sumiswalder
ihr partner für gesundheit

Bearbeitungsreglement

Ausgabe 2024

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Rechtliche Grundlage

Gestützt auf Art. 5 und Art. 6 der Verordnung über den Datenschutz (DSV) in Verbindung mit Art. 84b des Bundesgesetzes über die Krankenversicherung (KVG) hat die Sumiswalder Krankenkasse (Sumiswalder) ein Bearbeitungsreglement zu erstellen, weil besonders schützenswerte Daten bearbeitet werden.

Die nachfolgenden Bestimmungen gelten sinngemäss auch für den Bereich der Zusatzversicherungen.

1.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren und den Betrieb der elektronischen Datenbearbeitung. 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.

Weiter beschreibt dieses Reglement das Verfahren für die Erteilung der Zugriffsberechtigungen auf die entsprechenden Informationssysteme und Verzeichnisse.

1.3 Zweck der Datenbearbeitung

Der Zweck der Datenbearbeitung ist in Art. 84 KVG geregelt. Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes beauftragten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile, zu bearbeiten, um die ihnen nach dem Gesetz übertragenen Aufgaben zu erfüllen.

1.4 Verantwortliche Stelle

Die Sumiswalder ist verantwortlich für die Abwicklung der Krankenversicherung und somit Inhaberin der Personendaten. Mit den im Reglement vorgesehenen Massnahmen sorgt die Sumiswalder für die Einhaltung der gesetzlichen Vorschriften.

1.5 Schweigepflicht nach Art. 33 ATSG

Bei Stellenantritt unterzeichnen die Mitarbeitenden der Sumiswalder die Datenschutzrichtlinien. Die Datenschutzrichtlinien beinhalten alle relevanten datenschutzrechtlichen Punkte, die während der Tätigkeit bei der Sumiswalder auftreten können und geben entsprechende Regeln vor.

Anlässlich von periodischen Schulungen werden die Mitarbeitenden über die Entwicklung im Datenschutz informiert und sensibilisiert. Die Mitarbeitenden sind in ihrer Funktion für die Schaffung der notwendigen und angemessenen Rahmenbedingungen für den Datenschutz und die Datensicherheit verantwortlich.

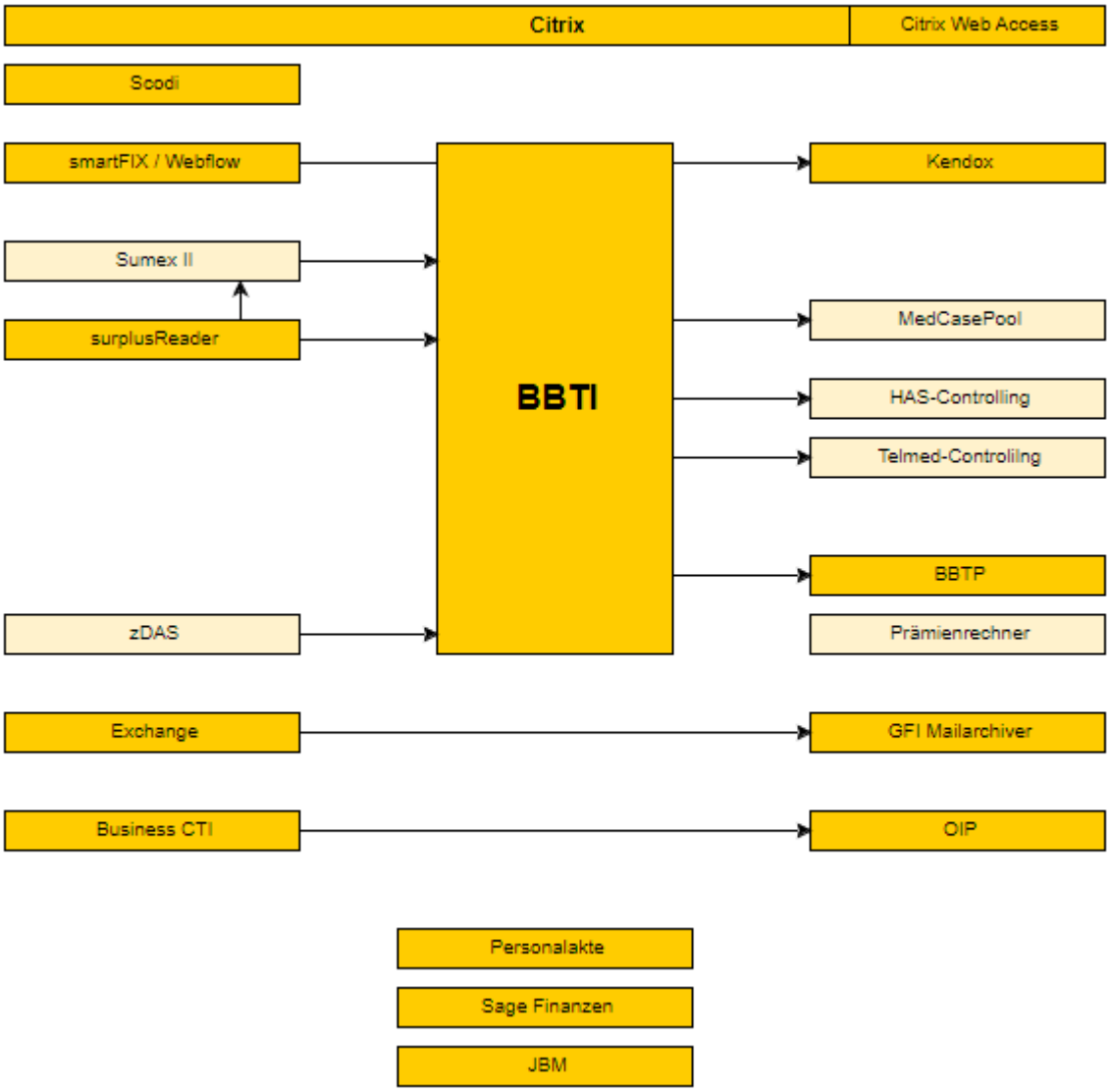
2 Struktur Informationssystem

2.1 Bestandteile Informationssystem

Die Kernapplikation des Informationssystems der Sumiswalder für die Abwicklung der Krankenversicherung ist das BBTIndividual (BBTI), entwickelt von der BBT Software, Root/Zermatt.

Das Informationssystem der Sumiswalder besteht nebst der Kernapplikation BBTI aus weiteren Umsystemen, die entweder direkt das Krankenversicherungsgeschäft betreffen oder für den allgemeinen Betrieb der Sumiswalder verwendet werden. Die Kernapplikation sowie viele weitere Umsysteme werden auf der eigenen Serverumgebung betrieben. Auf die Umsysteme der Outsourcing-Dienstleister werden mittels gesicherter Leitungen zugegriffen.

2.1.1 Systemübersicht des Sumiswalder-Informationssystems



Grafik: Systemübersicht des Sumiswalder-Informationssystems

Legende

Inouse bei der Sumiswalder
Outsourcing

2.1.2 Kernapplikation BBTI

Subsystem	Zweck
BBTI	Das BBTI ist die Kernapplikation für die Durchführung des Kranken- und Unfallversicherungsgeschäfts. Hier werden sowohl Privat- wie Firmenkunden bewirtschaftet und folgende Geschäfte abgewickelt: ▪ Versicherungspolicen ▪ Leistungsabrechnungen ▪ Prämienrechnungen (ESR, LSV+, DD, eBill) ▪ Mahnwesen ▪ Prämienverbilligung ▪ Integriertes DMS ▪ Datenlieferungen für Behörden und Verbände ▪ Statistiken

2.1.3 Umsysteme Krankenversicherungsgeschäft

Umsystem	Zweck
Sumex II	▪ Austausch von elektronischen XML-Dokumenten zur schematischen und tariflichen Prüfung (Tarmed, LOA, SL, Analysenliste) ▪ Empfangen von elektronischen Rechnungen direkt vom Leistungserbringer ▪ Prüfung von eingescannten Rechnungen
surplusReader	Leistungsrechnungen werden mittels surplusCapture in elektronische XML-Dokumente erfasst, mit dem surplusReader nachbearbeitet und entweder direkt dem BBTI oder zur Prüfung an den Sumex II weitergeleitet.
zDAS	Zertifizierte Datenannahmestelle BBT Software AG.
MedCasePool	Webbasiertes Tool „Fallführung“ Vertrauensärztlicher Dienst.
HAS-Controlling	Webbasiertes Tool „Filtersystem“ für das Controlling der Hausarztversicherten.
Telmed-Controlling	Webbasiertes Tool „Telmed-Controlling“ für das Controlling der Telmed-Versicherten.
BBTP	BBTPortal: ▪ Web-Portal für Kunden ▪ Einsicht in eigenes Dossier Webrechner für Offerten

2.1.4 Unternehmensführung

Umsystem	Zweck
Scodi	Handbuch für das Managementsystem.

2.1.5 E-Mail, Internet/Extranet und Telefon

Umsystem	Zweck
Exchange	Zum Versenden von E-Mail und Verwalten der ein- und ausgehenden E-Mail.
GFI Mailarchiver	Archiviert alle ein- und ausgehenden E-Mail.
CWA	Citrix Web Access Zugriff für Heimarbeitsplätze, inklusive 3 Phasen Identifizierung
OIP Tool Box	Konfiguration der Telefonzentrale und Erstellen von Statistiken.
Business CTI	Software zum Anzeigen der Erreichbarkeit per Telefon.

2.1.6 HR-Management

Umsystem	Zweck
Digitale Personalakte	Die Personaldossiers werden elektronisch geführt.
Sage 50 Lohnbuchhaltung	Software für das Lohnwesen.
JBM	Zeiterfassungs- und Bewirtschaftungssoftware

2.1.7 Dokumentenmanagement

Umsystem	Zweck
smartFIX / Webflow	Papierdokumente werden beim Posteingang eingescannt, mit smartFIX indexiert und zur weiteren Bearbeitung an die definierte Stelle im Webflow weitergeleitet.
Kendox	Subsystem für Dokumentenmanagement und Archivierung.

2.1.8 IT-Betrieb

Umsystem	Zweck
Citrix	Stellt jedem Mitarbeitenden einen personalisierten und einheitlichen Desktop mit allen nötigen Anwendungen zum Arbeiten zur Verfügung.

2.2 Schnittstellen

Verschiedene Schnittstellen ermöglichen den Kontakt und Datenaustausch mit Leistungserbringern und weiteren Stellen zur Durchführung des Krankenversicherungsgeschäfts. In der Schnittstellenbeschreibung werden folgende Angaben zur Datenweitergabe festgehalten:

- Von wem stammen die Daten?
- Wer erhält die Daten?
- Standort der Server
- Zu welchem Zweck werden die Daten weitergegeben?
- Welche Daten werden weitergegeben?
- In welcher Periodizität werden die Daten weitergegeben?
- Von wem wurde die Weitergabe initiiert?
- Mit Hilfe welchen Mediums werden die Daten weitergegeben?

3 Beteiligte Stellen

3.1 Organisationsbereiche der Sumiswalder

Die Mitarbeitenden (MA) der nachfolgend aufgeführten Organisationsbereiche haben für die Durchführung des Krankenversicherungsgeschäfts Zugriff auf die Informationssysteme der Sumiswalder:

1. Leistungsabteilung (18 MA)
   - Kontrolle/Erstattung von ambulanten Rechnungen (keine Einsicht in Arztberichte)
   - Kontrolle/Erstattung von stationären Rechnungen (keine Einsicht in Arztberichte und MCD mit Confidential-Flag für DRG-Sachbearbeiterin)
   - Kontrolle/Erstattung von Taggeld-Leistungen nach KVG
   - Kontrolle von Unfalldossiers

2. Kundendienst (10 MA)
   - Bestandesverwaltung Beitritte und Austritte
   - Stammdatenverwaltung
   - Vertragsänderungen
   - Offerten erstellen und bearbeiten
   - Mahnwesen (4 MA)

3. Finanzbuchhaltung (2 MA)
   - Zahlungseingänge
   - Zahlungsausgänge

4. Logistik / IT (2 MA)
   - Betreiben und administrieren der Informationssysteme der Sumiswalder

3.2 Vertrauensärztlicher Dienst (VAD)

- Rechnungen und medizinische Informationen gemäss Art. 42 Abs. 5 KVG
- Expertenteam DRG: Prüfung von ausgelenkten DRG-Rechnungen, Nachcodierung

Direkt an den VAD oder der VAD Hilfspersonen (2 MA) übermittelte Rechnungen und Informationen werden im VAD durch die Vertrauensärzte und/oder VAD-Hilfspersonen überprüft und zuhanden der Leistungsabteilung zur Zahlung freigegeben. Die Erstattung erfolgt durch die zuständige Organisationseinheit der Leistungsabteilung. Die medizinischen Informationen verbleiben im VAD.

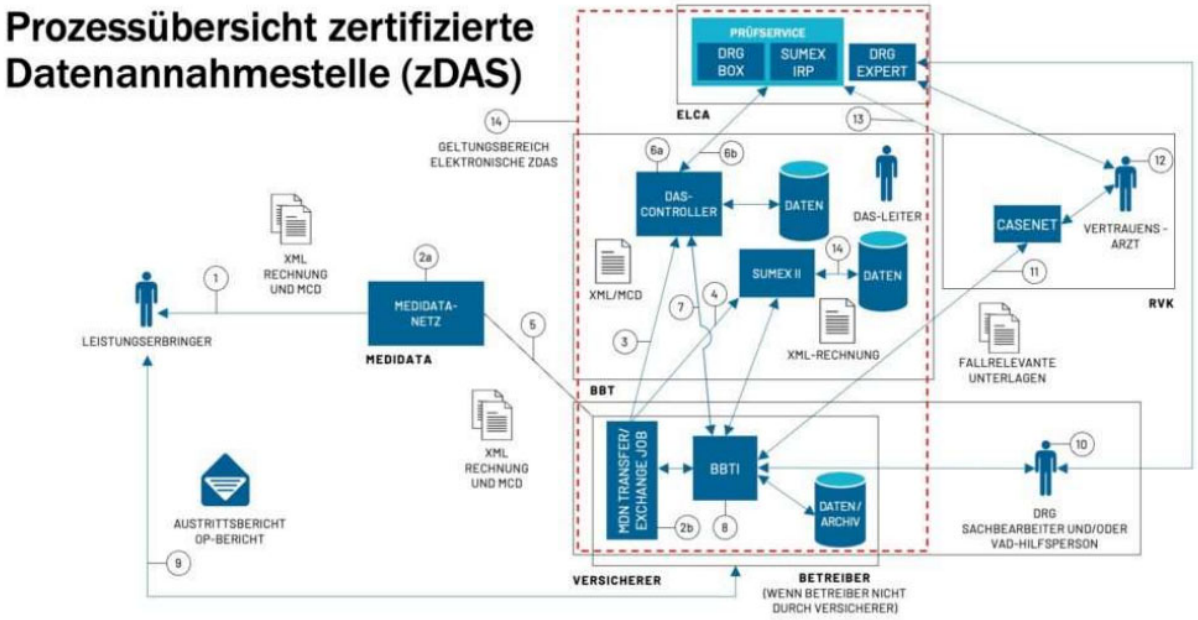
Aufgrund der Bearbeitung von sehr sensitiven Daten wird dieser Organisationsbereich speziell behandelt. Die Verarbeitung von Dokumenten erfolgt nach eigenen Prozessen mit begrenzten Zugriffsrechten. An den VA adressierte Post wird ungeöffnet an die VAD-Hilfspersonen

weitergeleitet. Das Büro der VAD-Hilfspersonen ist räumlich abgegrenzt mit eigenem Fax und Drucker. Zugang zu den Räumlichkeiten haben nur die VAD-Hilfspersonen.

Die VAD-Hilfspersonen haben eine spezielle Schweigepflichtserklärung unterschrieben mit einem eigenen Pflichtenheft.

3.3 DRG Datenbearbeitung

DRG- und Tarpsy-Rechnungen werden mit der Datenannahmestelle (DAS) bearbeitet. Die Datenannahmestelle wird von der BBT Software AG betrieben. Die Bearbeitung umfasst elektronisch übermittelte SwissDRG-Abrechnungen und in Ausnahmen – nur wenn der Leistungserbringer die Daten nicht elektronisch übermitteln kann - die Bearbeitung von in Papier zugestellten SwissDRG-Abrechnungen gemäss KVV.



Grafik: schematische Darstellung des DRG-Prozesses.

Übermittlung

(1) Der Leistungserbringer übermittelt Rechnung und MCD via MediData-Netz an MediData. Rechnung und MCD können, müssen aber nicht gleichzeitig eingesandt werden.

(2a) MediData-Netz übergibt die empfangenen Daten dem MediData-Netz Transfer/Exchange Job (2b).

(2b) Mit dem MediData-Netz Transfer/Exchange Job werden alle XML's schemageprüft. XML's, welche das Schema verletzen, werden automatisch zurückgesandt. Alle anderen Rechnungen werden weiterverarbeitet.

(3) Die Übermittlung der MCD's erfolgt unmittelbar nach der Triage mittels MediData-Netz Transfer/Exchange Job an den DAS-Controller (6a) der zertifizierten Datenannahmestelle.
Die übrigen Files (DRG Invoice) werden einerseits an Sumex II (4) bei BBT und andererseits an das Kernsystem BBTI (8) des adressierten Versicherers weitergereicht. In Sumex II werden die Rechnungen gemäss dem integrierten Regelwerk geprüft.

Datenhaltung bei MediData

Grundsätzlich wird ein Dokument so lange auf dem MediData-Netz aufbewahrt, bis es vom Empfänger abgeholt wird. In der Regel geschieht die Abholung täglich oder gar mehrmals pro Tag. Diese Einstellung obliegt dem Empfänger.

Auf dem MediData-Netz abgeholte Dokumente bleiben für weitere 90 Tage auf den MediData-Systemen gespeichert. Dies allerdings ausschliesslich zum Zweck einer erneuten Abholung, falls die Dokumente beim Empfänger verloren gegangen sind. Für die erneute Abholung bedarf es eines schriftlichen Antrages an MediData. MediData nimmt dabei weder Änderungen noch statistische Auswertungen in irgendwelcher Form an den Dokumenten vor.

Auf dem MediData-Netz bleibt ein nicht abgeholtes Dokument (Tiers Payant und Tiers Garant) bleibt maximal 90 gespeichert.

Nach Ablauf der vorhin genannten Fristen (90 Tage für abgeholte Dokumente, 2 Jahre für nicht abgeholte TG-Dokumente) werden die Dokumente bei MediData unwiderruflich gelöscht.

Bezüglich Datenschutzes kommuniziert MediData-Netz über mit Zertifikaten gesicherte Verbindungen. Des Weiteren ist die MediData ISO/IEC 27001 und VDSZ zertifiziert.

Prüfung und Speicherung MCD

Die Datenannahmestelle wird durch BBT betrieben. Sie nutzt den Prüfservice. Der Prüfservice wird durch ELCA im Auftrag der Suva betrieben.

ELCA betreibt zusätzlich DRG-Expert. Dieser Service wird für die Analyse des MCD genutzt.

Der MediData-Netz Transfer/Exchange Job des Versicherers (2b) holt Daten vom MediData-Netz ab und reicht das MCD an den DAS-Controller (6a) weiter. Die Pseudonymisierung ist erreicht, da DRGRechnung und MCD getrennt in unterschiedlichen Systemen gehalten und das MCD keinerlei Hinweise zur betroffenen Person enthält.

Der DAS-Controller (6a) empfängt die MCD aller Versicherer und speichert diese als Data BLOB ab.

Es wird kein Backup der Datenbank ausserhalb der zDAS gespeichert. Ein Verlust der gespeicherten MCDs infolge Totalausfalls des ZDAS-Servers wird aus Kostengründen bewusst in Kauf genommen, da
diese Daten jederzeit vom Leistungserbringer eingefordert werden könnten und das Risiko eines Totalausfalles sehr klein ist.

Mittels Rechnungsnummer, Rechnungsdatum und Request-Timestamp können MCD und Prüfresultat ermittelt werden. Zusätzlich wird die GLN des Versicherers verwendet. MCD's werden nach Ablauf von 180 Tagen automatisch gelöscht.

Der Prüfservice mit der DRG-Box und Sumex IRP muss keine MCD's speichern und langfristig aufbewahren. Er wird als zustandsloser Service betrieben.

Empfangene MCD's werden zwischengespeichert und erst an den Prüfservice übermittelt, wenn diese durch einen Versicherer im BBTI identifiziert worden sind.

Die frei geschalteten MCD's werden an den Prüfservice gesandt (6b). Es werden folgende Prüfungen durchgeführt:

- Kostengewicht
- Kostengewicht/Tag
- Verweildauer
- Beatmungszeit
- PCCL
- Alter
- DRG-Häufigkeit

- DRG-spezifische Hauptdiagnose
  Plausibilität Hauptdiagnose
- DRG-Klassifikation
- Plausibilität Nebendiagnosen
- Plausibilität Prozeduren
- Plausibilität PCCL
- Medizinische Plausibilisierung (ICD-/CHOP-Exklusiva, Kreuz-Stern)
- Nachgruppierung
- Prüfungen Kodierungsänderung (Simulation)

Der Prüfservice ist so konzipiert, dass in Zukunft IRP-Prüfungen bzw. auch individuelle Prüfungen erweitert/geändert werden können.

Das Prüfresultat wird an den DAS-Controller zurückgegeben und dort gespeichert.

Der DAS-Controller sendet auf Anfrage (7) den Status an den Anfragesteller wie folgt an BBTi:

- „kein MCD gefunden"
- „MCD unauffällig" oder falls das MCD als auffällig erkannt worden ist,
- „MCD auffällig" und den DRG-Expert Link mit den MCD-Daten sowie den Wert des MCDFeldes „isConfidential aka VAD"
- „Fehler in der zDAS", wenn das MCD nicht überprüft werden konnte
- „MCD bereit zum Validieren", wenn das MCD zwar freigeschaltet wurde aber noch nicht
- überprüft ist
- „Fehler in der zDAS beim Freischalten des MCD's" Das MCD konnte nicht freigeschaltet
- werden
- „MCD ist nicht Schemakonform"

Ist ein auffälliges MCD vorhanden, liefert der DAS-Controller nebst dem Status und dem Prüfresultat auch den DRG Expert URL-Link. Dieser Link dient dem Zugriff zum DRG-Expert. In DRG- Expert kann im Fallanalyse-Tab der Fall durch die DRG-Sachbearbeiterin analysiert werden.

Die Funktion des Prüfservices wird überwacht und ausgewertet. Ziel ist es, Schwachstellen und Optimierungspotential zu erkennen und so periodisch Verbesserungen einzubringen.

Verarbeitung in BBTI

(8) Empfang DRG Invoice erfolgt in BBTI. BBTI überprüft der DRG Invoice mittels Check's (s. Dokument BBTI_Checks).

Wenn ein Check anschlägt, wird die DRG Invoice ausgelenkt. Wenn keine Regel anschlägt, wird die DRG Invoice mit einem nicht auffälligen MCD direkt zur Zahlung freigegeben. Ebenfalls wird die DRG Invoice ausgelenkt, wenn ein MCD auffällig ist.

(7) Beim Empfang einer DRG-Rechnung stellt das System nach erfolgreicher Deckungsprüfungen zwei Anfragen an den DAS-Controller.

Die Anfrage setzt sich aus den Merkmalen GLN, Rechnungsnummer, Rechnungsdatum und Invoice Timestamp zusammen.

Die erste Anfrage hat zum Ziel, ein MCD für die Übermittlung an den Prüfservice zu legitimieren. Es sollen nur MCD's geprüft werden, welche zu DRG-Rechnungen mit erfolgreicher Deckungsprüfung gehören.

Mit der zweiten Anfrage wird das Prüfresultat abgefragt. Die Rückmeldung des DAS-Controllers wird bei der Rechnung gespeichert.

MCD und DRG Rechnung mit Flag vertraulich gelangen gemäss KVG 42.5 nur zur VAD Hilfsperson Ansicht und Bearbeitung von DRG-Rechnungen werden mit einem speziellen Recht versehen. Sie werden der DRG-Sachbearbeiterin oder der VAD Hilfsperson (MCD und/oder Rechnung mit VAD-Flag) im BBTI in der Inbox vorgelegt.

Ist ein MCD auffällig, liefert der DAS-Controller nebst dem Status auch den DRG Expert URL-Link.

Dieser Link dient dem Zugriff zum DRG-Expert und enthält zur weiteren Analyse die Prüfresultate:

Bei DRG-Rechnungen, welche den Status „MCD nicht vorhanden" aufweisen, stellt das System mittels Batchjob periodisch erneut eine Anfrage an den DAS-Controller.

Bei Rechnungen, welche über kein MCD verfügen oder bei denen zusätzliche Informationen (z.B. Austrittsberichte) notwendig sind, kann die Sachbearbeiterin diese elektronisch einfordern.

(9) Auf dem Postweg nachgereichte Dokumente werden eingescannt und zum elektronischen Dossier des Versicherten abgelegt.

(10) Die DRG-Sachbearbeiterin analysiert aufgrund der vorhandenen Informationen, ob die Rechnung
- bezahlt
- zurückgewiesen
- dem DRG-Prüfer von RVK zur vertieften Prüfung vorgelegt werden soll.

Zahlung und Rückweisung erfolgen durch die entsprechenden Action-Buttons.

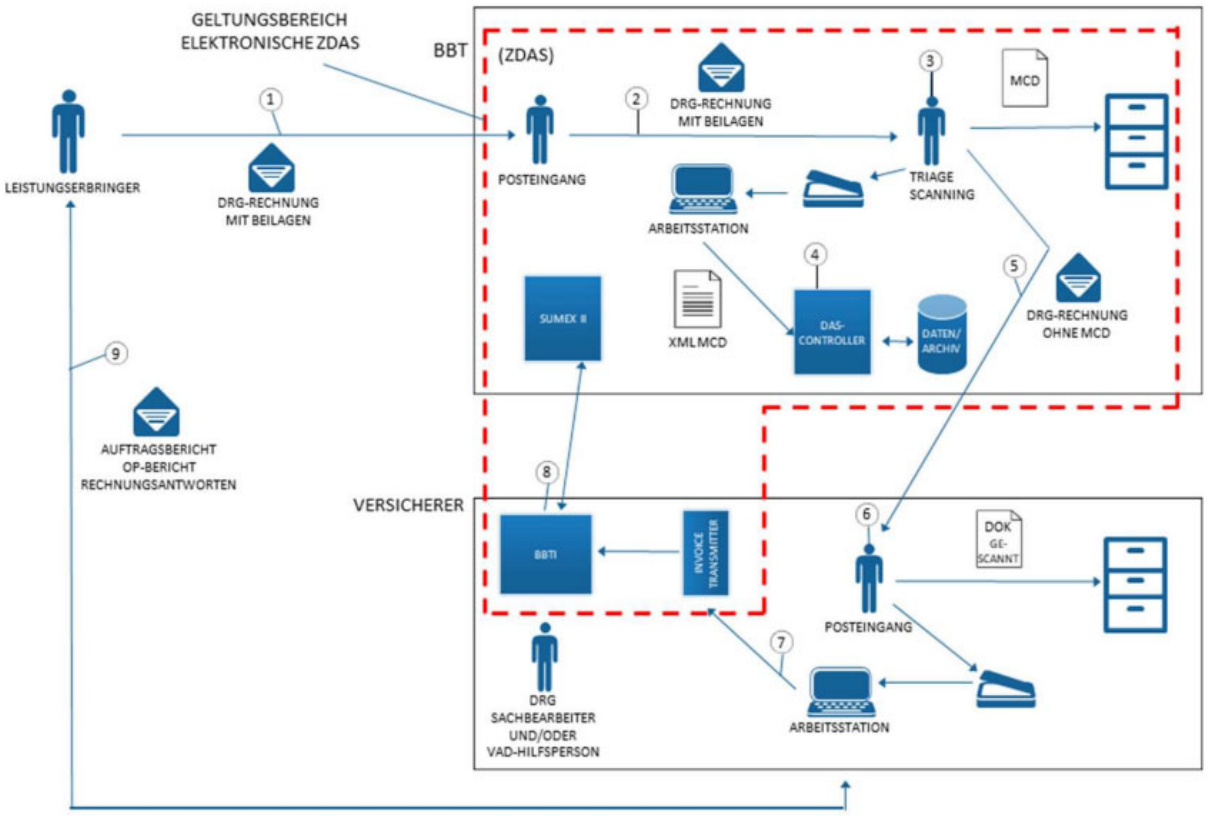
(11) Für die vertiefte Prüfung durch den RVK ist ein Auftrag an den RVK sowie die Übermittlung der für die erweiterte Abklärung notwendigen Unterlagen notwendig. Der DRG-Prüfer von RVK entscheidet mittels DRG-Expert und sendet seine Antwort zurück an die DRG-Sachbearbeiterin, oder die VAD Hilfsperson, welche(r) mit BBTI die Rechnung zurückweist oder für die Auszahlung frei gibt.

(5) Rechnungsantworten erfolgen mittels MediData-Netz Transfer/Exchange Job und MediData-Netz an den Leistungserbringer.

Vertrauensärztlicher Dienst

Der Prozess bezüglich Ablaufs zwischen der DRG-Sachbearbeiterin und dem DRGPrüfer der RVK ist im Dokument «BBT_Betrieb_Regelupdates_DRG». Der Prozess ist generisch aufgebaut und es besteht eine Schnittstelle zu CaseNet.

Datenempfang in Papierform



Grafik: schematische Darstellung des DRG-Papierprozesses.

Der Leistungserbringer versendet die DRG-Rechnung als Papierdokument an die Sumiswalder Krankenkasse, c/o zDAS BBT, BBT Software AG, Platz 4, 6039 Root D4. Die Post mit dieser Adresse wird direkt der Triage der zDAS weitergeleitet. Bei der erstmaligen Lieferung eines Leistungserbringers wird überprüft, ob bestehende Dokumenttypen verwendet werden können und so eine genügend hohe Erkennungsquote erreicht werden kann. Trifft dies nicht zu, wird bei IT-Surplus ein neuer Dokumenttyp angefordert.

Die Triage öffnet die Post (3). MCD's werden separiert und bezüglich Qualität beurteilt. Ist ein Scannen nicht oder nur mit grossem Aufwand möglich, erfolgt eine Rückfrage beim Leistungserbringer (Nachlieferung zusätzliche Informationen oder Neulieferung MCD).

Das Couvert dort geöffnet, als DRG-Rechnung erkannt, separiert, gescannt und nachbearbeitet. Anschliessend wird das Papierdokument vernichtet. Ebenfalls werden unaufgefordert zugestellte Papier-MCD vernichtet. Diese müssen nach der Dunkelprüfung und einer allfälligen Auslenkung z. H. des vertrauensärztlichen Dienstes neu angefordert werden. Sobald die Rechnung im Standard XML 4.4 oder 4.5 erstellt ist, läuft der Prozess analog den elektronisch eingelieferten Daten ab.

Die MCD werden gescannt und anschliessend reworked. Das System verlangt vor dem Speichern von der Sachbearbeiterin die Bestätigung für die Parameter:
- Versicherer (Versicherername und GLN)
- Rechnungsnummer
- Rechnungsdatum
- Timestamp (Konstante IT-Surplus Versicherer muss ebenfalls IT-Surplus fürs Scannen einsetzen)

Diese Informationen sind essenziell für die spätere Erkennung durch BBTI.
Die gescannten MCD werden dem DAS-Controller übergeben (4). Diese werden ab Übergabeschnittstelle gleich verarbeitet wie die elektronisch empfangenen MCD's.

Zusätzlich entstehen beim Scan-Prozess Bilder des MCD. Diese werden beim Scannen in ein spezielles Verzeichnis gespeichert. Der Inhalt dieses Verzeichnisses wird täglich automatisch mittels Standardprozess gelöscht, da diese Bilder nicht weiter benötigt werden.

Das Original-MCD wird unmittelbar nach der Verarbeitung in einem verschlossenen Couvert im Schredder von BBT vernichtet. Die übrigen Dokumente werden neu verpackt, an den Ziel-Versicherer adressiert und versandt.

4 Benutzer und Datenzugriff

4.1 Benutzer

Zugriffsberechtigt auf BBTI sowie auf die Subsysteme sind die Mitarbeitenden der Sumiswalder, soweit sie dies zur Ausübung ihrer Tätigkeit benötigen. Zwecks Installation und Support haben externe Dienstleistungsunternehmen im Rahmen der Ausübung ihrer Tätigkeit temporär Zugriff auf Teile der Serverumgebung.

Zugriffberechtigung DRG haben:
- Expertenteam DRG/Codierspezialisten
- VAD (Vertrauensärztinnen, Vertrauensärzte und deren Hilfspersonen)
- DRG-Sachbearbeiterin

4.2 Benutzerverwaltung

Die Benutzerverwaltung erfolgt zentral durch den Leiter IT im Auftrag der Geschäftsleitung. Der Leiter IT koordiniert zusammen mit der Geschäftsleitung, dass die Mitarbeitenden, die für die Ausübung ihrer Tätigkeit notwenigen Zugriffsrechte erhalten. Die Zugriffsberechtigungen werden im File „Benutzer Erfassung“ dokumentiert und verwaltet.

4.3 Aufhebung der Zugriffsberechtigung

Die Benutzer sind nur so lange und in dem Umfang zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Arbeitsfunktion benötigen. Bei Austritt wird die Zugriffsberechtigung entzogen.

4.4 Ausbildung der Benutzer

Die Benutzer werden auf BBTI und auf allen Subsystemen intern und extern geschult. Mit dem Datenschutz-Quiz sowie Schulungen mit externen Spezialisten werden die Mitarbeitenden zudem regelmässig im Bereich Datenschutz sensibilisiert.

4.5 Prozesse

Die Arbeitsprozesse werden im internen Management-System (Scodi) abgebildet und beschrieben.

5 Datenbearbeitung / Datenkategorien

5.1 Datenherkunft

Die Daten stammen hauptsächlich von den Versicherten selbst sowie von Personen oder Stellen, die von den Versicherten berechtigt wurden, die Daten an die Sumiswalder zu übermitteln (Leistungserbringer, Versicherungen, Amtsstellen).

5.2 Datenkategorien

Wir teilen die Personendaten in folgende Kategorien ein:
A Schützenswerte Personendaten
B Besonders schützenswerte Personendaten
C Persönlichkeitsprofile

Im Anhang 1 werden die Personendaten, die bei der Sumiswalder bearbeitet werden, aufgeführt und klassifiziert.

5.3 Datenweitergabe nach Art. 84a KVG in Verbindung mit Art. 84 KVG

Daten werden bekanntgegeben, um:
- den ununterbrochenen Versicherungsschutz zu prüfen (Art. 7 Abs. 5 KVG: Mitteilung des Vorversicherers an den neuen Versicherer)
- Leistungsansprüche zu beurteilen (z. B. Limitierungen nach KLV)
- die Leistungen mit denen anderer Sozialversicherer zu koordinieren (Art. 27 KVG: Koordination mit der IV in Zusammenhang mit Geburtsgebrechen)
- ein Rückgriffsrecht gegenüber haftpflichtigen Dritten geltend zu machen
- Statistiken zu führen
- die AHV-Versichertennummer zuzuweisen oder zu kontrollieren

Unter die Datenempfänger fallen:
- Versicherte und von ihnen bevollmächtigte Dritte
- Leistungserbringer (Online-Prüfungsverfahren mit Versichertenkarte)
- Behörden (Kantone, BAG, IV-Stellen u.a.)
- der Verband der Krankenversicherer santésuisse
- Partnerversicherungen
- Gerichte
- Sozialdienste
- Vertrauensärzte und -ärztinnen

5.4 Weitere Datenweitergabe nach Art. 84a KVG

Die weitere Datenbekanntgabe ist abschliessend in Art. 84a KVG geregelt. So können im Einzelfall und auf schriftlich begründetes Gesuch hin Daten gemäss den spezifischen Anforderungen an Sozialhilfebehörden, Zivilgerichte, Strafgerichte und Strafuntersuchungsbehörden, Betreibungsämter, sowie mit schriftlicher Einwilligung der betroffenen Person an Dritte weitergegeben werden.

6 Datenarchivierung

6.1 Archivierungspflicht

Archivierungspflichtige Dokumente werden während der gesetzlich verlangten Dauer archiviert und vor Veränderungen und unbefugten Zugriffen geschützt. Dies betrifft sowohl physisch vorhandene Dokumente als auch elektronisch gespeicherte Daten.

6.2 Aufbewahrungsdauer

Die Aufbewahrungsdauer der Daten entspricht den spezifischen gesetzlichen Bestimmungen des schweizerischen Rechts.

Die Aufbewahrungsdauer richtet sich nach den festgesetzten Aufbewahrungsfristen für auf Papier erstellte Akten.

6.3 Löschung der Daten

Nach Ablauf der gesetzlichen Aufbewahrungsfristen sind die Daten aus dem Sumiswalder Informationssystem zu löschen.

7 Technische und organisatorische Massnahmen (TOM)

7.1 Zugangskontrolle

Unbefugten Personen wird der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, verwehrt.

Bezeichnung	Beschreibung
Sicherheitszonen	Sensitive Räumlichkeiten (Bsp. Serverräume, Räume mit wichtigen Telekommunikationseinrichtungen, Räume für Backup-Kopien, Archive) werden Sicherheitszonen zugewiesen.
Regelung der Zutrittsberechtigungen	Der Zutritt zu Informatikräumen und -mitteln ist mittels einer verbindlichen und nachvollziehbaren Zutrittsberechtigung geregelt. Diese wird sinnvoll abgestuft.
Schliess- und Zutrittsplan	Die Einträge zu den Sicherheitszonen verfügt über ein sicheres Schliess- und Zutrittssystem. Der Schliessplan dokumentiert, wie Verantwortlichkeiten, Verwaltung, Vergabe und Rücknahme der Zutrittsmittel geregelt sind.
Kontrolle Schliess- und Zutrittssystem	Schliess- und Zutrittssysteme werden regelmässig auf ihre korrekte Funktionsweise überprüft.
Raumsichernde Massnahmen	Der Zutritt durch andere Gebäudeöffnungen wird durch raumsichernde Massnahmen, wie Alarmanlage, Fenstergitter, Sicherheitstoren usw. verhindert.

7.2 Datenträgerkontrolle

Unbefugten Personen wird das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern verunmöglicht.

Bezeichnung	Beschreibung
Vergabe von Benutzeraccounts	Die Vergabe von Benutzeraccounts ist verbindlich geregelt, dokumentiert und wird überwacht.
Sperrung bzw. Löschung von Benutzeraccounts	Accounts und Zugriffsrechte die nicht mehr benötigt (z.B. Austritt) werden oder über längere Zeit nicht mehr benutzt worden sind, werden gesperrt oder gelöscht.
Einsicht auf periphere Geräte	Im Umfeld von Schaltern, Sekretariaten und anderen publikumszugänglichen Bereichen haben Unberechtigte keine Einsicht auf periphere Geräte.
Authentifizierung	Die Zugangsberechtigung auf Systeme erfolgt mit einer Benutzeridentifikation und einem sicheren Passwort entsprechend den Vorgaben im IT-Zonenplan.

7.3 Transportkontrolle

Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Bezeichnung	Beschreibung
Bezeichnung von Datenträgern	Datenträger (Papier, Festplatten, Bänder, Sticks, usw.) mit klassifizierten Daten werden als solche bezeichnet.
Verpackung und Adressierung von Datenträgern	Datenträger mit Personendaten werden für den Versand entsprechend verpackt und adressiert.
Gesicherte Übertragung von kritischen Daten	Die Vertraulichkeit und Integrität von Authentifikationsdaten, Schlüsseln oder anderen kritischen Systemdaten wird bei der Übertragung der Daten über Netzwerke geschützt.
Protokollierung von/zu Verbindungen zu Fremdnetzen	Übertragungen von/zu Fremdnetzen werden protokolliert (Verbindungsaufbau, Benutzer).

7.4 Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstelle identifiziert. Die Übermittlung von Personendaten findet immer über einen verschlüsselten Kanal statt (z.B. SFTP).

7.5 Speicherkontrolle

Unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten werden verhindert.

Durch sicherheitstechnische Vorkehrungen ist es ausschliesslich berechtigter Personen möglich, Daten im Informationssystem abzufragen oder zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf das Informationssystem.

Der Zugriff auf das Informationssystem der Sumiswalder wird durch einen User-Account kombiniert mit einem zeitlich limitierten, individuellen Passwort geschützt. Die Passwortrichtlinie wird über entsprechende technische Vorgaben durchgesetzt.

Gewisse Umsysteme sind mit der Verwendung eines zusätzlichen Passwortes geschützt.

7.6 Benutzerkontrolle

Die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert. Dies wird mittels Zugriffsberechtigungen gesteuert und wird im Kapitel 4 näher beschrieben.

7.7 Zugriffskontrolle

Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie für die Erfüllung ihrer Aufgabe benötigen. S. Kapitel 4.

7.8 Eingabekontrolle

Wir können mittels Log-Files überprüfen, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden. Die Protokollierung wird nur dann eingesehen, wenn sie sinnvoll oder notwendig ist. Die Mitarbeitenden sind über die Protokollierungen informiert.

7.9 Massnahmen im Bereich der Endgeräte

Es dürfen nur Sumiswalder eigene Endgeräte am internen Netzwerk angeschlossen werden. Die Schnittstellen für einen möglichen Datenaustausch sind nur einem dezidierten Personenkreis freigegeben.

Beim Verlassen des Arbeitsplatzes sind die Mitarbeitenden angewiesen, das Endgerät entsprechend mit einer Zugangssperre zu belegen. Findet innerhalb einer bestimmten kurzen Zeit keine Aktivität auf dem Endgerät statt, wird dieses automatisch mit einer Zugangssperre belegt.

Die lokalen Datenspeicher in den mobilen Endgeräten werden durch ein starkes Verfahren verschlüsselt und mit einem Passwort geschützt.

Papierakten werden so aufbewahrt, dass Drittpersonen diese nicht einsehen, entwenden oder kopieren können. Diese Daten werden in abschliessbaren Behältnissen aufbewahrt oder mit Aktenvernichter (Schredder), respektive über die Spezialcontainer der Firma Datarec entsorgt.

8 Rechte der betroffenen Person

8.1 Auskunftsrecht

Jede Person kann von der Sumiswalder schriftlich Auskunft darüber verlangen, welche Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 25 und 26 DSG sowie Art. 16 - 19 DSV.

Die Auskunftsgesuche sind unter Beilage der Kopie eines amtlichen Ausweises an die Sumiswalder Krankenkasse, zu Handen Datenschutzberater, Spitalstrasse 47, 3454 Sumiswald, zu richten.

9 Abschliessende Bestimmungen

9.1 Anhang

Der im vorliegenden Bearbeitungsreglement erwähnte Anhang 1 ist integrierendender Bestandteil dieses Bearbeitungsreglements.

9.2 Änderungen des Reglements

Das Bearbeitungsreglement wird gemäss Art. 6 DSV regelmässig aktualisiert. Änderungen bedürfen der Schriftform und der Zustimmung der Geschäftsleitung.

9.3 Inkrafttreten

Dieses Reglement tritt per 1. Januar 2024 in Kraft. Es ersetzt alle älteren Ausgaben und Versionen.

Sumiswalder Krankenkasse

Rolf Pfister
Geschäftsführer

Christoph Pfister
stv. Geschäftsführer

Anhang 1: Datenkategorien

Kategorie	Stamm- und Vertragsdaten
A	Name, Vorname
A	Geschlecht
A	Geburtsdatum / Alter
A	Anrede
A	AHVN13
A	Sprache
A	Nationalität
A	Kantonszugehörigkeit
A	Gemeindezugehörigkeit
A	Versichertennummer
A	Adresse
A	Bank- / Postverbindung
A	Telefonnummern
A	Art der Versicherung und Deckung
A	Angaben zum Begünstigten
A	Vor- und Nachversicherer
A	Sistierung
A	Prämie
A	Prämienfakturierung
A	Franchisen
A	Kostenbeteiligungen
B	Kantonale Prämienverbilligung
B	Mahndaten

Kategorie	Rechnungsdaten:
B	Leistungserbringer
B	Rechnungsteller
B	EAN-Nummer
B	Rechnungsdatum
B	Rechnungsnummer
B	Behandlungsbeginn-Datum
B	Behandlungsende-Datum
B	Behandlungsdauer
B	Rechnungsbetrag
B	Taxpunkte
B	Taxpunktwert
B	Tarifdaten
B	SwissDRG-Nummer
B	Kostengewicht SwissDRG
B	Basisfallpreis
B	Medikamente
B	Leistungsart: Krankheit, Unfall, Mutterschaft

Kategorie	Medizinischer Datensatz
B	Geburtsgewicht
B	Hauptdiagnose ICD-10-GM-Kode
B	Zusatz zu Hauptdiagnose ICD-10-GM-Kode
B	Nebendiagnosen IDC-10-GM-Kode
B	Hauptbehandlung CHOP-Code
B	Seitigkeit der Hauptbehandlung
B	Beginn der Hauptbehandlung
B	Nebenbehandlungen CHOP-Code
B	Seitigkeit der Nebenbehandlung
B	Beginn der Nebenbehandlung
B	Dauer der künstlichen Beatmung
B	Aufnahmegewicht
B	Abklärung Garant
B	Operationsbericht
B	Arztbericht
C	Ausführlicher Arztbericht / Gutachten

Kategorie	Administrativer Datensatz
A	Alter bei Eintritt
B	Eintrittsdatum und -stunde
A	Aufenthaltsort vor dem Eintritt
B	Eintrittsart
B	Administrativer Urlaub und Ferien
B	Austrittsdatum und -stunde
B	Entscheid für Austritt
B	Aufenthalt nach Austritt
B	Zwischenaustritt
B	Wiedereintritt
B	Einweisende Instanz
B	Behandlungsart
B	Klasse
B	Geburtsdatum Mutter

Kategorien:
A = Schützenswerte Personendaten
B = Besonders schützenswerte Personendaten
C = Persönlichkeitsprofile