



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.....	4
4. Organigramm des die Datensammlung betreibenden Organs.....	4
5. Verantwortlichkeiten.....	4
6. Dokumentation über die Planung, Realisierung und den Betrieb der Datensammlung	5
7. Anmeldung der Datensammlung beim EDÖB nach Rücksprache mit DSB	5
8. Prozessdokumentation welche die Datensammlungen betreffen	5
9. Die Herkunft der Daten	5
10. Die Zwecke, für welche die Daten regelmässig bekannt gegeben werden	5
11. Die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen nach Art. 20 VDSG	5
11.1 Zugangskontrolle.....	5
11.2 Datenträgerkontrolle.....	5
11.3 Transportkontrolle	6
11.4 Bekanntgabekontrolle.....	6
11.5 Speicherkontrolle	6
11.6 Benutzerkontrolle	6
11.7 Zugriffskontrolle.....	6
11.8 Eingabekontrolle (Protokollierung).....	6
12. Die Beschreibung der Datenfelder und die Organisationseinheiten, die darauf Zugriff haben.....	6
13. Art und Umfang des Zugriffs der Benutzer der Datensammlung	6
14. Die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung (Pseudonymisierung), Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten	7
15. Die Konfiguration der Informatikmittel	7
16. Verfahren zur Ausübung des Auskunftsrechts	7

1. Ausgangslage

Die CONCORDIA Schweizerische Kranken- und Unfallversicherung AG ist Inhaberin der automatisierten Datensammlung nach KVG. Die Datensammlung bezweckt die Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung gemäss Bundesgesetz über die Krankenversicherung (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 und als Inhaberin der automatisierten Datensammlungen das dafür verantwortliche Organ.

3. Schnittstellenbeschreibung

3.1 Schnittstellen zu externen Datenbezüglern 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 Inhaberin der Datensammlung weiterhin verantwortlich für die Einhaltung des Datenschutzes für die ausgelagerten Bereiche (Art. 22 VDSG).

Im Rahmen der Durchführung und Abwicklung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung gemäss KVG unterhält die CONCORDIA Schnittstellen zu Datenbezüglern und Datenlieferanten, welche nachfolgend beschrieben werden.

Empfänger/Lieferant	Zweck	Besonders schützenswerte Daten	Auslöser
Banken	Zahlungsverkehr	nein	Automatisch
Behörden/Gerichte	Art. 82 KVG, Art. 84a KVG	ja	Manuell
Externe Druckerei	Kundenmagazin	nein	Automatisch
Finanzdienstleister	Bankenstamm	nein	Automatisch
Gemeinsame Einrichtungen KVG	Risikoausgleich, Spitaltage	nein	Manuell
HMO Partner	Art. 84a KVG	ja	Manuell
Internetvergleichsdienste	Kalkulierte Offerte	nein	Automatisch
Kantone	IPV, KVG64	ja	Automatisch
Leistungserbringer	Art. 84a KVG, KVV59	ja	Automatisch / Manuell
Medidata	Austauschplattform von elektronischen Dokumenten	ja	Automatisch

Empfänger/Lieferant	Zweck	Besonders schützenswerte Daten	Auslöser
Partner Telemedizinische Dienstleistungen	Gesundheitsbetreuung	ja	Manuell
Santésuisse	Auskünfte, ZSR, Datenpool	nein	Automatisch
Sedex	IPV	ja	Automatisch
Sozialversicherer	Art. 84a KVG	ja	Manuell
SwissPost Solution	Anzeigen der Zahlungsbelege	nein	Manuell
VEKA	Versichertenkarte (KVG Art. 42a, VVK)	Ja	Automatisch
Versicherte	Auskunft, Korrespondenz, Leistungsabrechnungen	ja	Automatisch / Manuell
ZVR	Auskunft	nein	Manuell

3.2 Datenherkunft

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

4. Organigramm des die Datensammlung betreibenden Organs

Organigramm der CONCORDIA Kranken- und Unfallversicherung AG



5. Verantwortlichkeiten

Die Geschäftsleitung der CONCORDIA Schweizerische Kranken- und Unfallversicherung AG trägt als Inhaberin der Datensammlung 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 Datensammlung

Der Betrieb der Datensammlung 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 der Datensammlung beim EDÖB nach Rücksprache mit DSB

Die CONCORDIA Schweizerische Kranken- und Unfallversicherung AG hat gemäss Art. 11a Abs. 5 lit. e DSGVO einen Datenschutzverantwortlichen bezeichnet, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt. Damit ist die CONCORDIA von der Anmeldepflicht der Datensammlung beim EDÖB gemäss Art. 11a Abs. 2 DSGVO befreit.

Die CONCORDIA erfüllt die Vorlagepflicht an den EDÖB gemäss Art. 84b KVG.

8. Prozessdokumentation welche die Datensammlungen betreffen

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

9. Die Herkunft der Daten

Siehe Tabelle Kapitel 3

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

Siehe Tabelle Kapitel 3

11. Die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen nach Art. 20 VDSG

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 in den Richtlinien „Zutritt zu Betriebsliegenschaften der CONCORDIA“ und „Zutritts- und Schliessorganisation“ geregelt.

Für den Zutritt zu den Informatikräumlichkeiten gibt es eine zusätzliche Weisung „Zutrittsrechte bei der Informatik“.

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. Zentral ist die Weisung „Umgang mit Hardware, Software und elektronischen Daten“.

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. Die Beschreibung der Datenfelder und die Organisationseinheiten, die darauf Zugriff haben

Im Rahmen des Meldeprozesses der Datensammlung werden in separaten Bearbeitungsreglementen die Datenfelder beschrieben und das Berechtigungskonzept dokumentiert.

13. Art und Umfang des Zugriffs der Benutzer der Datensammlung

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.

Auf MCD-Daten (minimal clinical dataset), welche bei der unabhängigen Datenannahmestelle eingehen und durch diese automatisiert verarbeitet werden, haben die Mitarbeitenden der CONCORDIA keinen Zugriff. Werden Rechnungen durch die Datenannahmestelle zur Überprüfung ausgelenkt, erhalten die mit der Fallüberprüfung beauftragten Mitarbeitenden bis zum Fallabschluss Zugriff auf die Rechnungen sowie die dazugehörigen MCD.

14. 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 (siehe auch Kapitel 13 - 15).

Benutzer einer Datensammlung werden regelmässig in Belangen des Fachprozesses und des Datenschutzes geschult.

15. 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.

16. Verfahren zur Ausübung des Auskunftsrechts

Auskunftsbegehren gemäss Art. 8 DSG sind an den betrieblichen Datenschutzbeauftragten zu richten:

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