Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Hilfestellung des Bundesamtes für Gesundheit (BAG)

Datum: 17. Februar 2020

Für ergänzende Auskünfte: Sandra Burri

Zertifizierung der (Stamm-)Gemeinschaften nach dem Bundesgesetz über das elektronische Patientendossier: Durchführung von komplexen Anwendungsfällen

Ausgabe 1.2 vom 17. Februar 2020

Kontakt:
Sandra Burri
Sektion eHealth und Krankheitsregister
Bundesamt für Gesundheit BAG
sandra.burri@bag.admin.ch

Änderungen:

Die Ausgabe 1.2 enthält keine materiellen Veränderungen an den einzelnen komplexen Anwendungsfällen. Es wurden einzelne Aspekte präzisiert und die Referenzierung zur jeweiligen Ziffer des Anhang 2 der EPDV-EDI (im weiteren als TOZ [steht für Technische und Organisatorische Zertifizierungsvoraussetzungen] bezeichnet) ergänzt.

- Nicht nur die Patientinnen und Patienten, sondern auch die GFP müssen über ein Identifikationsmittel eines zertifizierten (oder sich im Zertifizierungsverfahren befindlichen) Herausgebers verfügen, mit welchem sie das Login vornehmen. Diese Ergänzung dient der Vollständigkeit im vorliegenden Dokument, auch wenn dieser Sachverhalt in den KAF nicht explizit abgeprüft wird.
- Bei Aufhebung des EPD muss die Stammgemeinschaft den Patientinnen und Patienten vorgängig die Dokumente inklusive der Metadaten zur Verfügung stellen. Ob dies mit der Funktionalität «Herunterladen» oder «auf andere Weise» bereitgestellt wird, ist der Stammgemeinschaft freigestellt. Die Aufteilung in KAF 16 a) und b) ist damit eine Anpassung im Sinne der Stammgemeinschaften, da sie Wahlfreiheit bei der Umsetzung lässt.

Ausgabe	Kapitel	Kommentar zu den Änderungen
1.2	2.4	Ergänzung: Für sämtliche Systeme ~~(inklusive der zentralen Dienste)~~ gilt, dass jeweils eine produktionsnahe (aber nicht produktive) Umgebung angesprochen wird und dass keine echten Daten vorliegen oder verwendet werden.
1.2	2.4	Präzisierung: Alt: Es ist vorgängig zu organisieren, dass der IdP während der Zertifizierung zur Verfügung steht um die notwendigen Identitäten von Benutzern anzulegen. Neu: Es ist vorgängig zu organisieren, dass die GFP und Patientinnen über ein IDM eines zertifizierten (oder sich im Zertifizierungsverfahren befindlichen) Herausgebers verfügen und diese während der Durchführung der KAF verwendet werden.
1.2	2.4	Ergänzung: Bei der Durchführung der KAF dürfen die Bezeichnungen der medizinischen Daten nicht verändert werden, denn diese dienen innerhalb des Ablaufes als Orientierung.
1.2	2.4	Ergänzung um Varianten der Konvertierung von medD Doc_A1.
1.2	2.4	Ergänzung: Jede GFP sowie die Gesundheitseinrichtung soll über möglichst realitätsnahe Personendaten bzw. Bezeichnung verfügen. Die Zuordnung zu den in Tabelle 4 aufgeführten Akteuren muss eineindeutig und für alle ersichtlich festgehalten werden.
1.2	2.4	Ergänzung: Protokollierung: Mit den in den KAF verlangten Protokollierungen sind diejenigen Protokoll-Einträge gemeint, welcher die Patientin oder der Patient in ihrem oder seinem Patientenportal einsehen kann.
1.2	Alle KAF	Referenzierung der relevanten Vorgaben in der TOZ
1.2	3.2	KAF-Id 002. Präzisierung Ablaufbeschreibung und Ergebnisse: - Varianten 1 und 2 möglich - medD Doc_A1 kann nachträglich hochgeladen werden, dies muss nicht zwingend durch GFP_A erfolgen.
1.2	3.08	Ab KAF-Id 008. Ergänzung: medD Doc_A1 «deprecated» / medD Doc_A2 «approved»

Ausgabe	Kapitel	Kommentar zu den Änderungen
1.2	3.10	KAF-Id-010. Korrektur und Ergänzung: EGFP_E überweist den P an GFP_A und erteilt GFP_A das Zugriffsrecht (…) Alt: normal zugänglich Neu: eingeschränkt zugänglich GFP_A sieht neu auch: Doc_XCA2 / Doc_XDA2 / Doc_A2 (approved) / Doc_XCA1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ)
1.2	3.11	KAF-Id 011. Präzisierung: Es kann nach Belieben eine STV aus den alt: 10 individuellen Kombinationen neu: zur Verfügung stehenden fiktiven Personen ausgewählt werden.
1.2	3.14	KAF-Id 014. Präzisierung: Die Änderung der Vertraulichkeitsstufe ist sinngemäss wie folgt protokolliert: Das medD Doc_XCA2 wurde verändert bzw. aktualisiert.
1.2	3.15	KAF-Id 015. Präzisierung: Die erwarteten Ergebnisse sind konkretisiert worden. Die Formulierung «vollständig» wurde gestrichen.
1.2	3.16	KAF-Id 016. Präzisierung: Aufteilung in Varianten a) und b). Herunterladen von einzelnen Dokumenten ist nicht mehr Bestandteil des KAF.

1 Ausgangslage

Die Überprüfung einzelner Transaktionen im Rahmen der technischen Zertifizierung (technische Konformitätsprüfung) stellt nicht hinreichend sicher, dass das Zusammenspiel der verschiedenen Transaktionen in den konkreten Anwendungsfällen (z. B. Eröffnen eines EPD) funktioniert. Zudem kann mit einer Konformitätsprüfung auf Transaktionsebene nicht sichergestellt werden, dass das Verhalten der Systeme – vor allem die normativ geltenden (z. B. zur Steuerung der Zugriffsrechte) – auch tatsächlich erwartungsgemäss realisiert sind. Somit bedeutet eine erfolgreiche technische Konformitätsprüfung noch nicht zwingend, dass die EPD-Plattform auch im operativen Betrieb und in der jeweils spezifischen Konfiguration der zu zertifizierenden Stammgemeinschaft auch korrekt funktioniert.

Deshalb wird die Zertifizierungsstelle ausgewählte Anwendungsfälle im Sinne von fachlichen Abnahmetests direkt auf der EPD-Plattform der Stammgemeinschaft durchführen. Die zu prüfenden Anwendungsfälle werden vom BAG festgelegt und sind in folgendem Dokument «Durchführung von komplexen Anwendungsfällen» beschrieben.

2 Grundlagen für das Testen von komplexen Anwendungsfällen (KAF)

2.1 Abkürzungen

Folgende Abkürzungen werden nachfolgend verwendet:

Abkürzung	Beschreibung
KAF	komplexer Anwendungsfall
medD	medizinische Daten
EPD	Elektronisches Patientendossier einer Patientin bzw. eines Patienten
BAG	Bundesamt für Gesundheit
uuid	eineindeutige Identifikationsnummer der medizinischen Daten
ZTS	Zertifizierungstestsystem
ZAS	Zentrale Ausgleichsstelle
SG	Stammgemeinschaft
P	Patientin / Patient
STV	Stellvertretung einer Patientin bzw. eines Patienten
GFP	Gesundheitsfachperson
GR-GFP	Gruppe von Gesundheitsfachpersonen
HiP	Hilfsperson Sie besitzt die gleichen Rechte, wie die für sie verantwortliche und in der SG mit ihr verknüpfte GFP
MPA	Medizinische Praxisassistentin / Medizinischer Praxisassistent
EGFP	Von der Patientin oder dem Patienten ermächtigte Gesundheitsfachperson
IDM	Identifikationsmittel
TOZ	Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften, Anhang 2 der EPDV-EDI
EPDV-EDI	Verordnung des EDI über das elektronische Patientendossier (SR 816.111)

Tabelle 1: Definition von Abkürzungen

2.2 Inhalt und Zweck des Dokuments

Die Zertifizierung einer Stammgemeinschaft erfolgt in drei separaten Schritten. In Ergänzung zur Prüfung der organisatorischen Voraussetzungen (Prozesse, Dokumente etc.) sowie der technischen Prüfung der EPD-Plattform auf der Basis von Einzeltransaktionen werden komplexe Anwendungsfälle (KAF) auf der EPD-Plattform durchgeführt um die rechtskonforme Umsetzung des Zusammenspiels der verschiedenen Transaktionen im konkreten Anwendungsfall (z. B. Eröffnung eines EPD oder Änderungen an der Berechtigungssteuerung durch die Patientin oder den Patienten) zu prüfen.

Die stammgemeinschaftsübergreifenden Transaktionen (Interoperabilität) werden im Rahmen der technischen Zertifizierung abgeprüft. Die KAF beschränken sich auf Transaktionen innerhalb der Stammgemeinschaft.

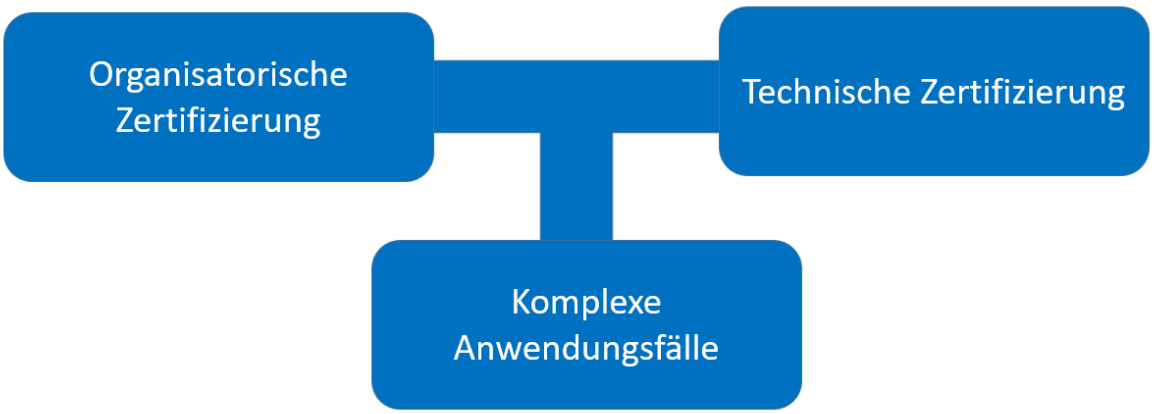

Abbildung 1: Die drei Teile der Zertifizierung

Die KAF können mit Ausgabe 1.2 nur bei einer Stammgemeinschaft abgeprüft werden, da in einer Gemeinschaft kein EPD eröffnet werden kann. Das BAG prüft die Umsetzung der KAF bei Gemeinschaften.

Die Definition der KAF erfolgte risikobasiert und deckt nicht alle denkbaren Geschäftsfälle ab. Es wurden diejenigen KAF ausgewählt, welche mit hoher Wahrscheinlichkeit bzw. Häufigkeit auftreten werden und/oder ein hohes Schadenspotenzial bei Fehlfunktion darstellen. Sie fokussieren sich insbesondere auf die korrekte Umsetzung der Bestimmungen von Artikel 1 bis 4 EPDV zu Vertraulichkeitsstufen und Zugriffsrechten.

Erfüllungs-ebene	Zielsetzung	Wesentliche Prüfgegenstände	Beispiele für Evidenzen	Prüfhandlungen durch
Organisatorische Zertifizierungsvo-raussetzungen	- Rechtskonforme Aufbau- und Ablauforga-nisation - Datenschutz und Datensicherheit rechts-konform (organisatorisch)	- Managementsystem der Stammgemein-schaft - Richtlinien - Prozesse - Verfahren - Organisationsstrukturen - Einrichtungen* - Personen*	- Prozess- / System-Dokumentationen - Verträge / Vereinbarungen - Weisungen - Umsetzungsnachweise - Interview-Ergebnisse - Organigramme - Systemprüfungen*	Akkreditierte Zertifi-zierungsstelle
Technische Zertifizie-rungsvoraussetzungen	- Datenschutz und Datensicherheit rechts-konform (technisch)	- Systeme* - Infrastrukturen* - Anwendungen* - Schnittstellen*		
	- Rechtskonforme technische und semanti-sche Interoperabilität	- EPD-Plattform	- Testergebnisse des Swiss Interoperability Assessments (SIA) - Testprotokolle des Zertifizierungstestsys-tems	Testlab
Komplexe Anwen-dungsfälle	- Rechtskonforme Benutzerfunktionalitäten auf der Ebene integrierter Systeme	- Schnittstellen / Services der Elemente der EPD-Plattform der Stammgemeinschaft und deren Einrichtungen*	- **Durchführung und Verifikation der kom-plexen Anwendungsfälle**	Akkreditierte Zertifi-zierungsstelle (Demonstration durch Personal der Stammgemein-schaft)

Tabelle 2: Orientierungshilfe zu den funktionalen Überprüfungen mittels komplexer Anwendungsfälle. * = risikobasierte Stichprobenprüfungen.

2.3 Prüfung der komplexen Anwendungsfälle

Die KAF sind von entsprechend geschulten Personen der Stammgemeinschaft durchzuführen. Es wird für die Prüfung vorausgesetzt, dass eine voll funktionierende EPD-Plattform in einer produktionsnahen Umgebungsversion zur Verfügung steht.

Die akkreditierten Zertifizierungsstellen sind für die Prüfung und Dokumentation der Ergebnisse verantwortlich. Bei der Dokumentation sind zwei Fälle zu unterscheiden:

- Im Normalfall («**Kategorie 1**») ist das Ergebnis am Bildschirm ersichtlich und wird mit einem Screenshot als Evidenz dokumentiert.
- In Einzelfällen («**Kategorie 2**») wie beispielsweise der Zustellung der Information an die Patientin oder den Patienten nach erfolgtem Notfallzugriff dokumentiert die Zertifizierungsstelle den Prozess, welcher zum geforderten Ergebnis führt.

Die für die Durchführung der KAF notwendigen Testpersonen (Patientin oder Patient, Stellvertreterin oder Stellvertreter, Gesundheitsfachperson) müssen über eine echte oder eine für Testzwecke erstellte elektronische Identität verfügen, die den rechtlichen Vorgaben an ein Identifikationsmittel für das EPD entspricht, und müssen mit dieser auf das EPD zugreifen.

2.4 Vorgaben

Die Angaben zu Testpatient, zu Stellvertretung sowie zu medizinischen Daten werden durch das BAG in geeigneter Form zur Verfügung gestellt.

Für sämtliche Systeme gilt, dass jeweils eine produktionsnahe (aber nicht produktive) Umgebung angesprochen wird und dass keine «echten» Daten vorliegen oder verwendet werden.

Es ist vorgängig zu organisieren, dass die GFP und Patientinnen über ein IDM eines zertifizierten (oder sich im Zertifizierungsverfahren befindlichen) Herausgebers verfügen und diese während der Durchführung der KAF verwendet werden.

Die Daten der Gesundheitsfachpersonen und der Gruppe von Gesundheitsfachpersonen werden durch die Stammgemeinschaft selber vorgängig zur Durchführung der KAF gemäss Tabelle 4 im HPD registriert.

Sämtliche bis anhin eröffnete EPD's sind zu löschen so dass keine Konflikte mit bestehenden und neuen Daten während dem KAF-Prozess entstehen.

Die komplexen Anwendungsfälle sind sequenziell und in der vorgegebenen Reihenfolge durchzuführen. Eine fiktive Patientin oder ein fiktiver Patient eröffnet bei der Stammgemeinschaft ein EPD, durchläuft anschliessend mehrere Stationen innerhalb eines Spitals und wird nach der Entlassung von der Hausärztin weiterbehandelt. Während und nach dem Spitalaufenthalt ändert die fiktive Patientin oder der fiktive Patient einige Einstellungen an der Berechtigungssteuerung. Letztlich widerruft sie oder er die Einwilligung zum Führen eines EPD und hebt das EPD damit auf.

Die Angaben zu medizinischen Daten, Gesundheitsfachpersonen und Gruppen sind nachfolgend beschrieben.

Medizinische Daten:

Doc_A1	Vertraulichkeitsstufe «normal zugänglich»
Doc_XCA2	Vertraulichkeitsstufe «eingeschränkt zugänglich»
Doc_XDA3	Vertraulichkeitsstufe «normal zugänglich»
Doc_XDA2	Vertraulichkeitsstufe «eingeschränkt zugänglich»
Doc_XCA1	Vertraulichkeitsstufe «normal zugänglich»
Doc_A2	Vertraulichkeitsstufe «eingeschränkt zugänglich»
Doc_XDA1	Vertraulichkeitsstufe «normal zugänglich»

Tabelle 3: In den komplexen Anwendungsfällen verwendete medizinische Daten

Die uuid und die Bezeichnung der medizinischen Daten werden in diesem Dokument bewusst nicht aufgeführt, weil die uuid beim Hochladen ins EPD zufällig vergeben wird und die Bezeichnung der medizinischen Daten beliebig vergeben werden kann.

Bei der Durchführung der KAF dürfen die Bezeichnungen der medizinischen Daten nicht verändert werden, denn diese dienen innerhalb des Ablaufes als Orientierung.

Mit Ausnahme des Dokuments «Doc_A1» dürfen die vom BAG zur Verfügung gestellten Dokumente vor dem Durchspielen der KAF in die Formate PDFA-1 oder PDFA-2 konvertiert werden. Mit dem nicht konvertierten medD Doc_A1 soll geprüft werden, dass Dokumente, die nicht im Format PDF-A vorliegen, entweder nicht hochgeladen werden können (Variante 1) oder automatisiert in die Formate PDFA-1 oder PDFA-2 konvertiert und dann erfolgreich hochgeladen werden können (Variante 2). Im Sinne der Vereinfachung kann bei Variante 1 vorgängig zum Durchspielen der KAF ein (zweites) medD Doc_A1 bereits konvertiert werden (siehe KAF-Id 002).

Test Akteure:

GFP_A	Hausärztin
GR-GFP «Gruppe1»	GFP_B, GFP_C, GFP_D des Spitals
GFP_E	Oberarzt des Spitals, nicht in «Gruppe1» integriert
EGFP_E	Ermächtigte Gesundheitsfachperson E
HiP der EGFP_E	MPA von EGFP_E

Tabelle 4: In den komplexen Anwendungsfällen verwendete Akteure

Jede GFP sowie die Gesundheitseinrichtung soll über möglichst realitätsnahe Personendaten bzw. Bezeichnung verfügen. Die Zuordnung zu den in Tabelle 4 aufgeführten Akteuren muss eineindeutig und für alle ersichtlich festgehalten werden.

Protokollierung:

Mit den in den KAF verlangten Protokollierungen sind diejenigen Protokoll-Einträge gemeint, welcher die Patientin oder der Patient in ihrem oder seinem Patientenportal einsehen kann.

3 Testen der komplexen Anwendungsfälle

3.1 EPD eröffnen (Ziff. 8.1, 8.2 und Ziff. 8.3 TOZ)

KAF-Id:	001
Vorbedingung	• P hat schriftliche Einwilligung für die Eröffnung seines EPD erteilt (Ziff. 7.1.1 TOZ) • P verfügt über eine gültige AHVN13 (Ziff. 8.2.1 Bst. d TOZ) • P verfügt über eine elektronische Identität, welche für das Login beim Patientenportal genutzt werden kann (Ziff. 8.3 TOZ) • P wurde von der ZAS noch keine EPR-SPID zugewiesen
Ablaufbeschreibung (Normalablauf)	• EPD wird durch die SG eröffnet: • P authentifiziert sich mit Hilfe seiner elektronischen Identität beim Patientenportal (Ziff. 8.3 TOZ)
Ergebnis	• Die EPR-SPID ist vergeben und mit MPI-ID in der Stammgemeinschaft von P verknüpft [Kategorie 2] (Ziff. 8.2.1 Bst. d TOZ) ☐ • Das Policy-Repository ist mit den Default-Policies des P eröffnet [Kategorie 2] (Ziff. 8.6 TOZ) ☐ • Die IDP-ID des P ist im Assertion Provider mit der EPR-SPID verknüpft [Kategorie 2] (Ziff. 1.4.4 TOZ) ☐

3.2 Bereitstellen von medD in EPD

KAF-Id:	002
Vorbedingung	KAF-Id 001 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• GFP_A stellt drei medD (Doc_A1 mit der Vertraulichkeitsstufe «normal zugänglich» / Doc_XCA2 mit der Vertraulichkeitsstufe «eingeschränkt zugänglich» / Doc_XDA3 mit der Vertraulichkeitsstufe «normal zugänglich») bereit • Variante 1 gemäss Ziffer 2.4: Das medD Doc_A1 wird im Format PDF-A1 oder PDF-A2 nachträglich hochgeladen • Variante 2 gemäss Ziffer 2.4: Keine Aktivität. Das medD Doc_A1 ist konvertiert und hochgeladen • P greift auf sein EPD zu und wechselt die Vertraulichkeitsstufe des medD Doc_XDA3 auf «geheim» (Ziff. 2.1 Bst. a TOZ) • GFP-A greift auf EPD von P zu
Ergebnis	• Variante 1 gemäss Ziffer 2.4: Das Bereitstellen des nichtkonvertierten medD Doc_A1 generiert die entsprechende Fehlermeldung. Das medD Doc_A1 ist konvertiert durch nachträgliches Hochladen im EPD für den P sichtbar [Kategorie 1] (Ziff. 2.4 Bst. d TOZ) ☐ • Variante 2 gemäss Ziffer 2.4: Das medD Doc_A1 ist im Format PDF-A1 oder PDF-A2 hochgeladen [Kategorie 1] (Ziff. 2.4 Bst. d TOZ) ☐ • P sieht alle bereitgestellten medD im EPD [Kategorie 1] (Ziff. 8.6 und Ziff. 9.2 TOZ) ☐ • Alle Doc wurden im Format PDF-A gespeichert [Kategorie 1] (Ziff. 2.4 Bst. d TOZ) ☐ • GFP_A sieht beim Zugriff auf das EPD keine medD [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.3 Notfallzugriff verweigern (Ziff. 8.6.3 Bst. e TOZ)

KAF-Id:	003
Vorbedingung	KAF-Id 002 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P schliesst den Notfallzugriff auf das EPD aus (Ziff. 8.6.3 Bst. e TOZ) • GFP_A sucht P mit demographischen Daten und findet P • GFP_A tätigt einen Notfallzugriff auf das EPD von P
Ergebnis	• GFP_A muss den Notfallzugriff auf eine Weise bestätigen, die einen (automatisierten) Missbrauch wirksam verhindert (z. B. vorgeschaltetes CAPTCHA, erneute Authentifizierung, etc.) [Kategorie 1] (Ziff. 2.2 Bst. a TOZ) ☐ • Der Zugriff auf das EPD durch GFP_A wird nicht gewährt (weder medD noch Metadaten zu medD sichtbar) [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.4 Notfallzugriff gewähren und zugreifen (Ziff. 2.2 und Ziff. 8.6.3 Bst. e TOZ)

KAF-Id:	004
Vorbedingung	KAF-Id 003 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P gewährt den Notfallzugriff bis auf medD der Vertraulichkeitsstufe «eingeschränkt zugänglich» (Ziff. 8.6.3 Bst. e TOZ) • GFP_A sucht P mit demographischen Daten und findet P • GFP_A tätigt einen Notfallzugriff auf das EPD von P
Ergebnis	• GFP_A erhält Zugriff auf die medD der Vertraulichkeitsstufe «normal zugänglich» und «eingeschränkt zugänglich» (Doc_A1 / Doc_XCA2) [Kategorie 1] (Ziff. 2.2 und Ziff. 2.3.1 TOZ) ☐ • P wird innert angemessener Frist über den Notfallzugriff informiert. Die Information darf keine besonders schützenswerten Informationen enthalten, sofern sie nicht via EPD übermittelt wird [Kategorie 2] (Ziff. 2.2 Bst. b und c TOZ) ☐

3.5 Gruppenberechtigung erteilen (Ziff. 8.6 TOZ)

KAF-Id:	005
Vorbedingung	KAF-Id 004 ist abgeschlossen Es existiert die GR-GFP «Gruppe1»
Ablaufbeschreibung (Normalablauf)	• P sucht und findet die GR-GFP «Gruppe1» bestehend aus GFP_B / GFP_C • P erteilt das Zugriffsrecht an die GR-GFP «Gruppe1» auf die medD mit der Vertraulichkeitsstufe «normal zugänglich» (Ziff. 8.6.1 TOZ) • GFP_B aus der GR-GFP «Gruppe1» greift auf das EPD zu
Ergebnis	• Aktuelle Zusammensetzung der GR-GFP «Gruppe1» durch P erkennbar [Kategorie 1] (Ziff. 9.1 Bst. c TOZ) ☐ • Zugriffsberechtigungen der GR-GFP «Gruppe1» erkennbar [Kategorie 1] (Ziff. 9.1 Bst. b TOZ) ☐ • GFP_B aus der GR-GFP «Gruppe1» kann auf das EPD von P zugreifen und sieht das medD Doc_A1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.6 Vertraulichkeitsstufe der neu hochgeladenen medD erhöhen (Ziff. 8.6.3 Bst. a TOZ)

KAF-Id:	006
Vorbedingung	KAF-Id 005 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P definiert, dass alle neu eingestellten medD die Vertraulichkeitsstufe «eingeschränkt zugänglich» aufweisen sollen (Ziff. 8.6.3 Bst. a TOZ) • GFP_C aus der GR-GFP «Gruppe1» lädt das neue medD Doc_XDA2 mit der Vertraulichkeitsstufe «eingeschränkt zugänglich» hoch • GFP_C aus der GR-GFP «Gruppe1» lädt neues medD Doc_XCA1 mit der Vertraulichkeitsstufe «normal zugänglich» hoch
Ergebnis	• Das Hochladen von medD Doc_XCA1 mit der Vertraulichkeitsstufe «normal» war nicht erfolgreich [Kategorie 2] (Ziff. 8.6.3 Bst. a TOZ) ☐ • Das medD Doc_XCA1 wurde aufgrund der Default-Einstellung Vertraulichkeitsstufe «eingeschränkt zugänglich» mit «eingeschränkt zugänglich» eingestellt. [Kategorie 2] (Ziff. 8.6.3 Bst. a TOZ) ☐ • GFP_C aus der GR-GFP «Gruppe1» sieht nur das medD Doc_A1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.7 Austritt aus einer Gruppe / Eintritt in eine Gruppe (Ziff. 8.6.3 Bst. c TOZ)

KAF-Id:	007
Vorbedingung	KAF-Id 006 ist abgeschlossen P hat festgelegt, dass eine Information über Gruppeneintritte an ihn erfolgen muss (Ziff. 8.6.3 Bst. c TOZ)
Ablaufbeschreibung (Normalablauf)	• GFP_C tritt aus der GR-GFP «Gruppe1» aus • GFP_D tritt neu in «Gruppe1» ein
Ergebnis	• GFP_C hat keinen Zugriff mehr auf EPD von P [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐ • GFP_D hat neu Zugriff und sieht medD Doc_A1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐ • P wird über Eintritt informiert [Kategorie 2] (Ziff. 1.5.2 Bst. a und Ziff. 8.6.3 Bst. c TOZ) ☐

3.8 Zugriffsrecht erweitern / medD ersetzen

KAF-Id:	008
Vorbedingung	KAF-Id 007 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P erweitert das Zugriffsrecht für die GR-GFP «Gruppe1» auf die medD mit der Vertraulichkeitsstufe «eingeschränkt zugänglich» (Ziff. 8.6.1 TOZ) • GFP_D aus der GR-GFP «Gruppe1» ersetzt medD Doc_A1 durch medD Doc_A2 (Vertraulichkeitsstufe «eingeschränkt zugänglich») (Ziff. 2.9.11 TOZ)
Ergebnis	• medD Doc_A1 ist weiterhin vorhanden, wird jedoch im Patientenportal als veraltet («deprecated») angezeigt [Kategorie 1] (Ziff. 2.9.11 und Ziff. 9.2.1 Bst. a TOZ) ☐ • medD Doc_A2 wird im Patientenportal als Ersatz von medD Doc_A1 als neue Version («approved») angezeigt [Kategorie 1] (Ziff. 2.9.11 und Ziff. 9.2.1 Bst. a TOZ) ☐ • GFP_D aus der GR-GFP «Gruppe1» hat Zugriff und sieht die medD Doc_A1 (deprecated) / Doc_XCA2 / Doc_XDA2 / Doc_XCA1 / Doc_A2 (approved) [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.9 Zugriffsrechte für Gruppe1 entziehen (Ziff. 8.6.1 TOZ)

KAF-Id:	009
Vorbedingung	KAF-Id 008 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P entzieht der GR-GFP «Gruppe1» die Zugriffsrechte (Ziff. 8.6.1 TOZ)
Ergebnis	• Die Mitglieder der GR-GFP «Gruppe1» haben keinen Zugriff mehr (Wird mit Login GFP_D aus der GR-GFP «Gruppe1» überprüft) [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.10 GFP ermächtigen / Zugriffsrechte erteilen / Zugriffsrechte weitergeben (Ziff. 8.6.3 Bst. g TOZ)

KAF-Id:	010
Vorbedingung	KAF-Id 009 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P erteilt Zugriffsrechte an die GFP_E auf die medD mit der Vertraulichkeitsstufe «eingeschränkt zugänglich» • P ermächtigt GFP_E (wird dadurch zur EGFP_E) zur Weitergabe von Zugriffsrechten auf medD mit maximal gleich hoher Vertraulichkeitsstufe (Ziff. 8.6.3 Bst. g TOZ) • EGFP_E überweist den P an GFP_A und erteilt GFP_A das Zugriffsrecht auf die medD mit der Vertraulichkeitsstufe «eingeschränkt zugänglich» (Ziff. 8.6.3 Bst. g TOZ) • HiP der EGHP_E greift im Auftrag der EGFP_ auf das EPD zu
Ergebnis	• GFP_A hat neu Zugriff und sieht die medD Doc_A1 (deprecated) / Doc_XCA2 / Doc_XDA2 / Doc_A2 (approved) / Doc_XCA1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐ • HiP kann im Auftrag von EGFP_E auf EPD zugreifen und sieht die medD Doc_A1 (deprecated) / Doc_XCA2 / Doc_XDA2 / Doc_A2 (approved) / Doc_XCA1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.11 STV benennen (Ziff. 8.4 TOZ)

KAF-Id:	011
Vorbedingung	KAF-Id 010 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P benennt STV mit den folgenden Angaben: Es kann nach Belieben eine STV aus den zur Verfügung stehenden Identitäten ausgewählt werden • STV authentifiziert sich mit Hilfe seiner elektronischen Identität und greift nach erfolgter Ernennung auf EPD von P zu und schaut die medD an (Ziff. 8.4.2 TOZ)
Ergebnis	• STV hat Zugriff und sieht die medD Doc_A1 (deprecated) / Doc_XCA2 / Doc_XDA2 / Doc_A2 (approved) / Doc_XDA3 / Doc_XCA1 [Kategorie 1] (Ziff. 2.3.1 und Ziff. 9.2.1 Bst. d TOZ) ☐

3.12 Einzelne GFP ausschliessen (Ziff. 8.6.3 Bst. b TOZ)

KAF-Id:	012
Vorbedingung	KAF-Id 011 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P schliesst EGFP_E vom Zugriff auf sein EPD aus (Ziff. 8.6.3 Bst. b TOZ) • HiP der EGFP_E greift auf das EPD von P zu
Ergebnis	• EGFP_E hat keinen Zugriff mehr auf das EPD [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐ • HiP der GFP_E hat keinen Zugriff auf das EPD [Kategorie 1] (Ziff. 2.3.1 und Ziff. 3.1.2 TOZ) ☐

3.13 medD hochladen / medD löschen (Ziff. 10.1 TOZ)

KAF-Id:	013
Vorbedingung	KAF-Id 012 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P lädt medD Doc_XDA1 mit Vertraulichkeitsstufe «normal zugänglich» hoch (Ziff. 9.4.3 Bst. a und Ziff. 10.1.1 TOZ) • P löscht medD Doc_XDA2 / Doc_A1 (deprecated) (Ziff. 9.4.1 Bst. b TOZ)
Ergebnis	• medD Doc_A2 (approved) / Doc_XCA2 / Doc_XDA3 / Doc_XDA1 / Doc_XCA1 sind für P ersichtlich [Kategorie 1] (Ziff. 2.3.1 und Ziff. 9.2.1 Bst. d TOZ) ☐

3.14 Vertraulichkeitsstufe für medD erhöhen

KAF-Id:	014
Vorbedingung	KAF-Id 013 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P erhöht für medD Doc_XCA2 die Vertraulichkeitsstufe von «eingeschränkt zugänglich» auf «geheim» (Ziff. 2.1. Bst. a TOZ)
Ergebnis	• Die Vertraulichkeitsstufe von medD Doc_XCA2 wurde von «eingeschränkt zugänglich» auf «geheim» geändert (wird durch P überprüft) [Kategorie 1] (Ziff. 2.3.1 und Ziff. 9.2.1 Bst. d TOZ) ☐ • Die Änderung der Vertraulichkeitsstufe ist sinngemäss wie folgt protokolliert: Das medD Doc_XCA2 wurde verändert bzw. aktualisiert [Kategorie 2] (Ziff. 2.10.4 TOZ) ☐

3.15 Detailliertes Protokoll anzeigen lassen (Ziff. 2.10 und Ziff. 9.3 TOZ)

KAF-Id:	015
Vorbedingung	KAF-Id 014 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P ruft die Protokolldaten auf und will explizit die KAF-Id 002, 003, 005, 012 überprüfen (Ziff. 2.10 und Ziff. 9.3 TOZ)
Ergebnis	• Die Protokolldaten von KAF-ID 002 zeigen dem P, dass das medD Doc XDA3 verändert wurde. [Kategorie 1] ☐ • Die Protokolldaten von KAF-ID 003 zeigen dem P, dass P den Notfallzugriff ausgeschlossen hat. [Kategorie 1] ☐ • Die Protokolldaten von KAF-ID 005 zeigen dem P, dass P Zugriffsrechte verändert hat. [Kategorie 1] ☐ • Protokolldaten von KAF-ID 012 zeigen dem P, dass P Zugriffsrechte verändert hat. [Kategorie 1] ☐

3.16 Alle medD herunterladen / EPD aufheben (Ziff. 10.2 und Ziff. 12.2 TOZ)

Der Patient wünscht lokal über alle medD zu verfügen. Er kann a) durch Herunterladen oder b) «auf andere Weise» in den Besitz der medD gelangen.

Herunterladen:

KAF-Id:	016 a
Vorbedingung	KAF-Id 015 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P lädt alle medD auf einmal herunter (Ziff. 10.2.1 TOZ) • P hebt EPD bei der SG auf (Ziff. 12.2 TOZ)
Ergebnis	• P verfügt lokal über alle medD mit den entsprechenden Metadaten [Kategorie 1] (Ziff. 10.2.1 TOZ) ☐ • Das EPD ist für GFP_A nicht mehr auffindbar [Kategorie 1] (Ziff. 2.6. Bst. b TOZ) ☐

Bezug auf eine andere Weise:

KAF-Id:	016 b
Vorbedingung	KAF-Id 015 ist abgeschlossen
Ablaufbeschreibung (Normalablauf)	• P bezieht seine medD von der SG auf eine andere Weise (Ziff. 10.2.1 TOZ) • P hebt EPD bei der SG auf (Ziff. 12.2 TOZ)
Ergebnis	• P verfügt lokal über alle medD mit den entsprechenden Metadaten [Kategorie 1] ☐ • Das EPD ist für GFP_A nicht mehr auffindbar [Kategorie 1] (Ziff. 2.6. Bst. b TOZ) ☐

4 Abbildungsverzeichnis

5 Tabellenverzeichnis