



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza Svizzera delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Funktionsabnahmen in EPD-Produktionsumgebungen

Umsetzungshilfe für die (Stamm-)Gemeinschaften

Bern, 22. November 2019

ehealthsuisse

Kompetenz- und Koordinationsstelle
von Bund und Kantonen

Centre de compétences et de coordination
de la Confédération et des cantons

Centro di competenza e di coordinamento
di Confederazione e Cantoni

Impressum

© eHealth Suisse, Kompetenz- und Koordinationsstelle von Bund und Kantonen

Lizenz: Dieses Ergebnis gehört eHealth Suisse (Kompetenz- und Koordinationsstelle von Bund und Kantonen). Das Schlussergebnis wird unter der Creative Commons Lizenz vom Typ „Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 Lizenz“ über geeignete Informationskanäle veröffentlicht. Lizenztext: <http://creativecommons.org/licenses/by-sa/4.0>

Weitere Informationen und Bezugsquelle:

www.e-health-suisse.ch

Zweck und Positionierung dieses Dokuments

Funktionsabnahmen in EPD-Produktionsumgebungen verbessern die Qualität des Produktionsbetriebes, indem fehlerhafte Veränderungen des Systems rasch festgestellt werden. Die vorliegende Umsetzungshilfe beschreibt die Instrumente, die den (Stamm-)Gemeinschaften für diesen Zweck zur Verfügung stehen, und regelt die Implementierung sowie die Anwendung dieser Instrumente.

Die vorliegende Umsetzungshilfe wurde von Thomas Kessler, TEMET AG, im Auftrag von eHealth Suisse und im Rahmen der temporären Arbeitsgruppe «Funktionsabnahmen in EPD-Produktionsumgebungen» erarbeitet. Der Bericht ist zugänglich unter www.e-health-suisse.ch.

Im Interesse einer besseren Lesbarkeit wird auf die konsequente gemeinsame Nennung der männlichen und weiblichen Form verzichtet. Wo nicht anders angegeben, sind immer beide Geschlechter gemeint.

Inhaltsverzeichnis

Zusammenfassung.....	3
1 Einleitung.....	4
1.1 Ausgangslage.....	4
1.2 Problemstellung.....	4
1.3 Zielsetzungen	5
1.4 Abgrenzung	5
1.5 Dokumentenstruktur	6
2 Funktionsabnahmen als QS-Element	7
2.1 Einbettung in ein Teststufenkonzept	7
2.2 Praxiserfahrung aus EPD-Pilotprojekten.....	8
3 Funktionsabnahmen im EPD	9
3.1 Scope der Funktionsabnahmen	9
3.2 Anwendungsfälle	9
4 Rahmenbedingungen	14
5 Lösungskonzept	15
5.1 Fiktive elektronische Patientendossiers (EPDs)	15
5.2 Hilfspersonen mit QS-Aufgaben.....	15
5.3 Trennung von QS-Kontext und Behandlungskontext.....	16
5.4 Umsetzung in den EPD-Komponenten	16
6 Umsetzungsmassnahmen.....	18
6.1 Implementierung dieser Umsetzungshilfe	18
6.2 Flankierende und ergänzende Massnahmen.....	21

Zusammenfassung

(Stamm-)Gemeinschaften müssen sicherstellen, dass die Funktionalität und Interoperabilität ihrer IT-Systeme bei der Einführung von Releases oder neuen technischen Komponenten sichergestellt bleibt.

Ausgangslage und Zielsetzung

Funktionsabnahmen in EPD-Produktionsumgebungen (auch «Post-deployment Checks» genannt) können die Qualität des Produktionsbetriebs sichern, indem fehlerhafte Veränderungen rasch festgestellt werden. Dies betrifft insbesondere Interoperabilitätsprobleme zwischen den verschiedenen Teilnehmern am Gesamtsystem, die auf Grund von Konfigurationsfehlern entstehen und in den Testumgebungen nicht festgestellt werden können. Funktionsabnahmen in den EPD-Produktionsumgebungen ersetzen keinesfalls die Durchführung umfassender Funktions- und Abnahmetests in den verschiedenen Testumgebungen, sondern setzen diese voraus.

Jede Stammgemeinschaft eröffnet für die Durchführung von Funktionsabnahmen in EPD-Produktionsumgebungen zwei fiktive elektronische Patientendossiers (EPDs). Die Inhaber dieser fiktiven EPDs sind fiktive Personen, die von der ZAS (Zentrale Ausgleichsstelle des Bundes) im produktiven UPI-Service eingerichtet werden und denen eine reale EPR-SPID zugeordnet wird. Die fiktiven EPDs enthalten ausschliesslich fiktive Dokumente mit fiktiven Inhalten ohne Bezug zu einer medizinischen Behandlung oder zu realen Personen.

Lösungskonzept

Die Funktionsabnahmen werden von «Hilfspersonen mit QS-Aufgaben» durchgeführt. Diese unterscheiden sich nicht von anderen Hilfspersonen, ausser dass sie das EPD-Produktionssystem in einem QS-Kontext und nicht in einem Behandlungskontext benutzen. Fiktive Personen erhalten keine elektronische Identität und können selber nicht auf das Patienten-Portal zugreifen. Die Funktionsabnahme von Patienten-Services werden deshalb ebenfalls von den Hilfspersonen mit QS-Aufgaben in der Rolle als EPD-Stellvertreter durchgeführt.

Hilfspersonen mit QS-Aufgaben sind einer Gesundheitsfachperson (GFP) zugeteilt, welche die Verantwortung für die ordnungsgemässe Durchführung der Funktionsabnahmen trägt. Diese «GFP mit QS-Verantwortung» wird von einem EPD-Stellvertreter des fiktiven Patienten für den Zugriff auf das fiktive EPD berechtigt.

Jede Stammgemeinschaft definiert ein Regelwerk für die Durchführung von Funktionsabnahmen und nominiert eine Hilfsperson mit QS-Aufgaben, die für die beiden fiktiven EPDs der Stammgemeinschaft verantwortlich ist. Diese Hilfsperson führt unter anderem eine Liste mit allen HIP mit QS-Aufgaben und allen GFP mit QS-Verantwortung in der (Stamm-)Gemeinschaft.

Regelwerk für Funktionsabnahmen

Hilfsmittel für automatisiertes Monitoring und effiziente Fehleranalyse können ebenfalls zu einer hohen Betriebsqualität beitragen, werden im vorliegenden Konzept aber nicht behandelt.

Ergänzende Massnahmen

1 Einleitung

1.1 Ausgangslage

Die EPD (Stamm-)Gemeinschaften nutzen eine komplexe Infrastruktur mit IT-Systemen unterschiedlicher Betreiber, die miteinander vernetzt sind. Sie müssen sicherstellen, dass die Funktionalität und Interoperabilität aller Komponenten auch bei der Einführung von Releases oder neuen technischen Komponenten sichergestellt bleibt. Zusätzlich zu den Entwicklungsumgebungen der einzelnen Betreiber verfügen die Gemeinschaften deshalb über Test- und Integrationsumgebungen, in welchen sie die Abnahmetests durchführen und die Interoperabilität zwischen allen Komponenten testen.

Teststufen

Auch wenn Software unverändert von der Integrationsumgebung in die Produktionsumgebung übernommen wird, können Unterschiede bei der Konfiguration dieser Umgebungen nicht gänzlich vermieden werden. IP-Adressen, URLs, Zertifikate, Firewall-Regeln und andere Konfigurationsparameter müssen verschieden sein und können in der Integrationsumgebung deshalb nicht abschliessend validiert werden.

Umgebungsspezifische Konfigurationen

Bei jeder Einführung eines Releases in die Produktionsumgebung besteht deshalb ein gewisses Risiko, dass das Gesamtsystem auf Grund eines Konfigurationsfehlers nicht mehr (korrekt) funktioniert. Solche Fehler können nicht nur in den veränderten Komponenten auftreten, sondern auch in solchen, die an die Veränderung angepasst werden müssen. (Stamm-)Gemeinschaften können dieses Risiko reduzieren, indem sie unmittelbar nach jeder Veränderung der EPD-Produktionsumgebung eine Funktionsabnahme (auch «Post-deployment Check» genannt) durchführen und allfällige Fehler rasch erkennen.

Risiko von Konfigurationsfehlern reduzieren

1.2 Problemstellung

Das Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG sieht keine Funktionsabnahmen in den EPD-Produktionsumgebungen vor. Allfällige Fehler bei der Einführung von Releases werden somit erst durch die Patientinnen und Patienten, Gesundheitsfachpersonen oder Hilfspersonen erkannt, was die Akzeptanz des EPD vermindern und die Fehlerbehebung verzögern würde. Fehlende oder fehlerhafte Funktionalität in einer EPD-Produktionsumgebung kann auch die Patientensicherheit gefährden, was mit allen verfügbaren Mitteln verhindert werden muss.

Funktionsabnahmen sind im EPDG nicht vorgesehen

1.3 Zielsetzungen

Funktionsabnahmen in den EPD-Produktionsumgebungen sollen die Qualität des Produktionsbetriebs sichern, indem fehlerhafte Veränderungen rasch festgestellt werden.

Qualitätssicherung (QS) durch administratives Personal

Die Funktionsabnahmen sollen durch administratives Personal durchgeführt werden können, ohne dass Patientinnen oder Gesundheitsfachpersonen und Hilfspersonen aus dem Behandlungsalltag mit einbezogen werden müssen. Letztere können dafür nicht aus dem Behandlungsalltag herausgenommen werden und dürfen – in Ermangelung eines konkreten Behandlungskontextes – auch nicht auf ein EPD zugreifen. Patientinnen und Patienten sind nur bedingt in der Lage, Funktionsabnahmen durchzuführen; es fehlt ihnen hierfür am vertieften (technischen) Fachwissen.

Ein national einheitliches Konzept für die Durchführung von Funktionsabnahmen in EPD-Produktionsumgebungen soll dafür sorgen, dass die relevante Funktionalität der EPD-Produktionssysteme gewährleistet ist und dass Funktionsabnahmen auch gemeinschaftsübergreifend durchgeführt werden können, soweit dies notwendig ist.

National einheitliches Konzept

Auf der Basis eines national einheitlichen Konzeptes ist es möglich, wichtige Elemente der Lösung zentral umzusetzen wie beispielsweise die Ausstellung von Patientenidentifikatoren (EPR-SPID) durch die Zentrale Ausgleichsstelle (ZAS) für eine begrenzte Zahl von fiktiven Personen.

Funktionsabnahmen finden in jedem Fall statt und es stellt sich nur die Frage, ob sie planmässig durch administratives Personal oder unbewusst durch die Benutzer durchgeführt werden. Die Standardisierung der Funktionsabnahmen kann improvisierte unausgereifte Lösungen verhindern, die kaum kontrollierbar sind und unerwünschte Nebenwirkungen zeitigen können.

Planmässiges Vorgehen

1.4 Abgrenzung

Funktionsabnahmen in den EPD-Produktionsumgebungen ersetzen keinesfalls die Durchführung umfassender Funktions- und Abnahmetests in den verschiedenen Testumgebungen, sondern setzen diese voraus.

Kein Ersatz von Teststufen

Die folgenden Massnahmen sind für eine hohe Betriebsqualität ebenfalls notwendig, werden im vorliegenden Konzept aber nicht behandelt:

Weitere Elemente der Qualitätssicherung

- Die laufende Betriebsüberwachung;
- Die Analyse von Fehlern im laufenden Betrieb;
- Der Support von Patienten und Patientinnen;
- Der Support von Gesundheitsfachpersonen und Hilfspersonen.

Einzelne Aspekte und Instrumente der Funktionsabnahmen können auch für diese Anwendungsfälle relevant sein, deren konkrete Umsetzung ist jedoch *out of scope* des vorliegenden Konzeptes.

1.5 Dokumentenstruktur

Kapitel 2 positioniert die Funktionsabnahmen als Element der Qualitätssicherung im Rahmen des umfassenden Teststufenkonzeptes und fasst die Praxiserfahrung aus den EPD-Pilotprojekten MonDossierMédical und myEPD zusammen.

Positionierung im
Teststufenkonzept

Kapitel 3 identifiziert und beschreibt die Anwendungsfälle der Funktionsabnahmen: Welche Funktionen werden von wem abgenommen und welche Interoperabilitätsprobleme können dabei typischerweise erkannt werden?

Anwendungsfälle
(Use Cases)

Im Kapitel 4 sind die Rahmenbedingungen seitens der Systemteilnehmer aufgeführt, die im Lösungskonzept berücksichtigt werden müssen.

Rahmenbedingungen

Kapitel 5 beschreibt die Lösung für zukünftige Funktionsabnahmen in EPD-Produktionsumgebungen. Es identifiziert die Instrumente, die den (Stamm-)Gemeinschaften für diesen Zweck zur Verfügung stehen, und skizziert deren Implementierung in den EPD-Komponenten.

Instrumente

Das Kapitel 6 identifiziert die Umsetzungsmassnahmen und schlägt zusätzliche flankierende Massnahmen für eine weitere Verbesserung der Betriebsqualität vor.

Massnahmen

2 Funktionsabnahmen als QS-Element

2.1 Einbettung in ein Teststufenkonzept

Funktionsabnahmen in den EPD-Produktionsumgebungen ersetzen keinesfalls die Durchführung umfassender Funktions- und Abnahmetests in den verschiedenen Testumgebungen, sondern setzen diese vielmehr voraus.

Funktionsabnahmen ersetzen keine Tests.

Die Abbildung 1 zeigt typische Teststufen einer EPD-Plattform mit den jeweiligen Datenbeständen, Systemkomponenten und Konfigurationen (blau hinterlegter Bereich in der Graphik) sowie wichtige Massnahmen der Qualitätssicherung auf den jeweiligen Stufen (grün hinterlegter Bereich):

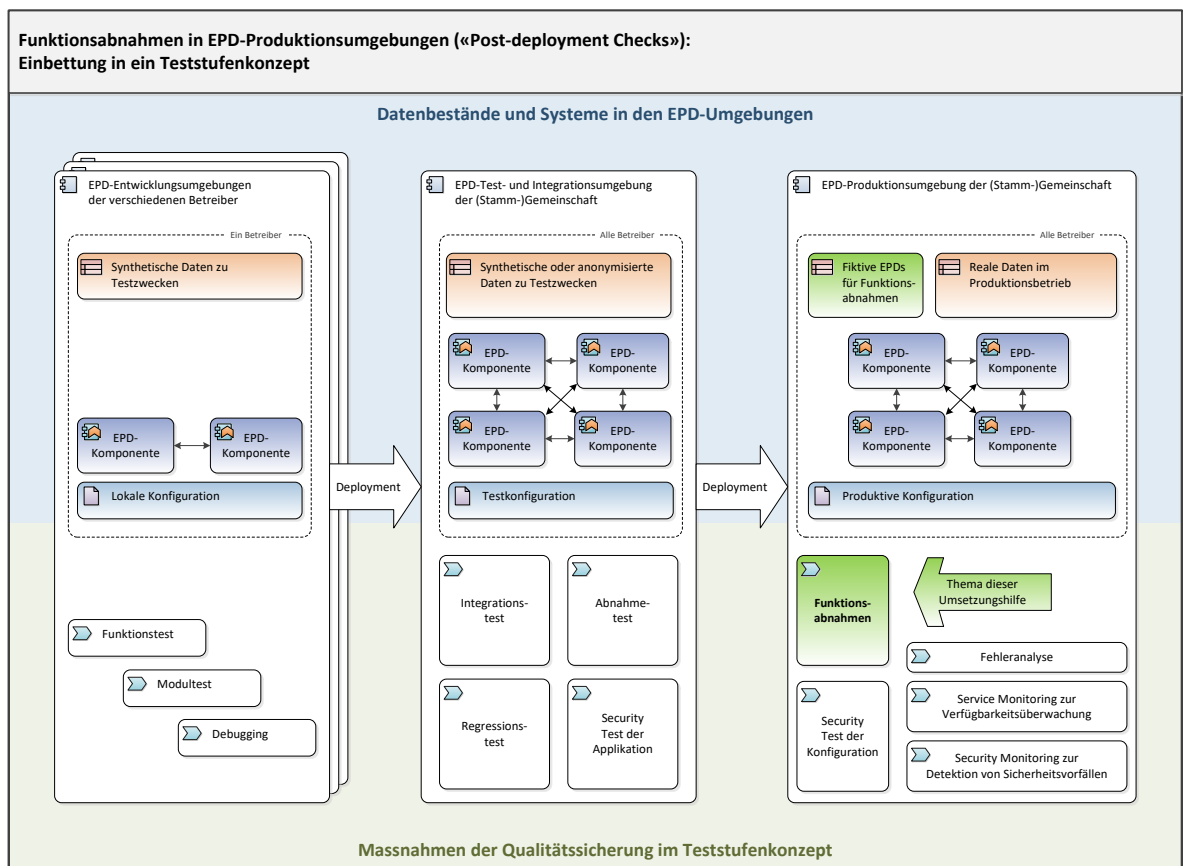


Abbildung 1: Funktionsabnahmen in EPD-Produktionsumgebungen, eingebettet in ein Teststufenkonzept

Funktionsabnahmen in den EPD-Produktionsumgebungen finden in jedem Fall statt. Es stellt sich lediglich die Frage, ob sie planmässig durch administratives Personal oder unbewusst durch die Benutzer durchgeführt werden, die Fehler im laufenden Betrieb bemerken und als Störung melden.

2.2 Praxiserfahrung aus EPD-Pilotprojekten

Aus zwei der grösseren EPD-Pilotierungsprojekte (MonDossierMédical in Genf und myEPD in Basel) wurde klar das Bedürfnis angemeldet, auch über Funktionsabnahme-Instrumente in den EPD-Produktionsumgebungen verfügen zu können. Beide Betriebsorganisationen stellten fest, dass sich trotz eines professionellen und umfassenden Testings in den Integrations-Umgebungen Fehler unterschiedlichster Art in die EPD-Produktion einschleichen können. Auszuschliessen seien Dysfunktionalitäten nie.

Im eHealth Pilot NW hat das Basler Gesundheitsdepartement den Betreibenden auf Anfrage deshalb explizit erlaubt, in der EPD-Produktion eine geringe Anzahl fiktiver myEPDs zu führen. Des Weiteren hat eine geringe und definierte Anzahl von Gesundheitsfachpersonen, welche in der ICT der angeschlossenen Gesundheitseinrichtung arbeiten, die Erlaubnis erhalten, auf fiktive EPDs oder gar echte, wenn deren Inhaber (hier: «friendly Users») anwesend sind, zuzugreifen. Allen Beteiligten wurden entsprechende reguläre digitale Identitäten ausgestellt.

In Genf verfügen die kantonalen Behörden über eine fiktive Gesundheitsfachperson, die auch für den Zweck der Qualitätssicherung eingesetzt wird. Diese fiktive Gesundheitsfachperson wiederum kann fiktive MonDossier-Médical erzeugen.

Diese Beispiele zeigen, dass die Betriebsverantwortlichen Möglichkeiten benötigen und auch bereits einsetzen, um in der «realen» EPD-Welt die definierte Funktions-Qualität einwandfrei und breitflächig feststellen zu können. «Bugs» und «Dysfunktionalität» erst via Kunden-Nutzung (Patienten- wie auch GFP-seitig) aufdecken zu lassen, ist eine zu riskante Strategie, weil sie in Kauf nimmt, dass EPD-Daten im entscheidenden Moment nicht zur Verfügung stehen.

Funktionsabnahmen in EPD-Produktionsumgebungen sind in der Praxis unverzichtbar

3 Funktionsabnahmen im EPD

3.1 Scope der Funktionsabnahmen

Funktionsabnahmen in den EPD-Produktionsumgebungen sollen die Qualität des Produktionsbetriebs sichern, indem fehlerhafte Veränderungen rasch festgestellt werden. Dies betrifft insbesondere Interoperabilitätsprobleme zwischen den verschiedenen Betreibern, die typischerweise auf Grund von Konfigurationsfehlern entstehen und in den Testumgebungen nicht festgestellt werden können. Der Scope der Funktionsabnahmen muss deshalb alle Systeme umfassen, deren Zusammenspiel für ein funktionierendes EPD-Gesamtsystem notwendig ist. Namentlich sind dies:

- Das Patienten-Portal, das GFP-Portal und die Admin-Portale;
- Die seitens der Gesundheitseinrichtungen integrierten GE-Systeme (Primärsysteme, EPD-Konnektoren, GE-eigene Zugangsportale);
- Die EPD-Backend-Systeme;
- Die Zugangspunkte / Gateways zwischen den Gemeinschaften;
- Die Systeme der Identity Provider (IdP) für Patienten und GFP/HIP;
- Die nationalen Dienste (UPI, Nationales HPD, CPI, MDI).

Auch die fehlerhafte Übernahme von Daten oder Programmcode im Rahmen des Deployment oder konfigurationsbedingte Performance-Probleme können erst in der EPD-Produktionsumgebung erkannt werden.

Alle Komponenten des Gesamtsystems sind im Scope

3.2 Anwendungsfälle

Auf den Folgeseiten sind die Anwendungsfälle (Use Cases) für die Funktionsabnahmen tabellarisch aufgeführt und priorisiert.

Angaben zu den Anwendungsfällen

Die Beschreibung der Anwendungsfälle umfasst folgende Angaben:

- Die Kolonne «Anwendungsfall» enthält die Funktionen des EPD, die abgenommen werden sollen («was wird abgenommen»);
- Die Kolonne «Prüfer» (gelb hinterlegt) zeigt an, wer die entsprechende Funktionsabnahme durchführt («wer nimmt ab»);
- Die Kolonne «automatisierbar» (rot hinterlegt) gibt an, ob die Abnahme automatisiert werden kann¹;
- Die Kolonne «Geprüfte Komponenten» (blau hinterlegt) zeigt an, welche Komponenten an der Funktion beteiligt und somit ein Objekt der Funktionsabnahme sind;
- In der Kolonne «Audit Trail» sind die Funktionen markiert, deren Ausführung im Audit Trail (ATNA Log) der Gemeinschaft protokolliert wird;
- Unter «Erkennbare Fehler» sind einige Fehlersituationen aufgeführt, die mit dieser Abnahme typischerweise erkannt werden. Diese Aufzählung ist nicht abschliessend.

Die Kolonne «Risiko» bewertet den Nutzen der Funktionsabnahme, der sich aus der zu erwartenden Häufigkeit und der Tragweite von erkennbaren Fehlern ergibt. Die in der Tabelle aufgeführte Risikobewertung ist eine nicht verpflichtende Hilfestellung für die (Stamm-)Gemeinschaften.

¹ Automatisierbarkeit setzt einen anonymen oder technischen Prüfer voraus. Für Endbenutzerfunktionen würde dies eine geeignete Emulationssoftware und ein Authentifizierungsmittel bedingen, das ohne Benutzerinteraktion genutzt werden kann (z.B. ein Soft Token). Beides ist im Umfeld des EPD derzeit nicht verfügbar.

Anwendungsfall		Prüfer						Automatisierbar?	Geprüfte Komponenten							Erkennbare Fehler	Risiko		
		Patient	Stellvertreter	GFP	HIP	Admin Personal	Technical User		Patienten-Portal	GFP-Portal	Admin-Portale	GE Systeme	EPD-Backend	IdP Systeme	Nationale Dienste		Häufigkeit	Tragweite	Risikozahl
1	Hinterlegte Value Sets							Ja								Dokumente mit ungültigen Metadaten oder GFP/HIP mit ungültigen Attributen. <i>Hinweis:</i> Die gültigen Metadaten für den Austausch medizinischer Daten sind im Anhang 3 der Verordnung des EDI spezifiziert und aus dem MetaDaten-Index MDI zu beziehen).	2	1	2
1a	Rolle der Autorin oder des Autors													X					
1b	Fachrichtung der Autorin oder des Autors													X					
1c	Organisatorischer Typ der Gesundheitseinrichtung											X	X						
1d	Fachrichtung der Gesundheitseinrichtung											X	X						
1e	Dokumentenklasse											X	X						
1f	Dokumententyp											X	X						
1g	Dokumentierter Vorgang											X	X						
1h	Sprache											X	X						
1i	Administratives Geschlecht Patientin/Patient											X	X						
1j	Vertraulichkeitsstufe											X	X						
1k	Technisches Format											X	X						
1l	MIME Type											X	X						
1m	Grund für das Bereitstellen											X	X						
1n	Rolle der bereitstellenden Person											X	X						
2	Monitoring der Endpunkte							Ja								Endpunkt steht nicht zur Verfügung / ist nicht erreichbar (Ausfall, fehlerhafte Netzwerk- oder Firewall-Konfiguration, ungültige MTLS-Zertifikate, ...)	3	2	6
2a	MPI												X						
2b	HPD der Gemeinschaft												X						
2c	Document Repository										(X) ¹	X							
2d	Document Registry												X						
2e	Audit Record Repository												X						
2f	IdP Patienten													X					
2g	IdP GFP und HIP													X					
2h	X-Assertion Provider Patienten												X	(X) ²					
2i	X-Assertion Provider GFP und HIP												X	(X) ²					
2j	UPI-Service														X				
2k	Nationales HPD														X				
3	Monitoring der Services							Ja								Service funktioniert nicht (fehlerhafte Zertifikate, Fehlfunktionen im Service, Fehlfunktion im GE-Client, ...)	3	2	6
3a	MPI						X						X						
3b	HPD der Gemeinschaft						X						X						
3c	Document Repository						X				(X) ¹	X							

Anwendungsfall		Prüfer						Automatisierbar?	Geprüfte Komponenten							Erkennbare Fehler	Risiko							
		Patient	Stellvertreter	GFP	HIP	Admin Personal	Technical User		Patienten-Portal	GFP-Portal	Admin-Portale	GE Systeme	EPD-Backend	IdP Systeme	Nationale Dienste		Audit Trail	Häufigkeit	Tragweite	Risikozahl				
3d	Document Registry						X	Nein					X											
3e	Audit Record Repository						X						X											
3f	IdP Patienten	X	X										X											
2g	IdP GFP und HIP			X	X								X											
3h	X-Assertion Provider Patienten						X	Ja				X	(X) ²											
3i	X-Assertion Provider GFP und HIP						X					X	(X) ²											
3j	UPI-Service													X										
3k	Nationales HPD													X										
4	On/Off-Boarding von Patienten							Nein								Integrationsprobleme der EPD-Plattform mit UPI-Service, Patienten-IdP	2	1 ⁴	2					
4a	EPD eröffnen	X				X			X		X	X	X	X	X									
4b	Wechsel Stammgemeinschaft	X	(X) ³			X			X		X	X	X	X	X									
4c	EPD Widerruf	X	(X) ³			X			X		X	X	X	X	X									
4d	Aufhebung bei Tod					X				X		X	X	X	X									
5	MPI Bewirtschaftung							Nein								Die lokalen Patienten-Identitäten und deren Attribute werden nicht korrekt verwaltet oder ausgetauscht	1	3 ⁵	3					
5a	Patient im MPI neu anlegen					X				X		X		X	X									
5b	MPI-Clearing					X				X		X			X									
6	On/Off-Boarding von GE					X	X	Nein			X		X		X	Fehlerhafte Provisionierung der GE in Systemen und HPD, z.B. wegen falsch hinterlegten OID für Produktion. Integrationsprobleme der EPD-Plattform mit dem nationalen HPD, dem GFP-IdP und GE IAM-Systemen (wo verfügbar)	1	2	2					
7	GFP/HIP Verwaltung (inkl. Gruppen)																							
7a	GFP/HIP manuell verwalten			X	X	X				X	X	X	X	X										
7b	GFP-Gruppen manuell verwalten					X				X		X	X	X										
7c	GFP/HIP über GE IAM verwalten						X	Ja			X	X	X	X	X									
8	GFP/HIP Login							Nein								Integrationsprobleme GFP-Portal / GE EPD-Viewer mit dem GFP IdP und/oder dem GE Active Directory.	2	2	4					
8a	Login am GFP-Portal aus dem Internet			X	X					X	X				X									
8b	Login am GFP-Portal mit GE-SSO			X	X					X		X	X		X									
8c	Login am GE EPD-Viewer			X	X					X		X	X		X									
9	Dokumenten-Verwaltung durch GFP/HIP							Nein								Integrationsprobleme EPD-Backend mit GE Upload-Client oder Assertion Provider. Cross-Community Integration?	2	2	4					
9a	Manueller Upload/Download von Dokumenten			X	X					X		X	X		X									
9b	Maschinelles Upload von Dokumenten (M2M)						X		Ja			X	X	(X) ²						X				

Anwendungsfall		Prüfer						Automatisierbar?	Geprüfte Komponenten							Erkennbare Fehler	Risiko				
		Patient	Stellvertreter	GFP	HIP	Admin Personal	Technical User		Patienten-Portal	GFP-Portal	Admin-Portale	GE Systeme	EPD-Backend	IdP Systeme	Nationale Dienste		Audit Trail	Häufigkeit	Tragweite	Risikozahl	
10	Weitergabe von Zugriffsrechten			X				Nein		X			X			X		1	1	1	
11	Allgemeine GFP-Portalfunktionen			X	X			Nein		X			X				Fehlerhafte GFP-Portal-Applikation (unbekannte Fehler)	1	2	2	
12	Patienten / Stellvertreter Login	X	X					Nein	X				X	X		X	Integrationsprobleme Patienten-Portal mit dem Patienten-IdP und/oder dem X-Assertion Provider für Patienten.	2	2	4	
13	Dokumenten-Verwaltung durch Patienten							Nein									Integrationsprobleme EPD-Backend mit Patienten-Portal. Cross-Community Integrationsprobleme.	2	2	4	
13a	Anzeige Dokumentenliste	X	X						X				X			X					
13b	Zugriff/Download Dokumente aus eigener SG	X	X						X				X			X					
13c	Zugriff/Download Dokumente Cross-Community	X	X						X				X			X					
13d	Zugriff DICOM Bild aus eigener SG	X	X						X				X			X					
13e	Zugriff DICOM Bild Cross-Community	X	X						X				X			X					
13f	Dokumente Upload	X	X						X				X			X					
13g	Vertraulichkeitsstufe anpassen (innerhalb SG)	X	X						X				X			X					
13h	Vertraulichkeitsstufe anpassen (Cross-Community)	X	X						X				X			X					
13i	Offline Archivierung Export (XDM)	X	X						X				X			X					
13j	Offline Archivierung Import (XDM)	X	X						X				X			X					
13k	Dokumentenlöschung nach 20 Jahren ausschliessen	X	X						X				X			X					
14	Zugriffsrechte-Verwaltung durch Patienten							Nein									Integrationsprobleme EPD-Backend mit Patienten-Portal.	1	1 ⁴	1	
14a	GFP Zugriffsrechte verwalten (inkl. Delegation)	X	X						X				X			X					
14b	GFP-Gruppen Zugriffsrechte verwalten	X	X						X				X			X					
14c	Notfallzugriff konfigurieren	X	X						X				X			X					
14d	Standard-Vertraulichkeitsstufe konfigurieren	X	X						X				X			X					
15	Stellvertretung einrichten / entfernen	X	(X) ³					Nein	X		X		X	X		X	Integrationsprobleme Patienten-Portal mit dem Patienten-IdP und dem EPD-Backend	2	1 ⁴	2	
16	Zugriffsprotokoll einsehen	X	X					Nein	X				X				Integrationsprobleme EPD-Backend mit Patienten-Portal.	2	1 ⁴	2	
17	Notifikationen							Nein									Integrationsprobleme EPD-Backend mit Patienten-Portal.	1	1	1	
17a	Notifikationseinstellungen	X	X						X				X			X					
17b	Notifikation bei Gruppenänderung	X	X						X				X			X					
17c	Notifikation bei Notfallzugriff	X	X						X				X			X					
18	Allgemeine Patienten-Portalfunktionen	X	X					Nein	X								Fehlerhafte Patienten-Portal-Applikation (unbekannte Fehler)	1	1	1	

Fussnoten zur Tabelle der Anwendungsfälle:

- ¹: Falls die Gesundheitseinrichtung ein eigenes Repository selber betreibt.
- ²: Falls der X-Assertion Provider vom IdP betrieben wird.
- ³: Stammgemeinschaften können die Rechte gewillkürter Stellvertreter einschränken und beispielsweise die Einrichtung weiterer Stellvertreter, den EPD-Widerruf oder den Wechsel der Stammgemeinschaft durch EPD-Stellvertreter unterbinden.
- ⁴: Administrative Use Cases (z.B. Verwaltung von Patienten und GFP/HIP) sind weniger verfügbarkeitskritisch als Laufzeit-Services (z.B. Login oder Upload/Download von Dokumenten).
- ⁵: Fehlerhaftes MPI Clearing kann zur Zuweisung von Dokumenten an falsche Patienten führen.

4 Rahmenbedingungen

In der temporären Arbeitsgruppe «Funktionsabnahmen / Quality Assurance in EPD-Produktivsystemen» wurden wichtige Anspruchsgruppen in die Erarbeitung des vorliegenden Konzeptes einbezogen.

Temporäre AGR
Funktionsabnahmen

Seitens dieser Anspruchsgruppen wurden die nachfolgend aufgeführten Rahmenbedingungen für die Lösungskonzeption eingebracht:

Rahmenbedingungen der Zentralen Ausgleichsstelle (ZAS):

Reale EPR-SPID für
(wenige) fiktive Personen sind möglich

- Die ZAS kann fiktive Personen in der UPI-Produktionsumgebung erstellen, denen die ZAS (bzw. die Stammgemeinschaften) reale EPR-SPID zuordnen können.
- Die (Stamm-)Gemeinschaften sollten keine fiktiven EPR-SPID in ihren Produktionsumgebungen benutzen, denn eine Kollision mit einer realen EPR-SPID ist früher oder später möglich.
- Die fiktiven Personen dürfen ausschliesslich dafür genutzt werden, im Rahmen von Funktionsabnahmen die korrekte Konfiguration und Verfügbarkeit des produktiven Gesamtsystems zu verifizieren.
- Die fiktiven Personen dürfen nicht für die Durchführung funktionaler Tests genutzt werden; für funktionale Tests sind ausschliesslich die EPD-Integrationsumgebungen zu verwenden.

Rahmenbedingungen des Bundesamtes für Gesundheit (BAG):

Es sind keine Änderungen am nationalen HPD erlaubt

- Die Funktionsabnahmen dürfen keine technischen oder konfigurativen Anpassungen am nationalen HPD erforderlich machen.

Rahmenbedingungen der Identity Provider für Patienten (IdP):

Fiktive Identitäten mit bestätigter Identität sind nicht möglich

- Die Erstellung von fiktiven Identitäten mit bestätigter Identität ist ein Compliance-Problem, dass nicht gelöst werden kann.

Das in den nachfolgenden Kapiteln beschriebene Lösungskonzept ist mit diesen Rahmenbedingungen konform.

5 Lösungskonzept

5.1 Fiktive elektronische Patientendossiers (EPDs)

Die Stammgemeinschaften eröffnen für die Durchführung von Funktionsabnahmen in EPD-Produktionsumgebungen fiktive elektronische Patientendossiers (EPDs). Die fiktiven EPDs inklusive der Berechtigung eines oder mehrerer EPD-Stellvertreter werden durch den Plattformbetreiber oder einen Systemadministrator der Stammgemeinschaft vorbereitet, ohne dass ein regulärer EPD Onboarding-Prozess durchlaufen wird.

Fiktive EPDs

Die Inhaber der fiktiven EPDs sind fiktive Personen, denen im produktiven UPI-Service eine reale aktive EPR-SPID zugeordnet wird. Es muss möglich sein, den fiktiven Personen über die eCH-0214 Schnittstelle eine aktive EPR-SPID zuordnen zu können.

Fiktive Personen erhalten keine elektronische Identität und können selber nicht auf das Patienten-Portal zugreifen. Die Funktionsabnahmen werden deshalb von den EPD-Stellvertretern durchgeführt, die für die fiktiven EPDs definiert sind. Die EPD-Stellvertreter verwenden hierfür eine echte EPD-konforme elektronische Identität und führen die Funktionsabnahme in der EPD-Stellvertreter-Rolle aus.

Funktionsabnahmen
durch
EPD-Stellvertreter

Für Stammgemeinschaften, welche die die Rechte gewillkürter EPD-Stellvertreter einschränken und beispielsweise die Einrichtung weiterer Stellvertreter, den EPD-Widerruf oder den Wechsel der Stammgemeinschaft durch EPD-Stellvertreter unterbinden, ergibt sich dadurch eine Einschränkung der Use Cases bei den Funktionsabnahmen, die in Kauf genommen werden muss.

5.2 Hilfspersonen mit QS-Aufgaben

Die Funktionsabnahmen werden durch entsprechend beauftragte Hilfspersonen (HIP) durchgeführt. Diese «Hilfspersonen mit QS-Aufgaben» unterscheiden sich nicht von anderen Hilfspersonen, ausser dass sie das EPD-Produktionssystem in einem QS-Kontext und nicht in einem Behandlungskontext benutzen. Es werden keine fiktiven HIP oder GFP eingerichtet und es sind somit keinerlei Anpassungen seitens des nationalen HPD oder seitens des IdP für GFP notwendig.

Hilfspersonen (HIP)
mit QS-Aufgaben

Die Hilfspersonen mit QS-Aufgaben benützen für die Funktionsabnahmen die folgenden Zugänge zum EPD:

- Das GFP-Portal der (Stamm-)Gemeinschaft oder ein GE-eigenes GFP-Portal, an dem sie sich mit ihrem persönlichen Authentifizierungsmittel anmelden. Damit sie auf die fiktiven EPDs zugreifen können, werden sie einer Gesundheitsfachperson mit QS-Verantwortung zugeteilt (siehe nächster Abschnitt);
- Hilfspersonen mit QS-Aufgaben können sich auch als EPD-Stellvertreter eines fiktiven Patienten am Patienten-Portal anmelden, sofern sie als EPD-Stellvertreter für das entsprechende fiktive EPD eingetragten sind (siehe Kapitel 5.1).

Hilfspersonen mit QS-Aufgaben sind einer Gesundheitsfachperson (GFP) zugeteilt, welche die Verantwortung für die ordnungsgemässe Durchführung der Funktionsabnahmen trägt.

Gesundheitsfachperson (GFP) mit QS-Verantwortung

Diese «GFP mit QS-Verantwortung» wird von einem EPD-Stellvertreter des fiktiven Patienten für den Zugriff auf das fiktive EPD berechtigt.

Die GFP mit QS-Verantwortung kann im Behandlungskontext auch auf reale EPDs zugreifen. Sie muss die ihr zugeteilten HIP mit QS-Aufgaben deshalb dahingehend instruieren und kontrollieren, dass der Zugriff auf reale EPDs im QS-Kontext nicht erlaubt ist.

5.3 Trennung von QS-Kontext und Behandlungskontext

Fiktive EPDs dürfen ausschliesslich fiktive Dokumente mit fiktiven Inhalten ohne Bezug zu einer medizinischen Behandlung oder zu realen Personen enthalten. Der Zugriff auf fiktive EPDs erfolgt somit nie in einem Behandlungskontext, sondern immer in einem QS-Kontext.

QS-Kontext und Behandlungskontext sind strikte getrennt

Die Zugriffsberechtigung für fiktive EPDs dürfen nur an Gesundheitsfachpersonen mit QS-Verantwortung erteilt werden und nur Hilfspersonen mit QS-Aufgaben dürfen auf fiktive EPDs zugreifen.

Für Funktionsabnahmen in EPD-Produktionsumgebungen dürfen ausschliesslich fiktive EPDs genutzt werden. Hilfspersonen mit QS-Aufgaben dürfen im Rahmen der Funktionsabnahmen ausschliesslich auf fiktive EPDs zugreifen, auch wenn sie über weitergehende Zugriffsrechte verfügen sollten. Wo dieser Grundsatz nicht technisch implementiert werden kann (z.B. Notfallzugriff), muss die GFP mit QS-Verantwortung das von der Gemeinschaft definierte Regulativ gegenüber den Hilfspersonen mit QS-Aufgaben organisatorisch durchsetzen.

5.4 Umsetzung in den EPD-Komponenten

Damit Funktionsabnahmen in EPD-Produktionsumgebungen möglich sind, müssen in verschiedenen Systemen und Umsystemen des EPD entsprechende Vorkehrungen getroffen werden:

Drei Umsetzungsbereiche

1. Einrichten fiktiver EPDs: Dies erfordert fiktive Personen mit realen EPR-SPIDs und entsprechende Einträge im produktiven UPI-Service sowie im MPI der (Stamm-)Gemeinschaft;
2. Einrichten von EPD-Stellvertretern für die fiktiven EPDs. Dies können, müssen aber nicht Hilfspersonen mit QS-Aufgaben sein;
3. Einrichten von Hilfspersonen mit QS-Aufgaben. Dies erfordert:
 - ⇒ Die Registrierung der beauftragten Personen im HPD der (Stamm-)Gemeinschaft;
 - ⇒ Die Zuteilung an eine GFP mit QS-Verantwortung;
 - ⇒ Die Zuteilung der Zugriffsrechte auf die fiktiven EPDs an diese GFP mit QS-Verantwortung.

Die Hilfspersonen mit QS-Aufgaben unterscheiden sich technisch nicht von anderen Hilfspersonen. Es sind deshalb weder im nationalen HPD noch im GFP-Portal Anpassungen oder Datenerfassungen erforderlich.

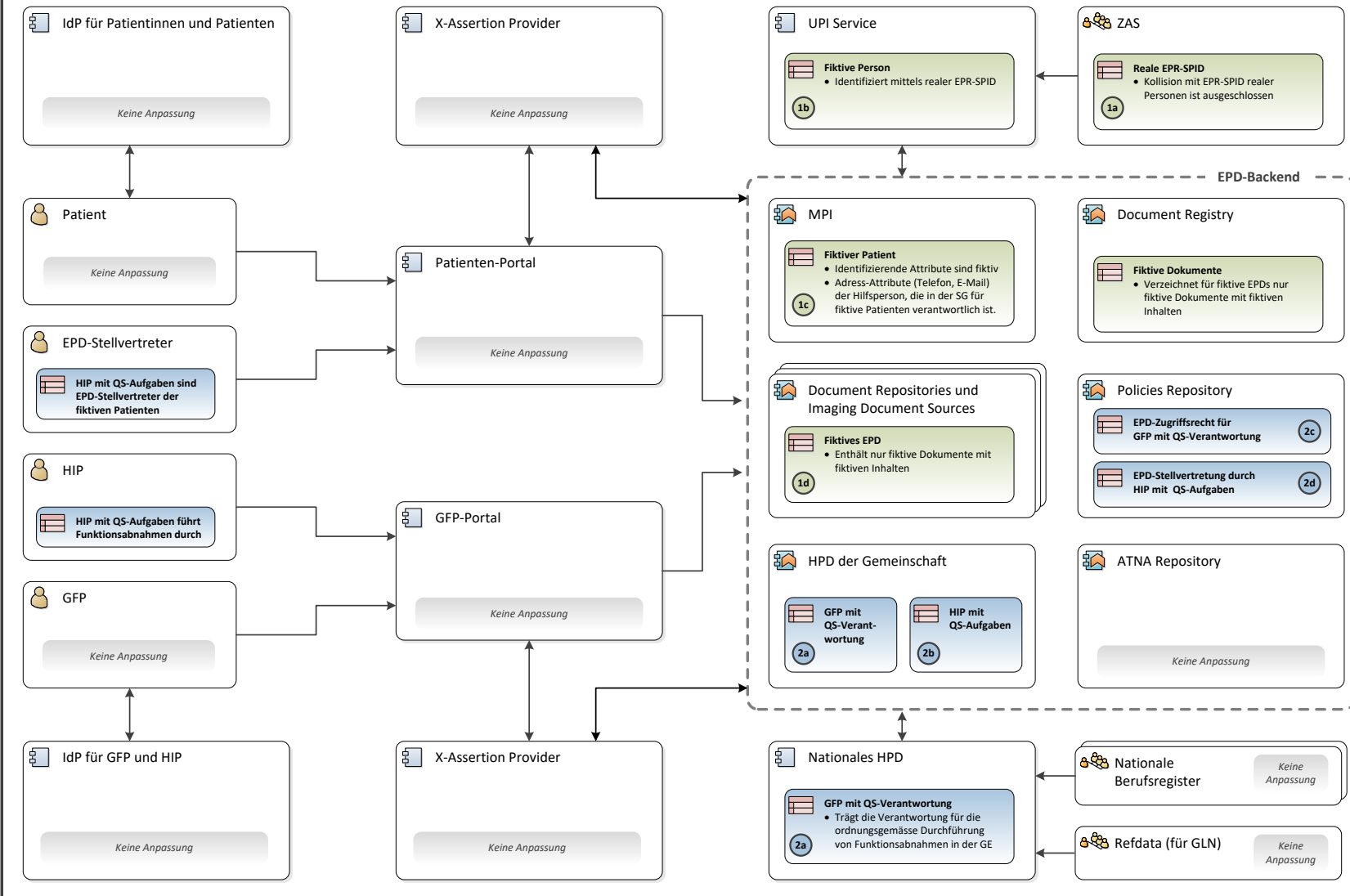
Die Abbildung auf der Folgeseite zeigt auf, in welchen EPD-Komponenten welche Vorkehrungen umgesetzt werden müssen:

Funktionsabnahmen in EPD-Produktionsumgebungen («Post-deployment Checks»): Umsetzung in den EPD-Komponenten

Umsetzungsbereiche

1 Einrichten fiktive EPDs

2 Einrichten HIP mit QS-Aufgaben



6 Umsetzungsmassnahmen

Nachfolgend werden die Massnahmen identifiziert und beschrieben, mit denen Funktionsabnahmen in EPD-Produktionsumgebungen ermöglicht werden. Zusätzlich werden flankierende Massnahmen skizziert, die für eine zusätzliche Verbesserung der Produktionsqualität ebenfalls empfohlen sind.

6.1 Implementierung dieser Umsetzungshilfe

M1 Einrichten von fiktiven Personen im UPI-Service

Die Zentrale Ausgleichsstelle (ZAS) erfasst bis Ende März 2020 im produktiven UPI-Service maximal 24 fiktive Personen, die von den EPD (Stamm-)Gemeinschaften für Funktionsabnahmen in EPD-Produktionsumgebungen verwendet werden können:

- Jeder Stammgemeinschaft stehen zwei fiktive Personen mit unterschiedlichem Geschlecht zur Verfügung, denen sie je eine EPR-SPID zuordnen kann.
- Stammgemeinschaften können je eine dieser fiktiven Personen für die Funktionsabnahmen von internen Transaktionen und cross-community Transaktionen nutzen.
- Zusätzlich gibt es vier fiktive Personen für nationale Zwecke, deren EPR-SPID von der ZAS generiert wird:
 - Eine fiktive verstorbene Person;
 - Je eine fiktive männliche und weibliche Person;
 - In einer zukünftigen Erweiterung des UPI-Service: Eine Person mit dem Geschlecht «other» gemäss Anhang 3 der Verordnung des EDI bzw. «unbestimmt» gemäss Registerharmonisierungsgesetz (siehe BFS «Amtlicher Katalog der Merkmale», Version 2014 § 33 Geschlecht).

Die fiktiven Personen mit ihren Attributen (Name, Vornamen, Geschlecht, Geburtsdatum) werden von der ZAS im produktiven UPI-Service erfasst.

eHealth Suisse weist jeder Stammgemeinschaft zwei fiktive Personen zu, für deren fiktive EPD (inkl. EPR-SPID) sie verantwortlich ist.

Auch der Anwendungsfall «EPD-Widerruf» muss abgenommen werden. Damit die Anzahl der für Funktionsabnahmen verwendeten EPR-SPID auf eine (im Vergleich zur Gesamtzahl aller möglichen EPR-SPID) kleine Zahl begrenzt bleibt, darf eine Stammgemeinschaft nicht mehr als 400 EPR-SPIDs pro Jahr im Rahmen von Funktionsabnahmen in der Produktion annullieren.

Hinweise:

- Gemäss den Grundregeln der ZAS werden EPR-SPID zufällig generiert und annullierte EPR-SPID dürfen nie mehr gebraucht werden. Es ist deshalb nicht möglich, nach einem EPD-Widerruf dieselbe EPR-SPID nochmals zu nutzen.
- Die fiktiven Personen können auch von anderen Kunden des UPI-Service abgefragt werden.

M2 Einrichten der fiktiven EPDs in den (Stamm-)Gemeinschaften

Die Stammgemeinschaften eröffnen für die ihnen zugeteilten fiktiven Personen je ein fiktives elektronisches Patientendossier (EPD).

Die fiktiven EPDs inklusive der Berechtigung von mindestens einem EPD-Stellvertreter werden durch den Plattformbetreiber oder einen Systemadministrator der Stammgemeinschaft vorbereitet, ohne dass ein regulärer EPD Onboarding-Prozess durchlaufen wird. Dabei werden die folgenden Objekte angelegt:

- MPI Eintrag mit aktiver EPR-SPID, welche von der ZAS für den fiktiven EPD Inhaber in einer bestimmten Stammgemeinschaft bereitgestellt wird (via Patient Identity Feed HL7 V3 [ITI-44], keine besondere EPD Berechtigungsrolle erforderlich);
- EPD Setup Policies (21, 22, 23), in denen die entsprechende EPR-SPID eingetragen wird (via Privacy Policy Feed [PPQ-1], EPD Berechtigungsrolle "Policy Administrator" erforderlich);
- EPD Access Policy (33) für mindestens einen oder mehrere Stellvertreter, welche einem EPD-Stellvertreter den Zugriff auf das EPD mit der entsprechenden EPR-SPID erlaubt (via Privacy Policy Feed [PPQ-1], EPD Berechtigungsrolle "Policy Administrator" erforderlich);
- Ggf. weitere EPD Plattform spezifische Objekte, welche z.B. gemäss Datenmodell für die Funktion des Patienten-Portals erforderlich sind (via applikationsspezifische Methoden, keine besonderen EPD Berechtigungsrollen erforderlich).

Dokumente und Metadaten sowie Zugriffsrechte können im fiktiven EPD dann durch den EPD-Stellvertreter angelegt werden.

Hinweis: Nur Stammgemeinschaften können fiktive EPDs eröffnen, da bei Gemeinschaften die entsprechende Infrastruktur nicht vorhanden ist.

M3 Verantwortliche HIP für die fiktiven EPDs

Die Stammgemeinschaft bestimmt genau eine Hilfsperson mit QS-Aufgaben (inkl. Stellvertreter), die für die beiden fiktiven EPDs der Stammgemeinschaft verantwortlich ist.

Diese ausgewählte Hilfsperson mit QS-Aufgaben:

- Ist für die Daten der beiden fiktiven Patienten verantwortlich;
- Ist EPD-Stellvertreter der beiden fiktiven Patienten;
- Verwaltet weitere EPD-Stellvertretungen für die fiktiven Patienten, eingeschränkt auf den Kreis der HIP mit QS-Aufgaben;
- Erteilt allen GFP mit QS-Verantwortung in der eigenen Stammgemeinschaft das Zugriffsrecht auf die fiktiven EPDs;
- Kann GFP mit QS-Verantwortung aus anderen Gemeinschaften das Zugriffsrecht auf die fiktiven EPDs erteilen;
- Prüft während der Funktionsabnahmen, dass sich in den fiktiven EPDs nur fiktive Dokumente mit fiktiven Inhalten befinden.

M4 Attribute der fiktiven Patienten

Die Stammdaten der fiktiven Personen (Name, Vornamen, Geschlecht, Geburtsdatum) werden von der ZAS im UPI-Service erfasst. Alle weiteren Daten der fiktiven Patienten werden von der für

die fiktiven EPDs verantwortlichen Hilfsperson erfasst gemäss folgenden Vorgaben:

- Postadresse der fiktiven Patienten:
Postadresse der Stammgemeinschaft
- E-Mail-Adresse der fiktiven Patienten:
E-Mail-Adresse der verantwortlichen HIP
- Telefonnummern der fiktiven Patienten:
Telefonnummern der verantwortlichen HIP

Die übrigen Attribute werden nach den Bedürfnissen der Stammgemeinschaft festgelegt.

M5 Regulativ für die Durchführung von Funktionsabnahmen

Jede (Stamm-)Gemeinschaft definiert für die Durchführung von Funktionsabnahmen («Post-deployment Checks») ein Regelwerk, das mindestens umfasst:

- Die Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) der Hilfspersonen mit QS-Aufgaben und der Gesundheitsfachpersonen mit QS-Verantwortung;
- Instruktion der HIP mit QS-Aufgaben in Bezug darauf, dass der Zugriff auf reale EPDs im QS-Kontext nicht erlaubt ist;
- Das Drehbuch für die Durchführung von Funktionsabnahmen. Zu klären ist beispielsweise:
 - ⇒ In welchen Fällen werden fiktive EPDs widerrufen (gemäss M1 dürfen pro Stammgemeinschaft jährlich maximal 400 EPR-SPID von fiktiven Personen annulliert werden)?
 - ⇒ Werden Zugriffsrechte und Stellvertretungen nach jeder Funktionsabnahme entzogen oder sind sie dauerhaft?
 - ⇒ Welche Regeln gelten für die Durchführung manueller Funktionsabnahmen unter Verwendung fiktiver EPDs der eigenen (Stamm-)Gemeinschaft oder von anderen Stammgemeinschaften?
 - ⇒ Welche Regeln gelten für den maschinellen Upload von fiktiven (als solche ersichtlichen und gekennzeichneten) Dokumenten in fiktive EPDs?
- Regeln für die Nutzung der fiktiven EPDs in den Primärsystemen angebundener Gesundheitseinrichtungen (Patientenadministration, KIS, ...), falls dazu eine Notwendigkeit besteht.

M6 Liste aller HIP und GFP mit QS-Funktionen

Die für die fiktiven EPDs verantwortliche Hilfsperson führt eine Liste mit:

- Allen HIP mit QS-Aufgaben in der (Stamm-)Gemeinschaft;
- Allen GFP mit QS-Verantwortung in der (Stamm-)Gemeinschaft

(Stamm-)Gemeinschafts-übergreifende Fragestellungen und Koordinationsaufgaben werden durch eHealth Suisse bearbeitet bzw. wahrgenommen.

6.2 Flankierende und ergänzende Massnahmen

Ergänzend zu den unter 6.1 beschriebenen Massnahmen für die Implementierung dieser Umsetzungshilfe sollten weitere Massnahmen für die nachhaltige Verbesserung der Produktionsqualität in Betracht gezogen werden:

FM1 Automatisiertes Monitoring

Laufende automatisierte Kontrolle, ob die EPD-Endpunkte erreichbar und die EPD-Services verfügbar sind (Anwendungsfälle 2a bis 2k sowie 3a bis 3e und 3h bis 3k).

FM2 Hilfsmittel für Fehleranalyse

Bereitstellen von Hilfsmitteln für die Analyse von Fehlersituationen in EPD-Produktionsumgebungen, allenfalls unter Nutzung der fiktiven EPDs.