Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern
Bundesamt für Gesundheit

Nicht klassifiziert

Bearbeitungsreglement zentrale Abfragedienste EPD

Klassifizierung *	**Nicht klassifiziert**
Status **	Abgeschlossen/Genehmigt
Projektname	Zentrale Abfragedienste EPD
Projektnummer	22194
Auftraggeber/-in	Daniel Megert
Inhaber der Datensammlung (Amt, OE)	Bundesamt für Gesundheit
Datenherr (Data Owner)	Pascal Strupler
Anwendungsverantwortliche/-r	Thorsten Kühn
Projektleiter/-in	Thorsten Kühn
DSBO	Federica Liechti
Bearbeitende	Redguard AG
Prüfende	Thorsten Kühn
Genehmigung durch Projektauftraggeber/-in	Salome von Greyerz
Version	1.0

* INTERN, VERTRAULICH, GEHEIM
** In Arbeit, In Prüfung, Abgeschlossen/Genehmigt

Druckdatum: 30.07.2019

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name
0.10	25.07.2019	Initialisierung des Dokuments basierend auf dem Bearbeitungsreglement ZAD EPD Interne Version	Redguard AG
1.0	30.07.2019	Genehmigung/Freigabe zur Nutzung	BAG

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Generelles

1.1 Beschreibung

Die zentralen Abfragedienste (ZAD) liefern die notwendigen Referenzdaten für die Kommunikation zwischen Gemeinschaften und Stammgemeinschaften, die am Vertrauensraum des elektronischen Patientendossiers (EPD) teilnehmen. Die ZAD werden durch das Bundesamt für Informatik und Telekommunikation (BIT) aufgebaut und richten sich nach den in der Verordnung über das elektronische Patientendossier (EPDV) des Bundesrates und der Verordnung des Eidgenössischen Departements des Innern über das elektronische Patientendossier (EPDV-EDI) genannten Standards. Gemäss Art. 39 EPDV können bei den ZAD folgende Daten abgefragt werden:

- im Community Portal Index (CPI) Stammdaten und Endpunkte der Gemeinschaften und Stammgemeinschaften (G/SG).
- im Health Provider Directory (HPD) Gesundheitseinrichtungen und Gesundheitsfachpersonen (GFP)
- im Metadata Index (MDI) Metadaten nach Art. 10 Abs. 3 Bst. a EPDV

Die Bearbeitung der Daten des CPI und des MDI erfolgt durch das Bundesamt für Gesundheit (BAG). Die Daten des HPD werden durch die G/SG gemäss Art. 41 EPDV bearbeitet und können vom BAG zu Evaluationszwecken eingesehen werden.

Das Bearbeitungsreglement zu den ZAD ist regelmässig zu aktualisieren.

1.2 Zweck des Dokuments

Ein Bearbeitungsreglement soll für die notwendige Transparenz im Rahmen der Systementwicklung und -adaption, wie auch der elektronischen Bearbeitung von Personendaten sorgen. Im Rahmen der Erstellung der Sicherheitsdokumente zum Schutzobjekt ZAD wurde entschieden, dass dieses Schutzobjekt auch über ein Bearbeitungsreglement verfügen muss.

Das vorliegende Dokument beschreibt insbesondere die interne Organisation des BAG als verantwortliches Bundesorgan sowie die Datenbearbeitungs- und Kontrollverfahren.

Weiter bezweckt dieses Dokument die Schaffung einer Transparenz über die teils automatisierte Bearbeitung von Personendaten sowie über Bearbeitungen von Daten innerhalb der Datensammlung, welche nicht durch das BAG erfolgen, um eine fachgemässe Auswertung und Beurteilung allfälliger Datenschutzrisiken zu ermöglichen.

1.3 Abgrenzung

Eingesetzte Hardware der Gemeinschaften und Stammgemeinschaften liegen nicht in der Obhut des Bundesamts für Gesundheit und werden in diesem Bearbeitungsreglement nicht eingehender thematisiert.

2 Allgemeines

2.1 Gesetzliche Grundlagen

Dokumententyp	Titel
Gesetz	SR 235.1 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)
	SR 152.1 Bundesgesetz vom 26. Juni 1998 über die Archivierung (Archivierungsgesetz, BGA)
	SR 816.1 Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG)
Verordnung	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV)
	SR 510.411 Informationsschutzverordnung (ISchV)
	SR 235.11 Verordnung zum Bundesgesetz über den Datenschutz (VDSG)
	SR 172.010.442 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen
	SR 816.11 Verordnung vom 22. März 2017 über das elektronische Patientendossier (EPDV)
	SR 816.111 Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier (EPDV-EDI)

Tabelle 1: Übersicht gesetzliche Grundlagen

2.2 Zweck der Datensammlung

Die ZAD liefern Referenzdaten, welche für die Kommunikation zwischen den G/SG benötigt werden. Die ZAD werden vom BIT betrieben und so den Akteuren des EPD zur Verfügung gestellt.

2.3 Inhalt der Datensammlung

Die ZAD beinhalten die folgenden Verzeichnisse / Indexe:

Community Portal Index (CPI): Verzeichnis aller zertifizierten G/SG und deren Zugangspunkte, welche zum gegebenen Zeitpunkt am EPD teilnehmen. Dieses Verzeichnis enthält die Identifikationsnummer der G/SG. Es sind keine Personendaten in diesem Verzeichnis vorhanden.

Datenlieferant: G/SG

Datenempfänger: BAG, G/SG

Datenbearbeitung: BAG

Health Provider Directory (HPD): Verzeichnis aller Gesundheitseinrichtungen und GFP, die als EPD-Nutzer registriert sind. Dieses Verzeichnis enthält Personendaten.

Datenlieferant: G/SG

Datenempfänger: G/SG

Datenbearbeitung: G/SG

Metadata Index (MDI): Verzeichnis aller gültigen Metadaten (Value Sets), die bei der Registrierung und beim Austausch von EPD-Dokumenten und bei der Registrierung von Gesundheitseinrichtungen und GFP im HPD durch die G/SG verwendet werden müssen.

Datenlieferant: BAG

Datenempfänger: G/SG

Datenbearbeitung: BAG

Die folgende Tabelle gibt eine Übersicht über die Spezifikationen der einzelnen Inhalte bezüglich dem Schutzbedarf der vorhandenen Datensammlungen:

Verzeichnisse / Indexe	Form		Konstanz				DSG		ISchV		Sonstiger Schutzbedarf		
	Digital	Analog	Statisch	Fast statisch	Dynamisch	flüchtig	Personendaten	Bes. Schütz. / Pro-	Vertraulich	Intern	Hoch	Mittel	Gering
CPI – Community Portal Index	X			X								X	
HPD – Health Provider Directory	X				X		X					X	
MDI – Metadata Index	X			X								X	

Tabelle 2: Inhalt der Datensammlung

3 Verantwortlichkeiten

Den nachfolgenden Organisationseinheiten obliegen unterschiedliche Verantwortlichkeiten für die Datensammlungen des Kapitels 2.3 *Inhalt der Datensammlung*.
Wichtig: Es haben nur die rot markierten Organisationseinheiten Zugriff auf die ZAD.

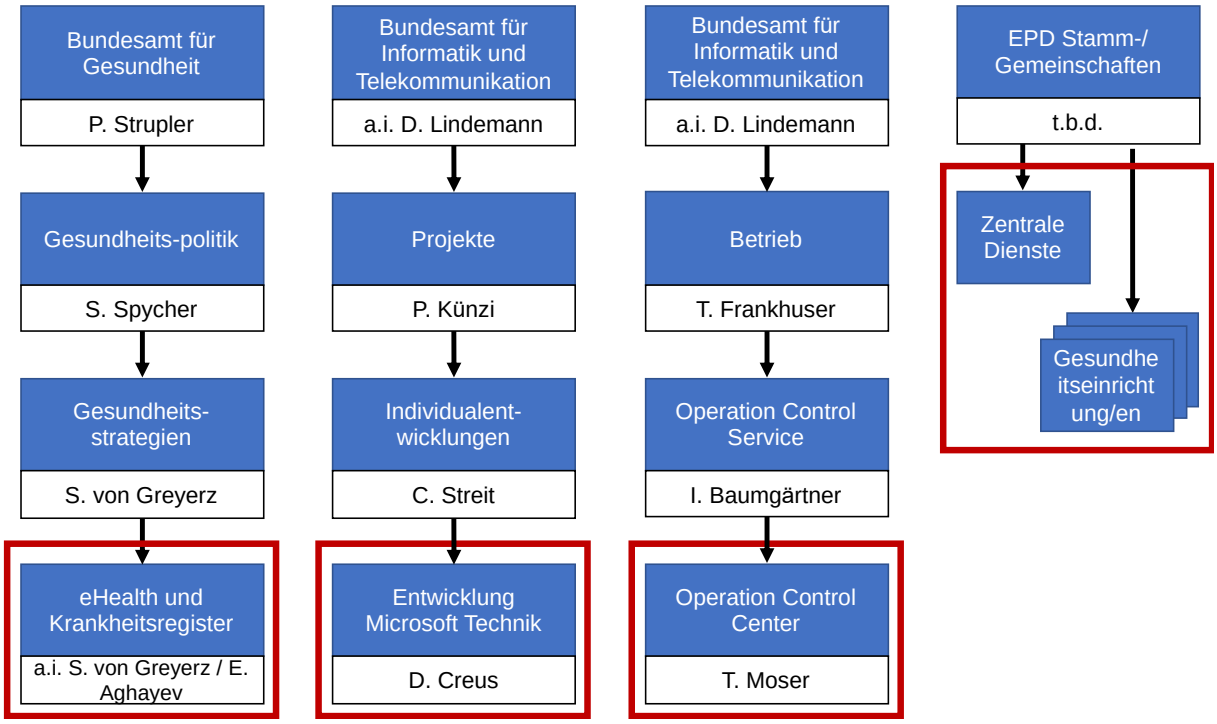

Abbildung 1: Übersicht Verantwortlichkeiten

3.1 Verantwortliches Bundesorgan

Verantwortliches Departement	Eidgenössisches Departement des Innern (EDI)
Verantwortliches Bundesamt	Bundesamt für Gesundheit (BAG), 3003 Bern
Verantwortlicher Direktionsbereich	Gesundheitspolitik
Verantwortliche Sektion	eHealth und Krankheitsregister
Benutzerkreis	• BAG • G/SG

Tabelle 3: Übersicht verantwortliches Bundesorgan

3.2 Leistungserbringer

Systembetreiber Departement	Eidgenössisches Finanzdepartement (EFD)
Leistungserbringendes Bundesamt	Bundesamt für Informatik und Telekommunikation (BIT)
Verantwortliche Sektion	Entwicklung Microsoft-Technologien
Benutzerkreis	• Team EPD, Abteilung Entwicklung Microsoft-Technologien • Team Operation Control Center

Tabelle 4: Übersicht Leistungserbringer

Sämtliche übergreifenden Verantwortlichkeiten auf Stufe des Leistungserbringers (Netzwerk, Datenbanken, Betriebssystem, etc.) sind dem dazugehörenden ISDS-Konzept, bzw. SLA und Vertrag zu entnehmen.

3.3 Datenlieferanten und Datenempfänger

Datenlieferant 1	Die G/SG liefern Daten für den HPD und sind verantwortlich für die Qualität und Korrektheit sowie die Verwaltung der Daten.
Datenlieferant 2	Das BAG liefert Daten für den CPI und den MDI. Es ist verantwortlich für die Validierung auf syntaktische Korrektheit der Anfragen an die ZAD sowie für die Einhaltung von notwendigen Geschäftsregeln, um die gesetzlichen Vorgaben zu erfüllen.
Datenempfänger 1	Die G/SG sind Endanwender der ZAD und empfangen Daten durch das Abfragen der Dienste.
Datenempfänger 2	Das BAG erhält von den G/SG die Daten zur Eintragung einer G/SG im CPI.

Tabelle 5: Übersicht Datenlieferanten und Datenempfänger

3.4 Schnittstellen

Dieses Kapitel zeigt auf wie die in den vorangegangenen Kapiteln genannten Organisationen im Kontext ZAD miteinander kommunizieren und über welche technische Infrastruktur sie miteinander verbunden sind. Die einzelnen Prozesse werden im Kapitel 5.2 *Geschäftsprozesse* dieses Dokumentes nochmals aufgeführt und detailliert beschrieben. Die technischen Gegebenheiten sind im ISDS-Konzept und weiteren Projektdokumenten detailliert beschrieben und werden daher in diesem Bearbeitungsreglement nicht weiter erläutert.

3.4.1 Organisatorisch

Organisatorische bzw. prozessuale Schnittstellen ergeben sich aufgrund der im Kapitel 5.2 beschriebenen Geschäftsprozesse. Die bildliche Darstellung und Beschreibung der Schnittstellen sind dem Kapitel 5.4 *Datenbekanntgabe und Schnittstellen* zu entnehmen.

3.4.2 Technisch

Der Datenbankserver der ZAD wird in der Infrastruktur des BIT betrieben. Die Architekturskizze mit den technischen Schnittstellen und die Kommunikationsmatrix des Leistungserbringers BIT sind für die Öffentlichkeit aus Betriebssicherheitsgründen nicht zugänglich.

Weitere Informationen zu den technischen Schnittstellen sind dem Kapitel 5.6 *Prozesse / Datenverfahren* zu entnehmen.

4 Benutzer und Datenzugriffe

4.1 Benutzerkreise

Benutzerkreis	Zweck
BAG – Sektion eHealth und Krankheitsregister	• Datenpflege CPI • Datenpflege MDI • Evaluation Daten des HPD
G/SG	• Datenpflege HPD • Datenabruf CPI • Datenabruf HPD • Datenabruf MDI
BIT - Operation Control Center	• Überwachung der ZAD (d.h. Prüfung, ob die ZAD korrekte Antworten senden)

Tabelle 6: Benutzerkreise

4.2 Zugriffsberechtigungen / Zugriffsmatrix

Die folgende Tabelle dokumentiert die Zugriffsberechtigungen für die Bearbeitung der Daten gemäss CRUD – Create, Read, Update und Delete.

	HPD				MDI				CPI			
Benutzerkreis	C	R	U	D	C	R	U	D	C	R	U	D
G/SG	X	X	X	X		X				X		
BAG		X			X	X	X	X	X	X	X	X
BIT – Operation Control Center	X	X	X	X		X				X		

Tabelle 7: Zugriffsberechtigungen Datensammlungen

Das BIT hat technisch die gleichen Zugriffsberechtigungen wie G/SG, da sie über die gleiche Schnittstelle zugreifen können. Organisatorisch wird jedoch sichergestellt werden, dass das Operation Control Center (OCC) nur Lesezugriffe ausführen darf. Die konkrete Definition derjenigen Anfragen, welche das OCC an die ZAD senden darf, wird im Monitoringkonzept des OCC dokumentiert. Das Monitoringkonzept des OCC wird aktuell erarbeitet.

4.3 Rollenkonzept

Rolle	Beschreibung
G/SG	• Liefern per elektronischer Schnittstelle Daten für den HPD • Rufen per elektronischer Schnittstelle Daten aus dem HPD ab • Liefern per E-Mail oder Formular Daten für den CPI • Rufen per elektronsicher Schnittstelle Daten aus dem CPI ab • Rufen per elektronischer Schnittstelle Daten aus dem MDI ab
BAG-ZAD-Administrator	Der BAG-ZAD-Administrator ist zuständig für die Qualitätssicherung der Daten im MDI und CPI. Er hat dazu folgende Rechte: • Trägt von den G/SG gelieferte Daten in den CPI ein • Mutiert Daten im CPI • Trägt das durch den Local Registration Authority Officer (LRAO) pro G/SG ausgestellte PKI-Zertifikat im CPI ein. Gewährt den G/SG damit Zugriff auf die ZAD und bestätigt sie als Mitglieder des EPD Vertrauensraums. • Importiert Value Sets (Datenquelle Art-Decor[1]) in den MDI • Liest Daten im HPD • Liest Daten im ZAD Audit-Log
Berechtigungsverantwortliche/r BAG	• Erteilt den Mitarbeitenden des BAG die erforderlichen Rollen und Rechte für den Zugriff auf die ZAD.
OCC	Das OCC nimmt funktionale Tests der ZAD vor. (Im Monitoringkonzept wird zu einem späteren Zeitpunkt genauer definiert auf welche Daten aus welchen Systemen zugegriffen wird. – Diese Information wird nach Freigabe des Monitoringkonzepts ergänzt.)

Tabelle 8: Rollenbeschreibung

4.4 Prozess Zugriffsberechtigung

4.4.1 Zugriffsberechtigung für Gemeinschaften und Stammgemeinschaften

Vergabe der Zugriffsberechtigung für G/SG

Der Prozess zur Vergabe der Zugriffsberechtigung für G/SG auf die ZAD ist dem Kapitel 5.2.1 *G/SG im CPI eintragen und ändern* zu entnehmen.

Eine G/SG erhält nur dann Zugriff auf die ZAD, wenn die nachfolgenden Voraussetzungen erfüllt sind:

- Es erhalten nur gemäss dem Bundesgesetz zum elektronischen Patientendossier (EPDG) zertifizierte G/SG Zugriff auf die ZAD. Die G/SG sind gesetzlich verpflichtet, sich von einer Zertifizierungsstelle entsprechend zertifizieren zu lassen.
- Sobald dem BAG die Bescheinigung der Zertifizierung vorliegt, stellt ein Local Registration Authority Officer (LRAO) des BAG ein Swiss Government PKI Zertifikat für diese G/SG aus.
- Die G/SG und das Swiss Government PKI Zertifikat wird vom BAG-ZAD-Administrator im CPI eingetragen und die G/SG wird im CPI aktiv geschaltet.
- Zudem wird das Zertifikat durch das BIT bei der elektronischen Schnittstelle hinterlegt.

[1] Art-Decor® ist eine Open-Source-Toolsuite, die die Erstellung und Pflege von HL7-Vorlagen, Value Sets, Szenarien und Datensätzen unterstützt. Im Projekt EPD wird Art-Decor zur Modellierung und Dokumentation von Value Sets eingesetzt. Siehe auch https://art-decor.org/art-decor/decor-project--ch-epr-

- Die G/SG erhält das Swiss Government PKI Zertifikat inkl. Passwort und kann dieses in seinen Systemen hinterlegen.

Entzug der Zugriffsberechtigung
Die Zugriffberechtigungen auf die ZAD können durch die Revokation des Zertifikats oder durch die Deaktivierung der G/SG im CPI durch das BAG (siehe dazu Kapitel 5.2.8 *Notfallausschluss Gemeinschaft oder Stammgemeinschaft*) wieder entzogen werden.

Die Revokation eines Zertifikats erfolgt via Meldung an die Swiss Goverment PKI.

Die genaue Ausgestaltung des Prozesses für den Entzug der Zugriffsberechtigung besteht zum aktuellen Zeitpunkt noch nicht.

4.4.2 Zugriffsberechtigung für BAG-ZAD-Administratoren

Die oder der Berechtigungsverantwortliche BAG erteilt den Mitarbeitenden des BAG die erforderlichen Rollen und Rechte für den Zugriff auf die ZAD.

Der Prozess der Vergabe (Beantragung, Freigaben, Ausführung und Nachhaltung der Berechtigung) muss zu einem späteren Zeitpunkt ergänzt werden. Die Dokumentation des Prozesses ist wichtig, um einerseits die Segregation of Duties sicherzustellen und anderseits den Mitarbeitenden die Anlaufstelle zur Beantragung der Vergabe der Zugriffsberechtigungen bekannt zu geben.

4.4.3 Zugriffsberechtigung für Operation Control Center

Das OCC erhält den Zugriff auf die ZAD, wenn die nachfolgenden Voraussetzungen erfüllt sind:

- Der LRAO des BAG stellt ein Swiss Government PKI Zertifikat für das OCC aus.
- Das OCC und das Swiss Government PKI Zertifikat wird vom BAG-ZAD-Administrator im CPI eingetragen und das OCC wird im CPI aktiv geschaltet.
- Zudem wird das Zertifikat durch das BIT bei der elektronischen Schnittstelle hinterlegt.
- Das OCC erhält das Swiss Government PKI Zertifikat inkl. Passwort und kann dieses in seinen Systemen hinterlegen.

5 Bearbeitung der Daten

5.1 Datenkategorien

Die Datenkategorien können der *Tabelle 2: Inhalt der Datensammlung* des Kapitels 2.3 *Inhalt der Datensammlung* entnommen werden.

5.2 Geschäftsprozesse

Die technischen Spezifikationen zur Implementierung der Geschäftsprozesse, die in den folgenden Kapiteln erwähnt werden, sind auf der Website des BAG verfügbar.[2]
Zum aktuellen Zeitpunkt liegen noch keine Dokumentationen zu den Geschäftsprozessen zum Monitoring durch das BIT (OCC) und der Evaluation des HPD durch das BAG vor.

5.2.1 G/SG im CPI eintragen und ändern

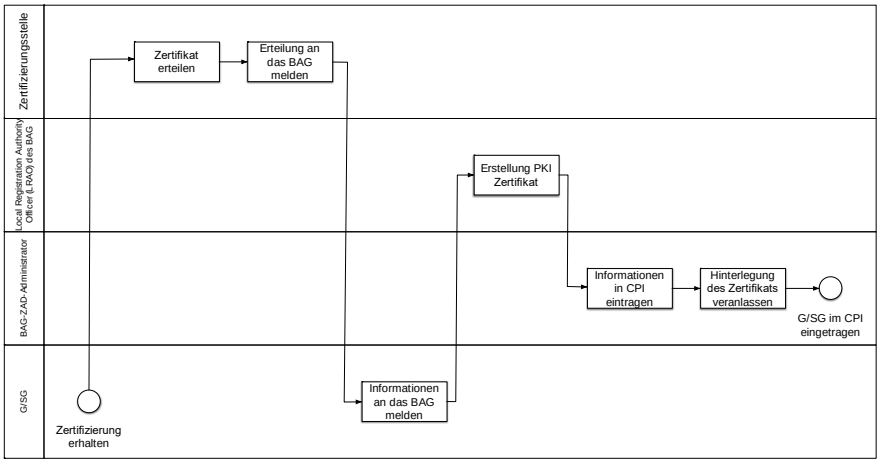

Abbildung 2: Prozess Dateneintrag CPI

Aufgabe	Beschreibung
Zertifikat erteilen	Die Zertifizierungsstelle erteilt einer G/SG das Zertifikat.
Erteilung an das BAG melden	Die Zertifizierungsstelle unterrichtet das BAG über die Erteilung des Zertifikats
Informationen an das BAG melden	Die G/SG stellt dem BAG alle für den Eintrag im CPI benötigten Informationen und Zertifikate zu.
Erstellung PKI Zertifikat	Der LRAO des BAG erstellt ein PKI Zertifikat für die G/SG
Informationen in CPI eintragen	Das BAG trägt die von der G/SG bereitgestellten Informationen und das PKI-Zertifikat im CPI ein und schaltet die G/SG aktiv.
Hinterlegung des Zertifikats veranlassen	Das BAG veranlasst, dass das PKI-Zertifikat durch das BIT bei der elektronischen Schnittstelle hinterlegt wird.

Tabelle 9: Prozessbeschreibung Dateneintrag CPI

[2] Vgl. https://www.bag.admin.ch/epra

5.2.2 Daten aus dem CPI abrufen

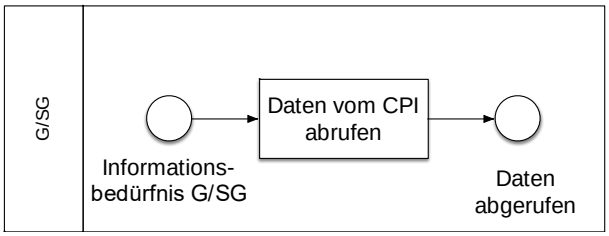

Abbildung 3: Prozess Datenabruf aus CPI

Aufgabe	Beschreibung
Daten vom CPI abrufen	Die G/SG ruft per Transaktion Community Information Query (CH:CPI) oder per Community Information Delta Download (CH:CIDD) Daten aus dem CPI ab. Art und Umfang der Daten, die im CPI abgerufen werden können, sind in Ergänzung 2.3 zu Anhang 5 der EPDV-EDI (CH:CPI) beschrieben.[3]

Tabelle 10: Prozessbeschreibung Datenabruf CPI

5.2.3 Daten im HPD eintragen und ändern

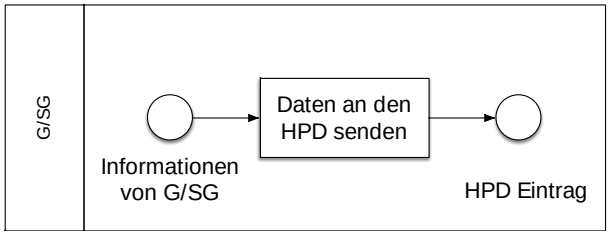

Abbildung 4: Prozess Dateneintrag HPD

Aufgabe	Beschreibung
Daten an den HPD senden	Die G/SG schickt per Transaktion Provider Information Feed (ITI-59) Daten an den HPD. Art und Umfang der Daten, die im HPD angelegt und geändert werden können, sind im Kapitel 1.11.5.1.2 *Attribute* der Ergänzung 1 zu Anhang 5 der EPDV-EDI[4] beschrieben.

Tabelle 11: Prozessbeschreibung Dateneintrag HPD

[3] Ergänzung 2.3 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_5_Ergaenzung_2.3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%202.3%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[4] Ergänzung 1 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_5_Ergaenzung_1_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%201%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

5.2.4 Daten aus dem HPD abrufen

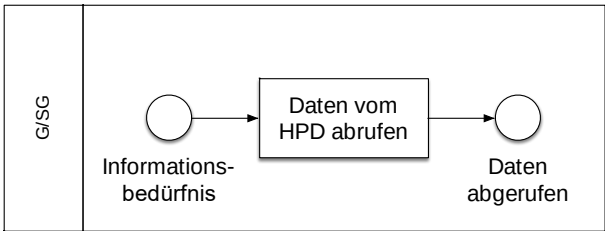

Abbildung 5: Prozess Datenabfrage HPD

Aufgabe	Beschreibung
Daten vom HPD abrufen	Die G/SG ruft per Transaktion Provider Information Query (ITI-58) oder per Provider Information Delta Download (CH:PIDD) Daten aus dem HPD ab. Art und Umfang der Daten, die im HPD abgerufen werden können, sind im Kapitel 1.11.5.1.2 *Attribute* der Ergänzung 1 zu Anhang 5 der EPDV-EDI[5] beschrieben.

Tabelle 12: Prozessbeschreibung Datenabfrage HPD

5.2.5 Daten in den MDI importieren

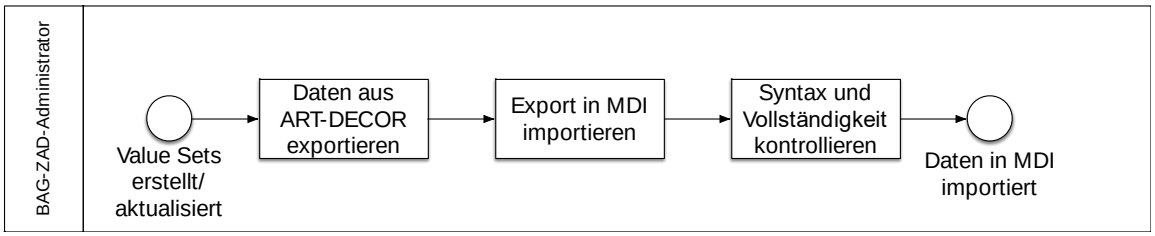

Abbildung 6: Prozess Datenimport MDI

Aufgabe	Beschreibung
Daten aus ArtDecor exportieren	Die Daten (Value Sets) für den MDI werden aus Art-Decor exportiert.
Export in MDI importieren	Die resultierende(n) Datei(en) werden vom BAG-ZAD-Administrator per Importschnittstelle in den MDI importiert.
Syntax und Vollständigkeit kontrollieren	Die Daten für den MDI werden beim Import in den MDI auf korrekte Syntax und Vollständigkeit gemäss IHE Integrationsprofil SVS geprüft.

Tabelle 13: Prozessbeschreibung Datenimport MDI

[5] Ergänzung 1 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_5_Ergaenzung_1_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%201%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

5.2.6 Daten aus dem MDI abrufen

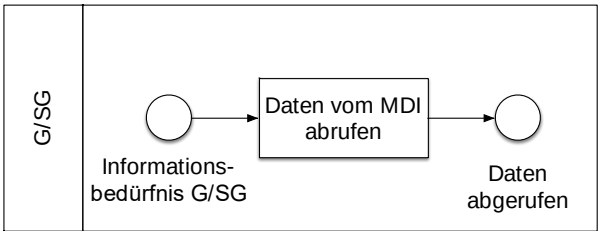

Abbildung 7: Prozess Datenabfrage MDI

Aufgabe	Beschreibung
Daten vom MDI abrufen	Die G/SG ruft per Transaktion Retrieve Value Set (ITI-48) oder per Retrieve Multiple Value Set (ITI-60) Daten aus dem MDI ab. Die Art und der Umfang der Daten, die im MDI bereitgestellt werden, richten sich nach den Anhängen 3 und 9 der EPDV-EDI[6][7]. Die strukturellen und syntaktischen Anforderungen der Daten, die im MDI abgerufen werden können, sind im Anhang 5 der EPDV-EDI beschrieben[8] (Verweis auf die gültige Version des IHE Integrationsprofils IHE:SVS).

Tabelle 14: Prozessbeschreibung Datenabfrage MDI

5.2.7 BAG-ZAD-Administrator berechtigen

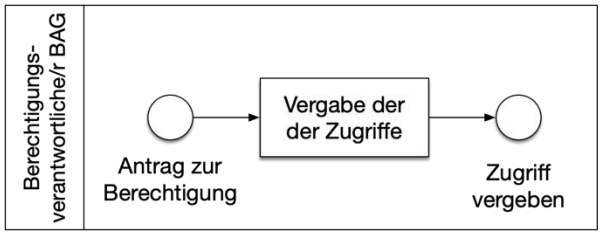

Abbildung 8: Prozess Vergabe Zugriff

Aufgabe	Beschreibung
Vergabe der der Zugriffe	Die oder der Berechtigungsverantwortliche BAG erteilt den Mitarbeitenden des BAG die erforderlichen Rollen und Rechte für den Zugriff auf die ZAD.

Tabelle 15: Prozessbeschreibung Berechtigung BAG-ZAD-Administrator

[6] Anhang 3 der EPDV-EDI – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%203%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[7] Anhang 9 der EPDV-EDI – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_9_EPDV_EDI_20190624.pdf.download.pdf/Anhang%209%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[8] Anhang 5 der EPDV-EDI: https://www.admin.ch/opc/de/classified-compilation/20163257/index.html

5.2.8 Notfallausschluss Gemeinschaft oder Stammgemeinschaft

Im Falle einer schwerwiegenden Gefährdung des Schutzes oder der Sicherheit der Daten des EPD, kann das BAG den G/SG gemäss Art. 37 Bst. a EPDV vorübergehend den Zugang zum EPD verweigern.
Dazu wird, sofern ausreichende Hinweise für die schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des EPD vorliegen, die betroffene G/SG im CPI deaktiviert. Die Deaktivierung hat zu Folge, dass die anderen G/SG per Community Information Query (CH:CPI) oder per Community Information Delta Download (CH:CIDD) darüber informiert werden, dass mit der deaktivierten G/SG keine Daten mehr ausgetauscht werden dürfen.
Ein Konzept zur Durchführung des Notfallausschlusses, dass diesen Prozess detailliert beschreibt, wird aktuell erarbeitet.
Zudem bestehen im CPI folgende weitere Möglichkeiten die Rechte von G/SG einzuschränken, um die Datensicherheit im EPD-Vertrauensraum zu gewährleisten:

- Deaktivierung Datenupload: die G/SG kann keine Daten in den HPD mehr hochladen
- Deaktivierung Datenabruf: die G/SG kann keine Daten mehr aus den ZAD abrufen

5.2.9 Support ZAD

Aktuell können die G/SG den Support für die ZAD über die E-Mail-Adresse Abfragedienste-EPDG@bag.admin.ch erreichen. Dieses E-Mail-Postfach wird vom BAG zu den üblichen Bürozeiten überwacht. Die Supportanfragen werden vom BAG triagiert und an die verantwortlichen Stellen (BAG, BIT, G/SG) weitergeleitet.

Der Supportprozess wird aktuell konzipiert und zum Ende des Jahres 2019 implementiert sein und entsprechend kommuniziert.

5.3 Bearbeitung Personendaten (nur HPD)

Personendaten werden lediglich im Geschäftsprozess «Daten im HPD eintragen» und «Daten aus dem HPD abrufen» bearbeitet. Die Beschreibung der Datenbearbeitungsprozesse sind den Kapiteln 5.2.3 *Daten im HPD eintragen und ändern* und 5.2.4 *Daten aus dem HPD abrufen* zu entnehmen.

5.4 Datenbekanntgabe und Schnittstellen

Die Schnittstellen unterscheiden sich pro Datensammlung, weshalb nachfolgend die Schnittstellen und die Datenbekanntgabe separat ausgewiesen werden.

5.4.1 CPI

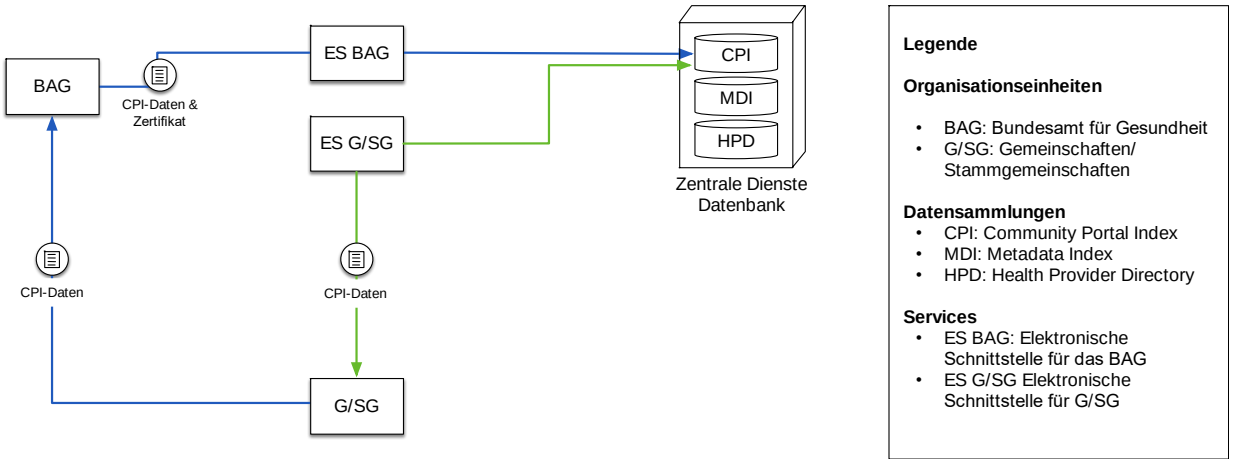

Abbildung 9: Schnittstellen und Datenbekanntgabe CPI

Datenlieferant / Lieferndes System	Datenempfänger / Empfangendes System	Daten	Zweck	Medium
G/SG	BAG	CPI-Daten	Angabe der Daten für den Eintrag der G/SG in den CPI	per Formular
BAG	CPI	CPI-Daten, Zertifikat	Eintrag der G/SG in den CPI und Hinterlegung des Zertifikats	ES BAG
G/SG	CPI	Abfragedaten	Anfrage zur Abfrage von Daten	ES G/SG
CPI	G/SG	CPI-Daten	Prüfung Status G/SG, Abruf der Daten zu den Endpunkten der G/SG	ES G/SG

Tabelle 16: Beschreibung Schnittstellen und Datenbekanntgabe CPI

Die Art und der Umfang der Daten, die im CPI eingetragen werden (CPI-Daten), sind der Ergänzung 2.3 zum Anhang 5 der EPDV-EDI zu entnehmen[9]. Das BAG pflegt die Daten in den CPI ein und kann deshalb sowohl als Datenlieferant bei der Eintragung einer G/SG in den CPI als auch als Datenempfänger auftreten kann.

Es gelten die folgenden Regelungen für den Abruf der Daten des CPI durch die G/SG:

- Eine G/SG muss die Daten aus dem CPI in einem Intervall abrufen, der sicherstellt, dass eine G/SG innert nützlicher Frist Kenntnis über eine G/SG mit dem Status *inaktiv* erlangt. Auf diese Weise soll gewährleistet werden, dass die G/SG schnell reagieren kann, falls eine G/SG im CPI deaktiviert wurde, respektive aus dem EPD Vertrauensraum ausgeschlossen wurde (siehe Punkt 2.9.26a des Anhang 2 der EPDV-EDI[10]).

[9] Ergänzung 2.3 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_5_Ergaenzung_2.3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%202.3%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[10] Anhang 2 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_2_EPDV_EDI_20190624.pdf.download.pdf/Anhang%202%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

5.4.2 MDI

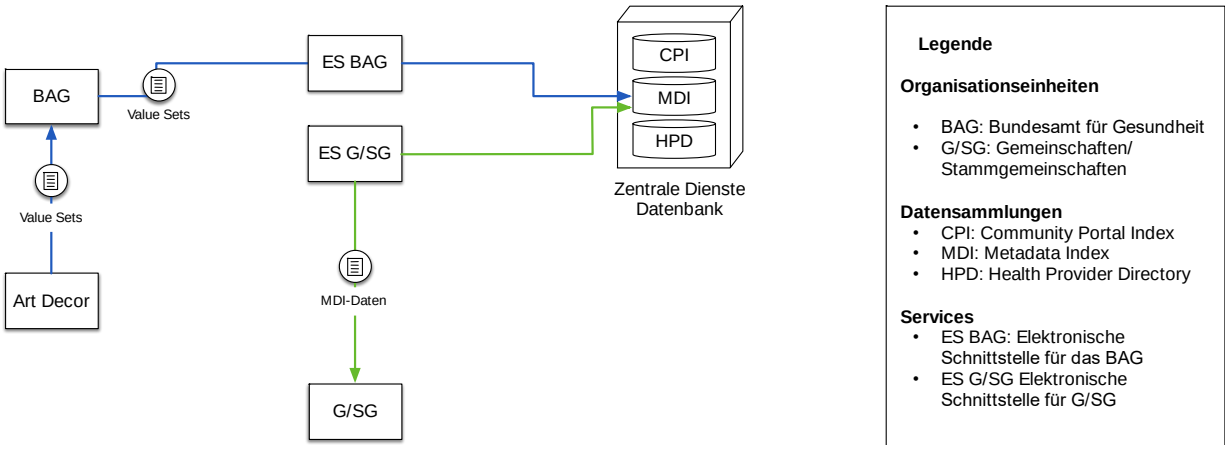

Abbildung 10: Schnittstellen und Datenbekanntgabe MDI

Datenlieferant / Lieferndes System	Datenempfänger / Empfangendes System	Daten	Zweck	Medium
Art-Decor	BAG	Value Sets	Export Value Sets	Art-Decor
BAG	MDI	Value Sets	Import Value Sets in den MDI	ES BAG
G/SG	MDI	Abfragedaten	Abfrage von MDI Daten	ES G/SG
MDI	G/SG	MDI-Daten	Lieferung der abgefragten MDI Daten	ES G/SG

Tabelle 17: Beschreibung Schnittstellen und Datenbekanntgabe MDI

Die Daten (sogenannte Values Sets), die im MDI bereitgestellt werden, sind in den Anhängen 3 und 9 der EPDV-EDI definiert[11, 12].
Die Value Sets werden in Art-Decor gepflegt und per Export-/Importschnittstelle in den MDI importiert.
Die strukturellen und syntaktischen Vorgaben zu den Daten, die im MDI bereitgestellt werden, sind in Anhang 5 der EPDV-EDI[13] beschrieben (Verweis auf die gültige Version des IHE Integrationsprofils IHE:SVS).

[11] Anhang 3 der EPDV-EDI – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%203%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[12] Anhang 9 der EPDV-EDI – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_9_EPDV_EDI_20190624.pdf.download.pdf/Anhang%209%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[13] Anhang 5 der EPDV-EDI: https://www.admin.ch/opc/de/classified-compilation/20163257/index.html

5.4.3 HPD

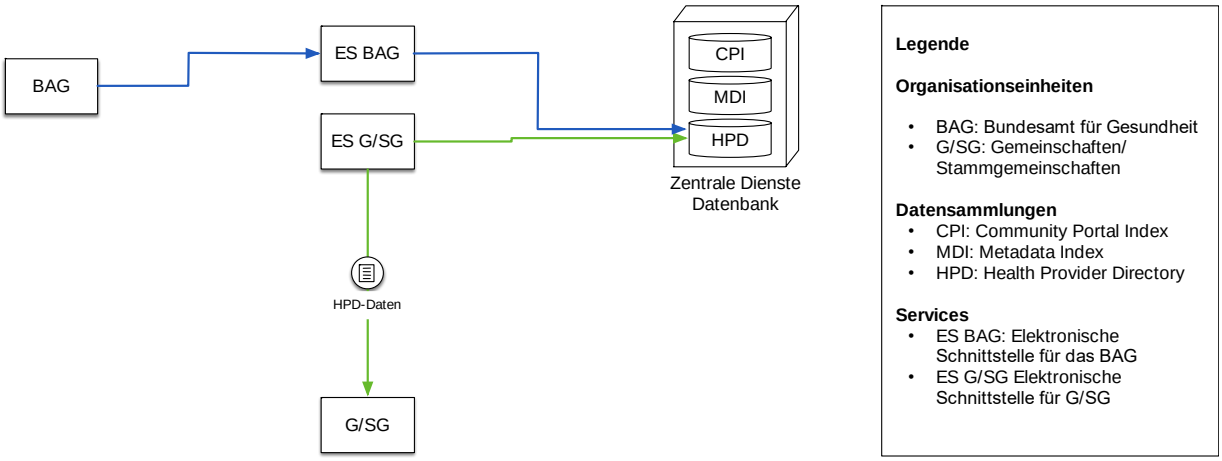

Abbildung 11: Schnittstellen und Datenbekanntgabe HPD

Datenlieferant / Lieferndes System	Datenempfänger / Empfangendes System	Daten	Zweck	Medium
G/SG	HPD	HPD-Daten	Eintrag der Daten einer GFP oder Gruppe im HPD	ES G/SG
G/SG	HPD	Abfragedaten	Abfrage Informationen einer GFP oder Gruppe	ES G/SG
HPD	G/SG	HPD-Daten	Lieferung der Informationen zur abgefragten GFP oder Gruppe	ES G/SG
HPD	BAG	HPD-Daten	Einsicht zu Evaluationszwecken	ES BAG

Tabelle 18: Beschreibung Schnittstellen und Datenbekanntgabe HPD

Es gelten die folgenden Regelungen für den Datenabruf des HPD durch die G/SG:

- Pro Gruppenobjekt (HCRegulatedOrganization) im HPD darf im Attribut hcIdentifier nur eine OID eingetragen werden. Diese und weitere Regeln werden zu einem späteren Zeitpunkt konsolidiert im HPD-Handbuch zur Verfügung gestellt.
- Die G/SG müssen dafür Sorge tragen, dass nur die Daten aktiver G/SG verarbeitet werden, denn der Provider Information Delta Download (CH:PIDD) liefert auch die Daten deaktivierter G/SG.

5.5 Kontrolle der erfassten Daten

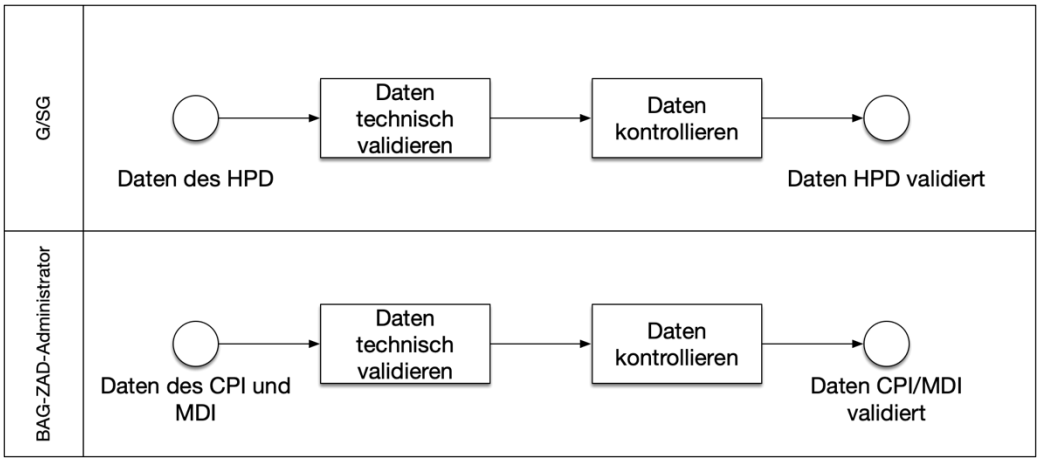

Abbildung 12: Prozesse der Kontrolle der erfassten Daten

Aktivität	Beschreibung
Daten technisch validieren	Der Minimalstandard der Datenqualität im HPD und CPI wird mit Hilfe einer technischen Validierung einiger kritischer Attribute sichergestellt. Die Attribute, die im HPD und CPI validiert werden, sind in der Ergänzung 1 zu Anhang 5 der EPDV-EDI[14] bzw. in der Ergänzung 2.3 zu Anhang 5 der EPDV-EDI[15] beschrieben. Die Daten des MDI werden beim Import auf SVS-Konformität geprüft, jedoch werden keine einzelnen Attribute technisch validiert.
Daten kontrollieren	Die Kontrolle der Daten für den HPD obliegt den G/SG, die die Datenqualität in den liefernden Systemen (siehe Abbildung 13: Ausschnitt aus der Übersicht IHE Integrationsprofile EPD des Kapitels 5.6 *Prozesse / Datenverfahren*) sicherstellen müssen. Die im CPI erfassten Daten (keine Personendaten gemäss DSG) werden von den BAG-ZAD-Administratoren nach dem 4-Augen Prinzip kontrolliert. Die inhaltliche Kontrolle der erfassten Daten im MDI nach dem Import erfolgt manuell durch den BAG-ZAD-Administrator.

Tabelle 19: Prozessbeschreibung der Kontrolle der erfassten Daten

[14] Ergänzung 1 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_5_Ergaenzung_1_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%201%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[15] Ergänzung 2.3 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_5_Ergaenzung_2.3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%202.3%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

5.6 Prozesse / Datenverfahren

Gemäss Anhang 2 der EPDV-EDI müssen G/SG sicherstellen, dass Daten des elektronischen Patientendossiers mit geeigneten und dem aktuellen Stand der Technik entsprechenden kryptografischen Massnahmen und unter der Berücksichtigung der Vorgaben von Ziffer 4.12

- bei jeglicher Übertragung gegen den Verlust der Vertraulichkeit, Authentizität und Integrität abgesichert werden;
- verschlüsselt gespeichert werden und gegen unzulässige oder unbemerkte Veränderung geschützt werden.[16]

Zudem müssen G/SG sicherstellen, dass

- nach dem Stand der Technik sichere Verfahren für die Erzeugung, die Verteilung, die Aktivierung, die Aktualisierung, den Widerruf oder die Deaktivierung und die Löschung von kryptografischen Schlüsseln eingesetzt werden;
- die verwendeten kryptografischen Schlüssel gegen Veränderung und Verlust geschützt werden;
- geheime und private Schlüssel vor unbefugter Benutzung und Offenlegung geschützt werden;
- Einrichtungen zur Erzeugung, Speicherung und Archivierung von Schlüsseln angemessen geschützt werden.[17]

Bei der vom BIT betriebenen Infrastruktur für die ZAD wird für den Datentransport ein TLS Verfahren eingesetzt.

Die nachfolgende Grafik zeigt alle liefernden und empfangende Systeme, die dazugehörenden Umgebungen sowie die Spezifikation der Datenübertragung der ZAD auf.

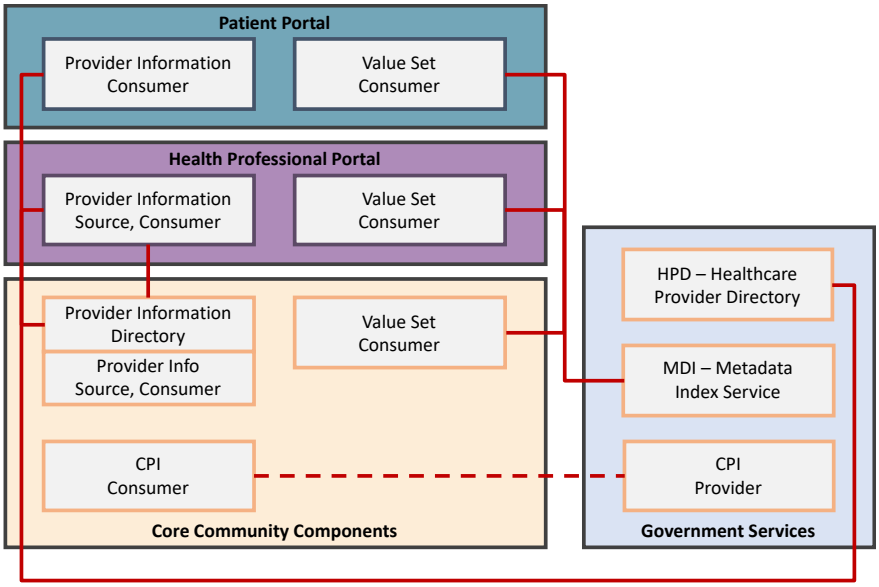

Abbildung 13: Ausschnitt aus der Übersicht IHE Integrationsprofile EPD[18]

In der *Abbildung 13: Ausschnitt aus der Übersicht IHE Integrationsprofile EPD* sind die ZAD-Komponenten rechts abgebildet und blau schattiert. Die liefernden/lesenden System der G/SG sind links in der Grafik abgebildet.

[16] Vgl. Kapitel 2.5 des Anhang 2 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_2_EPDV_EDI_20190624.pdf.download.pdf/Anhang%202%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[17] Vgl. Kapitel 4.12 Anhang 2 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019: https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_2_EPDV_EDI_20190624.pdf.download.pdf/Anhang%202%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

[18] Die Originalgrafik ist auf der Website von eHealth Suisse unter https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/E/overview-profiles-swiss-electronic-patient-record.pdf verfügbar.

Lieferndes System	Empfangendes System	IHE-Profil	Transaktion	Transport-kontrolle
Patient Portal	Health Professional Portal	CH:HPD	ITI-58 Provider Information Query	durch G/SG definiert
Health Professional Portal	Core Community Service	CH:HPD	ITI-58 Provider Information Query IT-59 Provider Information Feed	durch G/SG definiert
Core Community Service	HPD - Government Services	CH:HPD	ITI-58 Provider Information Query ITI-59 Provider Information Feed CH:PIDD Provider Information Delta Download	https
Patient Portal, Health Professional Portal, Core Community Services	MDI - Government Services	SVS	ITI-48 Retrieve Value Sets ITI-60 Retrieve Multiple Value Sets	https
Core Community Services	CPI - Government Services	CH:CPI	CH:CIQ: Community Information Query CH:CIDD: Community Information Delta Download	https

Tabelle 20: Beschreibung Prozesse / Datenverfahren

6 Konfiguration der Informatikmittel

6.1 Anwendungen

Die nachfolgenden Anwendungen werden für die ZAD eingesetzt.

- Art-Decor als Quellsystem für die Daten des MDI
- BIT Certificate Request Wizard als Quelle für die Swiss Government PKI Zertifikate
- HPDs der G/SG als Quellsysteme für die Daten des HPD

6.2 Netzwerk und kryptografische Funktionen

Zugriffe der Benutzer aus der Bundesverwaltung erfolgen im Netzwerk der Bundesverwaltung.
Daten auf Arbeitsplatzsystemen der Bundesverwaltung sind durch Festplattenverschlüsselung gesichert. Die Daten werden für den Transport verschlüsselt. Dazu wird das TLS-Verfahren eingesetzt.

6.3 Datenbank

Die eingesetzte Datenbank ist eine Net-basierte Webapplikation (Virtualisierung), welche auf einem SQL-Server beim Leistungserbringer BIT betrieben wird. Der Server befindet sich in gut geschützten Räumlichkeiten und ist durch geeignete physische Massnahmen geschützt. Die Backup- und Wiederherstellungsprozesse sind im dazugehörenden ISDS-Konzept unter Kapitel 5.2.2 *Beschreibung der sicherheitsrelevanten Aspekte* beschrieben.

6.4 Betriebssystem

Das Betriebssystem für den zuvor beschriebenen SQL-Server wird aus Betriebssicherheitsgründen der Öffentlichkeit nicht zugänglich gemacht. Der Betrieb und das Patch-Management obliegt komplett dem Leistungserbringer BIT.

6.5 Eingesetzte Hardware

Hardware (HW) des Leistungserbringers

Sämtliche eingesetzte Hardware bei den beiden Bundesorganen BAG und BIT obliegt dem IKT-Grundschutz des Informatiksteuerungsorgans des Bundes (ISB). Es wird eine Inventarliste beim BIT geführt.

HW der Bundesorgane

Sämtliche eingesetzte Hardware bei den beiden Bundesorganen BAG und BIT obliegt dem IKT-Grundschutz des ISB und wird durch den Leistungserbringer BIT betrieben. Die eingesetzte Hardware wird in einem eigenen ISDS-Konzept (BURAUT) geführt. Da Arbeitsgeräte der BAG-Mitarbeitenden zum einen austauschbar sind und zum anderen nicht nur für die Datenbearbeitung der ZAD Datenbanken eingesetzt werden, erfolgt keine Auflistung innerhalb dieses Bearbeitungsreglements. Die Übersicht der vorhandenen Zugriffe via die jeweiligen Arbeitsgeräte ist dem Kapitel 4.2 *Zugriffsberechtigungen / Zugriffsmatrix* zu entnehmen. Die Arbeitsgeräte innerhalb des BAG befinden sich in grundsätzlich geschützten Räumlichkeiten.

HW der G/SG

Die G/SG sowie die ihnen angeschlossenen Gesundheitseinrichtungen unterliegen dem EPDG. Dieses führt in Art. 12 Abs. 1 Bst. b EPDV aus, dass ein IT-Inventar geführt werden muss. Wichtige Hardwarekomponenten werden dort geführt und in regelmässigen Abständen aktualisiert.

6.6 Schutz- und Sicherheitsmassnahmen

Schutz- und Sicherheitsmassnahmen beim Leistungserbringer

Die Schutz- und Sicherheitsmassnahmen sind im ISDS-Konzept ZAD EPD unter Kapitel 5.2.2 *Beschreibung der Sicherheitsrelevanten Aspekte* dokumentiert.

Schutz- und Sicherheitsmassnahmen bei den Bundesorganen

Die Authentifikation sowie die technische Umsetzung der Rollen und Rechte von Benutzern in den ZAD, wird durch den Service eIAM (vormals eID / eZugang) des BIT sichergestellt und obliegt dem BVA (Benutzerverwalter Amt) Prozess:

- Der BVA von einer oder mehreren Fachapplikationen in einem Amt hat die Aufgabe, denjenigen Benutzern, die eine fachliche Rolle beantragt haben, diese zu erteilen oder abzulehnen.
- Der BVA nutzt pro Applikation ein Benutzer-Rollen-Konzept. Jeglicher Zugriff auf Applikationen muss gemäss dem «Need to know» Prinzip erfolgen. Dabei ist sicherzustellen, dass ein Benutzer nur die Informationen erhält bzw. nur die Funktionen ausführen darf, die er auch wirklich benötigt.
- Der BVA bestimmt und ändert den Umfang des Zugriffs durch die Erteilung der Applikations-Rollen in dem dafür vorgesehene IDM-Tool.
- Der BVA entzieht dem Benutzer den Zugriff auf die Fach-Applikationen, indem er die Rollen aus dem dafür vorgesehene IDM Administrations-Tool löscht.
- Der BVA meldet dem Benutzer die Änderungen seiner Berechtigungen.

Damit der BVA diese Aufgaben erfüllen kann, muss er seinerseits berechtigt werden. Dazu stösst der „BVA-Aspirant“ seine Ernennung bei dem für das Amt verantwortlichen Gesamtkoordinators eines Amtes (GKA) an.

Schutz- und Sicherheitsmassnahmen bei den G/SG

Grundsätzlich unterliegen die G/SG sowie die ihnen angeschlossenen Gesundheitseinrichtungen dem EPDG und den entsprechenden Verordnungen. In Art. 12 EPDV sind Anforderungen an den Datenschutz und die Datensicherheit festgehalten. Als Hilfsmittel dienen den G/SG der Anhang 2 der EPDV-EDI, die sogenannten technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ), sowie die Umsetzungshilfe Datenschutz und Datensicherheit im EPD der Organisation eHealth Suisse.

7 Aufbewahrungsdauer, Archivierung und Löschung

Für den CPI und den HPD bestehen Funktionalitäten zur Abfrage von Änderungen am Datenbestand. Diese Abfragen können einen beliebigen Zeitraum umfassen und werden dazu genutzt die lokalen HPD der G/SG[19] und CPI Kopien, die die G/SG bei Bedarf vorhalten können, mit dem Datenbestand des ZAD zu synchronisieren. Die Synchronisation des HPD und CPI verhält sich nach den folgenden Regeln:

- Die G/SG überschreiben die Daten des zentralen HPD mit den Daten ihres lokalen HPD, die die Daten der Gesundheitseinrichtungen und GFP dieser G/SG repräsentieren.
- Der zentrale HPD der ZAD überschreibt die lokalen HPD mit den Daten zu den Gesundheitseinrichtungen und GFP der anderen G/SG
- Der CPI der ZAD überschreibt die CPI-Kopien bei allen G/SG

Beim MDI können sämtliche Versionen eines Values Sets abgefragt werden, die zu einem beliebigen Zeitpunkt im MDI erfasst wurden.
Dass bedeutet für alle drei Komponenten, dass auch die historischen Daten zu jedem Zeitpunkt verfügbar sind und abgerufen werden können. Eine Archivierung und endgültige Löschung von Daten sind aktuell nicht vorgesehen.

7.1 Aufbewahrungsdauer

Die Daten bzw. die Datenhistorie aller drei Komponenten ist jederzeit verfügbar.
Es ist keine Beschränkung der Aufbewahrungsdauer der Daten des CPI, HPD und MDI vorgesehen.

7.2 Archivierung

Die Daten bzw. die Datenhistorie aller drei Komponenten ist jederzeit verfügbar.

7.3 Löschung

Die Daten bzw. die Datenhistorie aller drei Komponenten ist jederzeit verfügbar.

[19] Der lokale HPD ist eine Systemkomponente, die von den G/SG betrieben wird und somit in deren Verantwortungsbereich liegt. Die lokalen HPD ist nicht mit dem zentralen HPD der ZAD zu verwechseln.

8 Technische und organisatorische Massnahmen

8.1 Relevante TOZ nach EPDV

Folgende Tabelle zeigt auf, welche konkreten Vorgaben der TOZ (Anhang 2 der EPDV-EDI) für die ZAD relevant sind:

TOZ Nr-	Titel	Beschreibung
1.2.2	1.2 Verwaltung von Gesundheitseinrichtungen (Art. 9 Abs. 2 Bst. a und d EPDV)	Der Prozess für den Eintritt von Gesundheitseinrichtungen muss sicherstellen, dass: a. […] b. […] c. […] d. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden; e. […].
1.2.4	1.2 Verwaltung von Gesundheitseinrichtungen (Art. 9 Abs. 2 Bst. a und d EPDV)	Die Gemeinschaften müssen für die von ihr registrierten Daten im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV: a. eine verantwortliche Person benennen; b. sicherstellen, dass die Aktualität und Korrektheit der Daten regelmässig überprüft wird.
1.3.2	1.3 Verwaltung von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a bis f EPDV)	Sie stellen sicher, dass die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden.
1.3.3	1.3 Verwaltung von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a bis f EPDV)	Der Prozess für den Eintritt von Gesundheitsfachpersonen muss sicherstellen, dass: a. […] b. […] c. […] d. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden; e. […].
1.3.4	1.3 Verwaltung von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a bis f EPDV)	Der Prozess für die Verwaltung von Gesundheitsfachpersonen muss sicherstellen, dass: a. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden; b. […].
1.3.5	1.3 Verwaltung von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a bis f EPDV)	Der Prozess für den Austritt von Gesundheitsfachpersonen muss sicherstellen, dass: a. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden; b. […].
1.5.2	1.5 Verwaltung von Gruppen von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a, c, d und f EPDV)	Der Prozess muss sicherstellen, dass: a. […] b. die Daten im Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden; c. […].
2.9.8	2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV) – Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen	Die IHE-Akteure Provider Information Consumer und Provider Information Source müssen folgende Transaktionen des Integrationsprofils IHE HPD in der Version nach Anhang 5 der EPDV-EDI unterstützen: a. Provider Information Query [ITI-58]; b. Provider Information Feed [ITI-59]; c. Provider Information Delta Download (CH:PIDD).
2.9.26	2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV) – Authentisierung mit gültigen Zertifikaten	Gemeinschaften müssen über ein gültiges elektronisches Zertifikat verfügen, das bei einer nach dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES; SR 943.03) anerkannten Anbieterin von Zertifikatsdiensten bezogen wurde, für: a. […]

		b. die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber den Abfragediensten nach Artikel 39 Buchstaben a bis c EPDV; c. […]
2.9.26a	2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV) – Authentisierung mit gültigen Zertifikaten	Gemeinschaften müssen sicherstellen, dass: a. der gemeinschaftsübergreifende Datenaustausch nur mit gemäss Ziffer 2.9.26 Buchstabe a authentifizierten Endpunkten erfolgt, die im Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 Absatz 1 EPDV geführt sind. b. die Überprüfung, welche Endpunkte als vertrauenswürdige Kommunikationspartner im Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften geführt werden, so regelmässig durchgeführt wird, dass jegliche Kommunikation mit nicht mehr vertrauenswürdigen Endpunkte rasch unterbunden werden kann (vgl. Art. 37 Abs. 1 Bst. a EPDV).
2.9.26b	2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV) – Datenaustausch mit den Abfragediensten nach Artikel 39	Gemeinschaften müssen für den Datenaustausch mit dem Abfragedienst nach Artikel 39 Buchstabe a EPDV für den Akteur CPI Consumer die folgenden Transaktionen des nationalen Integrationsprofils CH:CPI nach Anhang 5 der EPDV-EDI verwenden: a. Community Information Query (CH:CIQ); b. Community Information Delta Download (CH:CIDD).
2.9.27	2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV) – Datenaustausch mit den Abfragediensten nach Artikel 39	Gemeinschaften müssen für den Datenaustausch mit dem Abfragedienst nach Artikel 39 Buchstabe c EPDV für den IHE-Akteur Value Set Consumer die Transaktion Retrieve Value Set [ITI-48] des Integrationsprofils IHE SVS nach Anhang 5 der EPDV-EDI verwenden.
2.9.28	2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV) – Authentisierung mit gültigen Zertifikaten – Datenaustausch mit den Abfragediensten nach Artikel 39	Gemeinschaften müssen für den Datenaustausch mit den Abfragediensten nach Artikel 39 Buchstaben a bis c EPDV die folgenden Transaktionen des Integrationsprofils IHE ATNA nach Anhang 5 der EPDV-EDI verwenden: a. Maintain Time [ITI-1]; b. Authenticate Node [ITI-19]; c. Record Audit Event [ITI-20].
4.15.4 c	4.15 Kommunikationssicherheit: Verwaltung von Netzwerken und Netzwerkdiensten (Art. 12 Abs. 4 EPDV)	Die Netzwerkstrukturen müssen folgende Anforderungen erfüllen: Antwortende Zugangspunkte (Respondieren Gateways) dürfen den Verbindungsaufbau nur zulassen, wenn das aufrufende System zu einer zertifizierten Gemeinschaft gehört, die im zentralen Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 EPDV geführt wird. c. Antwortende Zugangspunkte (Responding Gateways) oder andere für die gemeinschaftsübergreifende Kommunikation erreichbaren Endpunkte dürfen den Verbindungsaufbau nur zulassen, wenn das aufrufende System zu einer zertifizierten Gemeinschaft gehört, und im zentralen Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 EPDV geführt wird.

Tabelle 21: Relevante TOZ nach EPDV

8.2 Weiterführende Massnahmen

Im ISDS-Konzept des Schutzobjektes ZAD EPD wurden mehrere weiterführende Massnahmen zum Schutz und der Sicherheit definiert und festgehalten. Um die Vertraulichkeitsstufe dieses vorliegenden Dokumentes nicht zu erhöhen wird an dieser Stelle auf dieses ISDS-Konzept verwiesen und die einzelnen weiterführenden Massnahmen nicht abgebildet.

9 Rechte der betroffenen Personen

9.1 Informationspflicht BAG (Auskunftsrecht)

Die Rechte der in den ZAD erfassten Personen richten sich nach dem DSG; das Auskunftsrecht insbesondere nach Artikel 8 DSG. Jede Person kann vom Inhaber der Datensammlung (BAG) Auskunft darüber verlangen, ob und welche Daten über sie bearbeitet werden. Dieses Auskunftsrecht gilt nur für den HPD, da nur in diesem Verzeichnis Personendaten bearbeitet werden.

9.2 Instrumente und Verfahren

Das Verfahren zur Ausübung des Auskunftsrechts richte sich nach Art. 8 Abs. 5 DSG und Art. 1 VDSG. Die Beantwortung der Auskunftsgesuche erfolgt durch den Anwendungsverantwortlichen, der per E-Mail an ehealth@bag.admin.ch kontaktiert werden kann.

10 Datensammlung EDÖB

Das BAG ist gemäss Art. 11 a DSG verpflichtet seine Datensammlungen beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) anzumelden, bevor sie eröffnet werden. Die Verpflichtung wird in Art. 16 VDSG ausdrücklich festgehalten. Zum aktuellen Zeitpunkt sind die Datensammlungen der ZAD noch nicht angemeldet. Die Inhalte der nachfolgenden Tabelle werden deshalb zu einem späteren Zeitpunkt mit den Informationen der Anmeldung respektive Registrierung der Datensammlung beim EDÖB ergänzt.

11 Anhang

11.1 Referenzierte Dokumente

Dokument
Anhang 2 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019 https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_2_EPDV_EDI_20190624.pdf.download.pdf/Anhang%202%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf
Anhang 3 der EPDV-EDI – Inkrafttreten 15.07.2019 https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%203%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf
Anhang 9 der EPDV-EDI – Inkrafttreten 15.07.2019 https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_9_EPDV_EDI_20190624.pdf.download.pdf/Anhang%209%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf
Ergänzung 1 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019 https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossi-er/gesetze/Anhang_5_Ergaenzung_1_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%201%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf
Ergänzung 2.3 zum Anhang 5 der EPDV-EDI – Ausgabe 2 – Inkrafttreten 15.07.2019 https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossi-er/gesetze/Anhang_5_Ergaenzung_2.3_EPDV_EDI_20190624.pdf.download.pdf/Anhang%205%20Erg%C3%A4nzung%202.3%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf

11.2 Abkürzungen

Abkürzung	Bedeutung
Abs.	Absatz
Art.	Artikel
BAG	Bundesamt für Gesundheit
BIT	Bundesamt für Informatik und Telekommunikation
Bst.	Buchstabe
BVA	Benutzerverwalter Amt
CPI	Community Portal Index
DSBO	Datenschutzberater/-in der Organisationseinheit (Amt, Departement)
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EPD	Elektronisches Patientendossier
EPDG	Bundesgesetz über das elektronischen Patientendossier
G/SG	Gemeinschaften und Stammgemeinschaften
GFP	Gesundheitsfachperson
GKA	Gesamtkoordinators eines Amtes
HPD	Health Provider Directory

Abkürzung	Bedeutung
HW	Hardware
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan des Bundes
ISBO	Informatiksicherheitsbeauftragter der Organisationeinheit
ISBD	Informatiksicherheitsbeauftragter des Departements
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
OE	Organisationseinheit
MDI	Metadata Index
s.	siehe
TOZ	Technische und organisatorische Zertifizierungsvoraussetzungen
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11)
ZAD	Zentraler Abfragedienst

11.3 Begriffe

Begriff	Bedeutung
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (siehe Art. 3 Bst. e DSG).
Bekanntgeben	Das Zugänglichmachen von Personendaten wie das Einsicht gewähren, Weitergeben oder Veröffentlichen (Art. 3 Bst. f DSG).
Besonders schützenswerte Personendaten	Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; über Massnahmen der sozialen Hilfe; und über administrative oder strafrechtliche Verfolgungen und Sanktionen (Art. 3 Bst. c DSG).
Datensammlung	Im Sinne des Datenschutzgesetzes bedeutet Datensammlung „jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar ist“ (Art. 3 Bst. g DSG).
Gemeinschaften (G)	Eine Gemeinschaft ist ein Zusammenschluss von Gesundheitseinrichtungen. Gemeinschaften stellen das elektronische Patientendossier zur Verfügung und stellen sicher, dass die Verfügbarkeit des EPD gewährleistet wird sowie die notwendigen Zugriffe an Gesundheitsfachpersonen und Hilfspersonen vergeben werden.
Gesundheitsfachpersonen (GFP)	Eine nach eidgenössischem und kantonalem Recht Fachperson, die im Gesundheitsbereich Behandlungen durchführt, anordnet oder im Zusammenhang mit einer Behandlung Heilmittel oder andere Produkte abgibt.
Inhaber der Datensammlung	Inhaberin oder der Inhaber der Datensammlung sind private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden (Art. 3 Bst. i DSG).
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; darunter fallen natürliche wie auch juristische Personen (Art. 3 Bst. a und b DSG).
Persönlichkeitsprofile	Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (Art. 3 Bst. d DSG).
Stammgemeinschaften (SG)	Eine Stammgemeinschaft ist auch ein Zusammenschluss von Gesundheitseinrichtungen und bietet neben den Aufgaben einer Gemeinschaft weitere Dienste an, wie zum Beispiel die Eröffnung eines Dossiers, die

	Aufbewahrung der schriftlichen Einverständniserklärung oder die Verwaltung von Zugriffsrechten