

Bearbeitungsreglement der SwissDRG-Datenannahmestelle (DAS) der Krankenkasse vita surselva

Inhaltsverzeichnis

1. Versionskontrolle	3
1.1. Änderungskontrolle	3
1.2. Freigabe	3
1.3. Offene Punkte	3
2. Allgemeines	4
2.1. Einführung	4
2.2. Scope	4
2.3. Rechtliche Grundlagen	5
2.3.1. KVG	5
2.3.2. KVV	5
2.3.3. DSG	5
2.4. Zuständigkeiten und Verantwortung	6
2.5. Anmeldung Datensammlung beim EDÖB (Art. 16 VDSG)	6
2.6. Kontaktstelle bezüglich datenschutzrechtlichen Fragen:	6
2.7. Organigramm	7
2.8. Schweigepflicht nach Art. 33 ATSG	7
2.9. Datensicherheit	7
3. Übersicht der Datenbearbeitungsstruktur	7
3.1. Übersicht der Schnittstellen	9
3.1.1. Verarbeitung elektronisch	9
3.1.2. Verarbeitung Papier	10
4. Beteiligte Organisationseinheiten	11
4.1. H-Net AG	11
4.2. Secon AG	11
4.3. ELCA	11
4.4. Krankenkasse	11
4.5. Interne DAS	11
4.6. Vertrauensärztlicher Dienst	11
4.6.1. Aufgaben	11
4.6.2. Terminologie	11
5. Der Datenbearbeitungsprozess	12
5.1. Übersicht	12
5.2. Implikation des Vertrauensarztes	12
5.3. Prüfung von stationären Leistungsabrechnungen	13

Dateiname: Bearbeitungsreglement SwissDRG-DAS.docx
Erstellungsdatum: 22.05.2015
Letzte Änderung: 29.08.2020
Datum: 29.08.2020


5.3.1. Überblick und Begriffliches	13
5.3.2. Erste Prüfstufe: Dunkelprüfung	13
5.3.3. Zweite Prüfstufe: Triage	13
5.3.4. Dritte Prüfstufe: Prüfung durch den VA	14
5.4. Rechnung/MCD in Papierversion	14
5.4.1. Allgemein	14
5.4.2. Bearbeitung durch die interne DAS	15
5.4.3. Bearbeitung durch den VA/VAD	15
5.5. Outsourcing	16
5.6. Auslenkungskriterien	16
5.6.1. Änderung der Auslenkungskriterien	16
5.7. Auswertungen	16
6. Zugriff	16
6.1. Zugriffsdifferenzierung	16
6.2. Authentisierung durch Passwörter	16
7. Datenbearbeitung	17
7.1. Zweck der Datenbearbeitung	17
7.2. Datenherkunft	17
7.3. Datenbearbeitung	17
8. Technische, organisatorische und personelle Massnahmen	17
8.1. Zugangskontrollen	17
8.2. Instruktion und Schulung des Personals	17
9. Interne und externe Kontrollen	17
9.1. Massnahmen auf Unternehmungsebene	17
9.2. Kontrollen durch das Management	18
9.3. Kontrollen auf Prozessebene	18
9.4. IT-Kontrollen	18
9.5. Interne Audits	18
10. Archivierung und Vernichtung von Daten	18
11. Rechte der Versicherten	19
11.1. Auskünfte über Datenbearbeitungen	19
11.2. Berichtigungs- und Lösungsrechte	19
12. Abschliessende Bestimmungen	20
12.1. Verlinkte Dokumente	20
12.2. Änderungen des Reglements	20
12.3. Inkrafttreten	20

1. Versionskontrolle

1.1. Änderungskontrolle

Datum	Version	Name	Beschreibung
13.05.2014	0.1	Die Advokatur Sury AG / end	Erstellung
20.05.2014	0.2	Die Advokatur Sury AG / end	Anpassung
05.06.2014	0.3	Die Advokatur Sury AG / end	Anpassung
10.06.2014	0.4	Die Advokatur Sury AG / end	Anpassung
07.11.2014	1.1	Die Advokatur Sury AG / end	Anpassung Inhalt
03.12.2014	1.2	Die Advokatur Sury AG / end	Anpassung Format
27.04.2014	1.3	Cavigelli D. / Deplazes I.	Überarbeitung der Formulierungen / Anpassung Format
27.08.2015	1.4	vita surselva DCav IDep	Ergänzung 5.4.
18.11.2015	1.5	vita surselva DCav IDep	Ergänzung gemäss Auditbericht vom 29.09.2015
01.12.2015	1.6	vita surselva DCav	Ergänzung
07.12.2015	1.6	vita surselva IDep	Überarbeitung der Grafiken in Punkt 3.1.1
13.05.2016	1.7	vita surselva IDep	Anpassung Organigramm
20.09.2016	1.7	vita surselva IDep	Prüfung des Dokuments
01.02.2017	1.8	vita surselva MArp IDep	Anpassung gemäss Auditbericht vom 20.09.2016 (Minor NC 3 & 4)
24.10.2017	1.9	vita surselva IDep	Anpassung PC13 -> PC02
01.07.2019	1.10	Deplazes I.	Dokument geprüft und an neue Dateibenennungen und Dateiverweise angepasst
02.07.2019	1.10	Deplazes I.	Organigramm angepasst
04.11.2019	1.11	Deplazes I.	Dokument an Lizenzübertragung der SUVA an ELCA angepasst.
11.06.2020	1.12	Deplazes I.	Punkt 2.7 Organigramm angepasst
15.08.2020	1.12	Deplazes I.	Punkt 2.3 Gesetzliche Grundlagen überarbeitet und alle Gesetzestexte verlinkt

1.2. Freigabe

Datum	Version	Name	Beschreibung
29.08.2020	1.12	Ivan Deplazes	Stv. Geschäftsführer  Unterschrift:

1.3. Offene Punkte

Datum	Name	Thema

2. Allgemeines

2.1. Einführung

Das Bearbeitungsreglement umschreibt die Datenverarbeitungs- und Kontrollverfahren und den Betrieb der elektronischen Datenverarbeitung im Rahmen der SwissDRG-Rechnungsstellung (bezogen auf stationäre Leistungen) an die zugehörige Datenannahmestelle und die Bearbeitung der Rechnungen in Papierform. Es enthält Angaben über das für den Datenschutz und die Datensicherheit verantwortliche Organ, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden und beschreibt das Verfahren für die Erteilung der Zugriffsberechtigung auf die Daten, die im Rahmen der SwissDRG-Rechnungsstellung von der Datenannahmestelle bearbeitet werden, und von den Krankenkassen in diesem Rahmen empfangen bzw. weitergeleitet werden.

Der Zweck der Datenverarbeitung, für die dieses Bearbeitungsreglement gilt, ist die Leistungs- und Kostenkontrolle der Leistungserbringer im Rahmen des KVG, und die anschliessende Bezahlung oder Beanstandung der Rechnung.

Dieses Reglement gilt für alle Mitarbeitenden der Krankenkasse.

2.2. Scope

Der Scope dieses Bearbeitungsreglementes umfasst das Datenschutzmanagementsystem der Krankenkasse in den folgenden Bereichen und Schnittstellen:

- Eingehende Post (elektronisch und in Papierform) und deren Bearbeitung: Schnittstelle zwischen outgesourcten Elementen und der Krankenkasse. Insbesondere ist die DRG-Dunkelprüfung outgesourct.
- Die H-Net AG ist die Schnittstelle für die Rechnungszustellung zwischen Leistungserbringer und die Datenannahmestelle bei der Secon AG.
- Die Secon AG, in Zusammenarbeit mit der ELCA, ist als Outsourcingpartner der Krankenkasse für die meisten Tätigkeiten der DAS zuständig. Die Krankenkasse bleibt jedoch für die Tätigkeiten der Secon AG verantwortlich. Die Secon AG ist VDSZ zertifiziert.
- Die Sendung der Rechnung und des MCDs vom Leistungserbringer via H-Net an die Secon AG. Die Sondierung der MCD's durch die Secon AG und Weiterleitung an die ELCA für die DRG-Dunkelprüfung. Die Rechnung (ohne MCD) wird auf dem sftp-Server (Secure File Transfer Protocol) für die Krankenversicherung zur Verfügung gestellt. Das Resultat der DRG-Dunkelprüfung, ob das MCD auffällig oder nicht auffällig ist, wird an die Secon AG übermittelt, Das Resultat der DRG-Dunkelprüfung (0 oder 1) wird mit der Rechnungsnummer in ein Textdokument gespeichert. Dieses Textdokument stellt die Secon AG auf dem „sftp-Server“ für die Krankenversicherung zur Verfügung.
- Die Secon AG stellt ein Service zur Verfügung, welcher auf den Server installiert ist und die Daten vollautomatisch vom sftp-Server bei der Secon AG herunterlädt. Der Import der Daten ins operative System wird von Siddhartha im Tagesrhythmus automatisch vollzogen.
- Während des Imports wird die Siddhartha-Dunkelprüfung anhand der definierten Auslenkungskriterien vollzogen. Nach der Siddhartha-Dunkelprüfung setzt das System auf jeder Rechnung ein Hinweis, ob die Rechnung durch die DRG-Dunkelprüfung auffällig oder nicht auffällig ist.
- Sofern Papierrechnungen eingehen, werden diese von der internen DAS entgegengenommen, aufgrund der Auslenkungskriterien geprüft und entsprechend triagiert. Die Interne DAS wird von einer vertraglich verpflichteten Person (Pflichtenheft) der Krankenkasse besetzt. Die Interne DAS arbeitet in einem von den anderen Mitarbeitern separierten Büro.
- Eine Mitarbeitende der Krankenkasse ist als Hilfsperson des VA autorisiert. Diese Person ist nicht in der Abteilung betreffend die stationäre Leistungserbringung tätig, und arbeitet während ihrer Tätigkeit als Hilfsperson in einem separaten Raum.

- Der VAD der Krankenkasse kann durch die gesetzten speziellen Berechtigungen den MCD-Link bei der Secon AG abrufen. Der VAD ist für die Nachcodierung und insbesondere der Vertrauensarzt für die vertiefte Prüfung und die weitere medizinische Beurteilung ausgelenkter Rechnungen und MCDs zum Zweck der Abgabe von Empfehlungen zuständig.

2.3. Rechtliche Grundlagen

2.3.1.KVG

[Art. 84 KVG](#) bildet die gesetzliche Grundlage für die Bearbeitung von Personendaten im Bereich der obligatorischen Krankenversicherung, auch durch Dritte (Outsourcing).

[Art. 84a KVG](#) regelt die Bekanntgabe von Daten im Krankenversicherungsbereich an Dritte.

Ausführungen im Bearbeitungsreglement:

4. Beteiligte Organisationseinheiten

[Art. 84b KVG](#) regelt den Datenschutz bei der Durchführung der Krankenversicherung nach KVG.

Ausführungen im Bearbeitungsreglement:

2.4 Zuständigkeiten und Verantwortung

2.6 Kontaktstelle bezüglich datenschutzrechtlichen Fragen

2.8 Schweigepflicht nach Art. 33 ATSG

2.9 Datensicherheit

6. Zugriff

8. Technische, organisatorische und personelle Massnahmen

[Art. 21 VDSG](#) i.V.m. [Art. 84b KVG](#) regelt schliesslich die Pflicht zur Erstellung eines Bearbeitungsreglements für bestimmte automatisierte Datensammlungen:

Ausführungen im Bearbeitungsreglement:

2.2 Scope

2.3.2.KVV

Die Verordnung über die Krankenversicherung (KVV) enthält weitere spezifische Bestimmungen zur Rechnungslegung. So hält [Art. 59 KVV](#) die allgemeinen Grundsätze fest. [Art. 59a KVV](#) äussert sich explizit zu den Swiss-DRG-Rechnungen.

Ausführungen im Bearbeitungsreglement:

3. Übersicht der Datenbearbeitungsstruktur

5. Der Datenbearbeitungsprozess

2.3.3.DSG

Weitere datenschutzrechtlich relevante Bestimmungen ergeben sich aus dem Bundesgesetz über den Datenschutz (DSG). So sind insbesondere die Grundsätze der Datenbearbeitung nach [Art. 4 DSG](#) zu beachten: Rechtmässigkeit der Datenbearbeitung ([Art. 4 Abs. 2 DSG](#)), zweckgebundene Datenbearbeitung ([Art. 4 Abs. 3 DSG](#)), Erkennbarkeit der Datenbeschaffung ([Art. 4 Abs. 4 DSG](#)) und unter Umständen die Einwilligung der betroffenen Person ([Art. 4 Abs. 5 DSG](#)).

Ausführungen im Bearbeitungsreglement:

5.3 Prüfung von stationären Leistungsabrechnungen

5.4 Rechnung/MCD in Papierversion

5.6 Auslenkungskriterien

5.7 Auswertungen

10. Archivierung und Vernichtung von Daten

11. Rechte der Versicherten

Eine weitere Anforderung des Datenschutzgesetzes betrifft die Datensicherheit, also die technischen oder organisatorischen Massnahmen zum Schutz vor unbefugtem Bearbeiten.

Ausführungen im Bearbeitungsreglement

8. Technische, organisatorische und personelle Massnahmen

[Art. 10a DSG](#) bildet analog zu [Art. 84 KVG](#) die Grundlage für die Datenbearbeitung durch Dritte.

Ausführungen im Bearbeitungsreglement

4. Beteiligte Organisationseinheiten

5.5 Outsourcing

9. Interne und externe Kontrollen

10. Archivierung und Vernichtung von Daten

Ähnlich wie [Art. 3 VVG](#) ergibt sich aus [Art. 14 DSG](#) eine Informationspflicht des Versicherers bzw. des Inhabers der Datensammlung. Diese bezieht sich auf das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen.

Ausführungen im Bearbeitungsreglement

11. Rechte der Versicherten

2.4. Zuständigkeiten und Verantwortung

Die Gesamtverantwortung für den Datenschutz trägt die Geschäftsführung. Diese Verantwortung ist nicht übertragbar. Alle weiteren Aufgaben, Kompetenzen und Verantwortlichkeiten betreffend Datenschutz und Sicherheit sind in diesem Bearbeitungsreglement sowie im Dokument ‚Weisungen an die Mitarbeitende‘ festgehalten.

2.5. Anmeldung Datensammlung beim EDÖB (Art. 16 VDSG)

Die Krankenkasse hat den RVK mit dem Amt des betrieblichen Datenschutzbeauftragten beauftragt. Damit wird die Krankenkasse gemäss [Art. 11 Abs. 5 lit. e DSG](#) von der Pflicht befreit, die Datensammlungen beim EDÖB zu melden.

Die Konformität jeder einzelnen Datensammlung die Personendaten enthält, wird vor Implementierung sowie kontinuierlich für alle bestehenden Datensammlungen geprüft und im [Konformitätsnachweis](#) dokumentiert.

2.6. Kontaktstelle bezüglich datenschutzrechtlichen Fragen

Fragen im Zusammenhang mit dem Datenschutz sind an folgende Stelle zu richten:

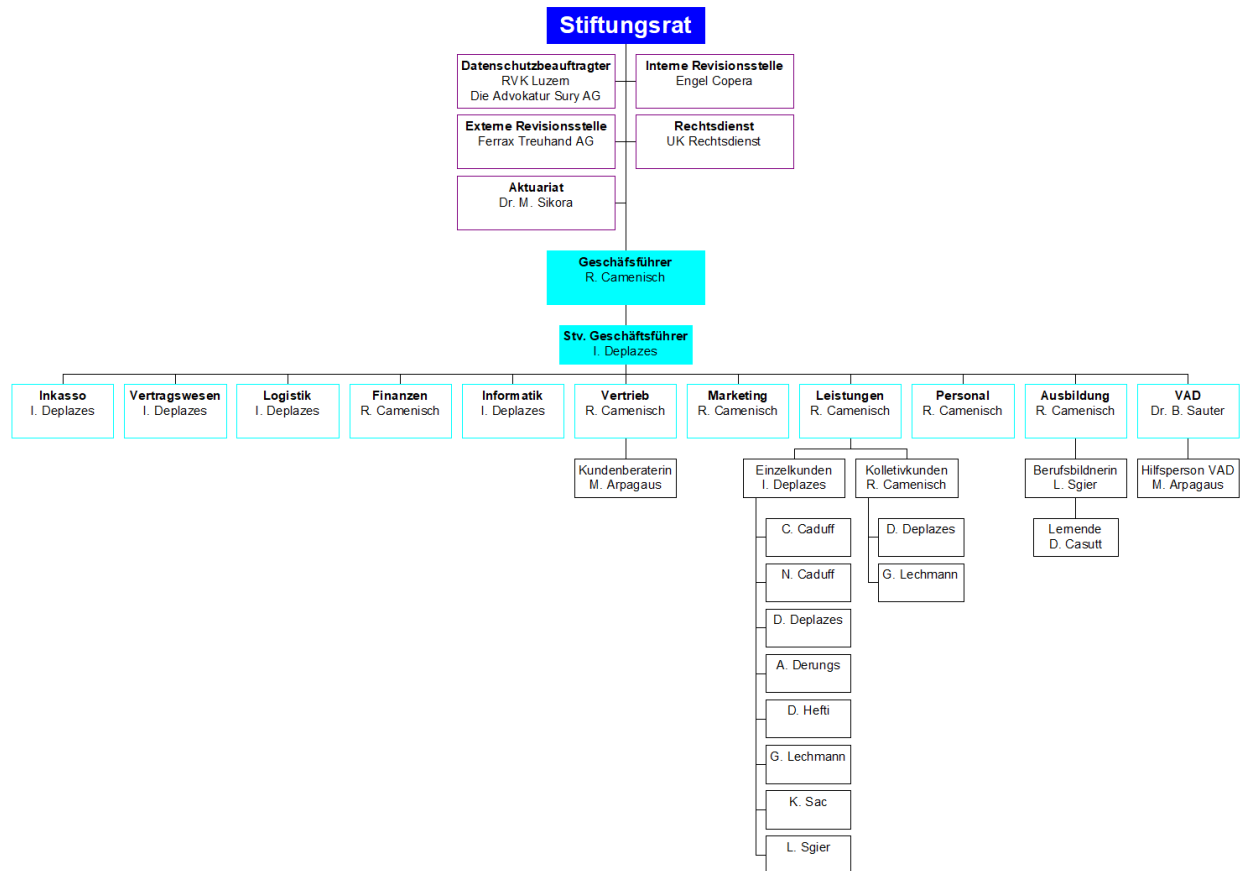
- Allgemein an den RVK in Ausübung der vertraglich vereinbarten Dienstleistung eines betrieblichen Datenschutzbeauftragten:

RVK
Haldenstr. 25
6006 Luzern
Tel. 041 417 05 00
Fax. 041 417 05 01
info@rvk.ch

- Betreffend spezifische Fragen im Rahmen des Outsourcings an die Secon AG:

Secon AG
Allmendstr. 17
8320 Fehraltorf

2.7. Organigramm



2.8. Schweigepflicht nach Art. 33 ATSG

Geschäftsleitung und Mitarbeitende unterstehen der Schweigepflicht nach [Art. 33 ATSG](#).

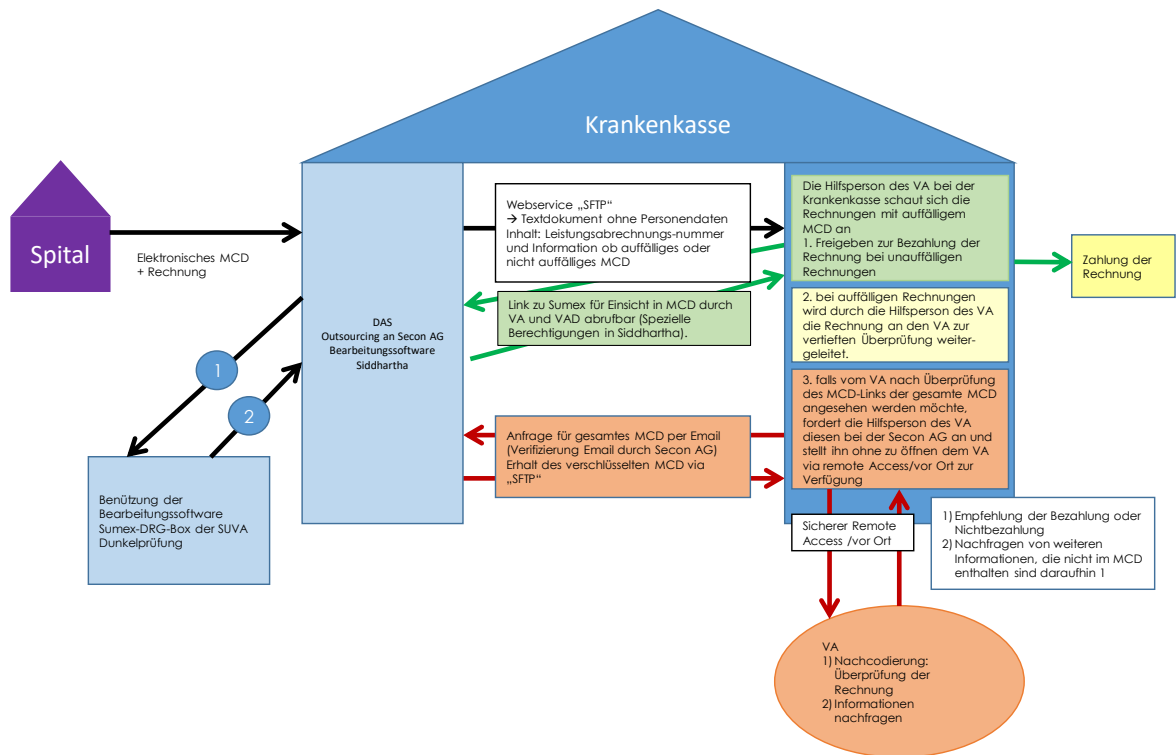
Bei Verletzung der Schweigepflicht unterstehen sie spezialgesetzlich den Strafbestimmungen des [Art. 92 KVG](#) und [Art. 33 ATSG](#). Die Mitarbeitenden sind über die Sanktionen informiert. Die Mitarbeitenden unterzeichnen mit Eintritt in das Unternehmen die [Schweigepflichterklärung](#).

2.9. Datensicherheit

Es werden technische, personelle und organisatorische Sicherheitsmassnahmen getroffen, um die verwalteten Personendaten vor unberechtigtem oder unrechtmässigem Zugriff, Verlust, Vernichtung oder Beschädigung zu schützen. Die Massnahmen sind detailliert im Dokument [Sicherheits- und Datenschutzweisung²](#) aufgelistet. Ausserdem sind alle Prozessabläufe die in der Krankenkasse relevant sind inklusive der Angaben zu Verantwortlichkeiten in vorliegendem Dokument und im Dokument [Weisung an Mitarbeitende²](#) definiert und dokumentiert. Die Funktion der Datenannahmestelle ist an die Secon AG outgesourct. Die Gewährleistung der Datensicherheit durch die Secon AG ist durch den Vertrag inklusive seiner Anhänge sowie deren internen Reglemente sichergestellt. Die relevanten internen Reglemente der Secon AG sind im physischen Ordner ‚SwissDRG-DAS Zertifizierung‘ abgelegt. Die Krankenkasse stellt sicher, dass sie über die aktuellsten Versionen der Reglemente verfügt.

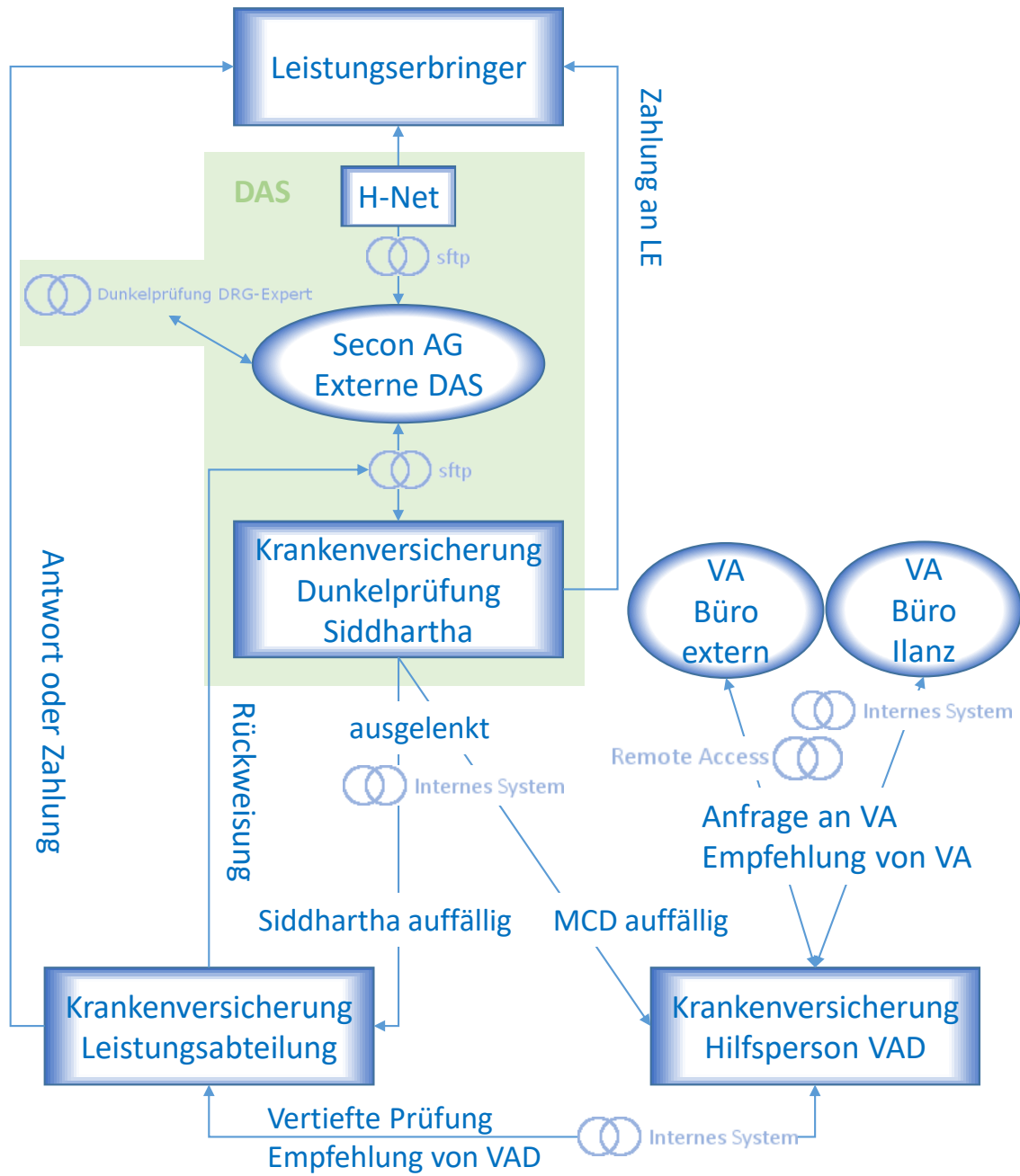
3. Übersicht der Datenbearbeitungsstruktur

Die nachfolgenden Grafiken zeigen die Struktur betreffend die Leistungsprozesse der Bearbeitung stationärer SwissDRG Rechnungen auf, in welche das automatisierte Datenbearbeitungssystem eingegliedert ist. In Punkt 4 werden die beteiligten Organisationseinheiten beschrieben. In Punkt 5 wird der Datenbearbeitungsprozess beschrieben.

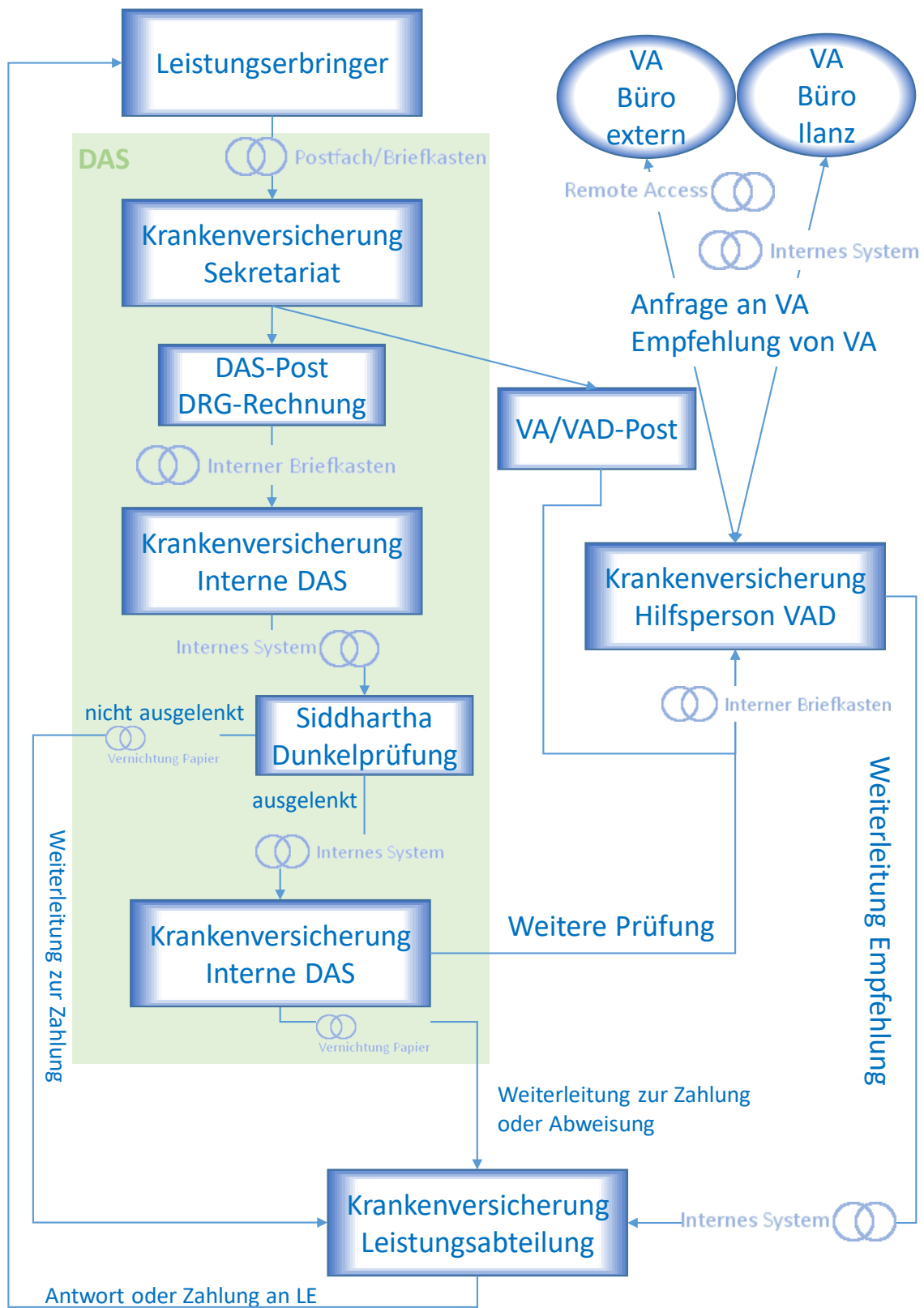


3.1. Übersicht der Schnittstellen

3.1.1. Verarbeitung elektronisch



3.1.2. Verarbeitung Papier



4. Beteiligte Organisationseinheiten

4.1. H-Net AG

Gestützt auf [Art. 59a KVV](#) dürfen die medizinischen Daten ausschliesslich an die zertifizierte Datenannahmestelle des Versicherers gesandt werden. Aufgrund einer vertraglichen Vereinbarung mit H-Net AG erfolgt die Zustellung der Rechnung inkl. der medizinischen Daten vom Leistungserbringer an die H-Net AG. Diese leitet die Daten an die Datenannahmestelle weiter.

4.2. Secon AG

Gestützt auf [Art. 59a KVV](#) dürfen die medizinischen Daten ausschliesslich an die zertifizierte Datenannahmestelle des Versicherers gesandt werden. Als Dienstleistung betreibt die Secon AG im Auftrag der ihr angeschlossenen Krankenversicherer diese zertifizierte Datenannahmestelle. Die Krankenkasse hat aufgrund einer vertraglichen Abmachung diese Leistung an die Secon AG ausgelagert. Die Verantwortung für die Tätigkeit der Secon AG bleibt jedoch bei der Krankenkasse. Die Aufbewahrung der Daten erfolgt gemäss dem internen Reglement der Secon AG.

Die detaillierten Anforderungen an den durch die Secon AG ausgeführten Prozess sind in deren Anwendbarkeitserklärung, die im Rahmen der DRG-DAS Zertifizierung der Secon AG erstellt wurde, und in dem Vertrag der Krankenkasse mit der Secon AG (Siehe [Secon Lizenzvertrag²](#), [Secon Zusatzvertrag²](#)) dargelegt.

4.3. ELCA

Die ELCA stellt die Software zur Beurteilung der SwissDRG-Rechnungen bereit (DRG-Dunkelprüfung). (Siehe [ELCA Lizenzvertrag Sumex²](#))

4.4. Krankenkasse

Die Krankenkasse ist als Krankenkasse Zertifikatsträger gemäss [Art. 59a KVV](#). Die Krankenkasse bleibt für die Tätigkeiten der Datenannahmestelle, die an andere Organisationseinheiten outgesourct wurden verantwortlich.

Der Krankenkasse sind keine Berechtigungen erteilt, welche zur Decodierung des MCDs benötigt werden.

Der Link, der mittels Sumex DRG-Expert Zugang zu sensiblen Daten ermöglicht, wird ausschliesslich vom VAD geöffnet. Die Einforderung von zusätzlichen Informationen bei den Leistungserbringern erfolgt nicht durch die Krankenkasse, sondern durch den VAD.

4.5. Interne DAS

Die Interne DAS wird von einer vertraglich verpflichteten Person (Pflichtenheft) der Krankenkasse besetzt. Sie besitzt ein eigenes Login für den System-Zugriff und ist für die Bearbeitung der in Papierform zugestellten Rechnungen zuständig. Die Interne DAS arbeitet in einem von den anderen Mitarbeitern separierten Büro.

4.6. Vertrauensärztlicher Dienst

4.6.1. Aufgaben

Der vertrauensärztliche Dienst (VAD) umfasst einen ausgebildeten Vertrauensarzt (VA) und dessen Hilfspersonal (HP). Der VAD ist für die Bearbeitung von medizinischen Daten zuständig, die ihm im Rahmen von [Art. 42 Abs. 5 KVG](#) zugesendet werden müssen/können:

- a. Der Leistungserbringer ist in begründeten Fällen berechtigt, medizinische Daten nur dem VA bekannt zu geben.
- b. Der Leistungserbringer muss, auf Verlangen der versicherten Person, medizinische Daten nur dem VA bekannt geben.

4.6.2. Terminologie

Der Grossteil der Arbeit des Vertrauensärztlichen Dienstes wird vom Vertrauensarzt auf der Grundlage des Vertrages der Krankenkasse mit dem Vertrauensarzt wahrgenommen. Der Vertrauensarzt erhält direkt von der Secon AG den Link, der den Zugriff auf die Informationen ermöglicht, die für eine gewöhnliche Nachcodierung nötig sind. Der Vertrauensarzt führt die Nachcodierung durch. Die vertraglich als Hilfsperson des VA (HP) verpflichtete Mitarbeiterin der Krankenkasse unterstützt den VA bei der Erfüllung seiner Aufgaben.

Diesbezüglich muss festgehalten werden, dass betreffend die Verwendung der Terminologie VA/VAD dem Verständnis des BAG gefolgt wird: Im Kreisschreiben 7.1 verwendet das BAG VA und VAD als Synonyme. Auf Nachfrage erläuterte das BAG, dass prinzipiell mit VA der mit Dr.med. ausgebildeten Arzt bezeichnet, während mit VAD der Arzt und seine Hilfspersonen bezeichnet werden, dass jedoch in rechtlich relevanter Hinsicht, VA und VAD als Synonyme verwendet werden. Dies gilt insbesondere für die Frage, wer an den VA adressierte Post bearbeiten darf: hier wird explizit davon ausgegangen, dass auch der VAD an den VA adressierte Post öffnen und bearbeiten darf. Sofern Hilfspersonen des VA jedoch in der Leistungsabteilung tätig sind, müssen besondere technische und organisatorische Massnahmen vorgenommen werden, um die Unabhängigkeit der Hilfsperson von der Arbeit in der Leistungsabteilung sicherzustellen.

Die HP nimmt keine Aufgaben im Rahmen der stationären Leistungserbringung wahr, und arbeitet in einem von den anderen Mitarbeitern separierten Büro, zu dem nur sie und der VA einen Schlüssel haben. Die Putzfrau kann nur bei Anwesenheit einer der beiden Personen das Büro reinigen. Der Computer der HP ist passwortgeschützt. Die präzisen Pflichten der Angestellten sind in der [Weisung an Mitarbeitende](#) festgelegt. Ausserdem hat sich die HP nochmals explizit vertraglich verpflichtet ihre Schweigepflicht und die Pflichten aus dem Datenschutzgesetz zu wahren (siehe [Vertrauensärztliche Beratung Anhang2¹](#)). Die HP informiert den Vertrauensarzt betreffend die ausgelagerten Rechnungen. Die Information des Vertrauensarztes findet entweder physisch im Büro von HP und des VA (siehe [Situationsplan²](#)) oder zwischen HP und dem Büro des VA in Basel mittels Remote-Verbindung (VPN –Verbindung) statt.

5. Der Datenbearbeitungsprozess

5.1. Übersicht

Mit der Einführung von DRG Pauschalen für die Abgeltung von stationären Spitalaufenthalten sind Spitäler und Ärzte verpflichtet, ab 1.1.2014 alle administrativen und medizinischen Patientendaten ausschliesslich an zertifizierte Datenannahmestellen der Versicherer zu übermitteln. Spitalrechnungen werden deshalb gemeinsam mit einem sogenannten MCD (Minimal Clinical Dataset) an die Kostenträger gesandt. MCDs enthalten neben administrativen Daten auch die für die Rechnungskontrolle erforderlichen medizinischen Patientendaten. Hierbei handelt es sich um besonders schützenswerte Daten. Deshalb bestehen höhere Anforderungen an den Datenschutz welche mit Befolgung der Regelungen im Bearbeitungsreglement eingehalten werden.

Die Bearbeitung der MCDs, und damit der sensiblen, als im Sinne des DSG besonders schützenswert klassifizierten Daten findet bei der Secon AG mit Hilfe der Software „Sumex DRG Box“, bei der internen DAS der Krankenkasse mittels Software Siddhartha sowie im Rahmen der Arbeit des vertrauensärztlichen Dienstes statt.

Die Krankenkasse bleibt für die Tätigkeiten ihrer Outsourcingpartner verantwortlich.

5.2. Implikation des Vertrauensarztes

Prinzipiell kann der VA/VAD aus folgenden Gründen in den Prozess involviert sein:

1. Auf Grund von [Art. 42 Abs. 5 KVG](#) gilt folgendes:
 - a. Der Leistungserbringer ist in begründeten Fällen berechtigt, medizinisch Daten nur dem VA bekannt zu geben.
 - b. Der Leistungserbringer muss, auf Verlangen der versicherten Person, medizinische Daten nur dem VA bekannt geben.
2. Gemäss [Art. 59a KVV](#) muss der Versicherer, wenn er im Laufe der Prüfung zusätzliche Auskünfte medizinischer benötigt, welche nicht auf Initiative des VA eingefordert werden, die versicherte Person über Ihre Wahlmöglichkeit nach [Art. 42 KVG Abs. 5](#) informieren.
3. Ausserdem verlangt das vertrauensrechtliche Verhältnismässigkeitsprinzip vorliegend, dass die Gesamtheit der im MCD enthaltenen Daten nur den Vertrauensarzt bekannt gegeben wird.

5.3. Prüfung von stationären Leistungsabrechnungen

5.3.1. Überblick und Begriffliches

Die Überprüfung der Rechnungen findet in drei Schritte statt:

1. Dunkelprüfung DAS: Standardisierte Rechnungsprüfung innerhalb der DAS des Krankensversicherers: automatische Aussonderung der auffälligen Rechnungen durch entsprechende Prüfsoftware.
2. Prüfstufe 2: Kontrolle und Triage der auffälligen Rechnungen durch die HP
3. Prüfstufe 3: Vertiefte medizinische Überprüfung durch VA

5.3.2. Erste Prüfstufe: Dunkelprüfung

Die Secon AG erhält die elektronischen Rechnungen und die MCDs von den Leistungserbringern. Die Software für die interne Verarbeitung ist ‚Siddhartha‘. Nach der Anlieferung der Daten werden diese in das System der Secon AG importiert und die Zuweisung an die Kunden der Secon AG vorgenommen. Falls die Rechnung keinem der Kunden der Secon AG zugewiesen werden kann, kommt der manuelle Prozess zum Zuge, in welchem die EAN-Nummer (=Kennung Leistungserbringer) geprüft und allenfalls korrigiert und die Rechnung weiter verarbeitet wird. Wenn keine Korrektur vorgenommen werden kann, bleibt die Rechnung stehen, und wird innert Wochenfrist gelöscht. Das Verfahren ist im [Zusatzvertrag zum Lizenz- und Wartungsvertrag Siddhartha, Anhang 2](#) festgehalten.

Im Regelfall empfängt die Secon AG die elektronischen Rechnungen der Leistungserbringer, isoliert die MCDs von den übrigen Daten, verschlüsselt und speichert die heiklen Daten mit einem nur dem VA bekannten Schlüssel und sendet die anonymisierten Daten zur DRG-Dunkelprüfung. Die Software für die DRG-Dunkelprüfung wird von der ELCA bereitgestellt. Die ELCA ist kein Lieferant der Secon AG, sondern ein direkter Vertragspartner der Krankenkasse. Einzig für den Transport setzt die Secon AG die Software von ELCA ein und bezahlt dafür eine jährliche Lizenzgebühr. Die Secon AG und die ELCA sind direkte Vertragspartner der Krankenkasse. Mithilfe der Software ‚Sumex DRG Box‘ wird entschieden, ob auf Grundlage der Auslenkungskriterien eine auffällige Rechnung vorliegt. Ob diese Rechnung auffällig ist, wird von der ELCA an die Secon AG gemeldet. Die Secon AG markiert die Rechnungen entsprechend der Resultate der Sumex SwissDRG Box- Prüfung und speichert diese. Die Secon AG stellt einmal täglich alle Prüfungsergebnisse für die Krankenkasse zusammen, und übermittelt ein txt-Dokument mit der Leistungsabrechnungsnummer und der Information ob die Rechnung auffällig oder nicht auffällig ist, dem Versicherer automatisiert via SFTP.

Die Daten werden automatisch vom sftp heruntergeladen und mit der Siddhartha-Software importiert. Beim Import der Daten wird die Siddhartha-Dunkelprüfung anhand der vordefinierten Auslenkungskriterien (Siehe Punkt 5.6 und [Auslenkungskriterien der Siddhartha-Dunkelprüfung²](#)) sowie der DRG-Dunkelprüfungsergebnisse ausgeführt. In der Siddhartha-Dunkelprüfung wird zwischen folgenden Auslenkungskriterien unterschieden:

- Technische Auslenkungskriterien → Rückweisung der Rechnung
- System-Dynamische Auslenkungskriterien → Rückweisung oder Zurückführung in die automatische Weiterverarbeitung der Rechnung
- Vom Versicherer definierte Auslenkungskriterien → Weiterleitung der Rechnung zur vertieften Prüfung durch den VAD

Die aufgrund der DRG-Dunkelprüfung auffälligen Rechnungen werden direkt dem VAD zur Prüfung weitergeleitet.

5.3.3. Zweite Prüfstufe: Triage

Die HP führt eine Kontrolle - in Form einer gewöhnlichen Nachcodierung - und Triage der auffälligen Rechnungen durch. Von den auffälligen als unauffällig beurteilte Rechnungen empfiehlt die HP der Leistungsabteilung der Krankenkasse zur Bezahlung. Erachtet die HP eine Nachcodierung als notwendig, so leitet diese die Rechnung zur vertieften Überprüfung an den Vertrauensarzt weiter.

Für den Fall, dass weitere Dokumente benötigt werden, die über das vom Leistungserbringer gelieferte Material hinausgehen, so fordert der VAD diese bei den Leistungserbringern an. Sobald die Rechnung freigegeben worden ist, wird der Link zum MCD automatisch gelöscht.

5.3.4. Dritte Prüfstufe: Prüfung durch den VA

Der Vertrauensarzt führt die Nachcodierung durch. Diese Arbeit führt der Vertrauensarzt entweder vor Ort bei der Krankenkasse in Ilanz, oder mithilfe von Remote-Verbindung (VPN) in seinem Büro in Basel aus. Bei der Krankenkasse in Ilanz ist ein separates Büro eingerichtet, zu dem nur er und seine Hilfsperson einen Schlüssel haben (Siehe [Situationsplan²](#)).

Hierfür ist er berechtigt den Link bei der Secon AG anzufordern, der ihm mittels der Sumex DRG-Expert Software (hergestellt von der ELCA) Zugang zu den Informationen ermöglicht, die für eine gewöhnliche Nachcodierung notwendig sind. Insbesondere besteht Zugang zu denjenigen Informationen des MCDs, die in der DRG-Dunkelprüfung die Auslenkung veranlassen haben. Die Secon AG übermittelt den Link via separater Applikation (MCDApp.exe). Der Link wird automatisch gelöscht, sobald die Rechnung freigegeben worden ist.

Sofern weitere Arztberichte zur Beurteilung der auffälligen Rechnung notwendig sind, informiert der VA die HP, welche die Dokumente zuhanden des VAD einfordert. Dieser Informationsaustausch findet vor Ort in dem Büro von HP und dem VA in Ilanz oder mittels Remote-Verbindung (VPN) statt.

Der Vertrauensarzt fordert gegebenenfalls bei der Secon AG die Bereitstellung des gesamten MCDs an. Diese Anforderung erfolgt mittels E-Mail und wird von der Secon AG erst nach interner Überprüfung beantwortet. Wird die E-Mail von der Secon AG als glaubwürdig eingestuft, so übermittelt die Secon AG dem Vertrauensarzt via E-Mail den mit pgp verschlüsselten MCD. Den Schlüssel für die Entschlüsselung des MCDs hat allein der VA.

Der VA empfiehlt auf Grundlage der Nachcodierung und gegebenenfalls auf Grundlage der zusätzlichen Informationen entweder die Zahlung oder Beanstandung der Rechnung. Weitere Präzisierungen werden im Vertrag der Krankenkasse mit dem VA dargelegt (Siehe [Vertrauensärztliche Beratung²](#), [Vertrauensärztliche Beratung Anhang1¹](#), [Vertrauensärztliche Beratung Anhang2¹](#))

5.4. Rechnung/MCD in Papierversion

5.4.1. Allgemein

Die Post wird vom Postfach bzw. aus dem Briefkasten jeden Morgen von einem Mitarbeitenden des Sekretariats geholt. Die dafür zuständige Person wechselt im wöchentlichen Turnus. Im Sekretariat wird die Post sortiert. Normale Post wird geöffnet und verteilt. Post, die an den VA/VAD oder an der DAS adressiert ist, wird ungeöffnet in den entsprechenden hausinternen Briefkasten gelegt. Der Zugriff auf die Briefkästen ist der jeweiligen Abteilung vorbehalten. Sofern Post nicht an den VA/VAD oder DAS adressiert war, sich nach dem Öffnen jedoch ergibt, dass der Inhalt der Sendung an den VA/VAD oder DAS adressiert hätte werden müssen, so wird die Sendung wieder verschlossen, und in den hausinternen Briefkasten gelegt. Der Absender wird durch die entsprechende Abteilung informiert, dass eine solche Sendung korrekt zu adressieren sei. (Siehe [STA Rechnungsstellung an interne DAS¹](#), [VAD Rückweisung VA Post¹](#))

Der Prozess kann wie folgt zusammengefasst werden:

Hauptschritte	Option	Optionsschritte
1. Start		
2. Eingang Post		
3. Briefe mit Anschrift Persönlich/Vertraulich vorhanden?	Ja	1. Couvert mit Eingangsstempel versehen 2. ungeöffnet an entsprechende Abteilung/Person weiterleiten 3. zum nächsten Hauptschritt
	Nein	1. zum nächsten Hauptschritt
4. Briefe mit Anschrift "VAD,VA" oder "DAS" vorhanden?	Ja	1. Couvert mit Eingangsstempel versehen 2. ungeöffnet im entsprechenden Briefkasten legen 3. zum nächsten Hauptschritt
	Nein	1. zum nächsten Hauptschritt
5. Bank- & Postbelege vorhanden?	Ja	1. Couvert mit Eingangsstempel versehen 2. ungeöffnet an Abteilung Zahlungsverkehr weiterleiten 3. zum nächsten Hauptschritt
	Nein	1. zum nächsten Hauptschritt
6. Briefe öffnen & nach Abteilung sortieren		
7. Briefe mit Eingangsstempel versehen		
8. Unzuteilbare Post vorhanden?	Ja	1. Dokument einscannen 2. Infoschreiben gem. Prozessbeschreibung versenden 3. Original in Fach "zur Abholung" legen 4. zum nächsten Hauptschritt
	Nein	1. zum nächsten Hauptschritt
9. Post an entsprechende Abteilungen weiterleiten		
10. Ende		

5.4.2. Bearbeitung durch die interne DAS

Die DAS-verantwortliche Person leert den hausinternen Briefkasten und verarbeitet die Rechnungen unter Berücksichtigung der definierten Auslenkungskriterien. Wird die Rechnung als unauffällig eingestuft, so wird die Rechnung der Leistungsabteilung zur Begleichung weitergeleitet. Eingegangene Dokumente (Rechnung und allfälliges MCD) werden durch die interne DAS geschreddert. In der Regel werden die Leistungserbringer aufgefordert, künftig elektronisch abzurechnen. (Siehe [STA Rechnungsstellung an interne DAS!](#)). Die Ausnahme bilden Leistungserbringer, welche nicht elektronisch abrechnen können.

Wird eine Rechnung für auffällig befunden, leitet die interne DAS die Dokumente dem VAD zur vertieften Prüfung weiter.

5.4.3. Bearbeitung durch den VA/VAD

Die HP leert den hausinternen Briefkasten VAD. An den VAD adressierte Dokumente öffnet sie, prüft sie, und leitet sie nötigenfalls an den VA weiter. Die Papierversion schreddert sie unverzüglich, nachdem das Dokument eingesehen wurde. Die Dokumente werden dem VA entweder vor Ort im Büro VAD oder mit Hilfe von Remote-Verbindung (VPN) im eigenen VAD Laufwerk verschlüsselt zur Verfügung gestellt.

Nach Abschluss der Prüfung durch den VAD wird ein allfällig eingesehenes MCD endgültig gelöscht, sodass keine MCD-Daten gespeichert bleiben.

5.5. Outsourcing

Der Grossteil der Bearbeitung der MCDs, und damit der sensiblen, als im Sinne des DSGVO besonders schützenswert klassifizierten Daten, findet bei der Secon AG mit Hilfe der Software ‚Sumex DRG Box‘ statt. Die Krankenkasse bleibt gem. [Art. 10a DSGVO](#) für das datenschutzrechtlich korrekte Handeln ihrer Outsourcingpartner verantwortlich. Die Krankenkasse stellt sicher, dass die Daten von den Outsourcingpartnern nur so bearbeitet werden wie die Krankenkasse sie bearbeiten dürfte. Und vergewissert sich, dass die Outsourcingpartner die Datensicherheit gewährleisten. Dies wird insbesondere durch die regelmässige Überprüfung vorgenommen, ob die Outsourcingpartner über ausreichende, und gültige Datenschutzzertifizierungen verfügen.

5.6. Auslenkungskriterien

Für die DRG-Dunkelprüfung werden die voreingestellten Auslenkungskriterien der ‚Sumex DRG Box‘ angewendet. Die Siddhartha-Dunkelprüfung erfolgt nach folgenden Einstufungen:

- A) Technische Auslenkungskriterien
- B) System-Dynamische Auslenkungskriterien
- C) Durch den Versicherer definierte Auslenkungskriterien

Die Definition der jeweiligen Auslenkungskriterien wird im Dokument [Auslenkungskriterien der Siddhartha-Dunkelprüfung²](#) aufgelistet.

5.6.1. Änderung der Auslenkungskriterien

Bei der DRG-Dunkelprüfung können die Kriterien von der vita surselva nicht angepasst werden. Die Geschäftsführung prüft periodisch die Siddhartha-Auslenkungskriterien auf ihren Nutzen. Eine beschlossene Änderung der Auslenkungskriterien wird von der Secon AG auf Antrag von der vita surselva ausgeführt. Die Änderung der Kriterien und die zugrunde liegenden Überlegungen werden in [Auslenkungskriterien der Siddhartha-Dunkelprüfung²](#) protokolliert.

5.7. Auswertungen

Zur Prüfung, der bestehenden Auslenkungskriterien, werden fortlaufend Auswertungen vorgenommen. Es gibt folgende Auswertungskriterien:

- Verhältnismässigkeit der Auslenkungsquote
- Anteil Verhältnis Rechnungen Dunkelverarbeitungen
- Auswertung Verhältnis von Einsparpotential und effektiv erreichten Einsparungen auf ausgelenkten Rechnungen

Die Auswertungen werden historisiert im Datei-System gespeichert. Aufgrund der Auswertungsergebnisse entscheidet die Geschäftsleitung jährlich, ob die bestehenden Auslenkungskriterien angepasst werden müssen.

6. Zugriff

6.1. Zugriffsdifferenzierung

Es werden nur die notwendigsten Zugriffsrechte auf Netzwerke, Programme und Daten an Benutzer vergeben. Jeder Mitarbeitende erhält nur Zugriff auf genau diejenigen Daten, die er zur Erfüllung seiner Aufgaben unbedingt braucht. Die Zugriffsrechte sind explizit im Dokument ‚Zugriffsedinitionen‘ geregelt (Siehe [Zugriffsedinitionen²](#)).

Im Namen der Geschäftsleitung entscheidet der Administrator über die Vergabe und den Umfang der Zugriffsrechte. Die Zugriffsrechte sind auf die Funktion und Tätigkeitsfelder jeder Person zugeschnitten.

6.2. Authentisierung durch Passwörter

Der Mitarbeitende hat eine persönliche Identifikation (Benutzername) und ein Passwort. Die Weitergabe des persönlichen Passworts ist untersagt. Die Erstellung sicherer Passwörter ist mittels Weisung explizit geregelt (Siehe [IT Umgebung²](#)).

7. Datenbearbeitung

7.1. Zweck der Datenbearbeitung

Der Zweck der Datenverarbeitung, für die dieses Bearbeitungsreglement gilt, ist die Leistungs- und Kostenkontrolle der Leistungserbringer im Rahmen des KVG.

7.2. Datenherkunft

Die Daten stammen von Leistungserbringern gemäss KVG.

7.3. Datenbearbeitung

Im Rahmen des zu zertifizierenden Prozesses werden von der Krankenkasse keine sensiblen Daten bearbeitet. Es werden lediglich von der Datenannahmestelle Informationen über aus-gelenkte Rechnungen an den vertrauensärztlichen Dienst weitergeleitet, und gegebenenfalls zusätzliche Informationen beim Leistungserbringer erfragt, die dann direkt an den VAD gesendet werden.

Die Bearbeitung sensibler Daten erfolgt ausschliesslich durch die Datenannahmestelle (Out- und Insourcing) sowie den vertrauensärztlichen Dienst (VAD/VA).

Die Datenbearbeitung erfolgt gestützt auf [Art. 42](#) i.V.m. [Art. 84 KVG](#). Die Bearbeitung der Diagnosedaten erfolgt ausschliesslich zur Überprüfung der Rechnungen auf die durch [Art. 56 KVG](#) vorgegebene Pflicht des Krankenversicherers, die Einhaltung der Wirtschaftlichkeit zu überprüfen. Darüber hinaus werden die Ausführungsbestimmungen nach [Art. 59a KVV](#) berücksichtigt.

8. Technische, organisatorische und personelle Massnahmen

8.1. Zugangskontrollen

Sämtliche Räumlichkeiten der Krankenkasse, in welchen besonders schützenswerte Personendaten bearbeitet werden sind mechanisch vor dem Zutritt unbefugter Personen gesichert. Allein VA und HP haben einen Schlüssel für das Büro des VAD und für den hausinternen Briefkasten des VAD. Das Weiterleiten der sensiblen Daten erfolgt nur durch die HP.

8.2. Instruktion und Schulung des Personals

Die Mitarbeitenden sind über die bei ihrer Tätigkeit anzuwendenden datenschutzrechtlichen Vorschriften unterrichtet und geschult. Der Nachweis über die letzte durchgeführte Schulung, sowie über die nächste geplante Schulung findet sich im Dokument, 'Nachweis Schulungen und Schulungskonzept' im Ordner SwissDRG-DAS-Zertifizierung.

Während der Einarbeitungszeit wird eine umfassende Unterrichtung über die einschlägigen Datenschutzbestimmungen durchgeführt.

Datenschutzrechtliche Vorschriften sind fester Bestandteil der Fortbildungsplanung. Dies schliesst auch die Fortbildung im Umgang mit technikunterstützter Informationsverarbeitung und den daraus resultierenden Datensicherheitsmassnahmen ein.

9. Interne und externe Kontrollen

Die Einhaltung der datenschutzrechtlichen Bestimmung wird intern folgendermassen sichergestellt und kontrolliert:

9.1. Massnahmen auf Unternehmensebene

- Schriftlich festgehaltene [Datenschutzpolitik](#), die allen Mitarbeitenden bekannt, und online publiziert ist.
- [Sicherheits- und Datenschutzweisung](#)?
- Regelungen von Aufgaben, Verantwortlichkeiten und Kompetenzen bezüglich Datenschutz und Datensicherheit in der [Weisung an Mitarbeitende](#)?
- Jährliche Schulung aller Mitarbeitenden bezüglich Datenschutz und Datensicherheit.
- Die Zugänge zu den Büros sowie zum Archiv sind mechanisch gesichert.

9.2. Kontrollen durch das Management

Die Geschäftsleitung nimmt ihre Führungs- und Überwachungsaufgaben durch folgende Kontrollen wahr:

- Prüfen der Bereiche der internen Kontrolle und Ableiten von Massnahmen.
- Prüfung der Umsetzung der Datenschutzpolitik.
- Verfassen von Datenschutz- und Datensicherheits-Vertragsklauseln mit allen Dienstleistern, die auf Daten zugreifen können oder an denen Daten weitergegeben werden sowie Kontrolle, ob die Dienstleister die Vorschriften bezüglich Datenschutz und Datensicherheit einhalten.
- Auswertung der Systemaufzeichnungen bezüglich Zugriffe auf Daten, Zeitpunkt sowie Umfang der Zugriffe und Abgleich mit der Zugriffsliste.
- Jährliche Risikoanalyse im Rahmen eines Management Reviews.
- Sorgfältige Auswahl und Instruktion aller externer Dienstleister, die auf Daten zugreifen können oder an die Daten weitergegeben werden.
- Regelmässige Überprüfung der Outsourcing-Partner, durch Kontrolle der Aktualität der VDSZ Zertifizierung, der aktuellen Reglemente, der Erfüllung von Projektplänen und der aktuellen Auditberichte.

Des Weiteren lebt das Management seine Vorbildfunktion aktiv und täglich und stellt die notwendigen Mittel für die kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit bereit.

9.3. Kontrollen auf Prozessebene

Es erfolgt eine Prüfung der Konformität von Einrichtung einer Datensammlung und Dokumentation im Konformitätsnachweis. Zudem erfolgt eine jährliche Kontrolle des Konformitätsnachweises auf dessen Vollständigkeit, Korrektheit und die Zweckmässigkeit der Datenbearbeitung.

9.4. IT-Kontrollen

Der Grossteil der IT-Kontrollen wurde bereits unter „2.9 Datensicherheit“ erläutert. Hier ist zusätzlich betreffend die outgesourceten Bearbeitungsprozesse folgendes festzuhalten: die Konformität der IT im Rahmen der an die Secon AG outgesourceten Bearbeitung der SwissDRG-Rechnungen wird durch die regelmässige Zertifizierung und durch die Einhaltung des Projektplans der Secon AG durch die Secon AG eingehalten. Die Krankenkasse beurteilt die Konformität der Secon AG auf der Grundlage der regelmässigen Auditberichten der Secon AG, die diese als zertifizierte Datenannahmestelle im Rahmen der SwissDRG-Rechnungsstellung durchzuführen hat, und die anschliessend der Krankenkasse zur Einsicht vorgelegt werden.

9.5. Interne Audits

Es erfolgt eine jährliche Kontrolle durch eine interne Revision. Diese Kontrollen sind in das umfassende interne Kontrollsystem des Unternehmens integriert. Der Nachweis für das letzte interne Audit sowie das Konzept und der Zeitraum für das nächste vorgesehene Audit findet sich im Dokument ‚Internes Audit‘ und ‚Auditkonzept‘ im Ordner SwissDRG-DAS Zertifizierung.

10. Archivierung und Vernichtung von Daten

Daten, die im Rahmen der Rechnungsstellung im SwissDRG Verfahren relevant sind, werden von der Secon AG verwahrt. Die Verwahrung bei der Secon AG wird im Dokument [Verfahren zur Identifikation von Anforderungen²](#) geregelt. Die Krankenkasse bleibt verantwortlich für eine rechtskonforme Regelung der Archivierung und Vernichtung von Daten durch die Secon AG.

11. Rechte der Versicherten

11.1. Auskünfte über Datenbearbeitungen

Jede Person kann von der Krankenkasse Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach [Art. 8 f. DSG](#) sowie [Art. 1 f., VDSG](#). Die Auskunftsgesuche sind schriftlich unter Beilage einer Kopie eines amtlichen Ausweises an folgende Adresse zu richten:

vita surselva
Bahnhofstrasse 33
Postfach 217
7130 Illanz
info@vitasurselva.ch

Die verantwortliche Person, respektive seine Stellvertreterin trägt die Verantwortung für eine termingerechte Betreuung des Antrags. Daten über die Gesundheit des Gesuchstellers werden an einen vom Gesuchsteller bestimmten Arzt übermittelt, nicht an den Gesuchsteller persönlich.

Auskunftsgesuche über medizinische Daten werden von der Krankenkasse an den VAD, zur Zustellung an einen vom Gesuchsteller bestimmten Arzt, weitergeleitet. Dadurch wird sichergestellt, dass die Krankenkasse keinen Einblick in Daten erhält, in die sie ohne ein gestelltes Auskunftsgesuch kein Einblicksrecht hätte.

11.2. Berichtigungs- und Löschungsrechte

Die Berichtigungs- und Löschungsrechte der betroffenen Personen richten sich nach [Art. 5 Abs. 2](#) und [Art. 25 DSG](#). Die Gesuche sind an die unter Kontaktstelle (Punkt 2.6) vermerkte Adresse zu richten.

12. Abschliessende Bestimmungen

12.1. Verlinkte Dokumente

Die im vorliegenden Bearbeitungsreglement verlinkten Dokumente sind integrierende Bestandteile dieses Bearbeitungsreglements.

12.2. Änderungen des Reglements

Das Bearbeitungsreglement wird gemäss [Art. 11 VDSG](#) regelmässig von den Eignern der Datensammlungen aktualisiert. Dieses Reglement kann jederzeit geändert werden. Änderungen bedürfen der Schriftform und der Zustimmung des Vorsitzenden der Geschäftsleitung und - sobald ein solcher etabliert wurde - des betrieblichen Datenschutzverantwortlichen.

12.3. Inkrafttreten

Dieses Reglement inkl. Anhänge tritt per 11. Juni 2014 in Kraft.

Legende Dokumentverweise

¹ Das Dokument kann auf Anfrage bei der vita surselva eingesehen werden.

² Internes Dokument, steht der Öffentlichkeit nicht zur Verfügung.