Datenschutzkonzept I/E-Health NRW

Inhaltsverzeichnis

1. Beschreibung und Zielsetzung der Vorhaben

Das Projekt

Der elektronische Arztbrief und die elektronische Fallakte sind bereits heute verfügbar. Über das SNK kann schon vor Verfügbarkeit der TI sicher kommuniziert werden. Wir fügen diese und weitere Bausteine so zusammen, dass niedergelassene Ärztinnen und Ärzte und Krankenhäuser in unseren Modellregionen Informationen zu ihren Patienten austauschen können – direkt aus der gewohnten Software heraus. Gemeinsam erproben wir die Technologien anhand von vier konkreten Versorgungsszenarien in vier verschiedenen Modellregionen in NRW. Wir arbeiten dabei eng sowohl mit Arztnetzen und Versorgungsverbünden als auch den Anbietern von PVS und KIS zusammen. Gemeinsam wollen wir im Projekt I/E-Health NRW den Weg für eine sichere und interoperable verteilte E-Health-Infrastruktur bereiten.

I/E-Health NRW

Das Projekt I/E-Health NRW. Hand in Hand bestens versorgt – Interdisziplinäre E-Health-Dienste für die Gesundheitswirtschaft in NRW ist in den vier Modellregionen Düren/Aachen, Dortmund, Borken/Ahaus und Münster/Kreis Warendorf und auf Landesebene gestartet. Das Verbundvorhaben ist ein Siegerprojekt des Leitmarktwettbewerbs Gesundheit.NRW mit einem Gesamtvolumen von rund 8 Millionen Euro, welches vom 01.09.2016 bis 30.06.2019 mit rund 4,7 Millionen Euro aus Mitteln des Landes und des Europäischen Fonds für regionale Entwicklung (EFRE) gefördert wird. Konkretes Ziel des Projektes der Gesundheitswirtschaft ist es, existierende sektorenspezifische Insellösungen für den übergreifenden Austausch von elektronischen Daten mittels einer gemeinsamen IT-Infrastruktur und standardisierter Schnittstellen für eine multiprofessionelle und interdisziplinäre Versorgung nutzbar zu machen und damit die Versorgung der Patientinnen und Patienten zu verbessern. Das Projekt soll Regelungen des E-Health-Gesetzes in NRW umsetzen und wird von wesentlichen Akteuren aus Selbstverwaltung, Gesundheitsversorgung, Wirtschaft und Wissenschaft getragen.

Was wir tun

Die existierende technische Infrastruktur (elektronischer Arztbrief, elektronische Fallakte, KV-Connect) wird so erweitert, dass damit alle an der Patientenbehandlung Beteiligten sicher kommunizieren können. Es wird ein einheitliches Verzeichnis geschaffen, mit dem sich Kommunikationspartner eindeutig identifizieren und adressieren lassen. So lassen sich komplexe Versorgungsszenarien durch den Austausch elektronischer Arztbriefe oder elektronischer Fallakten zwischen ambulanten und stationärem Sektor realisieren. Praxis- und Krankenhausinformationssysteme werden über Schnittstellen angebunden, um Anwendern die Kommunikation direkt aus dem gewohnten Software-System heraus zu ermöglichen. Datenschutz, die Nutzung internationaler Standards und Migrationsfähigkeit in die Telematikinfrastruktur sind dabei stets im Blick.

Die Modellregionen

Die Umsetzung erfolgt in vier Modellregionen anhand spezifischer Versorgungsszenarien in drei Schritten. Nach der Analyse der sektorenübergreifenden Prozesse, der bereits eingesetzten Technologien und des Informationsaustausches wird die IT-gestützte sektorenübergreifende Zusammenarbeit regionenspezifisch entworfen. Die Implementierung erfolgt in Kooperation zwischen den beteiligten Softwareherstellern und Gesundheitseinrichtungen vor Ort. In allen

Phasen der Umsetzung werden die Ärztinnen und Ärzte, sowie Pflegekräfte einbezogen. Folgende Regionen und Versorgungsszenarien sind Teil des Projektes:

- Borken/Ahaus: Demenz-Akte
- Münster/Kreis Warendorf: Geriatrie-Akte
- Dortmund: Pädiatrie-Akte
- Düren/Aachen: Notfall-Pflegeakte, Onkologie-Akte

Anwendungsbeispiel

Das Projekt soll eine reibungslose Kommunikation zwischen Krankenhäusern und niedergelassenen Ärzten zum Nutzen der Patienten etablieren. Folgendes Szenario stellt das Ziel unseres Vorhabens verdeutlichen: Patienten kommen zu ihrem Hausarzt und die Behandlungsinformationen aus dem Krankenhaus liegen bereits im IT-System der Praxis vor. Ein Arzt/ eine Ärztin wird am Freitagnachmittag zu einem Notfall in ein Pflegeheim gerufen und hat durch eine elektronische Akte die medizinische Vorgeschichte des Patienten oder der Patientin gleich zur Hand, um schnell und sicher diagnostizieren und behandeln zu können. Im Anschluss an die Behandlung können die Ergebnisse durch die Ärztin/ den Arzt digital und sicher an die Personen und Einrichtungen versendet werden, die weiterbehandeln.

1.1. Projektbeteiligte

I/E-Health NRW ist ein Kooperationsprojekt der Partner Kassenärztliche Vereinigung Westfalen-Lippe, Kassenärztliche Vereinigung Nordrhein, der gemeinsamen IT-Tochter KV-IT GmbH, Healthcare IT Solutions der Uniklinik Aachen, Krankenhausgesellschaft Nordrhein-Westfalen, Caritas Trägergesellschaft West, CompuGroup Medical, Duria eG, Fachhochschule Dortmund, St. Franziskus-Hospital Münster, FAC'T IT GmbH Münster, Klinikum Westmünsterland sowie Krankenhaus Düren. Weitere Partner sind das Klinikum Dortmund, Telekom Healthcare Solutions, KV Telematik GmbH, MedEcon Ruhr GmbH, Fraunhofer ISST, RZV Rechenzentrum Volmarstein GmbH sowie Schäfer & Selvi IT-Consulting GbR.

Der Verein Digital Healthcare NRW e. V setzt sich aus der Krankenhausgesellschaft Nordrhein-Westfalen, der Healthcare IT Solutions und der KV-IT GmbH zusammen, wobei die KV-IT GmbH stellvertretend für die KVNO und die KVWL steht. Digital Healthcare NRW e. V. ist Konsortialführer im Rahmen des von Land und EU geförderten Projektes."

1.2. Definitionen / Begrifflichkeiten

Begriff	Erläuterung
Aktenberechtigte EFA-Teilnehmer	Für Zugriff und Pflege spezifischer Fallakten berechtigte EFA-Teilnehmer sind Ärzte und das das nicht-ärztliche medizinische Fachpersonal (z. B. Pflegekräfte), das zur Behandlung und Dokumentation als berufsmäßig tätige Gehilfen der Ärzte auf die Fallakte zur Erfüllung ihrer Aufgaben Zugriff haben müssen. Der Fallaktenzugriff kann durch Änderung der Berechtigungen oder das Schließen der Fallakte aufgehoben werden.

Consent Document	Elektronische Einwilligungserklärung. Enthält die Zugriffsrechte zu einer spezifischen EFA.
EFA-Provider, Provider	Der EFA-Provider verantwortet und betreibt die technischen Dienste der EFA, welche die Interaktionsmuster der EFA implementieren. Sämtliche Dokumente einer spezifischen EFA werden bei einem Provider gespeichert.
EFA-Teilnehmer	EFA-Teilnehmer sind alle in dem System registrierten Ärzte sowie das nicht-ärztliche medizinische Fachpersonal (z. B. Pflegekräfte), das in die Behandlung und Dokumentation als berufsmäßig tätige Gehilfen der Ärzte einbezogen werden kann.
Einwilligung	Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist
Elektronische Fallakte (EFA)	Kommunikationsplattform für Ärzte die von ihrer Struktur her darauf ausgelegt ist, Ärzte über Sektor- und Einrichtungsgrenzen hinweg zu vernetzen und ihnen den datenschutzgerechten Austausch von medizinischen Informationen zu gemeinsam behandelten Patienten zu ermöglichen. Für jeden spezifischen medizinischen Fall des Patienten kann eine neue EFA angelegt werden.
Fallaktenmanager	Der Fallaktenmanager ist die einzige Stelle, die auf eine EFA im gesperrten Zustand über ein gesondertes Verfahren zugreifen kann und dem gegenüber invalidierte Daten sichtbar sind. Des Weiteren kann der Fallaktenmanager bei Bedarf jederzeit die Löschung einer EFA durchführen. Die Rolle des Fallaktenmanagers muss für jede angelegte EFA besetzt und in der Einwilligung angegeben sein.
Gesundheitsdaten	Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der

	Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
Kassenärztliche Vereinigung (KV)	Körperschaften des öffentlichen Rechts, denen alle Vertragsärzte und Vertragspsychotherapeuten angehören müssen. Sie sind für die vertragsärztliche Versorgung der Versicherten der gesetzlichen Krankenversicherungen zuständig
Offline-Token	Folge zusammengehöriger Zeichen die den Zugriff ohne vorherige Berechtigung auf eine bestimmte EFA ermöglichen.
Patient (Versicherter)	Patienten sind alle bürgerlichen Personen zu denen eine EFA vorliegt. Zu jedem Patienten können verschiedene EFA mit unterschiedlichen Zweckcodes erstellt werden. Der Patient besitzt keinen direkten Zugang zur EFA.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
Teilnehmersystem (KIS, PVS, Portal)	Software, welche die Verwaltung, die Organisation und den Betrieb von Krankenhäusern, Arztpraxen bzw. die ärztliche Tätigkeit unterstützen. Bieten Zugriff auf die die Fallakten.

2. Regionsübergreifende Aspekte

2.1. Zweckbestimmung

Die erhobenen medizinischen Daten einer EFA unterliegen einer konkreten Zweckbindung: Zweck der EFA ist das kooperative Zusammenwirken verschiedener Leistungserbringer bei der Behandlung eines konkreten Behandlungsfalls. Das bedeutet, dass nur für den Behandlungsprozess relevante Informationen zu diesem definierten Behandlungsfall in der Fallakte referenziert und zugänglich gemacht werden dürfen. Eine Vorratsdatenerhebung und -speicherung allgemein zum Gesundheitszustand des Patienten ist im Rahmen der Fallakte nicht zulässig. Doppelerhebungen von medizinischen Daten sind bestmöglich zu vermeiden.

Die Zweckbindung der Datenverarbeitung durch die Fallakte beinhaltet zusammengefasst, dass: medizinische Informationen über einen bestimmten Patienten in einem bestimmten Behandlungsprozess einem berechtigten Personenkreis in vollem benötigtem Umfang, ortsungebunden und korrekt zum benötigten Zeitpunkt zur Verfügung stehen, um den Patienten schnellst- und bestmöglich behandeln zu können. Nach dem Erlöschen des Zwecks einer EFA wird diese mit allen Daten gelöscht.

2.2. Rechtsgrundlage der Datenverarbeitung / Patienteneinwilligung

Die Rechtsgrundlage besteht durch die freiwillige Einwilligung des Patienten, in der dieser über den vorgesehenen Verwendungszweck der Erhebung, die Verarbeitung und die Nutzung informiert wird. Diese Einwilligung ist schriftlich einzuholen und besonders hervorzuheben sowie in einer einfachen Sprache geschrieben werden. Zudem muss die Einwilligung sich direkt und ausdrücklich auf die zu verarbeitenden Daten beziehen.

Die Einwilligung wird – bis zur Einführung eines elektronischen Verfahrens – schriftlich abgebildet und dokumentiert. Eine einmalig erteilte Einwilligung kann durch den Patienten jederzeit widerrufen werden. Mit dem Widerruf der Einwilligung verliert die EFA ihre rechtliche Grundlage und wird sofort für den externen Zugriff gesperrt und umgehend gelöscht.

Bevor ein Patient in die Nutzung der Akte einwilligen kann, muss er durch geschultes medizinisches Personal über die Funktionsweise und Risiken der EFA aufgeklärt werden. Diese Aufklärung erfolgt über eine schriftliche Patienteninformation, die die grundlegende Funktionsweisen sowie die Risiken in einfach zu verstehenden Worten enthält.

In der Patienteneinwilligung ist es dem Patienten möglich bestimmte EFA-Teilnehmer für seine Akte durch eine Positivliste zu berechtigen. In dieser Liste können Personen oder Einrichtungen angegeben werden, wobei die Einrichtungen folgende Einheiten darstellen können:

- Niedergelassene Ärzte (Einzel-/Gemeinschaftspraxis)
- Medizinische Versorgungszentren
- Krankenhäuser
- Ärzte- und Gesundheitsnetzwerke

Es existiert zu jedem Zeitpunkt nur eine gültige Einwilligungserklärung. Der Patient kann durch seine Einwilligung in eine neue Einwilligungserklärung die Liste der berechtigten EFA-

Teilnehmer ändern. Eine neue Einwilligung ersetzt in diesem Fall die bisher gültige Einwilligung.

Dem Patienten dürfen bei einer Nichteinwilligung keine vermeidbaren Nachteile entstehen. So ist steht bei einer Nichteinwilligung der klassische Weg des postalischen versandtes zur Verfügung. Hierbei ergeben sich für den Patienten Nachteile in Bezug auf die Versanddauer und der dadurch schnellen Verfügbarkeit der Dokumente. Dieser Nachteil ist jedoch für den Patienten zumutbar.

Bei nicht einwilligungsfähigen Betroffenen wird sichergestellt, dass die Einwilligung vom gesetzlichen Vertreter bzw. vom gerichtlich bestellten Vertreter abgegeben wird. Sollte der Betroffene die Einwilligungsfähigkeit (zurück)erlangen, wird unverzüglich die Einwilligung des Betroffenen selbst eingeholt. Vor Abgabe der Einwilligung wird der Betroffene vollumfänglich informiert. Weigert sich der Betroffene oder folgt dieser nicht der Einladung zu einem Gespräch, wird die Akte nach Ablauf der regulären Speicherdauer von 6 Monaten gelöscht.

2.3. Schweigepflicht in der EFA-Nutzung

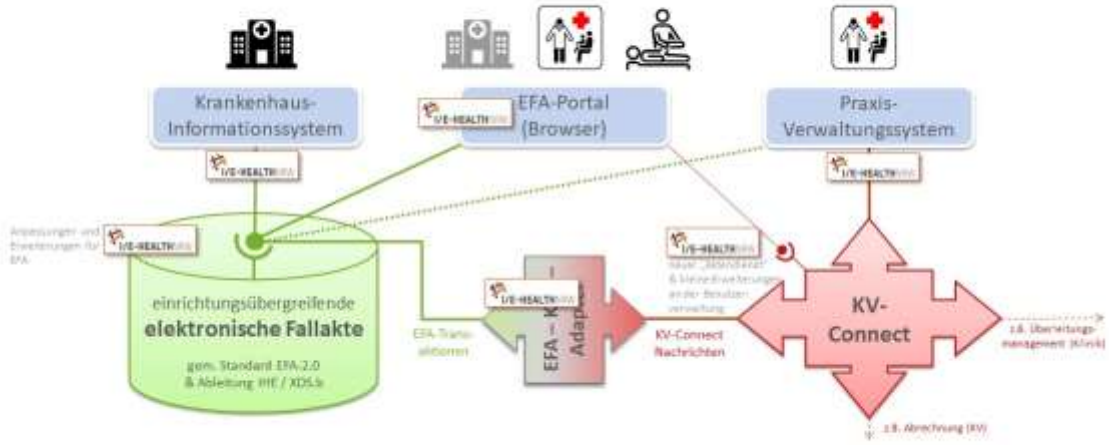
Ärztinnen und Ärzte, Zahnärzte und Zahnärztinnen sowie deren bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen in Deutschland sind dazu verpflichtet die ärztliche Schweigepflicht einzuhalten. Diese besagt, dass diese Personengruppen über das, was die Patienten ihnen anvertraut haben, schweigen zu bewahren. Geregelt ist diese Schweigepflicht in § 203 des Strafgesetzbuches. Neben dem Strafgesetzbuch findet ebenfalls der § 9 der Berufsordnung für Ärztinnen und Ärzte Anwendung. Auch bei der Nutzung der EFA finden diese Regelungen Anwendung.

2.4. Merkmale der technischen Infrastruktur

2.4.1. Architekturübersicht

In der nachfolgenden Abbildung 1 ist die Architekturübersicht der Systeme sowie deren Kommunikationskanäle abgebildet. Zu sehen sind die unterschiedlichen Kommunikationskanäle mittels derer auf die EFA eines Providers von den verschiedenen Primärsystemen zugegriffen werden kann:

1. Direkte Verbindung des Primärsystems eines Krankenhauses mittels der nativen Schnittstellen der EFA.
2. Direkte Verbindung des EFA-Portals über einen Browser mittels der nativen Schnittstellen der EFA.
3. Kommunikation des Primärsystems mit der EFA über einen Adapter, der ankommende Anfragen über KV-Connect entgegennimmt und diese in native Anfragen an die EFA transformiert.



2.4.2. Basissystem der EFA

Die EFA, ist eine Kommunikationsplattform für Ärzte und Ärztinnen: Von ihrer Struktur her ist sie darauf ausgelegt, Ärzte über Sektor- und Einrichtungsgrenzen hinweg zu vernetzen und ihnen den datenschutzgerechten Austausch von medizinischen Informationen zu gemeinsam behandelten Patienten zu ermöglichen. Eine EFA steht hierbei für einen medizinischen Fall eines Patienten. Standardisierte EFA-Schnittstellen ermöglichen einen reibungsfreien Informationsfluss unabhängig von verwendeten IT-Systemen. Die ausgefeilte Sicherheitsarchitektur gewährleistet den Schutz und die Sicherheit der sensiblen medizinischen Daten. Die EFA-Spezifikationen sind offengelegt und lizenzfrei verfügbar.

Die EFA ist keine Dokumentensammlung, sondern ein strukturiertes Inhaltsverzeichnis, das alle zu dem Fall zur Verfügung gestellten Dokumente auflistet: Das sind beispielsweise Befunde, Röntgenbilder, OP-Berichte, Entlassbriefe, Therapiepläne. Nur die vom Patienten autorisierten EFA-Teilnehmer dürfen auf diese Dokumente zugreifen. Die medizinischen Daten werden dezentral, getrennt vom Ort der Erhebung, gespeichert. Das EFA-Konzept basiert auf dem Grundsatz der Gleichberechtigung: Alle beteiligten Ärzte haben die gleiche Sicht auf den Fall; sie können sämtliche aufgelisteten Dokumente einsehen und aus der EFA heraus in ihre eigene Falldokumentation integrieren. Die Zugriffrechte erteilt der Patient; er kann sie auch widerrufen. Weil die EFA ausschließlich für die medizinische Kommunikation bestimmt ist, ermöglicht sie eine hohe fachliche Qualität der Informationen. Sie wird von den Ärzten geführt, die an der Behandlung des Patienten, seiner konkreten Erkrankung beteiligt sind. Die Zugriffsrechte kann der Patient jederzeit erweitern oder - auch einzeln - widerrufen. So bleibt das Recht auf freie Arztwahl gewährleistet.

Die Anforderungen an den Schutz der medizinischen Daten vor unerlaubtem Zugriff oder gar vor Manipulation sind sehr hoch. Daher sind Datenschutz und Datensicherheit von

Entwicklungsbeginn an als wesentliche Elemente im Konzept der EFA-Plattform verankert. Zentraler Teil der EFA-Spezifikationen ist die mehrstufige Sicherheitsarchitektur, die das Fraunhofer Institut für Software- und Systemtechnik zusammen mit Datenschutzexperten der Bundesländer erarbeitet hat und gemeinsam mit ihnen kontinuierlich weiterentwickelt.

- Sicherer Zugang: Die Zugänge zu den EFA-Netzwerken sind nach aktuellem Stand der Technik verschlüsselt. Bereits vor Anlage einer neuen EFA für einen Patienten gleicht das System die technischen Verbindungsdaten mit den namentlich genannten Ärzten und Einrichtungen ab und stellt die Übereinstimmung sicher.
- Doppelte Zugriffsicherung: Es liegt in der Hand des Patienten, welchen Ärzten er Zugriff auf seine EFA gewährt. Dazu dient beispielsweise ein Offline-Token: Er zeigt der mitbehandelnden Arztpraxis oder Klinik an, dass eine EFA existiert und von den dazu berechtigten Personen geöffnet werden kann.
- Kontrolle: Anhand einer Zugriffsliste kann der Datenschutz-Verantwortliche überdies jederzeit nachprüfen, wer wann auf die EFA-Daten zugegriffen hat.

2.4.2.1. Fallaktenmanager

Die Rolle des Fallaktenmanagers muss für jede angelegte EFA besetzt und in der Einwilligung benannt sein. Eine Änderung dieser Festlegung durch den Patienten ist nicht möglich.
Der Fallaktenmanager ist die einzige Stelle, die auf eine EFA im gesperrten Zustand über ein gesondertes Verfahren zugreifen und diese entsperren kann und dem gegenüber invalidierte Daten sichtbar sind. Des Weiteren kann der Fallaktenmanager bei Bedarf jederzeit die Löschung einer EFA durchführen.
Standardmäßig besitzt der aktenanlegende Arzt die Rolle des Fallaktenmanagers.

2.4.2.2. Wege der Berechtigungsänderung

Dem Patienten stehen zwei unterschiedliche Möglichkeiten zur Verfügung um die Berechtigungen auf seine EFA zu bearbeiten. Diese werden durch den Patienten selbst gesteuert und bedürfen seiner ausdrücklichen Einwilligung.
Zum einem ist es möglich bei bereits berechtigten EFA-Teilnehmern eine neue Einwilligungserklärung zu Unterschreiben und die Liste der berechtigten EFA-Teilnehmer anzupassen, zum anderen kann der Patient mittels des Offline-Tokens einen noch nicht berechtigten EFA-Teilnehmer ohne Hilfe eines bereits berechtigten EFA-Teilnehmers berechtigen. Dazu übergibt der Patient dem noch nicht berechtigten EFA-Teilnehmer das Offline-Token und unterschreibt eine neue Einwilligungserklärung. Der noch nicht berechtigte EFA-Teilnehmer berechtigt sich durch diesen Offline-Token selbstständig auf die EFA.

2.4.2.2.1. Offline-Token

Um einen schnellen Zugriff für neue Beteiligte am Behandlungsszenario zu ermöglichen, wird ein Offline-Token zum Einsatz kommen. Dies ist ein Mechanismus, der es dem Patienten ermöglicht unabhängig relevante EFA-Teilnehmer für den Zugriff auf die Fallakte zu berechtigen. Das Offline-Token gilt immer für eine bestimmte Fallakte und ermöglicht EFA-Teilnehmern nach

Überreichung des Tokens durch den Patienten, sich selbst ein Zugriffsrecht auf diese Fallakte zu erteilen.
Um dem Datenschutz und der Datensicherheit Rechnung zu tragen, kann das Offline-Token nur von Personen eingelöst werden, die im EFA-Netzwerk registriert sind. Die Offline-Token Transaktionen werden dabei umfassend protokolliert. Außerdem ist die schriftliche Einwilligung des Patienten oder eines Vormunds wesentlich.
Um einen Missbrauch des Offline-Tokens zu verhindern ist es notwendig, dass der Patient sich mit einem gültigen Ausweisdokument identifiziert und die Daten mit den auf dem Offline-Token aufgedruckten Daten verglichen werden.

Der Patient kann einen erstellten Offline-Token jederzeit von einem aktenberechtigten EFA-Teilnehmer automatisiert durch das Erstellen eines neuen Offline-Tokens deaktivieren lassen. Zudem ist es möglich einen Offline-Token ungelöst von der Erstellung zu Deaktivieren.

2.4.3. KV-Connect

KV-Connect ist ein Kommunikationsdienst für Ärzte im sicheren Netz der KVen (SNK), das von der KV Telematik GmbH mit Sitz in Berlin betrieben wird. Unabhängig von den Sicherheitsvorteilen, die das SNK ohnehin schon bietet, werden durch KV-Connect alle übertragenen Nachrichten automatisch Ende-zu-Ende-verschlüsselt.

KV-Connect ermöglicht - direkt aus dem jeweiligen PVS heraus - den sicheren Datenaustausch zwischen Ärzten, Krankenhäusern, KVen und weiteren medizinischen Partnern, beispielsweise Psychotherapeuten. Im Audit-Register können Sie sehen, welche KV-Connect Anwendungen Ihr Praxisverwaltungssystem anbietet.

Eine Beschreibung - insbesondere der Sicherheitsfunktionen - befindet sich in den mitgeltenden Dokumenten.

2.4.4. KV-Connect-Adapter

Mit dem KV-Connect-Adapter (KVC-Adapter) ist es Benutzern von KV-Connect möglich Anfragen an die EFA zu senden und Daten zu empfangen, ohne dass das eigene System eine native Integration der EFA-Schnittstellen beinhaltet.
Dazu sendet der Benutzer eine verschlüsselte KV-Connect-Mail innerhalb von KV-Safenet mit der entsprechenden Anfrage an den Adapter. Der Adapter entschlüsselt diese Mail, wandelt jegliche Anfragen in eine Anfrage für die EFA um und leitet sie über die verschlüsselte Schnittstelle der EFA an diese weiter. Die Anfrage wird durch die EFA bearbeitet und die Antwort an den Adapter gesendet, welcher wiederum diese Antwort in eine KV-Connect-Nachricht umwandelt und dem Benutzer zusendet.
Jegliche Kommunikation zwischen dem Primärsystem, dem Adapter und der EFA läuft dabei verschlüsselt ab.

Während der Umwandlung der verschlüsselten KV-Connect-Nachricht in eine neue verschlüsselte EFA-Nachricht und umgekehrt, liegen die Daten für einen eine geringe Zeitspanne unverschlüsselt auf dem Server vor. Um die Vertraulichkeit und Integrität zu gewährleisten, wird der Server verschlüsselt und sämtliche Zugriffe auf diesen

protokolliert. Der Server wird von der Kassenärztlichen Vereinigung Westfalen-Lippe (KVWL) im Sicheren Netz der KV betrieben.

Den schematischen Ablauf einer Kommunikation zwischen Arzt und EFA mittels Adapter finden Sie in der nachfolgenden Abbildung 2.

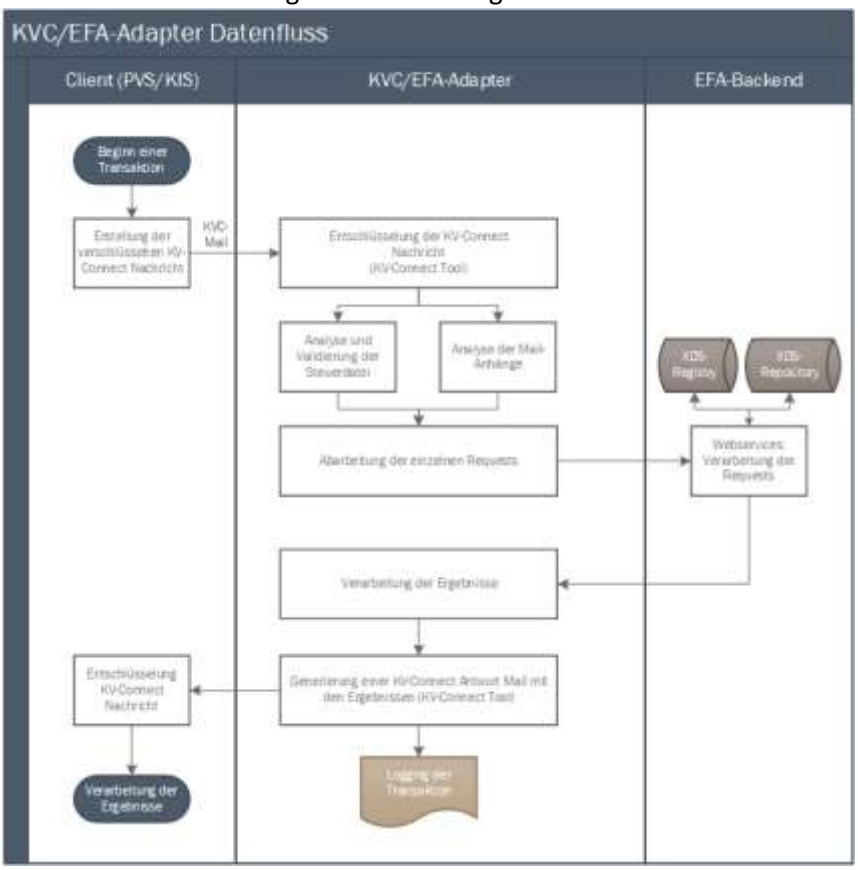


Abbildung 1: Schematischer Ablauf einer Kommunikation über den KVC-Adapter

Der KVC-Adapter wird in diesem Projekt durch die Kassenärztliche Vereinigung Westfalen-Lippe (KVWL) gehosted und zur Verfügung gestellt.

2.4.5. Master Patient Index

Der Master Patient Index (MPI) ermöglicht es in verschiedenen Systemen einen einheitlichen Patientenstamm zu pflegen. Dadurch besitzt jede Institution dieselben Stammdaten eines Patienten und kann diesen Eindeutig identifizieren. Dies ermöglicht es einen Patienten Einrichtungsübergreifend eindeutig zu behandeln. Jedem EFA-Teilnehmer ist es nach der Einwilligung des Patienten möglich diesen zu finden und eine neue Akte anzulegen. Bestehende Akten zu einem Patienten können nur bei bestehender Berechtigung auf diese von dem EFA-Teilnehmer gefunden werden.

In diesem Projekt wird der MPI für die Zuordnung eines Patienten zu seinen Akten genutzt. Dadurch können die verschiedensten Projektpartner auf die Daten eines Patienten zugreifen und neue einstellen.

Für das Anlegen einer neuen Fallakte zu einem Patienten ist es dem anlegenden EFA-Teilnehmer möglich unter Eingabe von personenbezogenen Daten (Vorname, Nachname,

Geburtsdatum, Geburtsort) den gesuchten Patienten im MPI zu suchen. Ist der Patient bereits vorhanden kann so die Fallakte dem richtigen Patienten zugeordnet werden. Dies verhindert eine mehrfache Speicherung von personenbezogenen Daten der Patienten.

2.4.6. Zugriffskontrolle auf die EFA

Beantragen eines Accounts

Möchte ein niedergelassener Arzt oder eine Einrichtung einen Zugang zur EFA beantragen, muss ein Antrag beim zuständigen Provider gestellt werden. Zur Identitätsprüfung stellt der Provider eine Anfrage bei der zuständigen Organisation der Selbstverwaltung. Fällt die Prüfung positiv aus, können die anfragende Stelle und der Provider einen Auftragsverarbeitungsvertrag (AV-Vertrag) abschließen. Nach Abschluss eines solchen AV-Vertrages erhält der Arzt oder die Einrichtung die erforderlichen Zugänge zur EFA. Sollte die Prüfung negativ ausfallen, wird die anfragende Stelle darüber benachrichtigt.

Löschen eines Accounts

Kündigt ein Vertragspartner den AV-Vertrag werden unverzüglich sämtliche vom Arzt oder von der Einrichtung eingestellten Dokumente sowie personenbezogene- und Gesundheitsdaten aus dem System gelöscht. Das Vorgehen ist in den Löschkonzepten der Provider beschrieben.

Rollen in der EFA

EFA-Teilnehmer

EFA-Teilnehmer besitzen folgende Rechte in der EFA:

- Fallakten anlegen
- Patienten suchen

Berechtigte EFA-Teilnehmer

EFA-Teilnehmer mit einer Berechtigung auf eine bestimmte Fallakte besitzen folgende Rechte auf diese:

- Neue Partitionen zu einer Fallakte anlegen
- Alle Daten der Fallakte einsehen und in das eigene System übernehmen
- Weitere Daten in die Fallakte einstellen
- Dokumente einer Fallakte invalidieren

Fallaktenmanager

Die Fallaktenmanager einer Fallakte besitzen neben allen bereits genannten Rechten ebenfalls folgende Rechte:

- Zugriff auf die Akte im gesperrten Zustand und deren Wiederherstellung auf Wunsch der Patienten
- Anzeige von sämtlichen, auch invalidierten Dokumenten
- Invalidierte Dokumente wieder validieren

2.5. Lebenszyklus der personenbezogenen Daten

2.5.1. Erheben, Sammeln der Daten

Der Lebenszyklus der personenbezogenen Daten beginnt noch vor Anlegung der EFA. Sofern der Patient bekannt ist liegen die personenbezogenen Daten bereits vor. Dabei ist zwischen Stammdaten, die unverändert bleiben und den Gesundheitsdaten, die bei jedem Praxisbesuch neu erhoben bzw. aktualisiert werden zu unterscheiden. Diese Daten werden im Primärsystem hinterlegt. Hier erfolgt die Primärdokumentation der Ärzte. Jeder Patient hat eine eigene Patientenakte, in der alle Informationen dokumentiert sind.

Nach Feststellung der Notwendigkeit Anlegung einer EFA wird diese angelegt und berechtigte EFA-Teilnehmer können die zur Versorgung relevanten Informationen in die EFA einstellen. Damit wird die EFA aus verschiedenen Primärsystemen mit Informationen gespeist.

2.5.2. Übertragung der Daten

Sämtliche EFA-Teilnehmer sind zuständig, den Bedarf für eine EFA festzustellen und diese im Bedarfsfall anzulegen. Die Generierung der Informationen erfolgt aus den bereits erhobenen Daten, die im Primärsystem gespeichert sind. Vor der Übertragung wird bei erfolgter Patienteneinwilligung eine EFA für den Patienten angelegt. Bei der Einstellung der Informationen sind zwei Möglichkeiten zu unterscheiden:

- manuell durch Direktreferenzierung aus einem KIS oder ähnlichem Primärsystem
- manuell durch Upload eines Arztes über das bereitgestellte Portal
- automatisiert durch das Primärsystem

Für den automatisierten Einstellungsprozess eines KIS/PVS sind aus Sicherheitsgründen nur freigegebene Dokumente zu übermitteln sowie vorab Regelsätze zu definieren, die folgende Struktur auf die medizinischen Datenobjekte abbilden:

- Dokumente, die automatisch in die Fallakte übernommen werden
- Dokumente, die unter keinen Umständen in die Fallakte übernommen werden
- Dokumente, die auf Rückfrage und mit ausdrücklicher Zustimmung des Arztes in die Fallakte übernommen werden

2.5.3. Verwendung der Daten

An der Datenverwendung nehmen das Primärsystem des Anwenders oder das Portal und das EFA-System, welches vom jeweiligen Provider angeboten wird, teil. Zu jedem hochgeladenen Dokument wird außerdem der Ersteller sowie das Erstellungsdatum und/oder das Einstellungsdatum vermerkt. Diese Informationen stehen allen Mitbehandlern, die in der Patienteneinwilligung benannt und im Consent Document vermerkt sind, zu Verfügung. Die berechtigten Teilnehmer können die verfügbaren Dokumente in ihr System herunterladen und der internen Patientenakte im Primärsystem zuordnen. Über das Offline-Token, welches auf die jeweilige EFA referenziert, können seitens des Patienten auch weitere Ärzte berechtigt werden. Bei der Datenverwendung der EFA sind folgende Szenarien zu berücksichtigen:

- Datenverwendung erfolgt erst, wenn Patient in der berechtigten Einrichtung/ Praxis anwesend ist.
- Datenverwendung erfolgt von berechtigten Anwendern im Rahmen der Konsultation unter Abwesenheit des Patienten statt.
- Datenverwendung erfolgt bei Verlegung des Patienten auf eine berechtigte weiterbehandelnde Abteilung innerhalb des Krankenhauses statt.
- Datenverwendung erfolgt, wenn Patient in eine unberechtigte Einrichtung/Praxis kommt (Berechtigung über Offline-Token).

2.5.4. Speichern der Daten

Die Daten werden je nach Modellregion bei folgenden Providern gespeichert:

- RZV Rechenzentrum Volmarstein GmbH (RZV)
  - Grundschötteler Str. 21, 58300 Wetter (Ruhr)
  - Gerichtsstand: Amtsgericht Hagen, HRB 5122
- Healthcare IT Solutions GmbH (HITS)
  - Pauwelsstraße 30, 52074 Aachen
  - Amtsgericht Aachen, HRB 13108
- FAC'T GmbH (FACT)
  - Schwachhauser Heerstr. 67, 28211 Bremen
  - Handelsregister Bremen, HRB 34199

Da es sich bei der EFA nicht um eine Primärdokumentation handelt, unterliegt diese nicht den gesetzlichen Aufbewahrungsfristen für medizinische Dokumente. Unabhängig davon, werden die Referenzen und Zugriffsrechte-/Protokolle der spezifischen EFA gesichert.

Eine EFA besitzt, je nach Modellregion, eine unterschiedliche Laufzeit von maximal Fünf Jahren. Diese wird in dem regionalen Abschnitt beschrieben. Endet die Laufzeit einer EFA wird sie gesperrt und kann innerhalb von 6 Monaten auf Wunsch des Patienten reaktiviert werden. Sollte dies nicht der Fall sein, wird sie innerhalb einer Woche gelöscht. Unberührt davon bleibt das Recht des Patienten die EFA zu jedem Zeitpunkt löschen zu lassen.
Die personenbezogenen Stammdaten werden gelöscht, sobald diese für keine EFA genutzt werden.

Die Löschfristen der erhobenen Daten werden in den Löschkonzepten der Provider detailliert mit den Datenklassen, Löschklassen beschrieben.

2.5.5. Maßnahmen zur Zugriffsverhinderung

Im Rahmen der Patienteneinwilligung entscheidet der Patient, beraten durch eine ärztliche Vertrauensperson, wer auf diese Daten in der EFA zugreifen darf. Eine Zugriffsverhinderung wird damit gewährleistet, dass sich nur die EFA-Teilnehmer authentifizieren können, die sich vorher registriert haben. Durch Autorisierung des EFA-Providers erhalten die registrierten und authentifizierten Teilnehmer die Berechtigung, auf die jeweilige EFA zuzugreifen.
Ein Zugriff auf die Daten durch physischem Zugang zum Server wird durch eine lokale Verschlüsselung der Server sowie die Umsetzung von technisch- und organisatorischen Maßnahmen der einzelnen Provider verhindert.

2.6. Akteure / Beteiligte

Die Akteure einer Fallakte umfassen den Patienten und ihre rechtlichen Vertreter, den/ die niedergelassenen Arzt/ Ärzte samt beauftragtem Personal, das/ die Krankenhaus/ Krankenhäuser, Heilberufler sowie den Fallakten-Provider.

Grundsätzlich können im Laufe der Umsetzung der Fallaktenkommunikation in der Modellregion weitere Professionen und Einrichtungen hinzukommen.

Natürliche bzw. Juristische Personen als Akteure im Versorgungsszenario Demenz-Akte	
Anwender	Person, die ein Gerät oder eine Software verwendet
Patient	eine oder mehrere Personen, die terminlich eingeplant sind, eine Leistung des Gesundheitswesens zu erhalten, diese gerade erhalten oder diese bereits erhalten haben (Quelle: DIN CEN ISO/TS 14441)
Datenschutzbeauftragte/r	Natürliche Person, die auf die Einhaltung des Datenschutzes im Unternehmen hinwirken soll
Empfänger	natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. (Quelle: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Heilberufler	Person, die von einer anerkannten Stelle autorisiert ist, zur Erbringung gewisser medizinischer Dienstleistungen qualifiziert zu sein. (Quelle: DIN CEN ISO/TS 14441)
Hersteller	natürliche oder juristische Person, die für die Auslegung, Herstellung, Verpackung oder Kennzeichnung eines Medizinprodukts, für den Zusammenbau eines Systems oder für die Anpassung eines Medizinprodukts vor dem Inverkehrbringen oder der Inbetriebnahme verantwortlich ist, unabhängig davon, ob diese Tätigkeiten von dieser Person selbst oder stellvertretend für diese von einer dritten Person ausgeführt werden. (Quelle: DIN EN ISO 14971)
Person, behandelte	Siehe „Patient
Person, betroffene	Personen, auf die sich Daten beziehen (Quelle: DIN EN ISO 25237)
Person, identifizierbare	jemand, der direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer

	Identifikationsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind (Quelle: DIN CEN ISO/TS 14441)
Verantwortlicher (Für die Verarbeitung)	Zugriffsberechtigte Ärzte auf eine spezifische Akte.

In den beteiligten Einrichtungen werden unterschiedliche Systeme zur Verarbeitung der gesundheits- und behandlungsbezogenen Daten teil.

Die Kommunikation erfolgt dabei auf Seiten der Klinik über das Krankenhausinformationssystem und auf Seiten der niedergelassenen Arztpraxen über die Praxisverwaltungssysteme, die dabei entweder über den KV-Connect Adapter oder über das Webportal Daten in die Fallakte einstellen.

Beteiligte Systeme im Versorgungsszenario Demenz-Akte	
Arztpraxisinformationssystem	Ein oder mehrere Informationssysteme zur Erhebung und Speicherung sowie Bereitstellung von in einer Arztpraxis anfallenden Daten eines Patienten
EFA-Backend	Anwendungssystem zum Bereitstellen des EFA-Fallaktensystems.
Kommunikationsserver	Softwarelösung um Empfang und zur Verteilung von digitalen Nachrichten zwischen verschiedenen Informationssystemen wie bspw. KIS, RIS, LIS
Krankenhausinformationssystem	Gesamtheit aller in einem Krankenhaus eingesetzten informationstechnischen Systeme zur Verwaltung und Dokumentation elektronischer Patientendaten. Dabei handelt es sich in aller Regel um einen Verbund selbständiger Systeme meist unterschiedlicher Hersteller. Auf einzelne Fachbereiche beschränkte Verfahren wie z. B. Labor-, Radiologie- oder Diagnosesysteme gehören als Subsysteme ebenfalls zum Krankenhausinformationssystem.

In der Rolle des niedergelassenen Arztes werden die Informationen zunächst im Primärsystem erhoben und anschließend in eine Dokumentenform (PDF, HL7 CDA-Dokument) überführt. Diese werden über das Fallaktensystem den berechtigten Weiterbehandlern zu Verfügung gestellt. Auf gleiche Weise ruft der niedergelassene Arzt Daten aus der Fallakte ab und speichert sie in seinem PVS. Auf Klinikseite werden die Informationen im Krankenhausinformationssystem verarbeitet. Hier findet ebenfalls ein Download und Upload von Daten statt.

Datenverarbeitende Akteure

Akteur der EFA	Beschreibung
EFA-Provider	Ein EFA-Provider ist ein Dienstleister, der EFA-Teilnehmern und Fallaktenmanagern die Dienste der EFA bereit stellt.
EFA-Teilnehmer	Inhaber der Rolle "EFA-Teilnehmer" haben das Recht, • Fallakten anzulegen und in einen geordneten Schließungsprozess zu überführen • neue Partitionen zu einer Fallakte anzulegen • alle in eine Fallakte eingestellten, gültigen Daten einzusehen und aus der Akte in ihre IT-Systeme zu übernehmen • selbst erhobene oder von Dritten (einschießlich des Patienten) empfangene medizinische Daten in eine Fallakte einzustellen • in eine Fallakte eingestellte Dokumente zu invalidieren
Fallaktenmanager	Der Fallaktenmanager ist die einzige Stelle, die auf eine Fallakte im gesperrten Zustand über ein gesondertes Verfahren zugreifen kann und dem gegenüber invalidierte Daten sichtbar sind. Des Weiteren kann der Fallaktenmanager bei Bedarf jederzeit die Löschung einer Fallakte durchführen. Zusätzlich besitzt er sämtliche Rechte eines EFA-Teilnehmers.
Patient (Versicherter)	Der Patient hat keinen Zugriff auf die Fallakte. Stattdessen kann er mit der Abgabe einer Einwilligungserklärung Fallaktenmanager und EFA-Teilnehmer zum Zugriff berechtigen. Das Recht zur Einholung einer Selbstauskunft bleibt davon unberührt.

2.6.1. Verantwortlihce Stelle

Als zentraler technischer Dienstleister sind die EFA-Provider der einzelnen Modellregionen verantwortlich für die Infrastruktur der Elektronischen Fallaktenkommunikation. Datenverantwortliche Stelle sind der Aktenanleger sowie alle weiteren auf die EFA berechtigten Teilnehmer. Diese sind gemeinsam verantwortlich. Dabei verbleibt die Verantwortung für eine auftragsgemäße und gesetzeskonforme Verarbeitung der Daten durch das Rechenzentrum Volmerstein bei dem einstellenden EFA-Teilnehmer. Neben natürlichen und juristischen Personen stehen auch die Hersteller in der Verantwortung zur ordnungsgemäßen Bereitstellung der Daten.

2.7. Datenschutzbezogene Anforderungen

2.7.1. Geeignetheit

Das hier vorliegende Datenverarbeitungsverfahren ist ein automatisiertes Vorgehen zur Speicherung, Verarbeitung und Bereitstellung notwendiger Information für an der Behandlung beteiligter Leistungserbringer. Die Zweckbestimmung einer EFA, welche die rechtzeitige Verfügbarkeit von medizinischen Behandlungsdaten für den interprofessionalen Austausch vorsieht, wird durch das Datenverarbeitungsverfahren

erfüllt. Im Sinne der lückenlosen Behandlungskette, werden die Informationen in einer EFA abgelegt und unter strengen Zugangsmechanismen für berechtigte EFA-Teilnehmer zur Verfügung gestellt.

2.7.2. Erforderlichkeit

Die Versorgung von Patienten bedarf einer umfangreichen Bandbreite von Informationen. Neben den persönlichen Stamm- und Gesundheitsdaten spielen außerdem die Sozial- und Eigenanamnese für die Versorgung eine große Rolle. Die Erfassung dieser Add-on-Information erweist sich häufig als zeitaufwendig und schwierig, sowohl für den Patienten als auch für den Arzt. Die zentrale Bereitstellung dieser Information ist somit nicht nur erforderlich, da viele verschiedene Professionen teilnehmen, sondern dient als Grundlage für weitere medizinische Therapieentscheidungen. Aufgrund dieser Anforderungen ist ein milderes Mittel zur Erreichung des beabsichtigten Zweckes nicht gegeben.

2.7.3. Verhältnismäßigkeit der Datenverarbeitung

Das Konzept der EFA fördert den angestrebten Zweck und bildet unter zeitlicher, datenschutzrechtlicher und logistischer Perspektive die zweckmäßigste Methode ab, bei der behandlungsrelevante Daten einer vordefinierten Behandlungsgruppe vollständig und zum richtigen Zeitpunkt bereitgestellt werden.

2.7.4. Grundsatz der Datenvermeidung und -sparsamkeit

Die EFA ist beschränkt auf einen bestimmten Zeitraum, welcher sich an einem klar abgegrenzten Behandlungsfall orientiert. Das bedeutet, dass nur für den Behandlungsprozess relevante Informationen zu diesem definierten Behandlungsfall in der EFA referenziert und zugänglich gemacht werden. Mittelfristig trägt die EFA zur Vermeidung der Doppeldokumentation bei, da eventuell benötigte Anamnesen, Diagnosen oder andere Daten bereits vorliegen und nicht erneut erhoben werden müssen. Unter dem Grundsatz "Qualität statt Quantität" sollen nur qualitätsgesicherte Daten bereitgestellt werden, die den medizinischen Behandlungsprozess maßgeblich darstellen und den Mit- und Weiterbehandlern entscheidungsrelevante Informationen bereithalten. In Anlehnung an die Rechtsvorgaben zur Dokumentations- und Nachweiszwecken müssen die beteiligten Leistungserbringer eventuelle Behandlungsdaten in ihre Primärdokumentation übernehmen.

2.7.5. Sperren, Löschen

Für die technische Umsetzung des Sperrens oder Löschens einer Akte sind die Provider verantwortlich. Generell werden die Daten auf Wunsch des Patienten, oder nach Ablauf der Zweckbindung gelöscht. Der genaue Löschprozess eines jeden Providers befindet sich bei den mitgeltenden Dokumenten.

2.7.6. Darstellung der Gewährleistungsziele/Schutzziele

2.7.6.1. Wahrung der Vertraulichkeit

Medizinische oder personenbezogene Daten, sowohl von Patienten als auch von Ärzten, dürfen nicht unerlaubt offenbart werden. Geschieht dies, ist die Vertraulichkeit des Systems verletzt.

Grundsätzlich gilt, dass die Mitarbeiter sowohl der medizinischen Einrichtungen als auch der technischen Betreiber auf die jeweils geltenden rechtlichen Vorgaben (z.B. Datengeheimnis, Fernmeldegeheimnis, §203 StGB) verpflichtet sind. Die Verpflichtung der einzelnen Mitarbeiter und Subunternehmer obliegt den einzelnen Einrichtungen.

Zur Sicherstellung der Vertraulichkeit wurden die folgenden Maßnahmen umgesetzt:

2.7.6.1.1. Allgemeine Maßnahmen

Nummer	Maßnahme
A.I	Schulung der EFA-Teilnehmer
A.II	Sichere Authentisierung der EFA-Teilnehmer
A.III	Ändern der Zugriffsberechtigungen einer EFA nur mit Einwilligung des Patienten möglich
A.IV	Eingrenzung der EFA-Teilnehmer auf nachprüfbar berechtigte
A.V	Zugriffsrechtemanagement
A.VI	Patientenaufklärung und Einwilligung
A.VII	Transportverschlüsselung
A.VIII	Verpflichtung der Provider und alle Subunternehmer auf das Datengeheimnis, Fernmeldegeheimnis sowie die Schweigepflicht nach §203 StGB
A.XVII	Generierung des Offline-Tokens mittels standardisierter UUID
A.XVIII	Authentifizierung von Patienten mittels amtlichen Lichtbildausweis bei Übergabe eines Offline-Tokens

2.7.6.1.2. Maßnahmen des RZV

Nummer	Maßnahme
R.I	Zutrittskontrollsysteme um unbefugten den Zutritt zu verhindern
R.II	Verschlüsselung der Hardware
R.III	Umsetzung eines Zugangssicherheitskonzepts
R.IV	Zugriff auf die Systeme nur durch kleinen Mitarbeiterkreis möglich
R.V	Umsetzung eines Konzepts zur Weitergabekontrolle
R.VI	Protokollierung der internen Zugriffe und striktes Einsetzen von Benutzeraccounts

2.7.6.1.3. Maßnahmen der FACT

Nummer	Maßnahme
F.I	Zutrittskontrollsysteme um unbefugten den Zutritt zu verhindern
F.II	Umsetzung eines Berechtigungskonzepts
F.III	Zugriff auf die Systeme nur durch mit dem jeweiligen Vorgang betrauten Mitarbeiter (Need-to-know-Prinzip)
F.IV	Umsetzung eines Konzepts zur Weitergabekontrolle
F.V	Protokollierung der internen Zugriffe

2.7.6.1.4. Maßnahmen der HITS

Nummer	Maßnahme
H.I	Zutrittskontrollsysteme um unbefugten den Zutritt zu verhindern
H.II	Umsetzung eines Berechtigungskonzepts
H.III	Zugriff auf die Systeme nur durch explizit berechtigten, kleinen Mitarbeiterkreis
H.IV	Umsetzung eines Konzepts zur Weitergabekontrolle
H.V	Externe Kommunikation über sichere VPN-Verbindungen
H.VI	Protokollierung der internen Zugriffe

2.7.6.2. Authentizität (Zurechenbarkeit)

Durch die Authentisierung des EFA-Teilnehmers beim EFA Provider wird ein Sicherheitskontext aufgebaut. Bei der Authentisierung werden die Benutzerdaten zur behaupteten Identität an den zentralen oder den KVC EFA ID Provider übergeben und geprüft. Durch diese Zugriffskontrolle können die eingestellten Dokumente, Aktualisierungen oder sonstige Datenzugriffe den berechtigten Leistungserbringern direkt zugeordnet werden. Änderungen in bereits bestehenden Dokumenten sind nicht möglich. Bei Aktualisierungen wird ein Vermerk mit den identifizierenden Attributen des Auslösers eingestellt.

2.7.6.2.1. Allgemeine Maßnahmen

Nummer	Maßnahme
A.I	Schulung der EFA-Teilnehmer

2.7.6.3. Integrität

Die Integrität der Daten sichert die Unveränderbarkeit und Zurechenbarkeit. Modifikationen von Daten müssen vom Anwender erkannt werden. In der EFA wird die Integrität auf verschiedenen Ebenen gewährleistet. Auf der Transport-Ebene durch die verwendeten sicheren Netzwerkprotokolle (TCP/IP, SSL), in der Applikations-Ebene durch die elektronischen Signaturen.

Zur Sicherstellung der Integrität wurden die folgenden Maßnahmen umgesetzt:

2.7.6.3.1. Allgemeine Maßnahmen

Nummer	Maßnahme
A.I	Schulung der EFA-Teilnehmer
A.VII	Transportverschlüsselung
A.IX	Dokumentierte Zuweisung von Berechtigung und Rollen
A.X	Verwendung sicherer Netzwerkprotokolle
A.XI	Protokollierung aller Zugriffe auf die Daten über einen Audit Trail

2.7.6.3.2. Maßnahmen des RZV

Nummer	Maßnahme
R.I	Zutrittskontrollsysteme um unbefugten den Zutritt zu verhindern
R.II	Verschlüsselung der Hardware
R.III	Umsetzung eines Zugangssicherheitskonzepts
R.IV	Zugriff auf die Systeme nur durch kleinen Mitarbeiterkreis möglich
R.VI	Protokollierung der internen Zugriffe und striktes Einsetzen von Benutzeraccounts

2.7.6.3.3. Maßnahmen der FACT

Nummer	Maßnahme
F.II	Umsetzung eines Berechtigungskonzepts
F.III	Zugriff auf die Systeme nur durch mit dem jeweiligen Vorgang betrauten Mitarbeiter (Need-to-know-Prinzip)
F.V	Protokollierung der internen Zugriffe

2.7.6.4. Verfügbarkeit

Bei der zeitlichen Verfügbarkeit ist die Priorität der Informationen im Hinblick auf die Entscheidungsfähigkeit der EFA-Teilnehmer entscheidend. So müssen die Daten zum richtigen Zeitpunkt, vollständig an der angeforderten Stelle zur Verfügung stehen. Für die Verfügbarkeit der Daten sind die jeweiligen technischen Betreiber der einzelnen Systeme verantwortlich.

Zur Sicherstellung der Verfügbarkeit wurden die folgenden Maßnahmen umgesetzt:

2.7.6.4.1. Maßnahmen des RZV

Nummer	Maßnahme
R.VII	Zertifizierung der Rechenzentren nach Trust Site Infrastructure (TSI), Level 3 und Level 2 durch die TÜV Informationstechnik GmbH
R.VIII	Zertifizierung nach ISO 27001, angestrebt für April 2019
R.IX	Automatisierte, in regelmäßigen Abständen stattfindende verschlüsselte Datensicherung
R.X	Dokumentation der Istzustände von Softwaresystemen, Rechner- und Netzwerkinfrastruktur, sodass diese von Dritten in akzeptabler Zeit verstanden werden können
R.XI	Notfall-/Wiederanlaufspläne für die wichtigsten Notfallszenarien
R.XII	Regelmäßige Test der Notfall-/Wiederanlaufspläne
R.XIII	Sicherung des LANs durch eine dreistufige, vom BSI zertifizierte Firewall gegen unerlaubte Zugriffe
R.XIV	Einsatz zweier unabhängiger, von einem jeweils anderen Hersteller entwickelten Virenscanner
R.XV	Generelle Umsetzung der Empfehlungen des BSI
R.XVI	Zeitnahes einspielen aktueller Updates für Betriebssysteme, Software und Hardware
R.XVII	Definierte Hardwarestandards um den laufenden Betrieb aufrechtzuerhalten
R.XVIII	Überwachung des LAN auf Funktionsfähigkeit und Performance

2.7.6.4.2. Maßnahmen der FACT

Nummer	Maßnahme
F.VI	Zertifizierung nach ISO 27001

F.VII	Automatisierte, in regelmäßigen Abständen stattfindende verschlüsselte Datensicherung
F.VIII	Notfall-/Wiederanlaufspläne für die wichtigsten Notfallszenarien
F.IX	Regelmäßige Test der Notfall-/Wiederanlaufspläne
F.X	Sicherung des LANs durch eine zertifizierte Firewall gegen unerlaubte Zugriffe
F.XI	Einsatz eines Virenscanners
~~F.XII~~	
F.XIII	Zeitnahes einspielen aktueller Updates für Betriebssysteme, Software und Hardware
F.XIV	Definierte Hardwarestandards um den laufenden Betrieb aufrechtzuerhalten
F.XV	Überwachung des LAN auf Funktionsfähigkeit

2.7.6.4.3. Maßnahmen der HITS

Nummer	Maßnahme
H.VII	Level 3-Zertifizierung des Rechenzentrums durch die TÜV Informationstechnik
H.VIII	Zertifizierung nach ISO 27001
H.IX	Automatisierte, in regelmäßigen Abständen stattfindende verschlüsselte Datensicherung
H.X	Dokumentation der Istzustände von Softwaresystemen, Rechner und Netzwerkinfrastruktur, sodass diese für Außenstehende verständlich ist.
H.XI	Notfall-/Wiederanlaufspläne für die wichtigsten Notfallszenarien
H.XII	Regelmäßige Test der Notfall-/Wiederanlaufspläne
H.XIII	Sicherung des LANs durch mehrstufige, vom BSI zertifizierte Firewall gegen unerlaubte Zugriffe
H.XIV	Einsatz von regelmäßig aktualisierten Virenscannern
H.XV	Zeitnahes einspielen aktueller Updates für Betriebssysteme, Software und Hardware
H.XVI	Definierte Hardwarestandards um den laufenden Betrieb aufrechtzuerhalten

H.XVII	Überwachung des LAN auf Funktionsfähigkeit und Performance
H.XVIII	Die Backup-Server sind aus Sicherheitsgründen in getrennten Brandabschnitten aufgestellt. Die Datenübertragung erfolgt verschlüsselt
H.XIX	Einlesen von DICOM-Daten wird programmseitig abgeglichen mit Patientendaten aus dem KIS und den auf den DICOM-Objekten vorhandenen Metadaten.

2.7.6.5. Zweckbindung, Nichtverkettung, Aufbewahrungsfristen

Die erhobenen medizinischen Daten einer EFA unterliegen einer konkreten Zweckbindung. Da jeder einzelne Datenzugriff und jede Übertragung anwenderorientiert protokolliert wird und verschlüsselt stattfindet, kann eine Zweckentfremdung auf diesem Weg ausgeschlossen werden.
Für die jeweiligen Einrichtungen ergeben sich die Aufbewahrungsfristen der in den einzelnen Prozessen anfallenden und verwendeten Daten aus den rechtlichen Vorgaben. Die Umsetzung der Einhaltung dieser Fristen mit anschließender Löschung obliegt der jeweiligen Einrichtung. Da die EFA selbst keine Primärdokumentation ist, werden sämtliche Daten fristgerecht durch das System gelöscht. Für die Umsetzung des Löschens sind die einzelnen Provider verantwortlich.

2.7.6.5.1. Allgemeine Maßnahmen

Nummer	Maßnahme
A.I	Schulung der EFA-Teilnehmer
A.XI	Protokollierung aller Zugriffe auf die Daten über einen Audit Trail
A.XII	Umsetzung eines Löschkonzepts
A.XIII	Zweckänderung einer EFA ist nicht zugelassen

2.6.6.6. Transparenz

Da Protokolldaten generell personenbezogene Daten enthalten sind diese im besonderen Maße Schützenswert und dürfen nur einem möglichst kleinen Benutzerkreis zur Verfügung stehen.

2.6.6.6.1. EFA

Die Gesundheitsdaten einer Akte genießen den höchsten Schutzbedarf. Deshalb ist es zwingend erforderlich sämtliche Zugriffe auf diese nachvollziehbar, überprüfbar, verständlich und rechtssicher nachweisen zu können.

Die Protokollierung jeder Anfrage an die EFA wird durch das Audit Trail and Node Authentication (ATNA) Profil sichergestellt. Dies ermöglicht es nachzuvollziehen, wann ein EFA-Teilnehmer auf welche Daten zugegriffen, sie geändert oder gar gelöscht hat.

2.6.6.6.2. KVC-Adapter

Um einen durchgängigen und zuverlässigen Betrieb gewährleisten zu können werden von dem Adapter bei jedem Nachrichteneingang die folgenden Angaben protokolliert:

- Datum und Zeitpunkt des Nachrichteneingangs
- Datum und Zeitpunkt des Nachrichtenausgangs
- ID des Senders (KV-Connect-Mailadresse)
- Nachrichten-ID (Message ID der Mail)

2.6.6.7. Validität

Für die Validität der Daten ist der einstellende EFA-Teilnehmer verantwortlich. Sie müssen darauf Achten, dass nur aktuelle, richtige und für den Fall benötigte Dokumente in eine EFA eingestellt werden.

Durch die Eingrenzung der EFA-Teilnehmer auf medizinisches Fachpersonal wird die Validität der Daten hergestellt.

2.6.6.7.1. Allgemeine Maßnahmen

Nummer	Maßnahme
A.I A	Schulung der EFA-Teilnehmer

2. 1. 2. Betroffenenrechte (Intervenierbarkeit)

Auch im Rahmen der Betroffenenrechte müssen bestimmte Einzelrechte des Patienten erfüllt sein/ werden. Der Patient kann sich zu jeder Zeit an jede von ihm berechtigte Person wenden. Alle Zugriffberechtigte sind gemeinsam Verantwortliche für die Datenverarbeitung.

2.1.2.1. Recht auf Benachrichtigung über die Datenerhebung

Die Datenerhebung erfolgt bereits vor dem Anlegen einer speziellen EFA für einen Patienten. Daher sind die EFA-Teilnehmer für eine eventuelle Benachrichtigung der Datenerhebung verantwortlich. Im Normalfall werden die Daten direkt persönlich bei dem betroffenen Patienten erhoben.

2.1.2.2. Recht auf Auskunft

Im Rahmen der informationellen Selbstbestimmung hat der Patient die Befugnis, jederzeit Einsicht in die gespeicherten Informationen zu erhalten. Dies muss in schriftlicher Form erfolgen. Jeder berechtigte EFA-Teilnehmer kann den Patienten die dokumentierten bzw. erhobenen Daten oder eine Kopie der vollständigen EFA zu Verfügung stellen.

2.1.2.3. Aushändigung einer Kopie der Daten

Durch integrierte Funktionen des Primärsystems oder dem Portal ist es den berechtigten EFA-Teilnehmern möglich sämtliche Dokumente einer bestimmten EFA

herunterzuladen und in das lokale Primärsystem zu übernehmen. Diese Daten können dann durch den EFA-Teilnehmer dem Patienten ausgehändigt werden.

2.1.2.4. Recht auf Datenübertragbarkeit (Migration der Daten)

Das normierte Recht auf Datenübertragbarkeit zielt darauf ab, personenbezogene Daten von einer verantwortlichen Stelle auf eine andere zu übertragen und damit den Schutz des freien Verkehrs personenbezogener Daten und der besseren Kontrolle zu Gunsten der Betroffenen zu erhöhen. Im Szenario muss demnach gewährleistet sein, dass die im PVS dokumentierten Daten über die Einstellung in die EFA auch in anderen Primärsystemen, z.B. im KIS, übertragen und richtig wiedergegeben werden. Eine möglichst einfache Weitergabe von Daten ist die Übertragung eines HL7 CDA-Dokumentes, welches sich auf einen Arztbrief, einen Befund oder auch auf Labordaten beziehen kann.

2.1.2.5. Recht zum Widerspruch bzgl. der Datennutzung

Eine mit der Patienteneinwilligung einhergehende Aufklärung des Patienten muss auch auf die Widerspruchsmöglichkeit des Patienten hinweisen. Dieser Widerspruch kann bei jedem berechtigten EFA-Teilnehmer der Akte erfolgen. Die gesamte Akte ist daraufhin aus dem System zu löschen.

2.1.2.6. Recht auf Berichtigung, Sperrung oder Löschung

Die Betroffenen haben das Recht auf unrichtige oder überholte Daten hinzuweisen und eine Berichtigung einzufordern. Die Korrektur wird im Rahmen eines Berichtigungsvermerks dokumentiert und dem Patienten mitgeteilt. Bereits bestehende Originaldokumente bleiben von der Berichtigung unberührt. Neben der Berichtigung hat der Betroffene auch die Möglichkeit, die Löschung der Akte zu fordern. Zudem müssen Daten zum Gesundheitszustand gelöscht werden, wenn deren Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann. Eine Sperrung der Daten bewirkt, dass diese Daten nur noch sehr eingeschränkt übermittelt oder genutzt werden dürfen. Fordert der Betroffene eine Löschung seiner Daten, welche jedoch gesetzlichen oder vertraglichen Gründen konfliktär entgegensteht, dann erfolgt nur die Sperrung dieser Daten.

2.1.2.7. Verpflichtung, Betroffene bzgl. Datenpannen zu informieren

Jede Verletzung des Schutzes personenbezogener Daten, die zu einem Risiko für die Rechte und Freiheiten einer natürlichen Person führt, muss an die zuständige Aufsichtsbehörde gemeldet werden. Entsprechend sind Meldungen an die Betroffenen innerhalb der gesetzlichen Meldefrist durchzuführen.
Für die Erstellung und Umsetzung eines Konzepts zur Gewährleistung der Verpflichtung sind die einzelnen Provider verantwortlich.

2.1.2.8. Anspruch auf Anrufung der Datenschutzkontrollinstanz

Betroffene, die vermuten, durch die Verarbeitung ihrer Daten in ihren Rechten verletzt worden zu sein, können sich an die zuständige Kontrollinstanz wenden. Diese Kontrollinstanz prüft diese Beschwerde und muss den Betroffenen über Ausgang und Ergebnis der Beschwerde unterrichten. Die zuständige Kontrollinstanz hängt von der

verarbeitenden Stelle ab. Werden die Daten von einer öffentlichen Stelle verarbeitet, sind die Bundesbeauftragte für den Datenschutz oder die Datenschutzbeauftragte der Länder zuständig. Bei der Verarbeitung durch nicht öffentliche Stellen, wie z.B. niedergelassene Hausarztpraxen sind die Aufsichtsbehörden der Länder (Vgl. Landesdatenschutzbeauftragte) zuständig. Es muss entsprechend ein Hinweis zu Verfügung stehen, dass dem Patienten oder, im Falle der Vertretungsvollmacht, dem gesetzlichen Betreuer Auskunft über die zuständige Kontrollinstanz gibt. Im Rahmen der Qualitätssicherung muss jede datenschutzverantwortliche Stelle einen Hinweis über den Ansprechpartner erhalten, sobald sie den Bedarf äußert.

2.1.2.9. Maßnahmen

Nummer	Maßnahme
A.XI	Protokollierung aller Zugriffe auf die Daten über einen Audit Trail
A.XII	Umsetzung eines Löschkonzepts
A.XIV	Einfache Einwilligungs- und Widerspruchsmöglichkeiten
A.XV	Einfaches Abrufen aller erhobenen Daten durch Portal
A.XVI	Umsetzung eines Notfallplans um betroffene zu Informieren

2. 2. Darstellung der Rechtskonformität

2. 2. 1. Rechtssicherheit der Datenverarbeitung

Alle Unterlagen und Dokumente, die in der EFA abgespeichert sind, dienen als Entscheidungsstütze und ermöglichen die zweckbezogene Weiterbehandlung des Patienten. Dazu muss aus dem Protokoll ersichtlich sein, welcher Arzt wann welche Informationen in welcher Form zu Verfügung gestellt hat. Unterzeichnete Dokumente wie z.B. Arztbriefe besitzen die Qualität einer Urkunde und können vor Gericht den vollen Beweiswert erreichen. Bei der Ablage der Daten in der EFA werden die einstellenden Ärzte über ihre eindeutigen Identifizierungsmerkmale erkannt und protokolliert. Hiermit ist sichergestellt das alle Aktivitäten in der EFA einer Person revisionsfähig zugeordnet werden können.

2. 2. 2. Revisionsfähigkeit

Bei der EFA werden Dokumente, bestehend aus verschiedenen Informationsobjekten, von unterschiedlichen Behandlern zu Verfügung gestellt. Um Änderungen festhalten zu können, wird im Rahmen des Protokolls eine Dokumentenhistorie geführt. Bereits eingestellte Dokumente können nicht ohne weiteres geändert werden. Jedoch kann ein Verweis auf ein aktuelleres Dokument, welches das alte Dokument ersetzt, angehängt werden. Dieser Verweis muss eindeutig und ersichtlich sein. Mit der Protokollierung wird festgehalten, wann die Aktualisierung bzw. das aktualisierte Dokument verfügbar war.

2. 2. 3. Nichtabstreitbarkeit

Wie im bereits beschrieben, werden alle Aktivitäten, die von Teilnehmer der EFA ausgehen, in der ATNA-Komponente beim EFA-Provider protokolliert. So werden auch

Dateneingaben mit Uhrzeit und Datum festgehalten. Ab diesem Zeitpunkt stehen die Dokumente allen berechtigten Anwendern zu Verfügung. Die Bereitstellung der Dokumente kann also sowohl von Seiten der Sender als auch von Empfängerseite nicht bestritten werden.
Weiterführende Informationen finden Sie in der EFA 2.0 Spezifikation.

2. 3. Konzeptuelle Risikobetrachtung

2. 3. 1. Risiken der Vertraulichkeit

Erlangt jemand unerlaubt persönliche- oder Gesundheitsdaten durch das System ist die Vertraulichkeit verletzt. Durch die Architektur der EFA ergeben sich folgende Angriffspunkte auf die Vertraulichkeit der Daten:

Risiko	Eintritts-wahrscheinlichkeit	Schadens-klassifizierung	Maßnahmen
1. Ein Angreifer übernimmt die Identität einer autorisierten Person. Das System akzeptiert diesen als berechtigten EFA-Teilnehmer und gewährt Zugriff auf Daten.	Niedrig	Hoch	A.I, A.II, A.IV, A.V, A.VII, A.IX, R.I, R.II, R.III, R.VI F.I, F.II, F.III, F.V H.I, H.II, H.III, H.IV, H.V, H.VI
2. Berechtigungen einer Akte werden falschen EFA-Teilnehmern zugeordnet beziehungsweise sie erschleichen sich diese.	Mittel	Mittel	A.I, A.II, A.IV, A.V, A.VII, A.IX R.I, R.II, R.III, R.VI F.I, F.II, F.III, F.V H.I, H.II, H.III, H.IV, H.VI
3. Ein Angreifer manipuliert die Kommunikation zwischen den Systemen.	Mittel	Hoch	A.VII. A.X R.IV, R.VI F.II, F.III, F.V H.II, H.III, H.VI
4. Ein Angreifer hört die Kommunikation zwischen den Systemen ab.	Hoch	Mittel	A.VII. A.X R.IV, R.VI F.II, F.III, F.V H.II, H.III, H.V, H.VI

5. Mitarbeiter der Provider greifen unerlaubt auf die Daten zu.	Mittel	Hoch	A.VII, A.VIII, A.XII R.I, R.II, R.III, R.IV, R.V, R.VI, R.VII, R.VIII F.I, F.II, F.III, F.IV, F.V H.I, H.II, H.III, H.IV, H.VI, H.VII, H.XII
6. Ein Angreifer erlangt Zugriff auf die Protokolldateien und kann daraus auf geschützte Informationen zurückschließen.	Mittel	Niedrig	A.VIII, A.X, A.XII R.I, R.II, R.III, R.IV, R.V, R.VI F.I, F.II, F.III, F.IV, F.V H.I, H.II, H.III, H.IV, H.V,H.VI, H.VII, H.VIII, H.XIII
7. Gesundheitsdaten eines Patienten werden in die EFA eines anderen Patienten eingestellt und so unbefugten offenbart	Mittel	Mittel	A.I, A.III, A.IV, A.VI, A.IX, A.XI H.XIX
8. MPI-Patienten sind dem falschen Referenzpatienten zugeordnet. Ihre Daten werden dadurch einem anderen als dem vom Patienten berechtigten Personenkreis zugänglich.	Mittel	Niedrig	A.I
9. Ein berechtigter EFA-Teilnehmer gibt unerlaubt Dokumente an unberechtigte weiter.	Niedrig	Mittel	A.I, A.XI
10. Berechtigungen einer Akte werden falschen EFA-Teilnehmern zugeordnet.	Mittel	Niedrig	A.I, A.III, A.IV, A.V, A.VI, A.IX

11. Ein Teilnehmer versucht durch Brute-Force ein Offline-Token zu erraten um unberechtigterweise an Daten eines Patienten zu gelangen.	Niedrig	Mittel	A.I, A.IV, A.V, A.IX, A.XVII
12. Ein Patient versucht durch einen Offline-Token, der nicht zu seiner persönlichen Akte führt, sondern auf eine fremde an fremde Unterlagen zu gelangen.	Niedrig	Mittel	A.I, A.XVIII

2. 3. 2. Risiken der Integrität

Durch falsche oder gelöschte Informationen können dem Patienten Schäden entstehen. Es ist daher zu gewährleisten, dass die Integrität der Daten sichergestellt wird.

Ein Teil der Angriffspunkte der Vertraulichkeit trifft auch auf die Integrität zu:

Risiko	Eintritts-wahrscheinlichkeit	Schadens-klassifizierung	Maßnahmen
1. Ein Angreifer übernimmt die Identität einer autorisierten Person. Das System akzeptiert diesen als berechtigten EFA-Teilnehmer und gewährt Zugriff auf Daten.	Niedrig	Hoch	A.I, A.II, A.IV, A.V, A.VII, A.IX, R.I, R.II, R.III, R.VI F.I, F.II, F.III, F.V H.I, H.II, H.III, H.IV, H.V, H.VI
2. Berechtigungen einer Akte werden falschen EFA-Teilnehmern zugeordnet beziehungsweise sie erschleichen sich diese.	Mittel	Mittel	A.I, A.II, A.IV, A.V, A.VII, A.IX R.I, R.II, R.III, R.VI F.I, F.II, F.III, F.V H.I, H.II, H.III, H.IV, H.VI

3. Ein Angreifer manipuliert die Kommunikation zwischen den Systemen.	Mittel	Hoch	A.VII. A.X R.IV, R.VI F.II, F.III, F.V H.II, H.III, H.VI
7. Gesundheitsdaten eines Patienten werden in die EFA eines anderen Patienten eingestellt und so unbefugten offenbart	Mittel	Mittel	A.I, A.III, A.IV, A.VI, A.IX, A.XI H.XIX
8. MPI-Patienten sind dem falschen Referenzpatienten zugeordnet. Ihre Daten werden dadurch einem anderen als dem vom Patienten berechtigten Personenkreis zugänglich.	Mittel	Niedrig	A.I
10. Berechtigungen einer Akte werden falschen EFA-Teilnehmern zugeordnet.	Mittel	Niedrig	A.I, A.III, A.IV, A.V, A.VI, A.IX

Des Weiteren müssen folgende Gefährdungen zusätzlich betrachtet werden:

Risiko	Eintritts-wahrscheinlichkeit	Schadens-klassifizierung	Maßnahmen
13. Daten werden fehlerhaft übertragen oder bei dem Provider fehlerhaft gespeichert.	Niedrig	Hoch	A.VII, A.X, A.XI R.IX F.VII H.IX
14. Inkonsistenzen in Metadaten oder falsch übernommene Änderungen dieser Daten können insbesondere in Zusammenhang mit Such- und Filteroperationen zu einer unvollständigen Anzeige von Fallakten führen.	Niedrig	Hoch	A.VII, A.X, A.XI R.IX F.VII H.VIII
15. Ein berechtigter EFA-Teilnehmer verändert	Mittel	Mittel	A.I, A.V, A.XI, A.XII

Datenbestände nachträglich.			
16. Ein Patient gibt sich als jemanden fremdes aus und verlangt eine Kopie der Daten oder die Löschung aus der Akte.	Mittel	Hoch	A.XVIII

2. 3. 3. Risiken der Verfügbarkeit

Steht das System nicht angemessen zur Verfügung, ist die Verfügbarkeit gefährdet. Dies geschieht übelicherweise durch organisatorische oder technische Mängel, Fehlhandlungen oder Vorsatz. Das Abrufen und Einstellen neuer Dokumente ist dann nicht weiter möglich:

Risiko	Eintritts-wahrscheinlichkeit	Schadens-klassifizierung	Maßnahmen
17. Ein Patient gibt sich als jemanden fremdes aus und verlangt die Löschung der Akte.	Mittel	Hoch	A.XVIII
18. Verlust von Daten durch technische oder organisatorische Mängel.	Mittel	Hoch	R.I, R.II, R.VII, R.VIII, R.IX, R.X, R.XI, R.XII, R.XIII, R.XIV, R.XV, R.XVI, R.XVII, R.XVIII F.I, F.III, F.V, F.VI, F.VII, F.VIII, F.IX, F.X, F.XI, F.XII, F.XIII, F.XIV, F.XV H.I, H.III, H.V, H.VII, H.VIII, H.IX, H.X, H.XI, H.XII, H.XIIIH.XIV, H.XV, H.XVI, H.XVII, H.XVIII

19. Verlust von Daten durch Ereignisse der höheren Gewalt.	Mittel	Hoch	R.I, R.II, R.VII, R.VIII, R.IX, R.X, R.XI, R.XII, R.XIII, R.XIV, R.XV, R.XVI, R.XVII, R.XVIII F.I, F.III, F.V, F.VI, F.VII, F.VIII, F.IX, F.X, F.XI, F.XII, F.XIII, F.XIV, F.XV H.I, H.III, H.VI, H.VII, H.VIII, H.VII, H.XII, H.IX, H.X, H.XI, H.XII, H.XIII, H.XIV, H.XV, H.XVI, H.XVII, X.XVIII

2. 4. Schutzbedarfe

Gesundheitsdaten von Patienten sowie deren personenbezogenen Stammdaten genießen zu jeder Zeit den höchsten Schutzbedarf. Die EFA eines Patienten dient ausschließlich zur bidirektionalen Kommunikation zwischen Ärzten und Einrichtungen und nicht zur Primärdokumentation. In jeder EFA eines Patienten wird durch ein Consent Document beschrieben welcher Teilnehmer Zugriff auf diese Akte besitzt. Dadurch erhalten nur berechtigte Teilnehmer Zugriff auf eine EFA. Die Zugriffe werden ebenfalls durch die EFA protokolliert. Durch den Zugriff der Projektteilnehmer mittels der verwendeten Primärsysteme wird deren höchster Schutzbedarf ohne Einschränkungen auf die EFA angewandt. Die einzelnen Maßnahmen der jeweiligen Konsortialpartner sind in deren Datenschutz- und IT-Sicherheitskonzeptionen beschrieben.

2. 5. Löschkonzept

Jeder Provider einer EFA ist für das datenschutzkonforme Löschen der personenbezogenen- und Gesundheitsdaten verantwortlich. Zu diesem Zweck wurden Löschkonzepte erarbeitet, die bei den mitgeltenden Dokumenten zu finden sind.

3. Regionale Datenverarbeitung

3. 1. Borken / Ahaus

3. 1. 1. Ziele

In der Modellregion Borken/Ahaus/Vreden (Westmünsterland) werden im Rahmen der einzuführenden Geriatrie-Akte Daten erfasst und zwischen den berechtigten Leistungserbringern auf elektronischem Weg kommuniziert. Die Geriatrie-Akte adressiert dabei keine bestimmte Krankheit, sondern ein spezifisches Patientenklientel. Besonders relevant sind in der Region Westmünsterland die Erkrankungsbilder Demenz, Herzinsuffizienz, Hypertonus sowie Diabetes Mellitus.

Der geriatrische Patient definiert sich durch ein höheres Lebensalter und eine geriatrietypische Multimorbidität (vgl. Deutsche Gesellschaft für Geriatrie e.V.). Aufgrund dieser Eigenschaften zählen geriatrische Patienten auch als vulnerable Gruppe. Infolge des teils hohen Lebensalters und/oder der vorherrschenden Erkrankung/en sind geriatrische Patienten häufig nicht mehr in der Lage, alle für eine sichere und bestmögliche Behandlung notwendigen Informationen den Leistungserbringern selbst zu übermitteln. Aus diesem Grund ermächtigt der Patient seine behandelnden Ärzte und Einrichtungen, auf seine Fallakte zuzugreifen, mit dem Zweck, darüber fallbezogen zu kommunizieren.

Aktuell erfolgt die sektorübergreifende Kommunikation in der betrachteten Region noch weitgehend papierbasiert. Dabei erfolgt die Datenerfassung sowohl auf ambulanter Seite als auch auf stationärer Seite im Krankenhaus bereits in einem elektronischen Primärsystem.

In der Modellregion gibt es bereits das Gesundheitsnetzwerk GG.WML (*Gesundheits-netzwerk GEMEINSAM Westmünsterland*). Das Gesundheitsnetzwerk ist ein Zusammenschluss von Haus- und Fachärzten aus Praxis, MVZ und Klinik sowie niedergelassenen Psychotherapeuten in Kooperation mit weiteren nichtärztlichen Leistungserbringern im Gesundheitswesen. Hierzu zählen u. a. ambulante und stationäre Pflegeeinrichtungen, Physiotherapeuten und Ergotherapeuten zur interdisziplinären, kooperativen und effizienteren medizinischen Betreuung und Behandlung der Patienten. Mit dem Ziel, dem Patienten eine kontinuierliche medizinische Versorgung, von der Prävention/Vorsorge bis hin zur Nachsorge, sicherzustellen. Aufgrund der sehr heterogenen Leistungserbringerstruktur und der teils langen Behandlungsphasen kommt es häufig zu einem vermehrten Kommunikationsaustausch, welcher derzeit noch größtenteils papierbasiert abläuft.

Die Vermischung von papierbasierter und elektronischer Datenverarbeitung birgt die Gefahr von Medienbrüchen mit Auswirkungen auf die Patientensicherheit. Zudem bedeutet der papierbasierte Versand der Behandlungsdokumentation einen erheblichen Zeitverlust mit möglicher Weise drastischen Auswirkungen auf das Patientenwohl.

Das Konzept der Fallaktenkommunikation ist eine Datenaustauschplattform, welche in diesem Szenario u.a. die folgenden Ziele verfolgt:

- Case Management: Professions- und sektorübergreifende Kommunikation und Kooperation zwischen Leistungserbringern zur zeitsparenden Datenübermittlung im Sinne einer optimalen Versorgung des Patienten unter Vermeidung von Medienbrüchen
- Vorsorge im Verdachtsfall einer beginnenden degenerativen Erkrankung

- Konsultationen/Expertenaustausch bei unklaren Befunden oder umfangreichen Therapiemaßnahmen
- Vermeidung von Kontraindikationen und Wechselwirkungen
- Vermeidung von Mehrfachuntersuchungen
- Steigerung der Patientensicherheit durch abgestimmte Dokumentation und Informationsweitergabe
- Schutz vulnerabler Gruppen (geriatrisches Klientel)

3. 1. 2. Zu verarbeitende Daten

3. 1. 2. 1. Daten / Datenklassen

Jede EFA besteht aus mehreren personenbezogenen-, größtenteils Gesundheitsdaten eines bestimmten Patienten zu einem spezifischen Behandlungsfall.

In der nachfolgenden Tabelle finden Sie eine Auflistung der Datenklassen einer EFA in der Geriatrie-Akte für die Modellregion Westmünsterland.

Datenklassen und Informationsobjekte im Versorgungsszenario Geriatrie-Akte	
Personenbezogene Daten (Basisdatensatz eines Patienten, um ihn innerhalb der EFA zu identifizieren)	• Name • Anschrift • Geburtsort/-Datum • eGK-Nummer
Weitere personenbezogene Daten des Patienten	• Familienstand • Adresse • (Notfall-)Kontakt
Gesundheitsdaten (Datensätze einer spezifischen EFA zu einer bestimmten Person)	• Arztbriefe • Befunde (Labor, Bildgebung, Funktionsdiagnostik) • Arzneimittel / Medikationsplan • Heil-/Hilfsmittel • Veranlasste Verordnungen • Assessment (Geriatrie) • Sozial- und Pflegeanamnese • Pflegestufeneinordnung • Dokumentierter Patientenwille • Krankenhaus-/ Reha-/ Kurzzeitpflegeaufenthalte • Protokolle (Fallbesprechungsprotokoll, Info-Transfer-Bogen) • *Behandler/Teilnehmer am*

	Patientenfall (Einwilligung)

Weitere Daten bzw. Datenklassen können mit der Fortentwicklung des Versorgungsszenarios bzw. auf der Basis des individuellen Ermessens der behandelnden Akteure hinzukommen.

3. 1. 2. 2. Speichern der Daten

Da die Versorgung von geriatrischen Patienten in der Regel über einen längeren Zeitraum stattfindet, kann der Fallakte in dieser Modellregion eine Laufzeit von bis zu fünf Jahren zugeordnet werden. Soll die Fallakte nach den 5 Jahren weiterhin Bestand haben, muss einer der Berechtigten die Gültigkeitsdauer verlängern. Gespeichert werden sämtliche Daten bei dem Provider RZV Rechenzentrum Volmarstein GmbH, Grundschötteler Str. 21, 58300 Wetter (Ruhr).

3. 2. Dortmund

3. 2. 1. Rahmenbedingungen und Ziele

3. 2. 1. 1. Rahmenbedingungen

In der Modellregion Dortmund wird die elektronische Fallakte im Rahmen der Kommunikation zwischen Kinder- und Jugendärzten aus verschiedenen Einrichtungen und Sektoren genutzt. Involviert sind sowohl niedergelassene Pädiaterinnen und Pädiater als auch Ärzte aus der Kinder- und Jugendklinik und der Klinik für Kinderchirurgie der Kliniken der Städtischen Kliniken Dortmund (Klinikum Dortmund).

Die Kommunikation mittels der elektronischen Fallakte bezieht sich dabei auf pädiatrische Patientinnen und Patienten – also Kinder und Jugendliche bis zur Vollendung des 18. Lebensjahrs. In bestimmten Fällen werden durch die Pädiatrie auch junge Erwachsene versorgt, so dass auch ihre Daten mittels elektronischer Fallakte unter den versorgenden Akteuren kommuniziert werden. Die sogenannten Pädiatrieakten sind dabei grundsätzlich indikationsunabhängig angelegt.

Im regulär / vor der Erprobungsphase von I/E Health erfolgt die sektoren- und einrichtungsübergreifende Kommunikation unter den oben genannten Akteuren auf zwei Wegen. Grundsätzlich werden Informationen papierbasiert ausgetauscht. Eine kleinere Gruppe, die auch hier die Gruppe der Akteure in der Erprobungsphase stellt, nutzt bereits den Kommunikationsweg über eine elektronische Fallakte. Dabei ist die Kommunikationsrichtung immer von Klinikum Dortmund in Richtung der pädiatrischen Praxen. Übermittelt wird zunächst lediglich der Arztbrief.

Die Erhebung der Daten erfolgt in beiden Fällen in den einzelnen Einrichtungen; die Erfassung dementsprechend in elektronischer Form in den einzelnen Primärsystemen (Praxisverwaltungssystem bzw. Krankenhausinformationssystem). Die Rechtsgrundlage ist die freiwillige Einwilligung des Patienten (vgl. Punkt 2.2).

3. 2. 1. 1. Ziele

Mit der elektronischen Fallakte wird der Prozess der einrichtungsübergreifenden Kommunikation von Daten/Dokumenten unabhängig vom individuell genutzten Primärsystem (PVS, KIS) digital unterstützt. Mittelfristige wird die Substitution der papierbasierten Kommunikation und daraus resultierend die schnellere und umfassende Verfügbarkeit von Behandlungsinformationen für alle am Behandlungsprozess beteiligten Akteure angestrebt.

Ziel der Umsetzung von I/E Health in der Modellregion Dortmund ist es, die Kommunikation über den Arztbrief hinaus auf weitere Informationen und Dokumente(-ntypen) auszuweiten und somit die papierbasierte Kommunikation unter den beteiligten Akteuren vollständig zu ersetzen. Weiterhin soll die Kommunikation in alle Richtungen erfolgen können, so dass Informationen auch durch die pädiatrischen Praxen in der Akte zur Verfügung gestellt werden können.

Die Kommunikation über Pädiatrieakte kann dabei zwei unterschiedliche Zwecke erfüllen: (1) Auf der einen Seite kann die Akte genutzt werden, um im Kontext eines geplanten oder ungeplanten stationären Aufenthalts Dokumente und Informationen sowohl im Vorfeld der Aufnahme als auch nach der Entlassung den jeweils nachsorgenden Akteuren zur Verfügung zu stellen. (2) Auf der anderen Seite kann die Akte für längerfristige Erkrankungen verwendet werden, bei denen eine Versorgung durch mehrere Institutionen gewährleistet werden muss. Bei der letzteren ist intendiert, mehreren Akteuren – unabhängig von Zeitpunkt ihrer Zugriffsberechtigung – einen Zugang zu den in der Akte gesammelten Dokumenten und somit einen umfassenden Überblick über die Krankheitsgeschichte und den Krankheits- und Versorgungsverlauf des Patienten zu geben.

Weiterhin wird angestrebt, nach der Phase der Erprobung, weitere Akteure für die Nutzung der elektronischen Fallakte hinzuzugewinnen. Dies betrifft zum einen weitere Kinder- und Jugendärzte, die an der Kommunikation über die Pädiatrieakte partizipieren. Es betrifft aber auch weitere Fachrichtungen. Aus dem Klinikum Dortmund heraus wird angestrebt, die Kommunikation mit einrichtungsexternen Akteuren in den jeweiligen Versorgungsketten auch auf weitere Kliniken zu übertragen.

3. 2. 2. Zu verarbeitende Daten

3. 2. 2. 1. Daten / Datenklassen

In der Grundidee werden elektronische Fallakten mit verschiedenen personenbezogenen Daten und Gesundheitsdaten eines bestimmten Patienten zu einem spezifischen Behandlungsfall gefüllt. Diese Dokumente werden als Informationsobjekte bezeichnet.

In der nachfolgenden Tabelle finden Sie eine Auflistung der häufigsten Datenklassen, die in der Modellregion Dortmund kommuniziert werden.

Datenklassen und Informationsobjekte im Versorgungsszenario Demenz-Akte	
Personenbezogene Daten (Basisdatensatz eines Patienten	• Name

um ihn innerhalb der EFA zu identifizieren)	• Anschrift • Geburtsort/-Datum • eGK-Nummer
Gesundheitsdaten (Datensätze einer spezifischen EFA zu einer bestimmten Person)	• Verlauf, Schwere und Dauer der Erkrankungen • Vorerkrankungen/Allergien • Ablauf und Inhalt medizinischer Behandlungen durch Ärzte, Krankenhäuser und medizinische Hilfsdienste/Epikrise • Arztbriefe • Therapieempfehlung • Arzneimittel und Medikationsplan • Heil-/Hilfsmittel • Veranlasste Verordnungen • Sonstige Therapie • Sozialanamnese • Pflegestufeneinordnung • Dokumentierter Patientenwille • Behandelnde Ärzte • Krankenhaus-/ Reha-/ Kurzzeitpflegeaufenthalte der letzten 12 Monate • Aufnahme- und Entlassdatum

Weitere Daten bzw. Datenklassen können mit der Fortentwicklung des Versorgungsszenarios bzw. auf der Basis des individuellen Ermessens der behandelnden Akteure hinzukommen.

3. 2. 2. 2. Speichern der Daten

Die Laufzeit der Fallakte soll entsprechend der beiden unterschiedlichen Nutzungszwecke unterschiedlich angelegt sein. Bei einer Nutzung, die lediglich auf die Kommunikation im Rahmen der Überleitung von einer Einrichtung hin zu einer anderen (und ggf. wieder zurück) wird von einer Laufzeit von drei Monaten ausgegangen. Eine Verlängerung der Laufzeit im Bedarfsfall ist durch die versorgenden Akteure jederzeit möglich.

Da die Versorgung durch verschiedenen Akteure in pädiatrischen Kontexten aber auch über längere Zeiträume notwendig werden kann (z.B. bei chronischen Erkrankungen) , kann in diesen Fällen eine Laufzeit von bis zu fünf Jahren zielführend sein. Soll die Fallakte nach den 5 Jahren weiterhin Bestand haben, muss einer der Berechtigten die Gültigkeitsdauer verlängern.

Gespeichert werden sämtliche Daten bei dem Provider RZV Rechenzentrum Volmarstein GmbH, Grundschötteler Str. 21, 58300 Wetter (Ruhr).

3. 3. Düren / Aachen

3. 3. 1. Notfall-/Pflegeakte (NPA)

3. 3. 1. 1. Ziele

In der Modellregion Düren / Aachen werden im Rahmen der einzuführenden Notfall-/Pflegeakte Patientendaten zwischen den berechtigten Leistungserbringern auf elektronischem Wege kommuniziert. Die Akte adressiert dabei keine bestimmte Krankheit, sondern ein spezifisches Patientenklientel. Dabei handelt es sich um Patienten, die aufgrund ihres Alters bzw. Vorliegen anderer Gründe im Pflegeheim versorgt werden.

Für Patienten, die eine hohe Multimorbidität aufweisen und bei denen damit gerechnet werden muss, dass diese abends, nachts bzw. am Wochenende notfallmäßig im Krankenhaus versorgt werden müssen, legt der das Pflegeheim betreuende Hausarzt präventiv eine Notfall-/Pflegeakte an (und hält diese immer aktuell) und generiert einen sog. Offline-Token, der im Pflegeheim aufbewahrt wird. Bei einem eintretenden Notfall wird dem Patienten (bzw. dem Notarzt im Rettungswagen) dieser Token mitgegeben. In der Notaufnahme können die behandelnden Ärzte mit diesem Token auf die angelegte Notfall-/Pflegeakte zugreifen. Somit stehen die personenbezogenen Daten wie auch die aktuellen Gesundheitsdaten bereits bei Aufnahme des Patienten den behandelnden Ärzten und Einrichtungen, den Fallaktennutzern, zur Verfügung.

Aktuell erfolgt keine elektronische, sektorübergreifende Kommunikation. Dabei erfolgt die Datenerfassung sowohl auf ambulanter als auch stationärer Seite bereits in einem elektronischen Primärsystem.

Mit dieser Art der intersektoralen Kommunikation werden daher folgende Ziele verfolgt:

- Professions- und sektorübergreifende Kommunikation und Kooperation zwischen Leistungserbringern zur zeitsparenden Datenübermittlung im Sinne einer optimalen Versorgung des Patienten unter Vermeidung von Medienbrüchen
- Vermeidung von Kontraindikationen und Wechselwirkungen
- Steigerung der Patientensicherheit durch abgestimmte Dokumentation und Informationsweitergabe.

3. 3. 1. 2. Zu verarbeitende Daten

3. 3. 1. 2. 1. Daten / Datenklassen

Jede Notfall-/Pflegeakte besteht aus mehreren personenbezogenen, größtenteils Gesundheitsdaten eines bestimmten Patienten.

In der nachfolgenden Tabelle finden Sie eine Auflistung der Datenklassen:

Datenklassen und Informationsobjekte im Versorgungsszenario Demenz-Akte	
Personenbezogene Daten (Basisdatensatz eines Patienten	• Name • Anschrift • Geburtsort/-Datum

um ihn innerhalb der EFA zu identifizieren)	• eGK-Nummer
Weitere personenbezogene Daten	• Kontaktdaten im Notfall • Adresse • Patientenverfügung • Name des Pflegeheims
Gesundheitsdaten (Datensätze einer spezifischen EFA zu einer bestimmten Person)	• Diagnosen (Aktuelle und Dauerdiagnosen) • Infektionen • Medikation (Aktuelle und Dauermedikation) • Allergien / Intoleranzen • Ergebnisse aktueller relevanter Vorbefunde (Komorbitäten, ggf. Hilfsmittel) • Aktuelle medizinische Probleme (Labordaten)

3. 3. 1. 2. 2. Speichern der Daten

Da die Versorgung von Patienten aus dem Pflegeheim in der Regel über einen längeren Zeitraum stattfindet, kann der Notfall-/Pflegeakte in dieser Modellregion eine Laufzeit von bis zu fünf Jahren zugeordnet werden. Soll die Fallakte nach den 5 Jahren weiterhin Bestand haben, muss einer der Berechtigten EFA-Teilnehmer die Gültigkeitsdauer verlängern. Gespeichert werden sämtliche Daten bei dem Provider Healthcare IT Solutions GmbH (HITS), Pauwelsstr. 30, 52074 Aachen.

3. 3. 2. Überleitungsakte

3. 3. 2. 1. Ziele

In der Modellregion Düren / Aachen werden im Rahmen der einzuführenden Überleitungsakte Patientendaten zwischen den berechtigten Leistungserbringern auf elektronischem Wege kommuniziert. Die Akte adressiert dabei keine bestimmte Krankheit, sondern ein spezifisches Patientenklientel, bei denen damit zu rechnen ist, dass sie im Urlaubsfall des Arztes behandelt werden müssen. Dabei handelt es sich insbesondere um multimorbide Patienten. Diese erwarten, dass eine Vertreterpraxis die für ihre optimale Weiterbehandlung notwendigen Kenntnisse über die aktuellen Behandlungsdaten der zu vertretenden Praxis abrufen kann.

Der zu vertretende Arzt wählt Patienten aus, bei denen mit einer Vertretungssituation zu rechnen ist und legt für diese die Überleitungsakte an. Die medizinisch-inhaltlichen Angaben in der Überleitungsakte beziehen sich auf den konkreten Vertretungsfall. Der Arzt entscheidet über die notwendigen

medizinisch relevanten Angaben (Minimalangaben zu Dauerdiagnosen, Medikation und Cave-Hinweisen werden jedoch empfohlen).

Somit stehen die personenbezogenen Daten wie auch die aktuellen Gesundheitsdaten bereits im Vorfeld dem behandelnden Vertreterarzt zur Verfügung und der Patient muss diese nicht vorhalten.

Aktuell erfolgt keine elektronische Kommunikation untereinander. Dabei erfolgt die Datenerfassung auf ambulanter Seite bereits in einem elektronischen Praxisverwaltungssystem.

Mit dieser Art der Kommunikation werden daher folgende Ziele verfolgt:

- Kommunikation und Kooperation zwischen Leistungserbringern zur zeitsparenden Datenübermittlung im Sinne einer optimalen Versorgung des Patienten unter Vermeidung von Medienbrüchen
- Vermeidung von Kontraindikationen und Wechselwirkungen
- Steigerung der Patientensicherheit durch abgestimmte Dokumentation und Informationsweitergabe.

3. 3. 2. 2. Zu verarbeitende Daten

3. 3. 2. 2. 1. Daten / Datenklassen

Jede Überleitungsakte besteht aus mehreren personenbezogenen, größtenteils Gesundheitsdaten eines bestimmten Patienten. Diese Dokumente werden als Informationsobjekte bezeichnet.

Datenklassen und Informationsobjekte im Versorgungsszenario Demenz-Akte	
Personenbezogene Daten (Basisdatensatz eines Patienten um ihn innerhalb der EFA zu identifizieren)	• Name • Anschrift • Geburtsort/-Datum • eGK-Nummer
Weitere personenbezogene Daten	• Adresse • Kontaktdaten im Notfall • Patientenverfügung
Gesundheitsdaten (Datensätze einer spezifischen EFA zu einer bestimmten Person)	• Diagnosen (Aktuelle und Dauerdiagnosen) • Infektionen • Medikation (aktuelle und Dauermedikation) • Allergien / Intoleranzen • Ergebnisse aktueller relevanter Vorbefunde (Komorbiditäten, ggf. Hilfsmittel) • Aktuelle medizinische Probleme (Labordaten)

3. 3. 2. 2. 2. Speichern der Daten

Da die Versorgung von multimorbiden Patienten im Rahmen der Vertretungsakte nur für die Dauer der Abwesenheit des betreuenden Hausarztes stattfindet, wird nach Ablauf der Vertretungszeit – spätestens jedoch nach 12 Wochen – die betreffende Überleitungsakte gelöscht. Gespeichert werden sämtliche Daten bei dem Provider Healthcare IT Solutions GmbH (HITS), Pauwelsstr. 30, 52074 Aachen.

3. 3. 3. Gastro-Onkologie-Akte

3. 3. 3. 1. Ziele

In der Modellregion Düren / Aachen werden im Rahmen der einzuführenden Gastro-Onkologie-Akte Daten zu Patienten zwischen den berechtigten Leistungserbringern auf elektronischem Wege kommuniziert. Die Akte adressiert dabei Patienten, bei denen ein Tumor im Gastrointestinaltrakt als „gesichert“ bzw. „Verdacht auf“ diagnostiziert wurde, da der Behandlungsprozess erheblich durch die Lokalisation des Tumors (Magen, Speiseröhre, Kolon, Pankreas, etc.) wie auch durch das Histologie-Ergebnis beeinflusst wird.

Für Patienten, bei denen eine gesicherte Diagnose festgestellt wurde, legt der Facharzt eine entsprechende Akte an und benennt, je nach Diagnosestellung, direkt das Behandlerteam. Der Facharzt legt somit von Beginn die einzelnen Berechtigungen auf die Akte fest; er fungiert hierbei grundsätzlich als Gatekeeper und Fallaktenanleger. Stellt ein Hausarzt die Verdachtsdiagnose „Magen-CA“, kann er ebenfalls eine Gastro-Onkologie-Akte anlegen mit dem deutlichen Hinweis auf die Verdachtsdiagnose in der Akte und dem Vermerk „Fallakte vorsorglich“. Er informiert den Patienten über die Anlage der Akte und überweist den Patienten an den Facharzt. Zu diesem Zweck generiert der Hausarzt den sog. Offline-Token. Die weitere Diagnosestellung folgt dann beim Facharzt, der auch die Gatekeeper-Funktion übernimmt. Auch das Krankenhaus kann eine entsprechende Fallakte anlegen, wenn der Patient direkt im Krankenhaus vorstellig wird und die Diagnose „Magen-CA“ festgestellt wird. In diesem Fall übernimmt das Krankenhaus die Gatekeeper-Funktion.

Aktuell erfolgt keine elektronische, sektorübergreifende Kommunikation. Dabei erfolgt die Datenerfassung sowohl auf ambulanter als auch stationärer Seite bereits in einem elektronischen Primärsystem.

Mit dieser Art der intersektoralen Kommunikation werden daher folgende Ziele verfolgt:

- Professions- und sektorübergreifende Kommunikation und Kooperation zwischen Leistungserbringern zur zeitsparenden Datenübermittlung im Sinne einer optimalen Versorgung des Patienten unter Vermeidung von Medienbrüchen
- Konsultationen / Expertenaustausch bei unklaren Befunden oder umfangreichen Therapiemaßnahmen
- Vermeidung von Kontraindikationen und Wechselwirkungen
- Steigerung der Patientensicherheit durch abgestimmte Dokumentation und Informationsweitergabe.

Die personenbezogenen und –beziehbaren Daten sind bereits bei den behandelnden Ärzten und Einrichtungen, den Fallaktennutzer, vorhanden. Die Fallakte stellt die Möglichkeit einer elektronischen Kommunikation dieser Daten nach Zustimmung des Patienten dar.

3. 3. 3. 2. Zu verarbeitende Daten

3. 3. 3. 2. 1. Daten / Datenklassen

Jede Gastro-Onkologie-Akte besteht aus mehreren personenbezogenen, größtenteils Gesundheitsdaten eines bestimmten Patienten. Diese Dokumente werden als Informationsobjekte bezeichnet.

Datenklassen und Informationsobjekte im Versorgungsszenario Demenz-Akte	
Personenbezogene Daten (Basisdatensatz eines Patienten um ihn innerhalb der EFA zu identifizieren)	• Name • Anschrift • Geburtsort/-Datum • eGK-Nummer
Weitere personenbezogene Daten	• Adresse • Kontaktdaten im Notfall • Patientenverfügung / Betreuungsvollmacht
Gesundheitsdaten (Datensätze einer spezifischen EFA zu einer bestimmten Person)	• Arztbriefe • Medikation (auch Dauermedikation) • Bildgebende Befunde (Sonographie, Szintigraphie, Echo, CT, Rö, MRT, Endoskopie, jedoch keine DICOM-Bilder) • Labordiagnostik • Histologie/Zytologie • Vorbefunde, falls relevant (insb. Kardio. und Pneumo.) • Onkologischer Erststatus (klinisches Stadium, Fazit Tumorkonferenz) • Eigen- und Sozialanamnese (Gewichtsverlust, Ernährungsarzt, Bewegung, Belastung, Pflegestufe, Pflegeanamnese, psychoonkologische Betreuung) • Therapien • CAVE (Allergien, Unverträglichkeiten) • Nachsorgeplan

3. 3. 3. 2. 2. Speichern der Daten

Da die Versorgung von Patienten mit dieser Diagnose nur für die Zeit der aktuellen Behandlung stattfindet, wird nach Ablauf der Behandlung – nach einer Übergangszeit von 12 Wochen– die Fallakte gelöscht. Wird im Verlauf der Behandlung festgestellt, dass die Diagnosestellung negativ ist, wird die Fallakte unmittelbar gelöscht. Gespeichert werden sämtliche Daten bei dem Provider Healthcare IT Solutions GmbH (HITS), Pauwelsstr. 30, 52074 Aachen.

3. 4. Münster / Warendorf

3. 4. 1. Ziele

In der Modellregion Münster/ Warendorf/ Niederrhein werden im Rahmen der einzuführenden Geriatrie-Akte Daten erfasst und zwischen den, durch den Patienten berechtigten, Leistungserbringern auf elektronischem Weg kommuniziert. Die Geriatrie-Akte adressiert dabei keine bestimmte Krankheit, sondern ein spezifisches Patientenklientel. Der geriatrische Patient definiert sich durch ein höreres Lebensalter und eine geriatrietypische Multimorbidität (vgl. Deutsche Gesellschaft für Geriatrie e.V.). Aufgrund dieser Eigenschaften zählen geriatrische Patienten auch als vulnerable Gruppe. Infolge des teils hohen Lebensalters und/ oder der vorherrschenden Erkrankung/en sind geriatrische Patienten häufig nicht mehr in der Lage, alle, für eine sichere und best mögliche Behandlung, notwendigen Informationen den Leistungserbringern selbst zu übermitteln. Aus diesem Grund ermächtigt der Patient seine behandelnden Ärzte und Einrichtungen auf seine Fallakte zuzugreifen, mit dem Zweck über sie fallbezogen zu kommunizieren.
Aktuell erfolgt die sektorübergreifende Kommunikation in der betrachteten Region noch weitgehend papierbasiert. Dabei erfolgt die Datenerfassung sowohl auf ambulanter Seite als auch auf stationärer Seite im Krankenhaus bereits in einem elektronischen Primärsystem. Die Vermischung von papierbasierter und elektronischer Datenverarbeitung birgt die Gefahr von Medienbrüchen mit Auswirkungen auf die Patientensicherheit. Zudem bedeutet der papierbasierte Versand der Behandlungsdokumentation einen erheblichen Zeitverlust mit möglicher Weise drastischen Auswirkungen auf das Patientenwohl.
Das Konzept der Fallaktenkommunikation ist eine Datenaustauschplattform, welche in diesem Szenario u.a. diese Ziele verfolgt:

- Professions- und sektorübergreifende Kommunikation und Kooperation zwischen Leistungserbringern zur zeitsparenden Datenübermittlung im Sinne einer optimalen Versorgung des Patienten unter Vermeidung von Medienbrüchen
- Konsultationen/ Expertenaustausch bei unklaren Befunden oder umfangreichen Therapiemaßnahmen
- Vermeidung von Kontraindikationen und Wechselwirkungen
- Vermeidung von Mehrfachuntersuchungen
- Steigerung der Patientensicherheit durch abgestimmte Dokumentation und Informationsweitergabe
- Schutz vulnerabler Gruppen (geriatrisches Klientel)

Die personenbezogenen und -beziehbaren Daten sind bereits bei den behandelnden Ärzten und Einrichtungen, den Fallaktennutzern, vorhanden. Die Fallakte stellt die Möglichkeit einer elektronischen Kommunikation dieser Daten nach Zustimmung des Patienten dar.

3. 4. 2. Zu verarbeitende Daten

3. 4. 2. 1. Daten / Datenklassen

Jede EFA besteht aus mehreren personenbezogenen-, größtenteils Gesundheitsdaten eines bestimmten Patienten zu einem spezifischen Behandlungsfall.

In der nachfolgenden Tabelle finden Sie eine Auflistung der Datenklassen einer EFA in der Geriatrie-Akte.

Datenklassen und Informationsobjekte im Versorgungsszenario Demenz-Akte	
Personenbezogene Daten (Basisdatensatz eines Patienten um ihn innerhalb der EFA zu identifizieren)	• Name • Anschrift • Geburtsort/-Datum • eGK-Nummer
Gesundheitsdaten (Datensätze einer spezifischen EFA zu einer bestimmten Person)	• Verlauf, Schwere und Dauer der Erkrankungen • Vorerkrankungen/Allergien • Ablauf und Inhalt medizinischer Behandlungen durch Ärzte, Krankenhäuser und medizinische Hilfsdienste/Epikrise • Arztbriefe • Therapieempfehlung • Arzneimittel und Medikationsplan • Heil-/Hilfsmittel • Veranlasste Verordnungen • Sonstige Therapie • Sozialanamnese • Pflegestufeneinordnung • Dokumentierter Patientenwille • Behandelnde Ärzte • Krankenhaus-/ Reha-/ Kurzzeitpflegeaufenthalte der letzten 12 Monate • Aufnahme- und Entlassdatum

Weitere Daten bzw. Datenklassen können mit der Fortentwicklung des Versorgungsszenarios bzw. auf der Basis des individuellen Ermessens der behandelnden Akteure hinzukommen.

3. 4. 2. 2. Speichern der Daten

Da die Versorgung von geriatrischen Patienten in der Regel über einen längeren Zeitraum stattfindet, besitzt jede EFA in dieser Modellregion eine Laufzeit von fünf Jahren. Gespeichert werden sämtliche Daten bei dem Provider FAC`T IT GmbH, Rechenzentrum, Lise-Meitner-Straße 5, 28359 Bremen.