
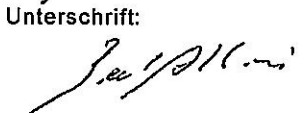


Bearbeitungsreglement

MCD-Datensatz in der Datenannahmestelle von Sanitas

Datensammlung Nr. 89
der
Sanitas Grundversicherungen AG
Sanitas Management AG
Jänergasse 3, 8004 Zürich

Version Nr.:	6.2	Datum Inkraftsetzung:	01.05.2023
		Ersetzt Version vom	01.04.2022
Dokumentenowner	DSB	Datum: 26.04.2023	Unterschrift: 
	Leiter DAS	Datum: 4.4.2023...	Unterschrift: 
Ablage Original:	Confluence / Laufwerk Datenannahmestelle		
Klassifizierung	Öffentlich		

Versionierung

Grund für die Änderung Übersicht was gegenüber der alten Version geändert worden ist	V6.2: <ul style="list-style-type: none">• Klassifizierung ergänzt, öffentlich• Heureka entfernt
Übergangslösung (Beschreibung, Gültigkeitsdauer – falls es eine Übergangslösung gibt)	n/a

Inhaltsverzeichnis

ABKÜRZUNGEN.....	4
1. ZWECK.....	5
2. INHABER, DATENOWNER UND VERWALTER DER DATENSAMMLUNG NR. 89.....	5
3. APPLIKATION KOLUMBUS	6
4. ART UND ZWECK DER DATENSAMMLUNG.....	6
5. ERFASSTE PERSONENDATEN UND HERKUNFT DER DATEN.....	7
6. DATENAUSTAUSCH / SCHNITTSTELLENBESCHREIBUNG	8
6.1. Datenaustausch / Schnittstellen mit <i>externen</i> Stellen	8
6.1.1. <i>Daten-Import</i>	8
6.1.2. <i>Daten-Export</i>	8
6.2. Datenaustausch / Schnittstellen mit <i>internen</i> Stellen	9
6.2.1. <i>Daten-Import</i>	9
6.2.2. <i>Daten-Export</i>	9
7. DATENÜBERMITTLUNG INS AUSLAND	10
8. ZUGRIFFSBERECHTIGUNG	10
9. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN NACH ART. 9 VDSG	11
9.1. Zugangskontrolle.....	11
9.2. Personendatenträgerkontrolle.....	11
9.3. Authentifizierung.....	11
9.4. Bekanntgabekontrolle.....	11
9.5. Chiffrierung.....	11
9.6. Speicherkontrolle	12
9.7. Mobile Speichergeräte	12
9.8. Home Office	12
9.9. Protokollierung.....	12
9.10. Programmentwicklung.....	12
9.11. Backup / Restore.....	12
9.12. Schulung.....	12
10. DATENBEARBEITUNGSVERFAHREN (ART. 21, ABS. 2, LIT. G VDSG)	12
10.1. Berichtigungsverfahren	12
10.2. Archivierung	12
10.3. Backup/Restore.....	13
10.4. Protokollierung.....	13
11. VERFAHREN ZUR AUSÜBUNG DES AUSKUNFTSRECHTS (ART. 21 ABS. 2 LIT. I VDSG) ..	13
12. MITGELTENDE BESTIMMUNGEN	13
12.1. Weisungen	13
12.2. Handbuch.....	14
12.3. Prozesse.....	14
13. SCHLUSSBESTIMMUNG UND INKRAFTTRETEN.....	14

Abkürzungen

DASA	Datensammlung ¹
DMS	Dokumenten- Management- System (elektronisches Archiv)
DRG	Diagnosis Related Groups (Diagnosebezogene Fallgruppen). Es handelt sich um ein einheitliches Patientenklassifikationssystem, welches die Patienten anhand von Kriterien wie u.a. Diagnosen, Behandlungen und Alter, in möglichst homogene Gruppen einteilt.
DSB	Datenschutzbeauftragter von Sanitas
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Datenschutzgesetz)
EDI	Electronic Data Interchange
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung (Krankenversicherungsgesetz)
KVV	Verordnung über die Krankenversicherung
MCD	Das Minimal Clinical Dataset bezeichnet die Angaben, welche für die Krankenversicherung zur Kontrolle der Spitalrechnungen nötig sind. Dazu gehören auch die Diagnosen und Prozeduren.
OKP	Obligatorische Krankenpflege
PCG	Psychiatric Cost Group
RCG	Rehabilitation Cost Group
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993
VVG	Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (Versicherungsvertragsgesetz)
VA	Vertrauensarzt
VAD	Vertrauensärztlicher Dienst
ZSR	Zahlstellenregister

¹ Falls es sich um einen Datenpool handelt, ist im Reglement der Begriff „Datensammlung“ bzw. DASA im Sinne von „Datenpool“ [ein Datenpool liegt vor, wenn mehrere DASA miteinander verknüpft sind und auf der gleichen Applikation laufen, wie z.B. Syrius] zu verstehen.

1. Zweck

Sanitas legt grossen Wert auf den Schutz von besonders schützenswerten Daten der Datenannahmestelle und informiert in diesem Bearbeitungsreglement:

- Wer für die Datenbearbeitung in der Datenannahmestelle verantwortlich ist
- Von welchen Personen welche Daten erhoben und bearbeitet werden
- Wie und von wem die Daten erhoben und bearbeitet werden
- Zu welchem Zweck die Daten bearbeitet werden und basierend auf welcher rechtlichen Grundlage dies erfolgt
- Wie lange Daten aufbewahrt werden
- Was die Rechte der betroffenen Personen sind

2. Inhaber, Datenowner und Verwalter der Datensammlung Nr. 89

Inhaberin der Datensammlung (DASA) gem. Art. 3 lit. 1 DSG ist die Sanitas Grundversicherungen AG. Die Sanitas Gruppengesellschaften haben die Leistungserbringung innerhalb der Sanitas Gruppe mit Vertrag vom 28. Juni 2008 geregelt. Die Inhaberin der DASA hat mit den anderen Gruppengesellschaften eine Dienstleistungsvereinbarung abgeschlossen, in der die zu erbringenden Dienstleistungen geregelt werden.

Die Sanitas Grundversicherungen AG betreibt für die in der OKP tätigen Gesellschaften der Sanitas Gruppe eine Datenannahmestelle gemäss Art. 59a KVV.

Die DASA liegt in der Zuständigkeit des Geschäftsbereichs Leistungen und Kundenberatung.

Da es sich bei den bearbeiteten Daten in erster Linie um hochsensitive Personendaten der Leistungsabwicklung handelt, ist der Leiter des Geschäftsbereichs Leistungen und Kundenberatung insbesondere für Fragen und die betroffenen Leistungsprozesse zuständig. Zudem obliegen dem Datenschutzbeauftragten von Sanitas diverse Aufgaben im Rahmen seines Aufgabengebiets.

Datenowner² gemäss Weisung A-0015 «Datensammlungen und Bearbeitungsreglemente» ist der Leiter Datenannahmestelle. Er trägt die Gesamtverantwortung für die DASA Nr. 89.

Der Verwalter der DASA wird vom Leiter Datenannahmestelle ernannt. Er ist für die administrativen Belange der Datensammlung zuständig und Kontaktperson für Datenschutzfragen im Zusammenhang mit der DASA.

Da Sanitas einen Datenschutzbeauftragten (DSB) ernannt hat, ist diese Datensammlung nicht beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemäss Art. 16 VDSG gemeldet.

² Der Datenowner ist der bei Sanitas intern Verantwortliche für eine Datensammlung. In der Regel handelt es sich um eine Leiterin / einen Leiter eines Geschäftsbereichs. Es dürfen aber auch andere Personen Datenowner sein.

3. Applikation Kolumbus

Die Datensammlung läuft auf der Applikation³ Kolumbus. Der Betrieb der Applikation wurde gestützt auf Art. 84 KVG bzw. Art. 10a DSG an die Swisscom Schweiz AG ausgelagert.

Der Applikationsowner⁴ ist auf einer separaten Liste, die im Sanitas Intranet (SanWeb) aufgeschaltet ist, festgehalten. Die Server, auf denen die Applikation betrieben wird, stehen im:

- Rechenzentrum Bern Wankdorf: Bern, Stauffacherstrasse 59
- Rechenzentrum Bern Zollikofen: Zollikofen, Industriestrasse 30 (Ausfall – RZ)

Der Vertrag mit Swisscom Schweiz AG enthält spezifische Datenschutz- und Datenbearbeitungsklauseln.

Falls die Applikation nicht durch die Inhaberin der DASA betrieben wird:

- | | |
|--|----|
| ▪ Der IT-Dienstleistungsprovider verfügt über die erforderlichen Sicherheitsvorkehrungen: | ja |
| ▪ Die IT-Sicherheitsvorkehrungen sowie die Einhaltung des Datenschutzes werden jährlich nach ISAE 3402 Typ II geprüft: | ja |
| ▪ Der Vertrag mit dem IT-Dienstleistungsprovider enthält eine spezielle Datenschutz- bzw. Datenbearbeitungsklausel | ja |

4. Art und Zweck der Datensammlung

Bei der Datensammlung handelt es sich um eine automatisierte Datensammlung gemäss Art. 21 VDSG.

Im Kolumbus werden die Datensätze mit den medizinischen Rechnungsdaten (MCD), welche Sanitas von den Spitälern erhält, gemäss Vorgaben SwissDRG bearbeitet. Mit Kolumbus wird mittels einer vollständig automatisierten Rechnungskontrolle, auch Dunkelprüfung genannt, eine Triage der Rechnungen vorgenommen. „Unauffällige“ Rechnungen werden zur Zahlung freigegeben, ohne dass ein Mitarbeitender der Leistungsverarbeitung von Sanitas die Rechnungen und namentlich das MCD sieht.

„Auffällige“ Rechnungen werden zur manuellen, vertieften Überprüfung ausgelenkt und der ausgewählten Mitarbeitenden der Leistungsverarbeitung von Sanitas zur Einsicht zur Verfügung gestellt.

Sofern angeforderte MCD in Papierform eintreffen, werden diese gemäss Weisung L.W-0247 verarbeitet und umgehend nach der Erfassung im Kolumbus datenschutzkonform vernichtet. Unaufgefordert zugestellte MCD in Papierform werden sofort datenschutzkonform vernichtet.

³ Siehe Applikationslandkarte im SanWeb

⁴ Siehe IT Architektur-Steckbrief inklusive Personendaten im SanWeb.

5. Erfasste Personendaten und Herkunft der Daten

In der Datensammlung werden Daten von natürlichen Personen gesammelt. Zudem ist über die ZSR-Nummer ersichtlich, welcher Leistungserbringer / welches Spital die Behandlung durchgeführt bzw. die Rechnung und das MCD zugestellt hat.

Folgende Kategorien von Personendaten werden in der Datensammlung erfasst:

Kategorie	Beschreibung
<input checked="" type="checkbox"/> Stammdaten 1	Name, Vorname, PLZ, Ort, Telefon-Nummer, Email-Adresse, Geschlecht, Familienstellung
<input checked="" type="checkbox"/> Stammdaten 2	Zivilstand, Heimatort, Nationalität, Niederlassungsbewilligung, Geburtsdatum, Todesdatum
<input type="checkbox"/> Stammdaten 3	Sozialversicherungsnummer, Lohn (versicherte Person), Arbeitgeber der versicherten Person
<input checked="" type="checkbox"/> Leistungsdaten 1	Behandlungsgrund, Behandlungsdatum, Unfalldatum
<input checked="" type="checkbox"/> Leistungsdaten 2	Kostenart, Tarmed-Tarifposition, Diagnosecode, DRG/PCG/RCG -Code
<input type="checkbox"/> Finanzdaten 1	Prämienverbilligung, Bankverbindung
<input type="checkbox"/> Finanzdaten 2	KOBE, Taggeld (ausbezahltes), Kapitaleistungen (ausbezahlte), offene Posten, Mahnungen
<input type="checkbox"/> Finanzdaten 3	Betreibung, Sozialleistungen, Vormundschaft, Pfändung, Leistungssperre, Zahler/Empfänger, Abzahlungsvereinbarung
<input checked="" type="checkbox"/> Vertrags-Produktdaten	Policen-Nummer, Offerten-Nummer, Rahmenvertrags-Nummer, Vertragsdaten (Produkt, Prämie etc.), Vorversicherer, Nachversicherer
<input type="checkbox"/> Vertragsnummer	
<input type="checkbox"/> Partnernummer	
<input type="checkbox"/> Provisionsdaten	Makler / Vermittler (Name, Adresse), Provision, Superprovision, Bonus
<input checked="" type="checkbox"/> Referenzdaten	Leistungserbringer (Name, Adresse, ZSR-Nummer), Bank-Clearing, PLZ, Gemeindefile
<input type="checkbox"/> Underwriting	Gesundheitsdeklaration (im Rahmen des VVG-Antrages), Vorbehalt
<input type="checkbox"/> Weitere ⁵	

Bemerkungen: keine

Bei den Leistungsdaten handelt es sich um besonders schützenswerte Daten gemäss Art. 3 lit. c DSGVO, sofern sie einem Versicherten zugeordnet werden können.

⁵ Wenn die Personendaten, die sich in der DASA befinden nicht in dieser Tabelle aufgeführt sind, ist konkret anzugeben, um welche Daten es sich handelt (Beispiel: "Arztberichte" sind nicht erwähnt, müssen also spezifisch erwähnt werden).

6. Datenaustausch / Schnittstellenbeschreibung

6.1. Datenaustausch / Schnittstellen mit externen Stellen

In den nachfolgenden Tabellen ist der Datenaustausch (Datenimport bzw. -export) mit Dritten ausserhalb der Sanitas Gruppe dargestellt.

6.1.1. Daten-Import

Von ⁶	Zweck	Daten/-kategorie ⁷	Periodizität (z.B. wöchentlich, monatlich, sporadisch)	Auslöser (manuell / System)	Medium (E-Mail, CD, Batch-Filetransfer, etc.)	Gesetzliche/ Vertragliche Grundlage	Vertrag mit Datenlieferant ⁸
Leistungserbringer	Leistungsabrechnung	Siehe Ziffer 5	Laufend	System	Filetransfer	Art. 42 / 56 KVG Art. 59a KVV	Mit Spitälern

Bemerkungen: keine

6.1.2. Daten-Export

Empfänger ⁹	Zweck	Daten/-kategorie ¹⁰	Periodizität (z.B. wöchentlich, monatlich, sporadisch)	Auslöser (manuell / System)	Medium (E-Mail, CD, Batch-Filetransfer, etc.)	Gesetzliche/ Vertragliche Grundlage	Vertrag mit Datenempfänger ¹¹

Bemerkungen: Es gibt keinen Datenexport.

⁶ Name des Dritten bzw. Kategorie, wie z.B. Leistungserbringer, Behörde etc.

⁷ Der Einfachheit halber können auch Datenkategorien verwendet werden; siehe oben Ziff. 5

⁸ Sanitas-ID gemäss Vertragsdatenbank SAP Ariba, bzw. pauschal „Vertrag mit Leistungserbringer“.

⁹ Name des Dritten bzw. Kategorie, wie z.B. Leistungserbringer, Behörde etc.

¹⁰ Der Einfachheit halber können auch Datenkategorien verwendet werden; siehe oben Ziff. 5.

¹¹ Sanitas-ID gemäss Vertragsdatenbank SAP Ariba

6.2. Datenaustausch / Schnittstellen mit *internen Stellen*

In den nachfolgenden Tabellen ist der Datenaustausch mit anderen Datensammlungen bzw. mit anderen Stellen/Bereichen innerhalb der Sanitas Gruppe dargestellt.

6.2.1. Daten-Import

Von ¹²	Zweck	Daten/-kategorie ¹³	Periodizität (z.B. wöchentlich, monatlich, sporadisch)	Auslöser (manuell / System)	Medium (E-Mail, CD, Batch-Filetransfer, etc.)
Syrius	Import von elektronisch übermittelten Rechnungs- und MCD Daten	Siehe Ziff. 5	Montag bis Samstag, mehrmals täglich	System	Microservice
Syrius	Import der Versicherungsnehmer Stammdaten	Stammdaten	Montag bis Freitag (Delta)	System	Datenbank, Microservice
Leistungserbringer Vertragsdatenbank	Import der Spitalbaserates sowie der kantonalen Kostenteiler und kantonalen Referenzbaserates	Referenzdaten	Jährlich	Manuell	Excel-File

6.2.2. Daten-Export

Nach ¹⁴	Zweck	Daten/-kategorie ¹⁵	Periodizität (z.B. wöchentlich, monatlich, sporadisch)	Auslöser (manuell / System)	Medium (E-Mail, CD, Batch-Filetransfer, etc.)
Kolumbus-DWH	Erstellung von Auswertungen, insb. zur Regelwerkeinstellungen	Es werden alle Datenkategorien ins DWH überführt (MCD pseudonymisiert)	täglich	System	Script

Bemerkungen: Die Daten im DWH werden „pseudonymisiert“, d.h. die Personen, welche Auswertungen vornehmen, sehen keine Versichertennummern und keine Kunden-, Vertrags- oder Rechnungsnummer.

¹² Name der DASA bzw. Bereich.

¹³ Der Einfachheit halber können auch Datenkategorien verwendet werden; siehe oben Ziff. 5.

¹⁴ Name der DASA bzw. Bereich.

¹⁵ Der Einfachheit halber können auch Datenkategorien verwendet werden, siehe oben Ziff. 5

7. Datenübermittlung ins Ausland

Es werden keine Daten ins Ausland übermittelt.

8. Zugriffsberechtigung

Der Zugriff auf die DASA wird nur berechtigten Personen gewährt. Zugriff haben grundsätzlich Mitarbeitende der in der obligatorischen Grundversicherung tätigen Gruppengesellschaften. Die Sanitas Gruppengesellschaften haben die Leistungserbringung innerhalb der Sanitas Gruppe mit Vertrag vom 28. Juni 2008 geregelt. Die Inhaberin der DASA hat mit den anderen Gruppengesellschaften eine Dienstleistungsvereinbarung abgeschlossen, in der die zu erbringenden Dienstleistungen geregelt werden.

Zugriff auf die DASA haben Mitarbeitende der Leistungsverarbeitung und des Leistungsmanagements Spital / Reha sowie Mitarbeiter des Vertrauensärztlichen Dienstes von Sanitas. Es erhalten nur diejenigen Mitarbeitenden, welche diesen für die Erledigung ihrer Arbeit benötigen. Die Anzahl der zugriffsberechtigten Personen richtet sich nach der Anzahl zu bearbeitender DRG-Rechnungen. Zudem muss die Stellvertretung sichergestellt sein.

Zugriff auf Versicherungsdaten von Sanitas Mitarbeitenden und damit auf die DASA Nr. 89 werden nur Mitarbeitenden des Vertrauensärztlichen Sekretariats, welche organisatorisch dem VAD unterstellt sind, gewährt (siehe Weisung A-0003 «Umgang mit Mitarbeiterdaten bei Sanitas»).

MCD, die vom Leistungserbringer gestützt auf Art. 42 Abs. 4 KVG mit dem sog. VA-Flag versehen sind, werden im Kolumbus verarbeitet. Auffällige Rechnungen werden ausgelenkt und ausschliesslich von Mitarbeitenden des VAD bearbeitet, welche vom LT VAD hierfür benannt werden.

Zugriffsberechtigungen sind im «Zugriffskonzept Kolumbus und Umsysteme» geregelt.

Administrative Zugriffe auf die Datenbank des vorgelagerten Systems haben nur definierte Personen der IT bzw. des Outsourcing-Partner.

Zugriff auf die DASA haben folgende Dritte ausserhalb der Sanitas Gruppe: IT- Dienstleister Swisscom Schweiz AG

Diese Dritte dürfen: Daten einsehen ☒

Daten eingeben/mutieren: ☒

9. Technische und organisatorische Massnahmen nach Art. 9 VDSG

9.1. Zugangskontrolle

Sämtliche Räumlichkeiten von Sanitas sind elektronisch vor dem Zugang durch unbefugte Personen gesichert. Details sind im Zutrittskonzept und in der daraus abgeleiteten Weisung A-0017 geregelt. Die Zutritte werden über die Applikation «KABA EXOS 9300» verwaltet und protokolliert.

Für die Vergabe von Zutrittsberechtigungen an Mitarbeitende und Dritte werden sämtliche Standorte/Gebäude/Räume aufgrund ihres Schutzbedarfes in (Sicherheits-) Zonen eingeteilt und einer Sicherheitsstufe zugewiesen. Der Schutzbedarf eines Raumes wird anhand der im Raum befindlichen materiellen und immateriellen Werte (z.B. Informationen, Personendaten) sowie anhand der Bedrohungslage bestimmt. Die Räume des VAD oder technische Räume sind der höchsten Schutzzone zugewiesen und dürfen nur von namentlich bekannten Personen betreten werden.

Die Räume des VAD sind von der Leistungsverarbeitung getrennt.

Als zusätzliche Sicherheitsmassnahme wurde für die Mitarbeitenden mit Zugriff auf ausgelenkte MCDs separate Büros eingerichtet, die batchgesichert sind. Zu diesen Räumlichkeiten haben nur für die Bearbeitung von MCDs berechnete Mitarbeitende Zutritt. Ebenfalls Zutritt haben Reinigungs- und Sicherheitspersonal, wobei diese Personen aufgrund der Arbeitszeit keine Einsicht auf MSC Rechnungen haben können.

Der Zutritt zu den Räumen der Swisscom Schweiz AG ist ebenfalls gesichert.

9.2. Personendatenträgerkontrolle

Durch informationstechnische Sicherheitsvorkehrungen können ausschliesslich berechnete Personen Daten in Kolumbus und den Umsystemen bearbeiten bzw. einsehen.

9.3. Authentifizierung

Der Zugriff auf die Systeme von Sanitas ist durch die User-ID kombiniert mit einem befristeten Passwort geschützt. Der Umgang mit Passwörtern ist in der Weisung A-0021 «Informatik- und Telekommunikationsmittel am Arbeitsplatz» geregelt.

9.4. Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, sind identifiziert (siehe auch Ziffer 6.2).

9.5. Chiffrierung

Da die Daten genügend gesichert sind und eine Chiffrierung vom Gesetzgeber nicht verlangt wird, werden die Daten nicht chiffriert.

9.6. Speicherkontrolle

Die Benutzer haben aufgrund ihrer Rolle und den damit verbundenen Zugriffsrechten im Kolumbus die Möglichkeit, Datenfelder zu mutieren bzw. Simulationen durchzuführen, welche zu Mutationen führen können.

9.7. Mobile Speichergeräte

Der Umgang mit mobilen Speichergeräten ist in der Weisung A-0013 «Umgang mit mobilen Speichermedien» geregelt.

9.8. Home Office

Arbeiten von zuhause ist mittels Laptop über VPN (2FA) möglich und unterliegt den gleichen Sicherheitsbestimmungen wie das Arbeiten in den Büros von Sanitas (siehe Weisung A-0022 «Home Office bei Sanitas»). Es gelten die Sicherheitshinweise für das Arbeiten im Homeoffice als Ergänzung zu den Weisungen «Datenschutz» (A-0014) und «Homeoffice bei Sanitas» (A-0022).

9.9. Protokollierung

Die Bearbeitung von Daten durch berechtigte Benutzer wird im Kolumbus protokolliert. Es werden für die Ereignisse „Anlage“, „Letzte Bearbeitung“, „Stornierung“, „Freigabe“ und „Prüfstatus“ jeweils Datum/Zeit und der User festgehalten. Diese Informationen werden während eines Jahres revisionssicher aufbewahrt.

9.10. Programmentwicklung

Es wird eine Trennung zwischen Entwicklung, Test und Produktion eingehalten. Die Entwicklung von Kolumbus liegt beim SW-Lieferanten.

9.11. Backup / Restore

Das Backup der Daten ist im Vertrag mit der Swisscom Schweiz AG geregelt-> siehe auch Punkt 10.3

9.12. Schulung

Zugriffsberechtigte Mitarbeitende werden regelmässig fach- und anwendungstechnisch sowie in Bezug auf den Datenschutz geschult.

10. Datenbearbeitungsverfahren (Art. 21, Abs. 2, lit. g VDSG)

10.1. Berichtigungsverfahren

Die in der DASA erfassten Personen können nach erfolgter Identifizierung verlangen, dass über sie erfasste Daten berichtigt werden.

10.2. Archivierung

Die Archivierung der Daten erfolgt gemäss Vertrag mit dem Dienstleister (Swisscom Schweiz AG) und ist wie folgt geregelt: ist im System gespeichert.

10.3. Backup/Restore

Das Backup der Daten erfolgt gemäss Vertrag mit dem Dienstleister Swisscom Schweiz AG und ist wie folgt geregelt: tägliche Sicherung während den Werktagen. -> siehe auch Punkt 9.11

10.4. Protokollierung

Die Protokollierung der Datenbearbeitung ist wie folgt geregelt:

Jede Aktion oder Bearbeitung der Daten wird durch das Kurzzeichen des Mitarbeiters protokolliert.

11. Verfahren zur Ausübung des Auskunftsrechts (Art. 21 Abs. 2 lit. i VDSG)

Das Auskunftsrecht wird detailliert in der Weisung A-0018 «Auskunftsverfahren nach Datenschutzgesetz» geregelt. Grundsätzlich gilt, dass Auskunftsbegehren schriftlich und unter Beilage eines Identitätsnachweises erfolgen müssen.

12. Mitgeltende Bestimmungen

Folgende Weisungen, Handbücher und Prozesse sind auf die Datensammlung bzw. dieses Reglement anwendbar:

12.1. Weisungen

Nummer	Titel
A-0003	Umgang mit Mitarbeiterdaten bei Sanitas
A-0013	Umgang mit mobilen Speichermedien
A-0012	Informationssicherheit
A-0014	Datenschutz
A-0015	Datensammlungen und Bearbeitungsreglemente
A-0017	Zutritt zu Gebäuden und Räumen von Sanitas - Badgeverwaltung
A-0018	Auskunftsverfahren nach Datenschutzgesetz
A-0021	Informatik- und Telekommunikationsmittel am Arbeitsplatz
A-0022	Home Office bei Sanitas
L.W-0240	Medizinische Prüfung von SwissDRG/TARPSY/ST Reha- Rechnungen ohne/mit elektronischem MCD bei zertifizierter Datenannahmestelle (DAS)
L.W-0244	Umgang mit medizinischen Daten und KOLUMBUS bei zertifizierter Datenannahmestelle (DAS)
L.W.-0247	Bearbeitung von SwissDRG/TARPSY/ST Reha- Rechnungen mit/ohne MCD in Papierform

12.2. Handbuch

Anwenderhandbuch Kolumbus SwissDRG vom Lieferanten

12.3. Prozesse

- DRG/PCG/RCG Rechnung in Kolumbus prüfen und MCD vernichten
- DRG/PCG/RCG Medizinische Prüfung von Rechnung und MCD in Kolumbus durchführen
- SwissDRG/TARPSY/ST Reha- Regelwerkanforderung prüfen und in Kolumbus anpassen
- SwissDRG/TARPSY/ST Reha- Regelwerk in Kolumbus analysieren Die Prozesse sind im Prozess Management Tool dokumentiert.

13. Schlussbestimmung und Inkrafttreten

Der Datenowner bzw. der Verwalter kontrolliert mindestens einmal pro Jahr, ob das Bearbeitungsreglement und die interne Anmeldung der Datensammlung beim DSB noch aktuell sind. Er meldet das Ergebnis seiner Kontrolle dem DSB von Sanitas.