Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature:
Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken

Version:	1.0.0
Revision:	401062
Stand:	31.08.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemF_ePA_FDZ_Anbindung

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	30.06.21		Ersterstellung und Abstimmung	gematik
1.0.0 RC	27.07.21		Einarbeitung der Kommentierung	gematik
1.0.0	31.08.21		freigegeben	gematik

Inhaltsverzeichnis

1 Motivation des Features

Auf Basis des § 342 Abs.1 SGB V sind alle gesetzlichen Krankenkassen zum 01.01.2021 zur Einführung und Bereitstellung einer elektronischen Patientenakte (ePA) für jeden gesetzlich Versicherten verpflichtet. In der ePA, die vom Versicherten selbst oder ab dem 01.01.2022 durch einen von ihm benannten Vertreter geführt wird, können unterschiedliche Dokumente entlang seiner persönlichen medizinischen Behandlungshistorie eingepflegt werden.

Der § 363 SGB V eröffnet zwei Szenarien, um Daten aus der elektronischen Patientenakte für Forschungszwecke bereitzustellen. Die Absätze 1 bis 7 des Paragraphen beschreiben den Vorgang der Datenfreigabe an das Forschungsdatenzentrum beim BfArM. Der Weg der Daten aus der ePA hin zum Forschungsdatenzentrum wird hierbei exakt geregelt, wobei zur Datenübermittlung an das Forschungsdatenzentrum eine aktive Datenfreigabe durch die Versicherten als zusätzliche Verarbeitungsbedingung erforderlich ist. Die Verarbeitung im Forschungsdatenzentrum erfolgt auf Grundlage der Absätze 1 bis 7.

Nach Absatz 8 ist einem Versicherten außerdem möglich Daten auf alleiniger Grundlage einer Einwilligungserklärung direkt an einen Forschenden zu geben. Alle technischen Voraussetzungen hierfür sind bereits mit der ePA Stufe 1 sowie ePA Stufe 2 geschaffen. Weitere Spezifikationen sind hier nicht notwendig. Der Ablauf der Datenverarbeitung nach Absatz 8 wird im Konzeptpapier "Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken nach §363 (8) SGB V" beschrieben. Zusätzlich wird das stufenweise Ausbauverfahren erläutert.

Die Grundlage für die Übermittlung der freigegebenen Daten, aus der ePA an das Forschungsdatenzentrum, ist die informierte Einwilligung (§ 363 (2) SGB V). Die Informationen dafür sind Bestandteile geeigneter Informationsmaterialien, die von der Krankenkasse bereitzustellen sind (§363 (5) Satz 2 SGB V). Die Einwilligungserklärung muss gegenüber der Krankenkasse als Anbieter der ePA erfolgen. Die Einwilligung erklärt der Versicherte über die Benutzeroberfläche des ePA Frontend des Versicherten (ePA FdV) (§363 (2) Satz 2 SGB V).

Die Krankenversicherungen sind dazu verpflichtet nachzuweisen, dass eine „betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat" (DSGVO Art. 7 Abs. 1), da die Verarbeitung der Daten auf einer Einwilligung beruht.

Die Einwilligung kann auch durch einen Vertreter erfolgen (§342 (2) 4. b) SGB V).

Die Datenfreigabe muss, zusätzlich zur Dokumentation der abgegebenen Einwilligungserklärung gegenüber den Krankenversicherungen, innerhalb der ePA dokumentiert werden (§363 (2) Satz 4 SGB V). Diese soll für Versicherte transparent und nachvollziehbar aufgearbeitet vorliegen.

In der ePA der Ausbaustufe 3 können eine Vielzahl von Dokumenten gespeichert werden. Die Auswahl der freizugebenden Dokumente erfolgt im FdV (§363 (2) Satz 2 SGB V). Den Umfang der Datenfreigabe können Versicherte frei wählen und auf bestimmte Kategorien oder auf Gruppen von Dokumenten und Datensätzen oder auf spezifische Dokumente und Datensätze beschränken (§363 (2) Satz 3 SGB V). Zur Umsetzung ist in einem ersten Schritt die Freigabe von strukturierten Daten in Form von MIOs für die Forschung vorgesehen. Nach Auswahl der freizugebenden Daten und der Einwilligung zur Datenfreigabe durch den Versicherten, werden die freigegebenen Daten durch den, für die Datenverarbeitung in der elektronischen Patientenakte,

Verantwortlichen pseudonymisiert und verschlüsselt (§363 (3) SGB V). Diese Verantwortlichkeit liegt bei den Krankenkassen (§341 (4) SGB V). Für die Pseudonymisierung müssen die einzelnen MIOs und deren Datenfelder auf das Vorhandensein von direkt personenbezogenen Daten geprüft werden. Datenfelder, die solche Informationen enthalten, sollen nicht an das Forschungsdatenzentrum übermittelt werden. Dies betrifft die direkt personenidentifizierenden Daten (wie z.B. Name, Anschrift, Geburtsdatum) von Versicherten und Leistungserbringern.

Die freigegebenen, pseudonymisierten Daten werden verschlüsselt und mit der Arbeitsnummer versehen (§363 (3) Satz 1 SGB V). Dies erfolgt aus dem ePA Frontend heraus an das FDZ (§363 (2) Satz 1 SGB V).

An die Vertrauensstelle wird die Arbeitsnummer sowie ein Lieferpseudonym zu den freigegebenen Daten übermittelt (§363 (2) Satz 1 SGB V). Die freigegebenen Daten samt Lieferpseudonym und Arbeitsnummer können an die jeweilige Empfangsstelle im Modus 24/7 über das Internet gesendet werden.

In der Vertrauensstelle erfolgt:

- eine Überführung der Lieferpseudonyme in periodenübergreifende Pseudonyme (§303 c (1) SGB V),
- eine Übermittlung der periodenübergreifenden Pseudonyme mit zugehörigen Arbeitsnummern an das Forschungsdatenzentrum (§303 c (2), (3) SGB V) und
- eine Löschung der Arbeitsnummer und des Lieferpseudonyms (§303 c (3) SGB V).

Im FDZ werden die periodenübergreifenden Pseudonyme mit den freigegebenen Daten unter Zuhilfenahme der Arbeitsnummer verknüpft (§363 (3) Satz 3 SGB V). Die Arbeitsnummer wird nach dem Verknüpfen der beiden Datensätze verworfen.

Als Antragsteller, die sich beim FDZ melden können, sind folgende nach § 363 Absatz 4 SGB V definiert: §303e (1) Nummer 6, 7, 8, 10, 13, 14, 15 und 16 SGB V. Es gibt vier rechtlich erlaubte Zwecke zu denen Daten beantragt werden können (§ 303e Absatz 2 Nummer 2, 4, 5 und 7 SGB V).

Das Forschungsdatenzentrum stellt den Nutzungsberechtigten die Daten aufbereitet zur Verfügung. Die Bereitstellung der Daten kann dadurch erfolgen, dass das Forschungsdatenzentrum

- den Nutzungsberechtigten standardisierte Datensätze in aggregierter und anonymisierter Form zur Verfügung stellt
- mit den Auswertungsprogrammen Daten auswertet und den Nutzungsberechtigten die aggregierten Ergebnismengen übermittelt,
- pseudonymisierte Einzeldatensätze zugänglich macht, wenn der antragstellende Nutzungsberechtigte nachvollziehbar darlegt, dass die Nutzung der pseudonymisierten Einzeldatensätze erforderlich ist (§10 (1) DaTrav).

Im Falle des Widerrufs der Einwilligung zur Datenfreigabe nach §363 (2) SGB V werden die entsprechenden Daten, die bereits an das Forschungsdatenzentrum übermittelt wurden, im Forschungsdatenzentrum gelöscht. Das Löschverfahren erfolgt analog zur Datenübermittlung und Verknüpfung in §363 (3) SGB V. Die bis zum Widerruf der Einwilligung nach Absatz 2 übermittelten und für konkrete Forschungsvorhaben bereits verwendeten Daten dürfen weiterhin für diese Forschungsvorhaben verarbeitet werden. Die Rechte der betroffenen Person nach den Artikeln 17, 18 und 21 der Verordnung (EU) 679/2016 sind insoweit für diese Forschungsvorhaben ausgeschlossen. Der Widerruf der Einwilligung kann ebenso wie deren Erteilung über die

Benutzeroberfläche eines geeigneten Endgeräts erfolgen. Ist der Widerruf mit der verbundenen Aufforderung zur Datenlöschung beim FDZ eingegangen, so erhält der Versicherte eine automatische Rückmeldung, dass diese Information angekommen ist. Die Löschung der Daten im FDZ muss unverzüglich (Art.17 DSGVO) erfolgen. Die technische Umsetzung der Auskunftsrechte ist nach DSGVO nicht geregelt. Die Auskunftsrechte können durch die Verordnung nach §363 (7) SGB V noch eingeschränkt werden.

Zum 30.06.2021 (§ 354 Abs. 2 Nr. 4 SGB V) sind durch die Gesellschaft für Telematik (gematik GmbH) die Festlegungen zu treffen, dass Versicherte mittels der Benutzeroberfläche eines geeigneten Endgeräts gemäß § 336 Abs. 2 SGB V die Verarbeitung von Daten zu Forschungszwecken zu ermöglichen (§ 363 Abs. (1-7) SGB V).

Die gesetzlichen Krankenversicherungen sind auf Basis der zuvor genannten Festlegungen durch die gematik dazu verpflichtet (§ 342 Abs. 2 Nr. 4 Buchstabe e SGB V-E), die Festlegungen entsprechend zum 01.01.2023 umzusetzen und den Versicherten in den jeweiligen ePA-Oberflächen anzubieten.

1.1 Zielsetzung

Dieses Dokument beschreibt die technische Umsetzung für alle Schritte, damit ein Versicherter aus seinem ePA-FdV strukturierte Dokumente für die Forschung zur Verfügung stellen kann.

1.2 Zielgruppe

Das Dokument bildet alle Schritte des Entwicklungsprozesses in verschiedenen Kapiteln ab. Daher unterscheidet sich die intendierte Zielgruppe zwischen den einzelnen Kapiteln.

Das Kapitel 2 betrachtet die fachliche Ebene. Es dient der fachlichen Abstimmung mit Stakeholdern und fachlichen Verbänden.

Kapitel 3 beschreibt das Umsetzungskonzept. Es schafft ein übergreifendes Verständnis der angestrebten Lösung und bildet das Bindeglied zwischen der fachlichen Ebene in Kapitel 2 und der Spezifikationsebene im Kapitel 4 und 5.

Kapitel 4 und 5 beschreiben die konkrete Lösung und deren Auswirkung auf Produkttypen. Es ist daher hauptsächlich für die Abstimmung mit Herstellern, Anbietern und deren Auftraggebern relevant.

1.3 Abgrenzungen

Das Dokument umfasst im Kapitel 4 und 5 nur Änderungen an Spezifikationen/Steckbriefen der gematik und ist daher als Ergänzung zur entsprechenden Spezifikation der gematik zu verstehen und zu lesen. Sollten als Teil eines Features neue Produkttypen eingeführt werden, so wird deren Spezifikation in einem neuen Dokument erfolgen und hier nur referenziert werden. Das neue Dokument für den Produkttyp wird dann ergänzend zur Feature-Spezifikation verteilt.

1.4 Methodik

1.4.1 User Story

User Stories werden durch eine eindeutige ID gekennzeichnet und werden im Dokument wie folgt dargestellt:
<USt-ID> - <Zusammenfassung der User Story>
Text / Beschreibung
[<=]

Dabei umfasst die User Story sämtliche zwischen USt-ID und der Textmarke [<=] angeführten Inhalte.

1.4.2 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

2 Epic und User Stories

Mit der Einführung der elektronischen Patientenakte und dem Ausbau der verfügbaren medizinischen Informationsobjekte (MIOs) und den somit strukturiert dokumentierten Gesundheitsdaten eröffnen sich außerdem neue Möglichkeiten für Forschende Forschungsfragen anhand von Versorgungsdaten zu erörtern. Neben den Abrechnungsdaten, die aufgrund der DaTrav jährlich, pseudonymisiert von allen gesetzlich Versicherten an das Forschungsdatenzentrum übermittelt werden, wird so eine weitere Datenquelle erschlossen. Die Daten aus der ePA und die Abrechnungsdaten können im Forschungsdatenzentrum zusammengeführt werden. Dazu muss jede Datenlieferung in zwei Teile aufgeteilt werden. Ein Paket, bestehend aus einer Arbeitsnummer und einem Lieferpseudonym geht an die Vertrauensstelle, die beim Robert-Koch-Institut liegt. Dort wird aus dem Lieferpseudonym ein periodenübergreifendes Pseudonym gebildet, welches für einen Versicherten immer gleich ist. Das Paket aus Arbeitsnummer und periodenübergreifendem Pseudonym wird im Forschungsdatenzentrum mit den pseudonymisierten ePA-Daten und Arbeitsnummer zusammengeführt. Die Arbeitsnummer wird im Anschluss gelöscht.

Weiterhin ist ein Widerruf samt Löschung einzelner oder aller freigegebenen Dokumente im Forschungsdatenzentrum möglich.

2.1 User Stories

USt-1 - Informierte Einwilligung
Als Versicherter möchte ich der Freigabe meiner Daten zu Forschungszwecken zustimmen, nachdem ich vorher ausreichend informiert wurde. [<=]

USt-2 - Daten für die Weitergabe zu Forschungszwecken auswählen
Als Versicherter möchte ich strukturierte Dokumente (MIOs) aus meiner ePA zu Forschungszwecken zur Verfügung stellen. Dazu möchte ich auswählen können, welche Daten das sein sollen, damit nur die Dokumente herausgeschickt werden, die ich teilen möchte. [<=]

USt-3 - Anwendung Pseudonymisierungsschablone
Als Versicherter möchte ich, dass meine ausgewählten Daten pseudonymisiert ausgeleitet werden. [<=]

USt-4 - Erstellung Arbeitsnummer
Als Vertrauensstelle und Forschungsdatenzentrum möchte ich Datensätze erhalten, die mit einer eindeutigen Arbeitsnummer versehen sind. [<=]

USt-5 - Daten an die Vertrauensstelle (RKI) senden
Als Vertrauensstelle möchte ich ein Datenpaket bestehend aus Arbeitsnummer und Lieferpseudonym erhalten. [<=]

USt-6 - Daten an das Forschungsdatenzentrum senden
Als FDZ möchte ich ein Datenpaket aus pseudonymisierten Dokumenten erhalten, das mit einer Arbeitsnummer versehen ist und bei denen die direkt personenidentifizierenden Daten entsprechend der Pseudonymisierungsschablone entfernt wurden. [<=]

USt-7 - Einwilligung widerrufen
Als Versicherter möchte ich die Datenfreigabe jederzeit für die Zukunft widerrufen

können und den Auftrag für die Löschung der gesamten Daten oder einzelner Datensätze geben. Bei Eingang meines Widerrufs möchte ich benachrichtigt werden. [<=]

USt-8 - eMP und PKA freigeben
Als Versicherter möchte ich auch meinen elektronischen Medikationsplan sowie meine Patientenkurzakte zu Forschungszwecken zu Verfügung stellen. [<=]

3 Technisches Konzept

3.1 Beschreibung

Die Freigabe von Daten aus der ePA eines Versicherten für Forschungszwecke beschränkt sich auf die Freigabe strukturierter Dokumente (MIOs), für die ein Pseudonymisierungsschema ("Schablone") verfügbar ist. Weitere Dokumente oder strukturierte Daten ohne verfügbares Pseudonymisierungsschema können nicht für die Forschung freigegeben werden.

Ein Pseudonymisierungsschema berücksichtigt jeweils ein MIO. Unter Verwendung der Vorgaben des Pseudonymisierungsschema erfolgt durch das ePA-FdV die Überführung eines MIOs der ePA in ein pseudonymisiertes Dokument (USt-3). Das Pseudonymisierungsschema definiert dafür alle Elemente eines MIO, die nicht in das pseudonymisierte Dokument übernommen werden dürfen, bzw. aus diesem entfernt werden müssen, da diese direkt personenidentifizierende Daten enthalten und eine Zuordnung der freizugebenen Daten für Forschungszwecke zu einer bestimmten Person ermöglichen würden.

Nach einer expliziten Freigabe der pseudonymisierten Dokumente (pD) durch einen Versicherten werden diese dem Forschungsdatenzentrum (FDZ) unter Einbindung einer Vertrauensstelle (VST) zur Verfügung gestellt.

Die VST erhält dazu vom ePA-FdV eine Arbeitsnummer (AN) und ein Lieferpseudonym (LP) und ordnet diese einem periodenübergreifenden Pseudonym (PÜP) zu (USt-4, USt-5, USt-6).

Das Forschungsdatenzentrum erhält vom ePA-FdV die pseudonymisierten Dokumente (pD) und die Arbeitsnummer (AN) und von der Vertrauensstelle das periodenübergreifende Pseudonym und die Arbeitsnummer. Das Forschungsdatenzentrum assoziiert anschließend die Arbeitsnummer und die pseudonymisierten Dokumente (pD) mit dem periodenübergreifenden Pseudonym (USt-5, USt-7).

Die Bereitstellung der pseudonymisierten Dokumente (pD) durch das ePA-FdV erfolgt dabei unter Verwendung der Schnittstellen der VST und des FDZ und unter Einbindung eines zusätzlichen Dienstes im Aktensystem (FD-Proxy). Dieser Proxy-Dienst agiert gegenüber den Endpunkten VST und FDZ als versendender, nicht personengebundener Client und kann serverseitig eindeutig identifiziert werden.

Die Authentizität des ePA-FdV wird gegenüber der VST und dem FDZ jeweils über ein nicht personengebundenes Transporttoken (Token_VST, Token_FDZ) der Komponente Autorisierung nachgewiesen.

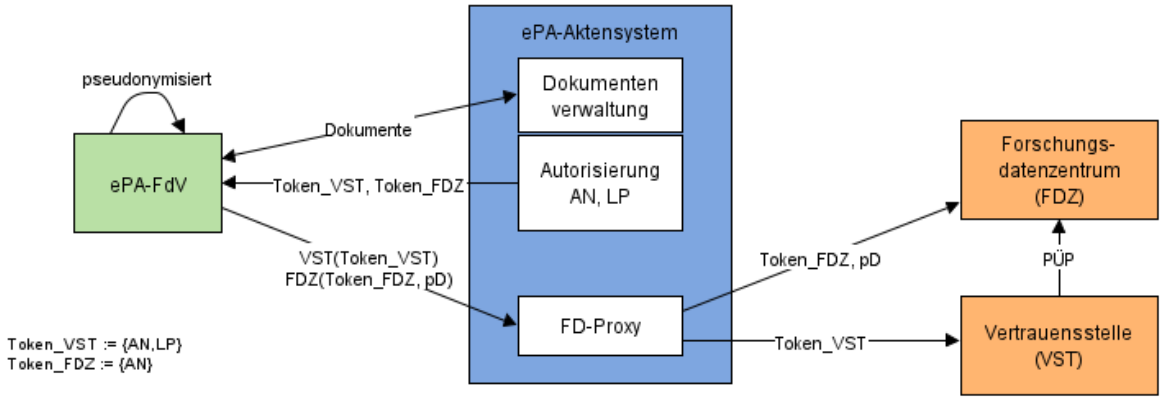

Abbildung 1 Übersicht

3.1.1 Einwilligung des Versicherten

Eine Übermittlung von Dokumenten an die Vertrauensstelle und an das Forschungsdatenzentrum darf nur dann erfolgen, wenn die Einwilligung des Versicherten für die Übermittlung der Daten an die genannten Stellen vorliegt.

Die Erteilung der Einwilligung in die Freigabe von Daten an die Forschung (USt-1) und deren Widerruf erfolgt explizit gegenüber dem Kostenträger. Die Erteilung der Einwilligung und auch der Widerruf dieser Einwilligung wird in der Akte des Versicherten vermerkt.

Das Widerrufen der Einwilligung (USt-7) verhindert die weitere Freigabe von Dokumenten für Forschungszwecke. Zuvor freigegebene Dokumente werden automatisch gegenüber dem FDZ widerrufen.

3.1.2 Auswahl der Daten

Der Vorgang der Freigabe von Dokumenten für Forschungszwecke muss aktiv durch den Versicherten oder einen Vertreter initiiert werden. Vor dem Versand der Daten kann der Versicherte oder ein Vertreter eine Auswahl treffen, welche Dokumente pseudonymisiert übermittelt werden sollen. Die Auswahlmöglichkeit beschränkt sich auf die Auswahl der freizugebenden MIOs aus der Menge der pseudonymisierbaren MIOs. Eine Beschränkung auf Teile eines MIOs ist nicht vorgesehen.

Der Vorgang der Freigabe kann durch den Versicherten oder einen Vertreter jederzeit initiiert werden.

3.1.3 Versenden der Daten

Der Versand der freigegebenen Dokumente erfordert stets die Verwendung von zwei externen Schnittstellen, eine der Vertrauensstelle (VST, gemäß § 303c SGB V) und eine des Forschungsdatenzentrums (FDZ, gemäß § 303d SGB V).

Über die Schnittstelle der Vertrauensstelle werden die Arbeitsnummer (AN) und das Lieferpseudonym (LP) des Versicherten als Bestandteil eines Transporttoken übermittelt. Die Vertrauensstelle stellt anhand der erhaltenen Daten einen Bezug zu einem periodenübergreifenden Pseudonym (PÜP) her.

Die Übertragung aus dem ePA-FdV erfolgt TLS-gesichert an den FD-Proxy und von dort TLS-gesichert an die Vertrauensstelle.

Über die Schnittstelle des Forschungsdatenzentrums werden die gleiche Arbeitsnummer (AN) als Bestandteil eines weiteren Transporttokens, sowie die freigegebenen und pseudonymisierten Dokumente (pD) übermittelt. Im Forschungsdatenzentrum kann anschließend der Bezug der erhaltenen freigegebenen Daten des Versicherten anhand des periodenübergreifenden Pseudonyms der VST zum vorhandenen Datenbestand hergestellt werden.

Die pseudonymisierten Dokumente werden vor der Übertragung für das FDZ Ende-zu-Ende verschlüsselt. Die Übertragung aus dem ePA-FdV erfolgt TLS-gesichert an den FD-Proxy und von dort TLS-gesichert an das FDZ.

3.1.4 Arbeitsnummer (AN) und Lieferpseudonym (LP)

Das Lieferpseudonym wird aus der KVNR des Versicherten gebildet. Das Verfahren zur Erstellung des LP aus der KVNR wird durch die VST definiert.

Die Arbeitsnummer wird so gewählt, dass im FDZ eine kollisionsfreie Zuordnung der freigegebenen Dokumente zu einem periodenübergreifenden Pseudonym ermöglicht wird, und somit nicht gleichzeitig freigegebene Dokumente mit gleicher Arbeitsnummer von verschiedenen Versicherten im FDZ vorliegen können.

Als Arbeitsnummer wird ein Zufallswert von mindestens 16 Byte Länge verwendet. Durch die Einbettung der Arbeitsnummer in die Transporttoken wird zusätzlich ein zeitlicher Kontext gesetzt.

3.1.5 Widerruf der Freigabe

Ein Versicherter oder ein Vertreter kann die Freigabe von Dokumenten gegenüber dem Forschungsdatenzentrum widerrufen. Der Vorgang wird analog zu einer Dokumentenfreigabe realisiert, mit dem Unterschied, dass keine pseudonymisierten Dokumente übertragen werden, sondern die Liste der widerrufenen Dokumente.

Der Widerruf der Freigabe kann für sämtliche Dokumente oder für einen Teil der freigegebenen Dokumente anhand der in der Aufzeichnung der freigegebenen Dokumente für jedes Dokument hinterlegten eindeutigen Dokumentenreferenz erfolgen. Widerrufene Dokumente können zu einem späteren Zeitpunkt erneut freigegeben werden

3.1.6 Aufzeichnung der freigegebenen Dokumente

Für jeden Freigabe- oder Widerrufsvorgang erfolgt eine Aufzeichnung der betroffenen Dokumente durch das ePA-FdV in einer Liste. Diese Liste wird in der ePA des Versicherten als *patientdoc* abgelegt und bei jedem weiteren Freigabevorgang oder Widerruf aktualisiert.

Ein Versicherter oder ein Vertreter kann anhand dieser Aufzeichnung nachvollziehen, welche Dokumente für Forschungszwecke freigegeben und welche widerrufen wurden, zu welchem Zeitpunkt dieses erfolgte und wer die jeweilige Aktion ausgeführt hat (Versicherter oder Vertreter). Die aufgezeichneten Daten der freigegebenen Dokumente werden für den Widerruf der Freigabe einzelner oder mehrerer Dokumente genutzt.

Die Liste der freigegebenen oder widerrufenen Dokumente vermerkt auch, ob eine Einwilligung durch den Versicherten erteilt oder widerrufen wurde.

3.1.7 Sicherheit

Die Authentizität des Absenders der Daten (ePA-Fdv) wird gegenüber der VST und dem FDZ jeweils durch ein Transporttoken ohne Personenbezug nachgewiesen. Diese Token werden durch die Komponente Autorisierung für autorisierte ePA-FdV erstellt und signiert. Ein Empfänger (VST, FDZ) erhält dadurch den Nachweis, dass die übermittelten Daten von einem ePA-FdV eines autorisierten Nutzers mit Aktenkonto stammen, ohne dass Rückschlüsse auf die Identität des Nutzers ermöglicht werden.

Die pseudonymisierten Dokumente für das Forschungsdatenzentrum werden ausschließlich verschlüsselt übertragen. Die Festlegungen zum Verfahren der Verschlüsselung und zur Bereitstellung der notwendigen Zertifikate erfolgt durch das FDZ.

3.1.8 Konfiguration des ePA-FdV

Das ePA-FdV benötigt für den Versand der Daten geeignete und authentische Daten der VST und des FDZ (z.B. Zertifikate, öffentliche Schlüssel, URLs). Die Festlegungen zu diesen Metadaten und deren Bereitstellung für die ePA-FdV erfolgen durch die VST, bzw. das FDZ, beispielsweise über eine *well-known-address*.

3.1.9 Datenfreigabe durch einen Vertreter

Ein Vertreter kann bei Vorliegen der Einwilligung des Versicherten in die Freigabe von Daten für Forschungszwecke analog zu einem Versicherten Dokumente freigeben oder zuvor freigegebene Dokumente widerrufen. Eine eigene Einwilligung des Vertreters ist für die Freigabe von Dokumenten des Vertretenen (Versicherter) nicht erforderlich.

Gibt ein Vertreter Dokumente eines Versicherten für Forschungszwecke frei oder widerruft diese, so wird für diese Vorgänge das Lieferpseudonym des Versicherten verwendet. Für die Aufzeichnung des Vorgangs in der Akte des Versicherten wird hingegen der Vertreter vermerkt.

3.1.10 Verwendung des Proxy für Forschungsdaten (FD-Proxy)

Das ePA-FdV kommuniziert niemals direkt mit den Schnittstellen der VST und des FDZ. Beide Schnittstellen werden dem ePA-FdV durch einen Reverse-Proxy auf Netzwerkebene angeboten. Eine Verwendung der Schnittstellen durch das FdV ist nur bei erfolgreicher Autorisierung des Versicherten oder eines Vertreters möglich. Die Verbindung des Proxy zu den Gegenstellen (VST, FDZ) wird TLS-gesichert mit beidseitiger Authentisierung.

Für die Gegenstellen (VST und FDZ) reduziert sich die Kommunikation durch die Verwendung des FD-Proxy auf wenige, direkt identifizierbare Clients. Eine Pufferung von Daten für die Übertragung an die Gegenstellen nach Verbindungsabbruch oder zeitweise nicht gegebener Erreichbarkeit ist nicht vorgesehen.

4 Spezifikation

Die Spezifikationen gemSpec_ePA_FdV, gemSpec_Autorisierung, gemSpec_Zugangsgateway_Vers und gemSpec_Dokumentenverwaltung werden um die Erläuterungen und normativen Anforderungen der folgenden Kapitel erweitert.

4.1 Funktionale Anforderungen (gemSpec_ePA_FdV)

4.1.1 Kapitel 6.1.9 Freigabe von Dokumenten für Forschungszwecke

Einem Versicherten oder einem Vertreter muss die Freigabe von Dokumenten der Akte des Versicherten in pseudonymisierter Form für Zwecke der Forschung gemäß §363 Abs. 1-7 SGB V nach erteilter Einwilligung nach § 363 Absatz 2 SGB V des Versicherten ermöglicht werden. Darüber hinaus muss es einem Versicherten oder einem Vertreter möglich sein, die Verwendung zuvor freigegebener Daten für Forschungszwecke zu widerrufen.

Die Freigabe von Dokumenten aus der Akte eines Versicherten ist auf die Freigabe von Daten in strukturierten Dokumenten (MIOs) beschränkt. Die freizugebenden Dokumente werden durch das ePA-FdV unter Verwendung eines Pseudonymisierungsschemas in ein pseudonymisiertes Dokument übertragen. Ausschließlich pseudonymisierte Dokumente dürfen für Forschungszwecke an das Forschungsdatenzentrum übermittelt werden. Der Versicherte oder ein Vertreter muss dabei für jeden Freigabevorgang auswählen können, welche Dokumente freigegeben werden sollen. Ein Freigabevorgang kann dabei auch die Freigabe zu einer automatisch zu wiederholenden Übermittelung eines Dokuments an das Forschungsdatenzentrum beinhalten, beispielsweise in bestimmten Intervallen oder Zeiträumen.

Neben der Pseudonymisierung der Daten des Versicherten (pD) wird eine Arbeitsnummer (AN) und ein Lieferpseudonym (LP) auf Basis der KVNR des Versicherten benötigt. Zum Nachweis der Authentizität des Absenders fordert das ePA-FdV die Erstellung von nicht personengebundenen Transporttoken von der Autorisierung des Aktensystems an, jeweils ein Token für die Vertrauensstelle mit der Arbeitsnummer und dem Lieferpseudonym und ein Token für das Forschungsdatenzentrum mit der Arbeitsnummer.

Das Transporttoken für die Vertrauensstelle wird anschließend an eine Vertrauensstelle (VST, gemäß § 303c SGB V) übertragen.

Das Transporttoken für das Forschungsdatenzentrum und die Ende-zu-Ende verschlüsselten pseudonymisierten Dokumente werden an ein Forschungsdatenzentrum (FDZ, gemäß § 303d SGB V) übertragen.

Eine Übersicht der freigegebenen Daten und etwaiger Widerrufe der Freigabe wird zentral in einem Dokument des Versicherten in seiner Akte verwaltet.

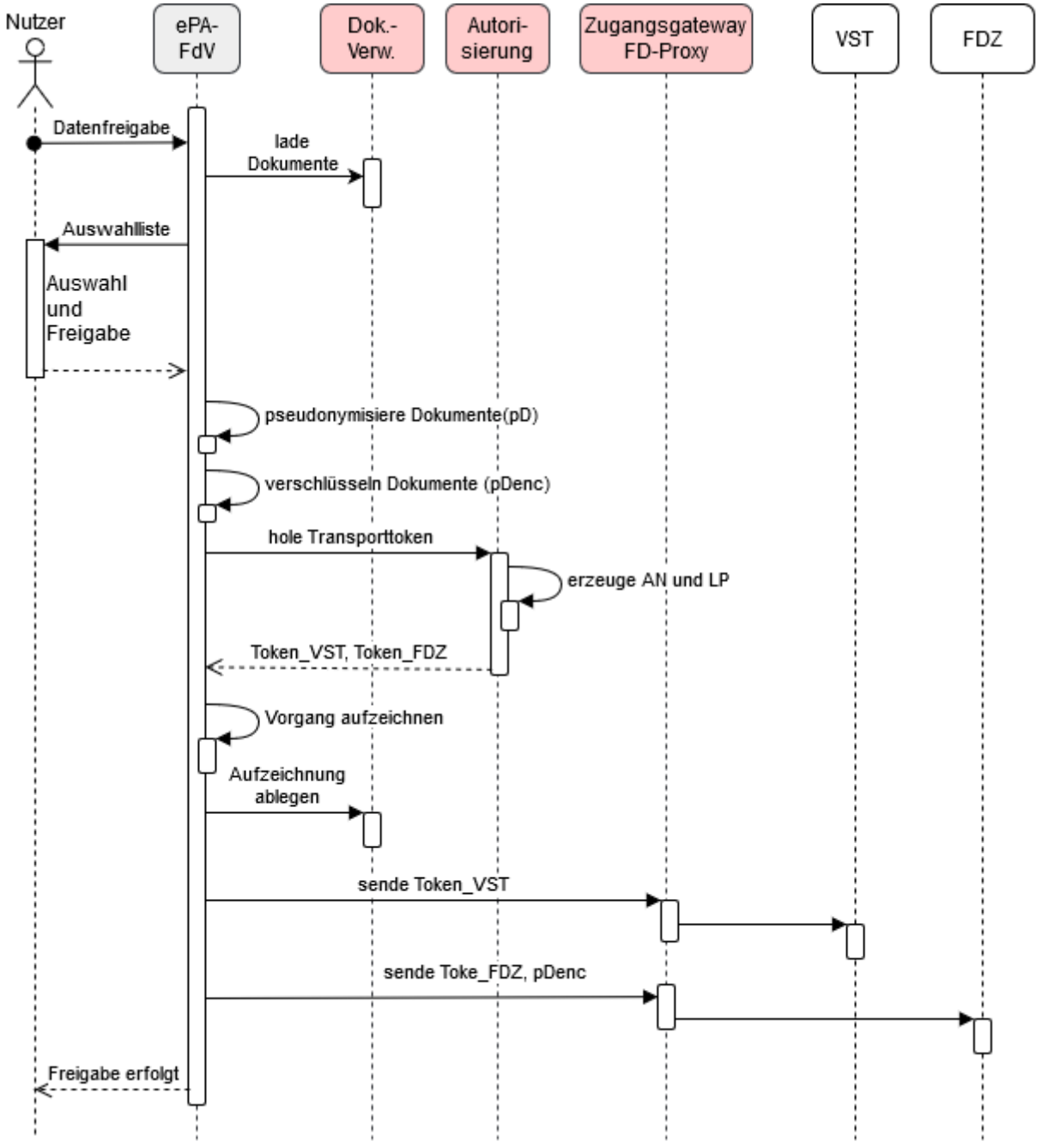

Abbildung 2 Übersicht des Ablaufs der Freigabe von Daten für Forschungszwecke

A_21843 - ePA-FdV: Einwilligung nach § 363 Absatz 2 SGB V in die Datenfreigabe für Forschungszwecke

Das ePA-FdV MUSS dem Versicherten eine Einwilligung nach § 363 Absatz 2 SGB V in die Datenfreigabe für die Forschung in einem informierten Dialog zur Anzeige bringen. Dabei MUSS der von der Krankenkasse des Versicherten vorgegebene Einwilligungstext verwendet werden. Der Text der Einwilligung muss auch im Nachhinein für den Versicherten zugänglich sein.**[<=]**

A_21844 - ePA-FdV: Datenfreigabe nur nach Einwilligung

Das ePA-FdV MUSS sicherstellen, dass eine Freigabe von Dokumenten zu Forschungszwecken am ePA-FdV erst erfolgen kann, nachdem der Versicherte seine Einwilligung nach § 363 Absatz 2 SGB V gegenüber der Krankenkasse erteilt hat. **[<=]**

A_21845 - ePA-FdV: Widerruf der Einwilligung nach § 363 Absatz 2 SGB V
Das ePA-FdV MUSS es dem Versicherten ermöglichen, die Einwilligung nach § 363 Absatz 2 SGB V gegenüber der Krankenkasse jederzeit zu widerrufen. Nach einem Widerruf MUSS das ePA-FdV die weitere Freigabe von Dokumenten für Forschungszwecke verhindern.**[<=]**

Hinweis: das ePA-FdV vermerkt den Status einer erteilten, bzw. widerrufenen Einwilligung nach § 363 Absatz 2 SGB V in der Akte des Versicherten im Dokument der aufgezeichneten Freigaben/ Widerrufe (A_21878).

A_21895 - ePA-FdV: Widerruf freigegebener Dokumente nach einem Widerruf der Einwilligung
Das ePA-FdV MUSS bei einem Widerruf der Einwilligung nach § 363 Absatz 2 SGB V automatisch alle zu diesem Zeitpunkt noch freigegebenen Dokumente widerrufen. **[<=]**

Hinweis: Es müssen alle Dokumente widerrufen werden, die in der Aufzeichnung der freigegebenen und widerrufenen Dokumente als freigegeben aber noch nicht widerrufen vermerkt sind.

A_21794 - ePA-FdV: Auswahl der freizugebenden Dokumente für Forschungszwecke
Das ePA-FdV MUSS dem Versicherten die Auswahl der freizugebenden Dokumente für Forschungszwecke vor jedem Freigabevorgang ermöglichen**[<=]**

A_21877 - ePA-FdV: Bestätigung der Freigabe oder des Widerrufs von Dokumenten für Forschungszwecke
Das ePA-FdV MUSS vor jeder Ausführung des Vorgangs der Freigabe von ausgewählten Dokumenten und vor jedem Widerruf von einem oder mehreren zuvor freigegebenen Dokumenten für Forschungszwecke die explizite Bestätigung des Versicherten einholen.**[<=]**

A_21896 - ePA-FdV: Anzeige der freigegebenen Dokumente für Forschungszwecke
Das ePA-FdV MUSS es dem Versicherten jederzeit ermöglichen, einzusehen, welche Dokumente aus seiner Akte für Forschungszwecke freigegeben sind. **[<=]**

A_21847 - ePA-FdV: Widerruf von freigegebenen Dokumenten
Das ePA-FdV MUSS es dem Versicherten ermöglichen, zuvor freigegebene Dokumente jederzeit zu widerrufen. Zum Zwecke des Widerrufs muss die Schnittstelle [I_FDZ] unter Angabe der zu widerrufenden, in der Vergangenheit freigegebenen Dokumente genutzt werden.**[<=]**

A_21792 - ePA-FdV: Pseudonymisierung von Dokumenten für Forschungszwecke
Das ePA-FdV MUSS die Daten eines für Forschungszwecke freizugebenden Dokuments unter Verwendung eines Pseudonymisierungsschemas in ein pseudonymisiertes Dokument überführen.**[<=]**

A_21793 - ePA-FdV: Verwendung eines geeigneten Pseudonymisierungsschemas

Das ePA-FdV MUSS für die Konvertierung der Daten eines Dokuments des Versicherten in ein pseudonymisiertes Dokument ein Pseudonymisierungsschema verwenden, welches für die Pseudonymisierung dieser Daten geeignet ist. **[**<=**]**

Hinweis: Das Schema zur Pseudonymisierung muss den Typ und die Version der MIO-Definition unterstützen.

A_21868 - ePA-FdV: Anzeige des pseudonymisierten Dokumentes
Das ePA-FdV MUSS dem Versicherten ermöglichen, sich das durch die Anwendung des Pseudonymisierungsschemas entstandene pseudonymisierte Dokument anzeigen zu lassen.
[<=**]**

Die Übertragung der freigegebenen und pseudonymisierten Dokumente an das Forschungsdatenzentrum erfolgt verschlüsselt und unter Verwendung einer Arbeitsnummer. Die gleiche Arbeitsnummer und das Lieferpseudonym werden an die Vertrauensstelle übermittelt. Als Identitätsnachweis gegenüber beiden Empfängern dienen jeweils Transporttoken der Autorisierung.

A_21822 - ePA-FdV: Erstellung der Transporttoken
Das ePA-FdV MUSS für den Übermittlungsvorgang an die Vertrauensstelle und an das Forschungsdatenzentrum von der Autorisierung erstellte Transporttoken verwenden. Beide Transporttoken MÜSSEN aus dem gleichen Aufruf der Schnittstelle [I_Authorization_Token_Service] stammen.
[<=**]**

A_21850 - ePA-FdV: Verwendungsdauer der Transporttoken
Das ePA-FdV MUSS für jeden Übermittlungsvorgang an die Vertrauensstelle und an das Forschungsdatenzentrum zeitlich gültige Transporttoken verwenden. Für die zeitliche Gültigkeit MUSS für die Token "Ausstellungszeitpunkt" <= aktuelle Zeit < "Zeitpunkt des Ablaufs der Gültigkeit" zutreffen. **[**<=**]**

A_21800 - ePA-FdV: Verschlüsselung der Daten für Forschungszwecke
Das ePA-FdV MUSS sicherstellen, dass die pseudonymisierten Dokumente ausschließlich für das Forschungsdatenzentrum verschlüsselt zum Forschungsdatenzentrum übertragen werden. **[**<=**]**

Hinweis: Die Anforderung A_21800 fordert eine Verschlüsselung der pseudonymisierten Daten auf Anwendungsebene. Eine Verschlüsselung auf Transportebene (TLS) ist nicht ausreichend, da die Daten über den FD-Proxy des Aktensystems an das Forschungsdatenzentrum versendet werden.

A_21803 - ePA-FdV: Verwendung der Schnittstelle der Vertrauensstelle
Das ePA-FdV MUSS das Transporttoken mit der Arbeitsnummer und dem Lieferpseudonym und unter Verwendung der Schnittstelle der Vertrauensstelle [I_VST] über den FD-Proxy an die Vertrauensstelle übermitteln.**[**<=**]**

A_21804 - ePA-FdV: Verwendung der Schnittstelle des Forschungsdatenzentrums
Das ePA-FdV MUSS die pseudonymisierten und verschlüsselten Dokumente und das Transporttoken mit der Arbeitsnummer unter Verwendung der Schnittstelle des Forschungsdatenzentrums [I_FDZ] über den FD-Proxy an das Forschungsdatenzentrum übermitteln**[**<=**]**

A_21894 - ePA-FdV: Reihenfolge des Aufrufs der Schnittstellen der Vertrauensstelle und des Forschungsdatenzentrums
Das ePA-FdV MUSS für einen Übermittelungsvorgang zuerst die Schnittstelle der Vertrauensstelle [I_VST] und erst danach die Schnittstelle des Forschungsdatenzentrums

[I_FDZ] verwenden. Dieser Vorgang und damit die Übermittelung freigegebener Dokumente MUSS abgebrochen werden, wenn der Aufruf der Schnittstelle der Vertrauensstelle [I_VST] nicht erfolgreich war. **[**<=**]**

Hinweis: Für das ePA-FdV gilt der Vorgang der Übermittelung von freigegebenen Dokumenten an das FDZ als abgeschlossen, wenn sowohl der Aufruf der Schnittstelle der Vertrauensstelle [I_VST], als auch der anschließende Aufruf der Schnittstelle des Forschungsdatenzentrums [I_FDZ] erfolgreich war.

Jedes freigegebene und jedes widerrufene Dokument muss für den Versicherten einsehbar erfasst werden. Für diese Aufzeichnungen wird ein vorgegebenes Dokument in der Akte des Versicherten verwendet. Der Versicherte kann anhand dieser Aufzeichnungen nachvollziehen, welche Dokumente freigegeben und an das Forschungsdatenzentrum übermittelt und welche widerrufen wurden. Die aufgezeichnete Dokumenteninformation zu einer Freigabe kann auch für einen eindeutigen Widerruf der Freigabe verwendet werden.

A_21878 - ePA-FdV: Aufzeichnung der erteilten oder widerrufenen Einwilligung des Versicherten in die Freigabe von Dokumenten für Forschungszwecke
Das ePA-FdV MUSS einen Nachweis der erteilten Einwilligung des Versicherten oder den Widerruf dieser Einwilligung zur Freigabe von Dokumenten für Forschungszwecke im Dokument [FD_Aufzeichnung] unter Beachtung von [FD_Aufzeichnung_Schema] im Ordner *patientdoc* ablegen. Ist das Dokument [FD_Aufzeichnung] zum Zeitpunkt der Aufzeichnung der erteilten Einwilligung nicht vorhanden, MUSS das ePA-FdV dieses Dokument gemäß [FD_Aufzeichnung] in der Akte des Versicherten anlegen**[**<=**]**

A_21805 - ePA-FdV: Aufzeichnung von Freigabe und Widerruf von Dokumenten für Forschungszwecke
Das ePA-FdV MUSS die Freigabe von Dokumenten für Forschungszwecke vor dem Aufruf der Schnittstelle [I_FDZ] und den Widerruf von Dokumenten nach dem erfolgreichen Aufruf der Schnittstelle [I_FDZ] aufzeichnen und in der Akte des Versicherten gemäß [FD_Aufzeichnung] und [FD_Aufzeichnung_Schema] ablegen. **[**<=**]**

Hinweis: Die vorgegebenen Zeitpunkte in A_21805 stellen sicher, dass freigegebene Dokumente auf jeden Fall aufgezeichnet werden, auch wenn die folgende Übertragung an das FDZ nicht erfolgreich ist. Ebenso erfolgt die Aufzeichnung widerrufener Dokumente erst nach der Bestätigung des Erhalts des Widerrufs durch das FDZ. Im Falle fehlerhafter Übertragungen ist dadurch sichergestellt, dass zwar im Einzelfall freigegebene Dokumente nicht mehr oder noch nicht im FDZ vorliegen können, jedoch niemals Dokumente im FDZ vorliegen, die nicht in der Aufzeichnung für den Versicherten erfasst sind.

Der Versicherte kann dem Forschungszentrum gegenüber die Freigabe einzelner oder aller zuvor freigegebenen Dokumente widerrufen. Der Widerruf erfolgt analog zu einer Freigabe unter Verwendung von Arbeitsnummer und Pseudonym und Übermittlung von Daten an die Vertrauensstelle und das Forschungsdatenzentrum. Anstelle freigegebener Dokumente erfolgt der Versand des Widerrufs an das Forschungsdatenzentrum.

Nach jedem Widerruf muss das Dokument mit den Aufzeichnungen zur Freigabe von Daten für Forschungszwecke aktualisiert werden.

4.2 Datenschutz und Sicherheit (gemSpec_ePA_FdV)

A_21795 - ePA-FdV: Ausschluss der Übermittlung nicht freigegebener Dokumente für Forschungszwecke
Das ePA-FdV DARF Dokumente des Versicherten, die nicht durch den Versicherten für die Verwendung zu Forschungszwecken freigegeben sind, NICHT an das Forschungsdatenzentrum übermitteln.**[<=]**

A_21802 - ePA-FdV: Ausschluss der Übermittlung nicht pseudonymisierter Dokumente für Forschungszwecke
Das ePA-FdV DARF Originaldokumente (nicht pseudonymisierte Dokumente) NICHT an das Forschungsdatenzentrum oder die Vertrauensstelle übermitteln.**[<=]**

A_21857 - ePA-FdV: Integrität und Authentizität Pseudonymisierungsschema
Das ePA-FdV des Versicherten MUSS sicherstellen, dass ausschließlich integre und authentische Pseudonymisierungsschemata genutzt werden.**[<=]**

A_22072 - ePA-FdV: freizugebende Dokumente und Transporttoken aus derselben Akte
Das ePA-FdV des Versicherten MUSS sicherstellen, dass die pseudonymisierten und verschlüsselten Dokumente und die Transporttoken der Autorisierung für die Übermittelung von Daten an die Vertrauensstelle und an das Forschungsdatenzentrum aus demselben Aktenkonto stammen.
[<=]

4.3 Funktionale Anforderungen (gemSpec_Autorisierung)

4.3.1 Kapitel 6.6 Authentisierung der Forschungsdatenfreigabe

Die Komponente Autorisierung erstellt für ePA-FdV signierte Transporttoken (JSON Web Token, JWS) für die Verwendung als Herkunftsnachweis bei der Übermittelung von Daten an das Forschungsdatenzentrum und die Vertrauensstelle. Die Ausstellung der Transporttoken erfolgt ausschließlich für autorisierte Nutzer.

A_21832 - Komponente Autorisierung: Realisierung der Schnittstelle zur Erstellung der Transporttoken
Die Komponente Autorisierung MUSS die REST-Schnittstelle zur Erstellung der Transporttoken für ein ePA-FdV gemäß [I_Authorization_Token_Service] anbieten.**[<=]**

A_21797 - Komponente Autorisierung: Erstellung des Lieferpseudonyms
Die Komponente Autorisierung MUSS das Lieferpseudonym des Versicherten gemäß [VST_LP] unter Verwendung der KVNR des Versicherten erstellen.**[<=]**

A_21796 - Komponente Autorisierung: Erstellung der Arbeitsnummer
Die Komponente Autorisierung MUSS für die Arbeitsnummer einen Zufallswert mit mindestens 16 Byte und maximal 64 Byte Länge verwenden.**[<=]**

A_21799 - Komponente Autorisierung: Verwendungsdauer der Arbeitsnummer
Die Komponente Autorisierung MUSS bei jedem Operationsaufruf eine neue Arbeitsnummer erzeugen und in den zurückgelieferten Transporttoken verwenden.**[<=]**

A_21892 - Komponente Autorisierung: Ausstellungszeitpunkt der Transporttoken

Die Komponente Autorisierung MUSS den Ausstellungszeitpunkt ("issued at") in den Transporttoken setzen. Dieser Ausstellungszeitpunkt MUSS in allen bei einem Operationsaufruf erzeugten Transporttoken gleich sein. **[<=]**

A_21893 - Komponente Autorisierung: Gültigkeitsdauer der Transporttoken
Die Komponente Autorisierung MUSS den Zeitpunkt des Ablaufs der Gültigkeit ("Expiration Time") in den Transporttoken setzen. Dieser Wert MUSS auf den Wert "Ausstellungszeitpunkt " plus 20 Minuten gesetzt werden. Der Zeitpunkt des Ablaufs der Gültigkeit MUSS in allen bei einem Operationsaufruf erzeugten Transporttoken gleich sein. **[<=]**

A_21821 - Komponente Autorisierung: Erstellung der Transporttoken
Die Komponente Autorisierung MUSS die Transporttoken gemäß [Authorization_Token_Service_FD_Token] für das ePA_FdV eines autorisierten Nutzer erstellen, wenn diese vom ePA_FdV über die Schnittstelle zur Erstellung der Transporttoken angefordert wird. Die Transporttoken MÜSSEN jeweils mit der Identität ID.FD.SIG der Autorisierung signiert werden. **[<=]**

4.4 Funktionale Anforderungen Proxy Forschungsdaten (gemSpec_Zugangsgateway_Vers)

4.4.1 Kapitel 4.8 Proxy Forschungsdaten

Der Proxy Forschungsdaten (FD-Proxy) stellt sicher, dass ein ePA-FdV die Schnittstellen der Vertrauensstelle (VST) und des Forschungsdatenzentrums (FDZ) zum Zweck der Freigabe von Daten für die Forschung verwenden kann. Die Verwendung der Schnittstellen wird durch den FD-Proxy auf autorisierte Nutzer eingeschränkt.

Der FD-Proxy tritt gegenüber den externen Schnittstellen als sendender Client auf. Die gegenseitige Authentifizierung des FD-Proxy und der externen Server erfolgt durch beidseitig authentifiziertes TLS.

A_21852 - Zugangsgateway des Versicherten: FD-Proxy - Zugriff auf die Schnittstellen der VST und des FDZ
Der Proxy Forschungsdaten MUSS sicherstellen, dass nur autorisierte ePA-FdV Zugriff auf die Schnittstellen der Vertrauensstelle und des Forschungsdatenzentrums erhalten.**[<=]**

A_21864 - Zugangsgateway des Versicherten: FD-Proxy - TLS-Client-Authentisierung
Der FD-Proxy der Komponente Zugangsgateway des Versicherten MUSS eine Identität ID.FD.TLS-C für die TLS-Client-Authentisierung besitzen.**[<=]**

A_21862 - Zugangsgateway des Versicherten: FD-Proxy - TLS zwischen FD-Proxy und Forschungsdatenzentrum
Der FD-Proxy der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass Daten an das Forschungsdatenzentrum ausschließlich über eine beidseitig authentisierte und verschlüsselte TLS-Verbindung gemäß den Vorgaben aus BSI TR-02102-2 übermittelt werden, wobei sich der FD-Proxy mit der Identität ID.FD.TLS-C authentisiert.**[<=]**

A_21863 - Zugangsgateway des Versicherten: FD-Proxy - TLS zwischen FD-Proxy und Vertrauensstelle

Der FD-Proxy der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass Daten an die Vertrauensstelle ausschließlich über eine beidseitig authentisierte und verschlüsselte TLS-Verbindung gemäß den Vorgaben aus BSI TR-02102-2 übermittelt werden, wobei sich der FD-Proxy mit der Identität ID.FD.TLS-C authentisiert.**[<=]**

A_21865 - Zugangsgateway des Versicherten: FD-Proxy - Keine Profilbildung am FD-Proxy
Der Anbieter des ePA-Aktensystems MUSS mit Maßnahmen am FD-Proxy der Komponente Zugangsgateway des Versicherten verhindern, dass am FD-Proxy Profile über das Verhalten der Versicherten bzgl. der Freigabe von ePA-Daten für die Forschung gebildet werden (z.B. welcher Versicherte wann wie oft Daten freigibt oder widerruft).**[<=]**

A_21876 - Zugangsgateway des Versicherten: FD-Proxy - Sichere Verbindung zur Vertrauensstelle und zum Forschungsdatenzentrum
Der FD-Proxy der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass der Zugriff auf die Vertrauensstelle und auf das Forschungsdatenzentrum jeweils erst erfolgt, nachdem die Authentizität der Vertrauensstelle, bzw. des Forschungsdatenzentrums, durch den FD-Proxy erfolgreich geprüft wurde und eine vertrauliche und integritätsgeschützte Verbindung zwischen FD-Proxy und Vertrauensstelle, bzw. Forschungsdatenzentrum, aufgebaut wurde.
[<=]

4.5 Funktionale Anforderungen (gemSpec_Dokumentenverwaltung)

A_21867 - Komponente ePA-Dokumentenverwaltung: Kein Löschen der Liste freigegebener Dokumente
Die Dokumentenverwaltung MUSS sicherstellen, dass die Liste der freigegebenen Dokumente nicht gelöscht werden kann (auch nicht von Versicherten oder durch sie befugte Vertreter).**[<=]**

Hinweis: Der Versicherte muss die Freigabe von Dokumenten jederzeit widerrufen können (auch von bereits aus der Akte gelöschten Dokumenten). Daher müssen die für den Widerruf benötigten Informationen für den Versicherten stets verfügbar sein.

4.6 Betrieb

Es werden keine gesonderten Anforderungen an den Betrieb des ePA-FdV im Kontext der dargestellten Lösung erhoben

4.7 Test

An die Testtreiberschnittstelle werden keine zusätzlichen Anforderungen gestellt. Weitere Unterstützungsleistungen für den Test sind nicht erforderlich.

5 Änderungen an Produkt- und Anbietertypsteckbriefen

Afo-ID	Titel	Prüfvorschrift	gemProdT
A_21878	ePA-FdV: Aufzeichnung der erteilten oder widerrufenen Einwilligung des Versicherten in die Freigabe von Dokumenten für Forschungszwecke	funktionaler Test	ePA-FdV
A_21877	ePA-FdV: Bestätigung der Freigabe oder des Widerrufs von Dokumenten für Forschungszwecke	funktionaler Test	ePA-FdV
A_21876	Zugangsgateway des Versicherten: Sichere Verbindung zur Vertrauensstelle und zum Forschungsdatenzentrum	Produktgutachten	Aktensystem_ePA
A_21868	ePA-FdV: Anzeige des pseudonymisierten Dokumentes	funktionaler Test	ePA-FdV
A_21867	Komponente ePA-Dokumentenverwaltung: Kein Löschen der Liste freigegebener Dokumente	funktionaler Test	Aktensystem_ePA
A_21865	Zugangsgateway des Versicherten: FD-Proxy - Keine Profilbildung am FD-Proxy	Sicherheitsgutachten	Aktensystem_ePA
A_21864	Zugangsgateway des Versicherten: FD-Proxy - TLS-Client-Authentisierung	funktionaler Test	Aktensystem_ePA
A_21862	Zugangsgateway des Versicherten: FD-Proxy - TLS zwischen FD-Proxy und Forschungsdatenzentrum	Produktgutachten	Aktensystem_ePA
A_21863	Zugangsgateway des Versicherten: FD-Proxy - TLS zwischen FD-Proxy und Vertrauensstelle	Produktgutachten	Aktensystem_ePA
A_21857	ePA-FdV: Integrität und Authentizität Pseudonymisierungsschema	Produktgutachten	ePA-FdV

A_21852	Zugangsgateway des Versicherten: FD-Proxy - Zugriff auf die Schnittstellen der VST und des FDZ	Produktgutachten	Aktensystem_ePA
A_21850	ePA-FdV: Verwendungdauer der Transporttoken	funktionaler Test	ePA-FdV
A_21847	ePA-FdV: Widerruf von freigegebenen Dokumenten	funktionaler Test	ePA-FdV
A_21843	ePA-FdV: Einwilligung nach § 363 Absatz 2 SGB V in die Datenfreigabe für Forschungszwecke	funktionaler Test	ePA-FdV
A_21845	ePA-FdV: Widerruf der Einwilligung nach § 363 Absatz 2 SGB V	funktionaler Test	ePA-FdV
A_21844	ePA-FdV: Datenfreigabe nur nach Einwilligung	funktionaler Test	ePA-FdV
A_21832	Komponente Autorisierung: Realisierung der Schnittstelle zur Erstellung der Transporttoken	funktionaler Test	Aktensystem_ePA
A_21822	ePA-FdV: Erstellung der Transporttoken	funktionaler Test	ePA-FdV
A_21821	Komponente-Autorisierung: Erstellung der Transporttoken	funktionaler Test	Aktensystem_ePA
A_21805	ePA-FdV: Aufzeichnung von Freigabe und Widerruf von Dokumenten für Forschungszwecke	funktionaler Test	ePA-FdV
A_21804	ePA-FdV: Verwendung der Schnittstelle des Forschungsdatenzentrums	funktionaler Test	ePA-FdV
A_21803	ePA-FdV: Verwendung der Schnittstelle der Vertrauensstelle	funktionaler Test	ePA-FdV
A_21802	ePA-FdV: Ausschluss der Übermittlung nicht pseudonymisierter Dokumente für Forschungszwecke	Produktgutachten	ePA-FdV
A_21800	ePA-FdV: Verschlüsselung der Daten für Forschungszwecke	Produktgutachten	ePA-FdV

A_21799	Komponente-Autorisierung: Verwendungsdauer der Arbeitsnummer	funktionaler Test	Aktensystem_ePA
A_21797	Komponente-Autorisierung: Erstellung des Lieferpseudonyms	funktionaler Test	Aktensystem_ePA
A_21796	Komponente-Autorisierung: Erstellung der Arbeitsnummer	funktionaler Test	Aktensystem_ePA
A_21795	ePA-FdV: Ausschluss der Übermittlung nicht freigegebener Dokumente für Forschungszwecke	Produktgutachten	ePA-FdV
A_21794	ePA-FdV: Auswahl der freizugebenden Dokumente für Forschungszwecke	funktionaler Test	ePA-FdV
A_21793	ePA-FdV: Verwendung eines geeigneten Pseudonymisierungsschemas	Produktgutachten	ePA-FdV
A_21792	ePA-FdV: Pseudonymisierung von Dokumenten für Forschungszwecke	funktionaler Test	ePA-FdV
A_21892	Komponente Autorisierung: Ausstellungszeitpunkt der Transporttoken	funktionaler Test	Aktensystem_ePA
A_21893	Komponente Autorisierung: Erstellung der Transporttoken	funktionaler Test	Aktensystem_ePA
A_21894	ePA-FdV: Reihenfolge des Aufrufs der Schnittstellen der Vertrauensstelle und des Forschungsdatenzentrums	funktionaler Test	ePA-FdV
A_21895	ePA-FdV: Widerruf freigegebener Dokumente nach einem Widerruf der Einwilligung	funktionaler Test	ePA-FdV
A_21896	ePA-FdV: Anzeige der freigegebenen Dokumente für Forschungszwecke	funktionaler Test	ePA-FdV
A_22072	ePA-FdV: freizugebende Dokumente und Transporttoken aus derselben Akte	Produktgutachten	ePA-FdV

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
VST	Vertrauensstelle
FDZ	Forschungsdatenzentrum
LP	Lieferpseudonym
AN	Arbeitsnummer
PÜP	periodenübergreifendes Pseudonym
pD	pseudonymisierte Dokumente des Versicherten (strukturierte Dokumente, auf welche das Pseudonymisierungsschema angewendet wurde)
pDenc	pseudonymisierte Dokumente, Ende-zu-Ende verschlüsselt für das Forschungsdatenzentrum
Token, Transporttoken	Durch die Komponente Autorisierung erstellte und signierte json-web-token
Token_VST	Transporttoken für die Vertrauensstelle, enthält die Arbeitsnummer und das Lieferpseudonym
Token_FDZ	Transporttoken für das Forschungsdatenzentrum, enthält die Arbeitsnummer

6.2 Referenzierte Dokumente

6.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der

aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[FD_Aufzeichnung_Schema]	vorläufig: sharedResearchDocumentLIst.json, Json-Schema für das Dokument zur Aufzeichnung der Freigabe und des Widerrufs von Daten für Forschungszwecke
[FD_Aufzeichnung]	vorläufig: Eindeutige Angaben zum Dokument zur Aufzeichnung der Freigabe und des Widerrufs von Daten für Forschungszwecke in der Akte des Versicherten
[I_Authorization_Token_Service]	vorläufig: REST-Schnittstelle zur Ausstellung der Transporttoken für die Freigabe von Daten für Forschungszwecke. https://github.com/gematik/api-epa/master/src/openapi/sharedResearchDocumentsTransportToken.yaml
[Authorization_Token_Service_FD_Token]	vorläufig: Struktur der Transporttoken für die Freigabe von Daten für Forschungszwecke (JWT, JWS)

6.2.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
[VST_LP]	Eigenschaften des Lieferpseudonyms: Robert-Koch-Institut: Konzept "Vertrauensstelle elektronische Patientenakte – Pseudonymisierungskonzept zur Datenfreigabe ePA" Version 1.0 25.06.2021
[I_VST]	Schnittstelle der Vertrauensstelle: Robert-Koch-Institut: Konzept "Vertrauensstelle elektronische Patientenakte –

	Pseudonymisierungskonzept zur Datenfreigabe ePA" Version 1.0 25.06.2021
[I_FDZ]	vorläufig: REST-Schnittstelle des FDZ
[gemKonzeptpapier_ePA_§363(8)_SGB_V]	gematik: Konzeptpapier Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken nach §363 (8) SGB V – in Vrobereitung

7 Anhang C – Offene Punkte, Fragen

7.1 offene Punkte

lfd-Nr.	offener Punkt	
1	Definition und Verfügbarkeit der Schablonen	Der Inhalt, Prozess, Termine und die Verantwortlichkeiten zur Bereitstellung von Schablonen an das FdV zur Pseudonymisierung von Dokumenten der ePA ist noch offen. Das vorliegende Dokument nimmt die Existenz geeigneter Schablonen für die Beschreibung des Features an.
2	Abstimmung der Dokumente [I_VST] und [VST_LP]	Die genannten Dokumente enthalten ein Konzept zur Schnittstelle der VST und zur Bildung des LP. Der Inhalt dieses Konzepts muss noch abstimmt werden, da u.a. die Übertragung des Transporttokens nicht berücksichtigt ist.
3	Definition der Schnittstelle des FDZ (I_FDZ)	Es liegt bisher keine Beschreibung der Schnittstelle des Forschungsdatenzentrums vor.
4	Technische Definition der Transporttoken [Authorization_Token_Service_FD_Token]	Die exakte Ausprägung der Token erfordert mindestens die Abstimmung / Klärung zu lfd-Nr. 2
5	Technische Definition der Schnittstelle [I_Authorization_Token_Service]	Die konkrete Beschreibung der REST Schnittstelle, bzw. Operation, der Autorisierung ist noch nicht vorhanden.

6	Technische Definition der Dokumentenparamter/ -metadaten zu [FD_Aufzeichnung]	Die konkrete Beschreibung der Metadaten des Aufzeichnungsdokuments ist noch nicht vorhanden
7	Technische Definition des Schemas zu [FD_Aufzeichnung_Schema]	Die konkrete Beschreibung des Schemas für Inhalte zu [FD_Aufzeichnung] ist noch nicht vorhanden