefugten Personen die Daten lesen, kopieren, verändern oder löschen können (z.B. durch Verschlüsselung oder Weisungen zum Umgang mit E-Mails)

11.4 Bekanntgabekontrolle

Der Empfänger von Personendaten wird entweder manuell oder durch technische Hilfsmittel verifiziert.

11.5 Speicherkontrolle

Siehe 11.2

11.6 Benutzerkontrolle

Die CONCORDIA verfügt über ein dem Schutzbedarf der Daten angemessenes mehrstufiges Sicherheitskonzept. Benutzer müssen sich authentisieren um Zugang zu den Informationssystemen zu erhalten.

11.7 Zugriffskontrolle

Die Berechtigungen für den Zugriff auf Daten werden nach dem Need-to-Know Prinzip vergeben, d.h. es werden nur die Rechte vergeben die für die Ausübung der Funktion benötigt werden. Die Vergabe basiert auf Berechtigungsprofilen. Für die Benutzer- und Berechtigungsverwaltung bestehen definierte Arbeitsabläufe, die mit technischen Hilfsmitteln unterstützt werden.

Die zugeteilten Berechtigungen werden im Rahmen der internen Kontrollprozesse periodisch überprüft.

11.8 Eingabekontrolle (Protokollierung)

Im zentralen Informationssystem werden Personendateneingaben historisiert abgelegt. Bei Missbrauch oder bei einem Verdacht auf Missbrauch können diese Daten ausgewertet werden. Die Mitarbeitenden werden im Reglement „Umgang mit Hardware, Software und elektronischen Daten“ darüber informiert.

12. Art und Umfang der Zugriffsberechtigungen

Jeder Mitarbeiter hat nur Zugriff auf diejenigen Daten, die er für seine Aufgabenerfüllung benötigt.

In einem Berechtigungskonzept wird festgehalten wie der Zugriff erfolgt, welche Berechtigungsprofile (Rollen) welche Funktionen ausüben können, und auf welchen Datenraum zugegriffen werden kann. Ebenfalls wird definiert und abgenommen, wer diese Rollen beantragen darf und wer die Zuteilung bewilligen muss.

13. Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung (Pseudonymisierung), Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten

Die Datenbearbeitungsverfahren sind in spezifischen Weisungen, Reglementen und Handbüchern dokumentiert.

Die Mitarbeitenden werden regelmässig in Belangen des Fachprozesses und des Datenschutzes geschult.

14. Die Konfiguration der Informatikmittel

Die von der CONCORDIA eingesetzten Informatikmittel (Hard- und Software) entsprechen internationalen und branchenüblichen Standards. Die Informatikmittel unterliegen einem geregelten Life-Cycle-Management Prozess.

Die Konfiguration der Informatikmittel wird in Betriebshandbüchern dokumentiert und bei Bedarf aktualisiert.

15. Verfahren zur Ausübung der Rechte der betroffenen Personen

Betroffene Personen können sich für die Ausübung der Rechte gemäss DSG an den betrieblichen Datenschutzbeauftragten wenden:

CONCORDIA Schweizerische Kranken-
und Unfallversicherung AG
Datenschutzbeauftragter
Bundesplatz 15
6002 Luzern