ELEKTRONISCHE
FALLAKTE

EFA-in-a-Box

Leitfaden für Kliniken

Dr. Jörg Caumanns, Fraunhofer ISST

Fraunhofer
ISST

EFA-in-a-Box
Leitfaden für Kliniken

von Dr. Jörg Caumanns, Fraunhofer ISST

Dokument-ID:	EFA-Box-Kliniken
Responsible:	Fraunhofer ISST
Status:	Release
Version:	1.2.0.3
Last Update:	12 September 2011
Category:	Application Architecture Non-Normative

Intellectual Property Rights

This specification can be downloaded from http://www.fallakte.de.

ELEKTRONISCHE FALLAKTE

Inhalt

1 Einleitung

»Das Krankenhaus-Geschäft ist ein regionales Geschäft«[1].

Aus dieser einfachen Aussage lassen sich drei wesentliche Implikationen für ein Krankenhaus ableiten:

- Das Krankenhaus ist regional verankert und spielt eine besondere Rolle in regionalen Versorgungsstrukturen. Die von der Politik initiierten Gesundheitsregionen sind ohne Krankenhäuser nicht denkbar und genauso ist für ein Krankenhaus eine Teilnahme an neuen Versorgungsformen ohne eine funktionierende Gesundheitsregion nicht denkbar.
- Der Betrieb eines Krankenhauses ist ein Geschäft, das über die stationäre Behandlung von Patienten hinausgeht. Teil dieses Geschäfts ist das Aufsetzen zeitgemäßer Angebote für andere Akteure im regionalen Verbund, um für Zuweiser und Patienten attraktiv zu bleiben und neue Kundengruppen zu gewinnen bzw. bestehenden Kunden zusätzliche Angebote zu machen.
- Ein regionales Geschäft ist immer geprägt durch Kooperation und Konkurrenz in wechselnden Partnerkonstellationen; dasselbe Ärztenetz kann je nach Fall und Versorgungsvertrag ein willkommener Partner oder ein unliebsamer Wettbewerber sein. In einigen Fällen möchten Partner im Verbund eng kooperieren, in anderen Fällen lediglich effizient kommunizieren.

1.1 Warum elektronische Fallakten?

Die elektronische Fallakte ist die Plattform für die regionale Vernetzung und Verankerung von Krankenhäusern. Während z. B. Zuweiserportale lediglich einzelne Aspekte der Datenkommunikation mit Niedergelassenen effizienter gestalten, bildet die elektronische Fallakte ein vollständiges regionales Versorgungsnetzwerk ab, in dem die einzelnen Akteure beliebige Gesundheitsdatendienste aufsetzen und eigene, fallspezifische Kooperationsnetze innerhalb des Verbunds ausbilden können:

- Als Anwendung vernetzt die elektronische Fallakte alle Ärzte, die in die Behandlung einer Erkrankung eines Patienten eingebunden sind. Alle behandelnden Ärzte haben Zugriff auf alle Daten eines medizinischen Falls und pflegen über die Fallakte eine gemeinsame Falldokumentation. Über die Fallakte werden somit bestehende Kooperationsbeziehungen in

[1] Dietmar Pawlik, kaufmännischer Vorstand des Klinikums Fulda

einem regionalen Netzwerk technisch unterstützt und auf eine einheitliche technische Basis gesetzt.

- Als Plattform bietet die elektronische Fallakte Sicherheits- und Datendienste an, auf denen neben der Anwendung »Fallakte« auch beliebige weitere Gesundheitsdatendienste (Fallkonferenz, Terminbuchung, Tele-Konsil, etc.) aufgesetzt werden können. Nutzeraccounts und Berechtigungen werden in den beteiligten Einrichtungen zentral verwaltet und können von allen Gesundheitsdatendiensten im regionalen Verbund genutzt werden; hierdurch wird nicht nur das Aufsetzen neuer Anwendungen einfacher und kostengünstiger, sondern auch der Nutzenkomfort für die Ärzte erhöht: ein Arzt muss sich nicht an jedem Portal neu anmelden und es spielt für ihn keine Rolle mehr, wo benötigte Daten nun gerade physikalisch gespeichert sind – er meldet sich einfach wie bisher an seinem System an und die Plattform sorgt dann dafür, dass er alle benötigten Dienste und Daten so nutzen kann, als wären diese lokal in seinem System verfügbar.
- Mit der Fallakte können Netze im Netz aufgebaut werden. Jeder Chefarzt kann Fallakten und andere von einer Klinik angebotene Gesundheitsdatendienste an sein konkretes Partnernetzwerk und die darin vereinbarten arbeitsteiligen Behandlungspfade anpassen. Der Chefarzt legt einmalig fest, welcher Partner für welche Behandlungen Zugang zu welchen Daten und Diensten haben soll und die IT-Abteilung der Klinik kann ihm mit diesen Informationen ein entsprechendes diagnosespezifisches Netzwerk innerhalb der Fallakten-Plattform aufsetzen. Ein Endoprothetiker kann so z. B. ein eigenes Netzwerk für die Behandlung von Patienten mit Hüftgelenksprothesen aufsetzen und ein Onkologe ein wieder anderes Netzwerk zur Nachsorge von Darmkrebs-Patienten – und dies alles innerhalb kürzester Zeit, sicher voneinander abgeschottet und ohne dass jedes Mal neue IT-Systeme beschafft werden müssten.

1.2 Warum EFA-in-a-Box?

In der IT sind Funktionalität und Flexibilität oftmals proportional zur Komplexität einer Lösung – je flexibler, desto komplexer. Hier macht auch die elektronische Fallakte keine Ausnahme. Genau wie vor hundert Jahren jeder Autofahrer gleichzeitig ein Automechaniker sein musste, so erfordert insbesondere die Integration der EFA-Sicherheitsfunktionen in eine bestehende Klinik-IT ein Verständnis von verteilten Infrastrukturen und Sicherheitsstandards, die eher aus dem Telekommunikationsumfeld kommen. Dieses Wissen ist alleine schon aufgrund der starken Betriebsausrichtung vieler Klinik-IT-Verantwortlicher in einem Krankenhaus oftmals nicht vorhanden und auch die Hersteller von Klinik-IT-Systemen besitzen es vielfach (noch) nicht. Letzten Endes ist dies auch kein Versäumnis von Klinik-IT-Leitern und Herstellern sondern vielmehr darin begründet, dass bei der Fallakte Sicherheitsdienste als Teil der von allen IT-Systemen in einem regionalen Verbund

genutzten Plattform angesehen werden. Genau wie beim Internet, das diese Systeme auf der Nachrichtenebene vernetzt, sollte der IT-Leiter in der Lage sein, die Klinik-IT an diese Dienste anzubinden. Er sollte hier aber immer in der Rolle des Anwenders angebotener Schnittstellen bleiben und nicht als Entwickler neuer Schnittstellen und Bausteine tätig werden müssen.

Umgekehrt verhielt es sich bei der Anbindung der Datendienste der elektronischen Fallakte: Die IT-Bereiche vieler Kliniken verfügen über extrem gute Kenntnisse und Erfahrungen in der Systemintegration über HL7-Nachrichten und Kommunikationsserver. Der bisherige Zuschnitt der elektronischen Fallakte hat jedoch diese Integrationsaufgabe eher auf die Hersteller verlagert, für die Systemintegration jedoch kein Produkt-, sondern ein Projektgeschäft ist. In der Konsequenz ist so eine Situation entstanden, in der die einen zwar integrieren konnten und wollten, aber kein Produkt zum Integrieren bekamen (Klinik-IT) und die anderen zwar integrieren sollen, dies aber aus ihren eigenen Geschäftsmodellen heraus eigentlich garnicht in der gewünschten Form wollten / konnten / durften (Hersteller).

Aus diesen in den laufenden Fallakten-Einführungen gemachten Erfahrungen heraus ist das Konzept der EFA-in-a-Box entstanden. Wie der Name ausdrückt geht es hierbei nicht um eine neue Fallakte, sondern um *eine neue Integrationsschicht um die bestehende* Fallakte. Um bei der Analogie des Autos zu bleiben: Viel Technik wird aus dem Fahrerraum unter die Motorhaube verlagert. Bei den Plattformdiensten sieht der Mechaniker nicht mehr unzählige Kabel und Schläuche, sondern einen Vergaser mit einfachen Anschlüssen zum Motor. Für Standardkonfigurationen kann man statt der Handschaltung mit Zwischengas auch eine Automatik mit Tempomat bekommen – wo vorher das Auto durch das Auge des Herstellers als technisches Wunderwerk sichtbar war, wird nun der Nutzerblick in den Vordergrund gestellt und dieser sieht vorrangig den Zweck des Autos als einfach bedienbares, komfortables Beförderungsmittel.

Hiermit einher geht eine Schärfung der Rolle und der Zuständigkeiten der Klinik-IT beim Aufsetzen und Betreiben einer Fallakte. Die EFA-in-a-Box ist darauf ausgerichtet, als Ganzes in eine bestehende Klinik-IT-Landschaft integriert zu werden und auch die Konfiguration muss nicht mehr über viele Dienste verteilt erfolgen, sondern erfolgt über definierte, von konkreten Technologien abstrahierende Schnittstellen und Werkzeuge.

2 EFA-in-a-Box: Übersicht

Das Konzept der »EFA-in-a-Box« vereinfacht den Umgang mit elektronischen Fallakten sowohl für Nutzer als auch für Anbieter indem die technischen Schnittstellen so gekapselt wurden, dass die Anbindung bestehender Systeme mit minimalem Aufwand möglich wird. In diesem Abschnitt wird ausgehend von dem einfachen Grundmuster der »EFA-in-a-Box« beschrieben, welche Möglichkeiten der Anbindung interner Systeme an eine EFA-Box bestehen, um elektronische Fallakten für die Nutzer weitgehend unsichtbar in klinische Abläufe einzubetten.

2.1 Grundmuster

Abbildung 1 stellt das Grundmuster von »EFA in a Box« im Überblick dar. Mit diesem Muster kann eine Klinik eine EFA weitgehend autonom von den bestehenden Systemen betreiben. Die Klinik tritt dabei in zwei Rollen auf: der IT-Bereich ist der EFA-Provider während die klinischen Bereiche genau wie die angebundenen niedergelassenen Ärzte EFA-Nutzer sind.

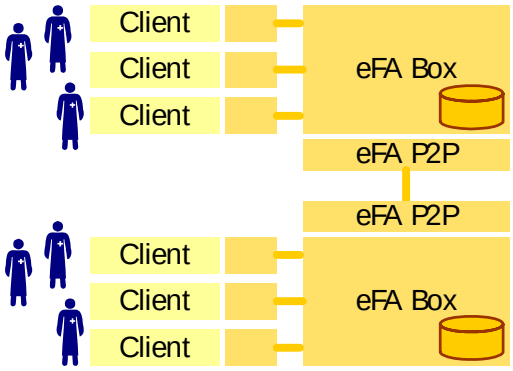

Abbildung 1: EFA-in-a-Box

Niedergelassene und Klinkärzte als Nutzer der EFA-Box sind auf der Client-Seite angesiedelt. Für die IT-Systeme der Nutzer (EFA Clients) bietet die EFA-Box einen so genannten EFA-Connector (kleine orangefarbene Boxen in Abbildung 1). Hersteller können den EFA-Connector in ihre Systeme integrieren. Alternativ kann ein EFA-Anbieter den EFA-Connector auch über ein Web-Portal kapseln, das dann die grafische Nutzerschnittstelle zum Zugriff auf die im EFA-Connector gekapselte EFA-Funktionalität bildet.

Der EFA-Connector bietet eine ganz einfache Schnittstelle an. Mit dieser Schnittstelle können Fallakten gesucht und angelegt werden, und es können Dokumente in Fallakten eingestellt und aus diesen ausgelesen werden. Der EFA-Connector kapselt alle Sicherheitsfunktionen in einer EFA-Session, die

einmalig bei der Anmeldung des Nutzers an der EFA-Box angelegt wird und in der der EFA-Connector dann selbstständig alle zum Zugriff auf Fallakten erforderlichen Identitäts- und Berechtigungsnachweise einholt und verwaltet.

Die EFA-Funktionalitäten zur Verwaltung von EFA-Daten und Berechtigungen sind komplett in der EFA-Box gekapselt. Diese verfügt über einen eigenen Datenspeicher, in dem die ggf. von Niedergelassenen und Klinikärzten in eine EFA eingestellten Dokumente vorgehalten werden (siehe auch 2.2 für alternative Umsetzungen).

Über einen so genannten Peer-to-Peer-Adapter (P2P) können in unterschiedlichen EFA-Boxen gekapselte EFA-Dienste miteinander vernetzt werden. Hiermit kann ein Nutzer über jede beliebige EFA-Box auf Daten jeder der vernetzten EFA-Boxen zugreifen. Alle hierzu erforderlichen Funktionen zum Suchen der Daten und zum Weiterleiten von Anfragen zwischen EFA-Boxen sind im Peer-to-Peer-Adapter gekapselt.

2.2 Anbindung eines bestehenden Datenspeichers

Falls medizinische Daten in der EFA-Box vorgehalten werden, erfordert dies, dass der Betreiber der Box Maßnahmen zum Schutz dieser Daten vor Verlust, Verfälschung und unerlaubter Offenbarung aufsetzt. Zusätzlich sind Prozesse zur Datensicherung und zur Archivierung geschlossener Fallakten erforderlich.

Üblicherweise besitzt jede Klinik den Anforderungen von IT-Sicherheit und Patientendatenschutz genügende IT-Systeme, für die die benannten Maßnahmen und Prozesse bereits bestehen. Es liegt daher nahe, diese Systeme – z. B. ein digitales Archiv oder eine IHE XDS-konforme interne Patientenakte – als Datenspeicher für Fallakten zu nutzen.

Abbildung 2 stellt dar, wie die EFA-Box an einen klinik-internen Datenspeicher angebunden werden kann.

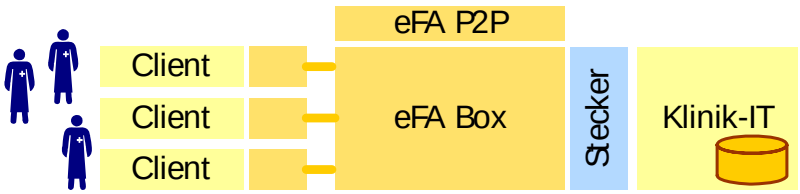

Abbildung 2: Anbindung eines bestehenden Datenspeichers (z. B. Archivsystem)

Die Anbindung erfolgt über einen so genannten EFA-Stecker. Dieser nimmt an die EFA gesandte Daten entgegen und leitet sie an einen klinik-internen Datenspeicher weiter. Anfragen nach Daten (Datenabruf aus der EFA) wer-

den ebenso über den Stecker an den internen Datenspeicher weiter gegeben. Die Prüfung der Authentizität und Zugriffsberechtigung des Nutzers erfolgt dabei weiterhin in der EFA-Box, d. h. der interne Datenspeicher muss lediglich sicher an die EFA-Box angebunden werden und benötigt keine zusätzlichen Schnittstellen zu den EFA-spezifischen Sicherheitsfunktionen.

2.3 Anbindung einer bestehenden Datenquelle

Üblicherweise werden Daten über die Client-Schnittstelle (PVS, KIS, Portal, etc.) und den EFA Connector in die EFA-Box eingestellt. EFA-Connector und EFA-Box handeln dabei intern alle Sicherheitsfunktionalitäten ab, die erforderlich sind, um einen übergreifenden Sicherheitskontext zwischen dem Nutzer und den datenhaltenden Systemen der EFA herzustellen.

Für den Fall, dass eine Klinik eine EFA-Box betreibt, besteht ein solcher Sicherheitskontext bereits zwischen der EFA-Box und den als EFA-Datenquellen fungierenden internen Klinik-IT-Systemen (KIS). Um im KIS freigegebene Daten in eine EFA einzustellen, können daher EFA-spezifische Sicherheitsfunktionen durch klinik-intern bestehende Sicherheitsmaßnahmen substituiert werden. Abbildung 3 stellt dar, wie hierdurch in einer Klinik freigegebene Daten durch eine Datenverbindung auf der Provider-Seite ohne »Umweg« über einen EFA-Client in eine EFA-Box eingespielt werden können.

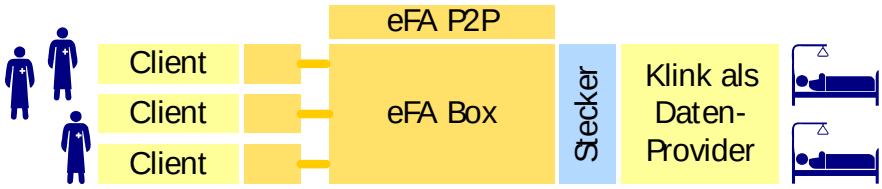

Abbildung 3: Anbindung einer bestehenden Datenquelle (z. B. KIS)

Um das direkte Einspielen von Daten aus einem Quellsystem in eine EFA innerhalb eines geschlossenen Sicherheitskontextes einer Klinik möglichst unkompliziert zu gestalten, führt die EFA das Konzept des »administrativen Falls« ein. Ein administrativer Fall in der Klinik fasst alle Daten zusammen, die klinik-intern unter einer gemeinsamen Fallnummer geführt werden. Hierbei wird ausgenutzt, dass alle internen Systeme diese Fallnummer mitführen und dass alle intern für die EFA freigegebenen Daten über diese Fallnummer klassifiziert sind. In der EFA wird für jeden administrativen Fall ein eigener Ordner angelegt und mit der internen Fallnummer verknüpft. Daten können so aus der Klinik heraus nur unter Angabe der internen Fallnummer in eine EFA eingestellt werden; anhand der Fallnummer kann die EFA-Box den damit verknüpften Ordner und anhand des Ordners die »richtige« Fallakte identifizieren und die Daten dort einstellen.

Die EFA-Box besitzt eine Schnittstelle, über die Quellsysteme beliebige HL7 v3 CDA-Dokumente (z. B. nach dem VHitG Arztbrief-Standard) direkt an einer EFA registrieren können. Quellsysteme, die keine Dokumente nach dem HL7 CDA-Standard ausspielen können, werden über einen EFA-Stecker angebunden, der vom Quellsystem bei der Datenfreigabe erzeugte Nachrichten so aufbereitet, dass die EFA-Box sie verarbeiten kann. Beispielsweise können über den HL7v2-Stecker HL7 v2.5 MDM und ADT-Nachrichten von einem KIS entgegengenommen und auf die HL7 v3 basierten Schnittstellen der EFA-Box abgebildet werden.

2.4 Verwaltung von Fallakten

Eine große Hürde bei der Integration einer EFA in eine Klinik-IT-Landschaft war bislang immer die Verwaltung von Fallakten aus den klinischen Systemen heraus. Diese Systeme können zwar üblicherweise Dokumente verschiedenster Formate erzeugen, sind aber nicht darauf ausgelegt, Funktionen wie z. B. die Anlage einer Fallakte, die Verknüpfung eines administrativen Falls mit einer Fallakte oder die Pflege der vom Patienten gegebenen Einwilligungen zu realisieren. Bislang mussten hier entweder kostspielige Erweiterungen des KIS durch dedizierte EFA-Masken vorgenommen oder interne Web-Portale mit entsprechenden Funktionen aufgesetzt werden.

Hier bringt die EFA-Box die größten Vereinfachungen für Kliniken, die Fallakten anbieten wollen. Sämtliche Steuerungsfunktionen – vom Anlegen einer Fallakte bis zur Administration der in einer Fallakte verlinkten Dokumente – können über HL7 v3 CDA Dokumente ausgelöst werden. Hierzu bildet die EFA-Box den internen Zustand einer Fallakte auf ein CDA-Dokument ab. Änderungen an einer Fallakte werden in diesem Dokument vorgenommen und anschließend wird das Dokument wieder in die EFA-Box eingespielt, die dann die Inhalte des veränderten Dokuments wieder auf den Systemzustand der Fallakte abbildet. Ebenso einfach ist das Anlegen einer Fallakte: Die anzulegende Fallakte wird über ein CDA Dokument beschrieben, dieses wird in die EFA-Box eingespielt und die EFA-Box legt eine entsprechende Fallakte an.

Ein solches Dokument kann man sich wie einen Arztbrief vorstellen, der nicht an einen anderen Arzt, sondern an die EFA-Box geschickt wird. Inhalte dieses Briefs sind der Name des Patienten, die Namen der Mitbehandler, die der EFA zugrunde liegenden Diagnosen und Hinweise zu den vom Patienten gegebenen Einwilligungen. Ein solches Dokument kann entweder direkt im KIS erstellt werden oder über einen EFA-Stecker aus HL7 v2.5 ADT-Nachrichten erzeugt werden.

2.5 Anbindung eines Master Patient Index

Eine der größten Herausforderungen bei der Datenkommunikation zwischen Einrichtungen (und oftmals auch zwischen Standorten und Fachabteilungen eines Krankenhauses) ist die Identifikation von Patienten. Für eine Integration von Fallakten in diese Systeme der Ärzte ist es daher unabdingbar, dass jeder Arzt mit den in seinem lokalen System bestehenden Patienten-IDs auf Fallakten des Patienten zugreifen kann. Um dieses zu ermöglichen, bietet die EFA-Box die Möglichkeit, über einen bestehenden Master Patient Index (MPI) mehrere Patienten-IDs pro Patient zu verwalten und auch eine Fallakte an mehrere Patienten-IDs zu binden (siehe Abbildung 4).

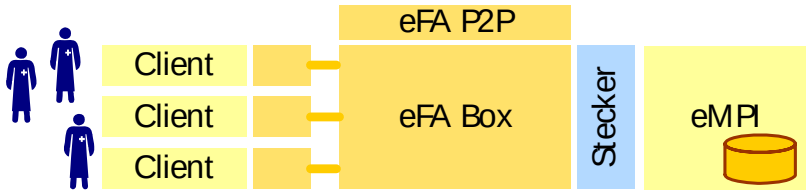

Abbildung 4: Anbindung eines Master Patient Index (eMPI)

Hierbei wird ausgenutzt, dass gemäß der EFA-Spezifikation eine Fallakte niemals direkt mit einer Patienten-ID verknüpft ist. Stattdessen werden Fallakten an so genannte Zugangscodes gebunden, wobei für jeden Zugriffsberechtigten ein eigener Zugangscode pro Patient eingerichtet wird. Diese Zugangscodes werden aus der ID des zugriffsberechtigten Arztes (bzw. der zugriffsberechtigten Einrichtung) und der Patienten-ID gebildet. Es gibt dabei kein technisches Erfordernis, dass für die Bildung der Zugangscodes für alle Berechtigten die gleiche Patienten-ID genutzt werden muss. Vielmehr ist es möglich, dass jeder Zugriffsberechtigte einen Zugangscode bekommt, in den die in seinem lokalen Kontext bekannte Patienten-ID eingeflossen ist. Es ist darüber hinaus auch möglich, dass ein Berechtigter mehrere Zugangscodes bekommt; z. B. einen für jede dem Patienten zugewiesene ID.

Über einen mittels eines Steckers angebundenen eMPI kann die EFA-Box die zu einem Patienten in verschiedenen Kontexten genutzten IDs abfragen und diese Information bei der Berechnung und Bindung der Zugangscodes für eine Fallakte berücksichtigen. Insbesondere können so auch im Rahmen der EFA genutzte Patienten-IDs am MPI registriert werden (siehe Kapitel 3.2 für ein Beispiel).

2.6 System- und anwendungsspezifische EFA-Stecker

Nach dem in den vorangegangenen Kapiteln beschriebenen Grundmuster der Anbindung bestehender Systeme an eine EFA-Box über EFA-Stecker können Kliniken und Hersteller beliebige weitere Stecker für spezifische

Problemstellungen und Systemschnittstellen entwickeln. Beispiele hierfür sind:

- Eine Klinik nutzt ein Laborsystem, das Labordaten in einem proprietären ASCII-Format ausspielt. Über einen spezifischen EFA-Stecker werden diese Daten in ein Formular eingespielt und in das PDF-Format übersetzt. Das PDF-Dokument wird in die EFA-Box eingespielt.

- Eine Klinik verwaltet Patientendaten intern über eine IHE XDS-Patientenakte. Über einen EFA-Stecker fungiert die EFA-Box gegenüber der XDS-Patientenakte als »Document Consumer«, d.h. alle Daten werden ausschließlich in der internen Akte gespeichert und die EFA-Box ruft daraus bei Bedarf die angefragten Daten ab.

Die Administration von Fallakten und deren Inhalten aus einem System des Providers heraus erfolgt über CDA-Dokumente. Diese Dokumente bilden den aktuellen Zustand einer Fallbehandlung und der daran gebundenen administrativen Fälle ab. Die Flexibilität des CDA-Standards erlaubt es, diese Dokumente um beliebige Inhalte zu erweitern. Die Inhalte werden dabei über spezifische EFA-Stecker aus den internen Systemen des Providers in die EFA-Box eingespielt.

Diese Option kann genutzt werden, um Informationen als kodierte Informationsbausteine verfügbar zu machen, so dass nicht zwingend für jede Information ein Dokument erstellt werden muss. Beispielsweise können so direkt in der Fallakte die aktuelle Medikation des Patienten oder vereinbarte Termine gepflegt werden. Hierdurch sind wichtige Informationen auf einen Blick verfügbar und die Zahl der Dokumente in der Akte wird deutlich verringert (wodurch die Akte wiederum übersichtlicher und damit effizienter nutzbar wird).

3 Szenarien: Einführung und Nutzung von Fallakten

Eine Fallakte soll regionale Versorgungsnetze technisch unterstützen. Dieses funktioniert umso besser, je besser die bestehenden organisatorischen und fachlichen Strukturen sind. Dementsprechend müssen sich in einem ersten Schritt die Klinikärzte und kooperierende Niedergelassene darüber verständigen, wie gemeinsame Behandlungsszenarien aufgesetzt werden sollen und wie die dazu erforderliche gemeinsame Dokumentation aussehen soll. Dies geht nicht von heute auf morgen, sondern ist ein schrittweiser Prozess, der auch stark von Erfahrungen und Ideen geprägt wird, die erst während der praktischen Nutzung entstehen.

Typischerweise ist die Einführung der elektronischen Fallakte damit per se ein Migrationsprojekt, in dem parallel zu der Ausdifferenzierung der Kooperationen zwischen den Ärzten auch die dazu benötigten technischen Funktionalitäten bereit gestellt werden. Dies hat den Vorteil, dass die Kosten mit dem Nutzen skalieren und dass jede neu hinzu kommende Funktionalität eng an realen Nutzererfahrungen und -wünschen ausgerichtet ist.

Im den nachfolgenden Abschnitten wird beschrieben, wie mit Hilfe von EFA-in-a-Box eine bestehende Kooperation eines Klinikarztes mit Niedergelassenen schrittweise von einer einfachen Datenbereitstellung über ein Zuweiserportal bis zur Unterstützung einer vollständig elektronisch unterstützten gemeinsamen Behandlungskette ausgebaut werden kann. Hierbei wird davon ausgegangen, dass die Vorbedingungen für eine elektronische Kommunikation – z. B. Definition eindeutiger Identifizierer für Kommunikationspartner – erfüllt sind (siehe Anhang A).

3.1 Szenario 1: Arztbrief-Portal

In einem 300-Betten-Krankenhaus werden einzelne Chefärzte immer wieder von den für die Nachsorge zuständigen Niedergelassenen mit dem Wunsch konfrontiert, schneller und umfänglicher Informationen zu den im Krankenhaus durchgeführten Behandlungen zu bekommen. Insbesondere möchte man auch einen direkten Kommunikationskanal zum Krankenhaus aufbauen, da es immer häufiger vorkommt, dass Patienten zur Nachsorge kommen, die die vom Krankenhaus bei der Entlassung mitgegebenen Unterlagen nur unvollständig dabei haben, oder dass Termine kurzfristig verschoben werden müssen, da erforderliche Unterlagen noch mit der Post unterwegs sind bzw. immer erst explizit beim Krankenhaus angefragt werden müssen (und dann kurzfristig auch nur in schlechter Qualität per Fax geliefert werden können).

Die Klinikleitung beauftragt die IT-Abteilung, zeitnah und kostengünstig eine Lösung aufzusetzen, mit der Niedergelassene über ein einfaches Web-

Portal ausgewählte Behandlungsdokumente zu ihren Patienten abrufen können. Zur Anmeldung an dem Portal sollen die Niedergelassenen ihren Heilberufsausweis nutzen können, da so für das Krankenhaus nur wenig zusätzlicher Aufwand für die Umsetzung der Anforderungen des Datenschutzes an eine sichere Kommunikation entsteht. Änderungen am KIS sind für die erste Umsetzungsstufe nach Möglichkeit zu vermeiden, um Kosten und Zeitaufwand gering zu halten.

Zur Umsetzung der Lösung wird eine EFA-Box beschafft. Der vorhandene Kommunikationsserver wird um einen vom Hersteller bereit gestellten HL7v2.5-EFA-Stecker erweitert.

Umsetzungsschritt 1: Einwilligungserklärung

Damit Klinikärzte den nachsorgenden niedergelassenen Ärzten Behandlungsdokumente elektronisch zur Verfügung stellen können, muss der betroffene Patient die Klinikärzte zunächst von ihrer Schweigepflicht gegenüber vom Patienten zu benennende nachsorgende Ärzte befreien. Hierzu ist eine entsprechende Einwilligung des Patienten erforderlich.

In Absprache mit dem Datenschutzbeauftragten der Klinik wird ein vorhandenes Muster einer Einwilligungserklärung[2] an die Erfordernisse des Ärzteportals angepasst. In der Erklärung kann der Patient angeben, welche Ärzte Zugriff auf seine Daten erhalten sollen. Es ist festgelegt, dass die Daten im Portal maximal drei Monate vorgehalten werden.

Der Patient kann die Einwilligungserklärung entweder schon vor der Einweisung bei seinem Arzt oder aber im Rahmen der Aufnahme im Krankenhaus unterschreiben. Auch eine spätere Einwilligung ist möglich, in diesem Fall werden aber nur die Daten über das Portal verfügbar gemacht, die nach dem Zeitpunkt der Einwilligung freigegeben wurden.

Alle Einwilligungen werden in der internen Patientenakte abgelegt (Papier oder digital als eingescanntes Dokument). Der Patient erhält eine Kopie der Einwilligung.

Da zum Zugriff auf die Daten und zum Widerruf einer Einwilligung die interne Patienten-ID verwendet werden, ist diese in der Einwilligung angegeben. Zusätzlich wird eines der bei der Aufnahme ausgedruckten Klebchen mit der Patienten-ID auf die Krankenversichertenkarte des Patienten geklebt.

[2] Eine sehr gute Vorlage wird z. B. vom Landesdatenschutz Hessen unter http://www.datenschutz.hessen.de/dg004.htm angeboten.

Umsetzungsschritt 2: Anlegen und Schließen von Fallakten

Das Anlegen einer Akte zur Speicherung der bereitgestellten Dokumente soll im Rahmen der Aufnahme erfolgen. Sofern ein Patient eine Einwilligung abgegeben hat, werden die dort benannten Ärzte als Mitbehandler im KIS registriert.

Mit der Freigabe der Aufnahmemaske wird vom Kommunikationsserver anhand der gegebenen Einwilligungen über das Anlegen einer Fallakte entschieden. Wenn keine Einwilligung gegeben wurde, wird keine Fallakte angelegt. Ansonsten wird eine Fallakte angelegt und mit dem aktuellen administrativen Fall (Aufnahmenummer) verknüpft. Für alle in der Freigabenachricht benannten Mitbehandler werden Zugriffsrechte auf die Akte gesetzt.

Technische Umsetzung (Beispiel): Mit der Freigabe der Aufnahmemaske sendet das KIS eine HL7v2.5 ADT^01 Nachricht an den Kommunikationsserver. Die in dieser Nachricht enthaltenen Segmente werden von dem in den Kommunikationsserver integrierten EFA-Stecker wie folgt verarbeitet:

- wenn PV1.9 (Patent Visit / Consulting Doctor) nicht angegeben ist, wird keine EFA angelegt. Die Verarbeitung durch den EFA-Stecker endet in diesem Fall. Zusätzlich wertet der Stecker das CON-Segment (Consent) aus; eine Fallakte wird nur angelegt werden, wenn CON.2 den Wert „001“ und CON.11 den Wert „A“ hat (Aktivierung einer Einwilligung zur Bereitstellung der Daten des aktuellen Falls).
- Der EFA-Stecker erzeugt ein CDA-Dokument mit Angaben zum Patienten (PID.3: Patient Identification / Patient Identifier List), den Mitbehandlern (PV1.8: Einweiser und PV1.9: Mitbehandler), der EFA-Diagnose (DG1.3: Diagnoseschlüssel) und der gegebenen Einwilligung (CON.2: Art der Einwilligung). Dieses Dokument wird an die EFA-Box geschickt.
- Der EFA-Stecker erzeugt ein weiteres Dokument, mit dem ein Ordner in der Fallakte angelegt wird. Als Ordner-ID wird der Wert von PV1.19 (Patient Visit / Visit Number) vorgegeben. Hiermit ist der aktuelle Behandlungsfall mit der Fallakte verknüpft.

Patienten haben das Recht, die Einwilligung jederzeit zu widerrufen. Dieses soll über die Aufnahme umgesetzt werden und kann dieser vom Patienten per E-Mail oder Fax angezeigt werden. Im KIS wird der Widerruf einer Einwilligung durch eine Änderung des Status der Einwilligung angezeigt.

Technische Umsetzung (Beispiel): Mit der Freigabe der Änderung der Patientendaten sendet das KIS eine HL7v2.5 ADT^08-Nachricht (Update Patient Notification) an den Kommunikationsserver. Die in dieser Nachricht enthaltene Segmente werden von dem in den Kommunikationsserver integrierten EFA-Stecker wie folgt verarbeitet:

- Es wird geprüft, ob ein CON-Segment in der Nachricht enthalten ist. Wenn CON.2 den Wert „001“ und CON.11 den Wert „X“ hat, wird die Fallakte gelöscht. Hierzu wird ein Dokument erzeugt, in dem die Rücknahme der Einwilligung kodiert ist. Dieses Dokument wird an die EFA-Box gesandt.

Umsetzungsschritt 3: Einspielen von Dokumenten

Das Einspielen von Dokumenten soll automatisiert erfolgen. Hierzu wird zunächst mit den Fachabteilungen abgestimmt, welche konkreten Dokumenttypen für Niedergelassene zur Nachsorge bereit gestellt werden sollen. Anschließend wird ein Regelwerk aufgestellt, in dem für jede Fachabteilung verzeichnet ist, welche konkreten Dokumenttypen in die Fallakte eingestellt werden sollen. Das Regelwerk wird gemäß den Vorgaben der »EFA-in-a-Box«-Spezifikation in den XACML-Standard übertragen und in die Konfiguration des EFA-Steckers übernommen.

Alle freigegebenen Dokumente werden nun automatisch über den Kommunikationsserver an die EFA-Box übermittelt. Hierbei prüft der Kommunikationsserver anhand des Dokumentenstatus und des Dokumententyp, ob das Dokument an die EFA weitergeleitet wird oder nicht.

Technische Umsetzung (Beispiel): Das KIS löst bei der Erstellung oder Freigabe eines Dokuments eine MDM^T01- bzw. MDM^T03-Nachricht aus. Diese Nachricht wird an den in den Kommunikationsserver integrierten EFA-Stecker gesandt. Der EFA-Stecker extrahiert aus der Nachricht zunächst den Dokumentenstatus und die Verfügbarkeit. Nur wenn das Dokument verfügbar und authentisiert ist (TXA.17 ist auf „AU“ oder „LA“ gesetzt und TXA.19 ist auf „AV“ gesetzt), wird die Verarbeitung fortgesetzt.

Anschließend werden der Dokumenttyp und die zuständige Fachabteilung aus der Nachricht extrahiert (TXA.2 und MSH.4 (sending facility) bzw. PV1.3 (Point of Care Element in der Patient Location)). Der EFA-Stecker prüft mit diesen Daten gegen das Regelwerk, ob die Übernahme des Dokuments in die EFA zulässig ist. Nur wenn dies der Fall ist, wird die Verarbeitung fortgesetzt.

Der Einfachheit halber sollen nicht nur Referenzen, sondern die Dokumente selber in der EFA-Box redundant gespeichert werden. Hierzu lädt der EFA-Stecker den Dokumenteninhalt aus dem Quellsystem (alternativ kann auch direkt eine MDM^T02- bzw. MDM^T04-Nachricht mit dem Dokumenteninhalt im OBX-Segment verwendet werden). Sofern es sich um ein CDA-Dokument handelt, wird dieses direkt an die EFA-Box gesandt, die alle benötigten Metadaten automatisch aus den Informationen im CDA-Header extrahiert. Falls das Dokument nicht im CDA-Format vorliegt, erzeugt der EFA-Stecker aus den Informationen in den Segmenten MSH, PID, PV1 und TXA einen CDA-Umschlag, in den das Dokument eingebettet und an die EFA-Box gesandt wird.

Das Dokument kann nun von den berechtigten Ärzten abgerufen werden.

Umsetzungsschritt 4: Aufsetzen des Portals

Über das Portal kann ein Arzt nach der Authentifizierung die für einen seiner Patienten bereit gestellten Dokumente abrufen. Hierzu muss er lediglich die ID des Patienten eingeben.

Sofern eine oder mehrere Fälle zu dem Patienten aktiv sind (und der Arzt die entsprechenden Zugriffsrechte besitzt) werden ihm diese in einem ersten Schritt angezeigt. Der Arzt kann nun einen der Fälle (Aufenthalte) auswählen und erhält eine Aufstellung der zu diesem Fall verfügbaren Dokumente. Per Mausklick kann er ein Dokument auswählen und abrufen.

Technische Umsetzung (Beispiel): Herzstück des Portals ist der mit der EFA-Box ausgelieferte EFA-Connector. Dieser wickelt nicht nur die Authentisierung und Berechtigungsprüfung komplett ab, sondern steuert auch die gesamte Kommunikation mit seinem im Krankenhaus installierten Gegenstück der EFA-Box. Seitens der Klinik-IT muss lediglich eine grafische Benutzeroberfläche vor den EFA-Connector gesetzt werden, über die der Nutzer die erforderlichen Eingaben und Auswahlen vornehmen kann. Die Anbindung der Nutzeroberfläche an den EFA-Connector ist denkbar einfach und erfolgt durch das Ansprechen von dre einfachen Funktionen zum Auflisten der verfügbaren Fälle / Aufenthalte, Auflisten der Dokumente und Abruf eines Dokuments.

3.2 Szenario 2: Regionales Netzwerk (Klinik und Ärztenetz)

Nachdem das in Szenario 1 aufgesetzte Ärzteportal ein halbes Jahr im Betrieb war, soll gemeinsam mit den Fachabteilungen über den weiteren Ausbau entschieden werden. Die Rückmeldungen der niedergelassenen Ärzte sind durchweg positiv, aber insbesondere für Behandlungen, bei denen bereits jetzt eine enge Verzahnung von stationären und ambulanten Prozessen besteht, wünschen sich sowohl Klinikärzte als auch Niedergelassene noch zusätzliche Funktionalitäten:

- Dokumente sollen auch von Niedergelassenen eingestellt werden können.
- Niedergelassene sollen neue Fallakten anlegen können, so dass über die Fallakte Informationen zu durchgeführten Maßnahmen schon zur Aufnahme in der Klinik verfügbar sind.
- Insbesondere für IV-Verträge und andere strukturierte Behandlungen wird eine fallbezogene Sicht über mehrere Aufenthalte hinweg gewünscht. In diesem Zuge sollen auch bestimmte administrative Vorgänge (Berechtigungserteilung, etc.) nicht mehr für jeden Aufenthalt, sondern für die gesamte Behandlungskette gelten.

Darüber hinaus hat sich gezeigt, dass die Klebchen auf der Versichertenkarte keine optimale Lösung sind, um die für die EFA genutzte ID des Patienten für alle beteiligten Ärzte bekannt zu machen. Es soll daher eine Lösung gefunden werden, mit der Niedergelassene auch mit ihren internen Patienten-IDs Fallakten identifizieren und nutzen können.

Nachfolgend wird skizziert, wie die in Szenario 1 aufgebaute Lösung um die genannten Funktionen erweitert werden kann.

Umsetzungsschritt 1: Schreibrechte für Niedergelassene

Der EFA-Connector verfügt bereits über eine Schnittstelle, mit der Niedergelassene Daten in eine bestehende Fallakte einstellen können. Um das Einstellen von Daten durch Niedergelassene technisch zu ermöglichen, muss diese Schnittstelle lediglich aktiviert und im Clientsystem (Portal) durch eine grafische Schnittstelle abgebildet werden. Die Aktivierung dieser Funktion erfolgt durch eine Konfiguration derEFA-Box, so dass für jede EFA ein spezieller Ordner angelegt wird, in dem die von Externen eingestellten Daten verwaltet werden.

Technische Umsetzung (Beispiel): Das Einstellen der Daten über das Portal erfolgt über ein HTTPS-Upload. Das Portal nimmt die Daten entgegen und leitet sie über den EFA-Connector an die EFA-Box weiter. Es findet keine Verarbeitung oder Speicherung der Daten im Portal statt.

In der EFA ist ein Ordner angelegt, in den die Daten der Niedergelassenen eingestellt werden. Dieser Ordner ist über einen EFA-Stecker direkt mit einem Datenspeicher in der Klink (z. B. dem Archivsystem) verknüpft (siehe Kapitel 2.2). Hierdurch werden die Daten nicht in der EFA-Box, sondern in einem speziell gesicherten System der Klink abgelegt und unterliegen damit auch automatisch allen bestehenden Prozessen zur Datensicherung und zur Archivierung.

Rechtlich entspricht die Speicherung von EFA-Daten für Niedergelassene einer »Datenverarbeitung im Auftrag«. Niedergelassene, die Daten in eine EFA einstellen möchten, müssen daher zunächst einen entsprechenden Vertrag mit der Klink als EFA-Anbieter schließen. An der EFA teilnehmende Patienten müssen zusätzlich zur Einwilligung in die Nutzung der EFA auch eine Einwilligung unterschreiben, dass sie damit einverstanden sind, dass die Klinik fallrelevante Daten im Auftrag der Ersteller (d.h. der teilnehmenden niedergelassenen Ärzte) in einer EFA vorhält und verarbeitet.

Umsetzungsschritt 2: Nutzung mehrerer Patienten-IDs

Anmerkung: Mit der Ende 2011 beginnenden Einführung der elektronischen Gesundheitskarte (eGK) ist zumindest jedem gesetzlich Versicherten eine lebenslang eindeutige Identifikationsnummer für das Gesundheitswesen zugewiesen. Diese Nummer ist sowohl auf der eGK aufgedruckt als auch elektronisch gespeichert. Durch Nutzung dieser Nummer als Patienten-IDs werden die nachfolgend beschriebenen Abläufe zum Umgang mit unterschiedlichen IDs für einen Patienten obsolet.

Damit alle EFA-Nutzer Fallakten anhand ihrer lokal bekannten Patienten-IDs auffinden und nutzen können, muss in der Klinik ein Master Patient Index verfügbar sein, über den verschiedene IDs eines Patienten aufeinander ab-

gebildet werden können. Dieser wird über einen EFA-Stecker an die EFA-Box angebunden (siehe Kapitel 2.4).

Um die so verfügbaren Funktionen des Identitätsmanagements nutzen zu können, wird ein zweites Portal aufgesetzt (das Sicherheitskonzept der EFA verlangt eine informationstechnische Trennung von Funktionen des Identitätsmanagements und Funktionen zum Austausch medizinischer Daten). Über dieses Portal kann ein Arzt durch Angabe von demografischen Daten eines Patienten prüfen, ob für den Patienten Fallakten bestehen, zu denen er zugriffsberechtigt ist. Ist dies der Fall, kann er Zugangscodes für seine intern genutzte Patienten-ID erzeugen lassen und mit den gefundenen Fallakten verknüpfen. Bei zukünftig für diesen Patienten angelegten Fallakten nutzt die EFA dann automatisch diese ID.

Technische Umsetzung (Beispiel): Über das Portal gibt der Arzt Name, Geburtsdatum und Wohnort des Patienten an. Das Portal leitet diese Daten an den für die Erzeugung von Zugangscodes zuständigen Admission Token Service[3] weiter. Der Admission Token Service fragt über den eMPI-Stecker beim Master Patient Index die zu diesem Patienten vergebenen IDs ab. Sofern der Patient vom Master Patient Index eindeutig identifiziert werden kann (was voraussetzt, dass dieser im Krankenhaus bereits bekannt ist), sendet der Master Patient Index die vergebenen Patienten-IDs zusammen mit weiteren demografischen Daten (z. B. Adresse und Geburtsort) an den Admission Token Service zurück. Der Admission Token Service erzeugt mit Hilfe der ID des anfragenden Arztes Zugangscodes für alle bekannten IDs des Patienten und fragt beim in der EFA-Box gekapselten Berechtigungsmanagement an, ob mit einem dieser Zugangscodes bereits Fallakten verknüpft wurden (was bedeutet, dass diesem Arzt eine Berechtigung erteilt wurde, er aber bislang aufgrund der Unkenntnis der verwendeten Patienten-ID den zum Zugriff benötigten Zugangscode nicht bilden konnte).

Der Admission Token Service liefert die IDs, zu denen Berechtigungen für den Arzt vergeben wurden, zusammen mit den zusätzlichen demografischen Daten an das Portal zurück. Dieses zeigt diese Daten an, so dass der Arzt noch einmal verifizieren kann, dass es sich wirklich um den gesuchten Patienten handelt. Anschließend gibt der Arzt seine lokal genutzte Patienten-ID im Portal an, das diese zusammen mit den gefundenen IDs wieder an den Admission Token Service sendet. Dieser erzeugt für die angegebene lokale Patienten-ID die erforderlichen Zugangscodes des Arztes und verknüpft diese mit den im ersten Schritt gefundenen Fallakten. Zusätzlich wird die vom Arzt angegebene Patienten-ID am eMPI registriert, so dass zukünftig bei einer Berechtigungsvergabe an diesen Arzt direkt die von diesem genutzte Patienten-ID verwendet werden kann.

[3] Ein Admission Token Service wird zusammen mit der EFA-Box ausgeliefert, muss aber getrennt von den anderen Komponenten der EFA-Box auf einem separaten System betrieben werden, um eine Zusammenführung von Identitätsdaten mit medizinischen Daten zu verhindern.

Umsetzungsschritt 3: Anlegen von Fallakten durch Niedergelassene

Bei der Anlage einer Fallakte durch einen niedergelassenen Arzt muss der Patient zunächst zwei Einwilligungen unterschreiben (siehe auch Schritt 1):

- Einwilligung in die Nutzung der Fallakte. Hierbei werden auch die initial zu berechtigenden Personen und Einrichtungen benannt.
- Einwilligung in eine Datenverarbeitung im Auftrag durch die Klinik in ihrer Rolle als EFA-Provider

Der EFA-Connector verfügt bereits über eine Schnittstelle, mit der Niedergelassene Fallakten bei einem EFA-Provider anlegen können. Um das Anlegen einer Fallakte durch Niedergelassene technisch zu ermöglichen, muss diese Schnittstelle lediglich aktiviert und im Clientsystem (Portal) durch eine grafische Schnittstelle abgebildet werden. Die Aktivierung erfolgt dadurch, dass im Berechtigungsmanagement der EFA-Box ein entsprechendes Recht zum Anlegen von Fallakten durch den Niedergelassenen eingetragen wird. Die einzige Voraussetzung hierfür ist das Vorliegen eines Vertrags, der besagt, dass die Klinik im EFA-Kontext für diesen Niedergelassenen eine Datenverarbeitung im Auftrag durchführt.

Wenn diese Voraussetzungen erfüllt sind, kann der Niedergelassene über das Portal Name und Geburtsdatum des Patienten, den Zweck der EFA beschreibende Diagnosen (als ICD-10) und die zu berechtigenden Mitbehandler angeben. Diese Informationen werden in einem standardisierten CDA-Dokument zusammengefasst und vom EFA-Connector verschlüsselt an die EFA-Box weitergeleitet, wo die Fallakte angelegt wird.

Abschließend kann der Arzt alle für die weitere Behandlung erforderlichen Dokumente in die neu angelegte Fallakte einstellen.

Umsetzungsschritt 4: Verknüpfung von Aufenthalten

Im Szenario 1 wurde für jeden Aufenthalt im Krankenhaus (administrativer Fall) bei der Aufnahme eine eigene Fallakte mit einem einzigen Ordner für diesen Aufenthalt angelegt. Wenn sich ein medizinischer Fall über mehrere Aufenthalte erstreckt oder wenn bereits von einem Niedergelassenen eine Fallakte zu dem medizinischen Fall erstellt wurde, soll jedoch bei der Aufnahme nicht jedes Mal eine neue Fallakte erstellt werden, sondern der aktuelle Aufenthalt soll vielmehr mit einer bestehenden Fallakte verknüpft werden.

Voraussetzung für eine automatisierte Verknüpfung ist, dass für das aufnehmende Krankenhaus bei der Anlage der EFA bereits eine Berechtigung vergeben wurde. Sofern die an die Fallakte gebundene Diagnose mit der Aufnahmediagnose übereinstimmt, wird in dieser Fallakte ein neuer Ordner erstellt und mit dem aktuellen Aufenthalt verknüpft. Das Einspielen von Da-

ten in diese Fallakte erfolgt ohne weitere Aktionen seitens des Krankenhauses automatisch wie in Szenario 1 beschrieben.

Technische Umsetzung (Beispiel): Wie in Szenario 1 wird auch in diesem Szenario die bei der Aufnahme erzeugte ADT^01-Nachricht vom EFA-Stecker verarbeitet und als den aktuellen administrativen Fall beschreibendes CDA-Dokument an die EFA-Box gesandt. Die EFA-Box ruft vom Admission Token Service (s.o.) den Zugangscode für das aufnehmende Krankenhaus ab. Gegen das Berechtigungsmanagement der EFA (Teil der EFA-Box) kann nun geprüft werden, ob schon Fallakten bestehen, auf die für diesen Zugangscode eine Berechtigung vergeben wurde. Ist dies der Fall, wird die an diese Fallakten gebundene Diagnose mit den in der ADT-Nachricht enthaltenen Diagnosen (DG1-Segment der ADT-Nachricht) abgeglichen. Falls die ersten drei Stellen des ICD-10-Codes übereinstimmen, wird wie in Szenario 1 ein neuer Ordner erstellt. Dieser wird anschließend mit der gefundenen Fallakte verknüpft. Sofern keine passende EFA gefunden wurde, wird – bei gegebener Einwilligung des Patienten – analog zu Szenario 1 eine neue Fallakte angelegt. Diese kann später ggf. mit einer schon bestehenden, aber anhand der verfügbaren Identitätsdaten oder aufgrund fehlender Einwilligungen für die Klinik nicht auffindbaren Fallakte verknüpft werden.

3.3 Szenario 3: Vernetzung von zwei Krankenhäusern

Eine ca. 100 km entfernte kardiologische Spezialklinik möchte ebenfalls Fallakten nutzen. Da es relativ viele Verlegungen von dem Grundversorger gibt, möchte man nicht ein zweites, isoliertes Portal aufsetzen, sondern den Niedergelassenen eine möglichst integrierte Sicht auf die bei beiden Kliniken verfügbaren Daten bieten.

Umsetzungsschritt 1: Vernetzung von EFA-Boxen

Da die Spezialklinik keine über die Wartung von Medizintechnik hinausgehenden Kompetenzen im Rechenzentrumsbetrieb besitzt, möchte man die beim Grundversorger betriebenen EFA-Sicherheitsdienste mitnutzen und lediglich die Register und Datenspeicher im eigenen Haus behalten.

Hierzu beschafft die Spezialklinik eine eFA-Box, die so konfiguriert ist, dass sie die Sicherheitsdienste einer anderen eFA-Box mitnutzt. Um einen sicheren Zugang zu den Sicherheitsdiensten herzustellen, wird mit entsprechender, wartungsarmer Hardware ein VPN zwischen der eFA-Box in der Spezialklinik und der eFA-Box beim Grundversorger aufgesetzt.

Anschließend werden die Fallakten-Register beider EFA-Boxen über die Peer-to-Peer Adapter miteinander vernetzt. Dies ist lediglich eine Konfigurationseinstellung in den EFA-Boxen, bei der die Netzwerkadressen und Dienstzertifikate einer EFA-Box bei der jeweils anderen EFA-Box als vertrauenswürdig registriert werden.

Umsetzungsschritt 2: Single Points of Access

Die Spezialklinik setzt ebenfalls ein EFA-Portal auf. Dieses nutzt die beim Grundversorger angesiedelten Sicherheitsdienste, leitet den Nutzer aber nach der Authentifizierung und Autorisierung an die eigene EFA-Box weiter.

Durch die eingebaute Peer-to-Peer Funktionalität werden Suchanfragen nach Fallakten eines Patienten von jeder der beiden EFA-Boxen automatisch auch an die jeweils andere EFA-Box weitergeleitet. Hierdurch sind über jedes der beiden Portale alle Akten auffindbar und zugreifbar – unabhängig davon, ob sie beim Grundversorger oder bei der Spezialklinik angelegt wurden. Für die Nutzer ist dies komplett unsichtbar: Ein Niedergelassener kann wie bisher über das Portal des Grundversorgers auf Fallakten seiner Patienten zugreifen – nur dass er jetzt auch die Daten sieht, die im Fall einer Verlegung bei der Spezialklinik angelegt wurden.

3.4 Szenario 4: Primärsystem-Integration der Fallakte

Nachdem immer mehr Ärzte in der Region mit den Kliniken über Fallakten kommunizieren, wird der Wunsch laut, die EFA direkt in die genutzten Primärsysteme zu integrieren. Hierdurch würde das Verschieben von Daten zwischen den internen Systemen und dem Portal entfallen und es könnten einige Funktionalitäten deutlich komfortabler genutzt werden. Darüber hinaus verwenden einige Ärzte auch noch weitere Gesundheitsdatendienste und möchten die Möglichkeit der EFA für ein Single Sign-On nutzen, d.h. mit einer Anmeldung auf alle genutzten Dienste zugreifen können.

Umsetzungsschritt 1 (beim Hersteller): Integration des EFA-Connectors

Die direkte Anbindung eines Primärsystems an eine EFA ist einfach realisierbar, da der bereits im Portal verwendete EFA-Connector als Software-Modul auch von Primärsystemherstellern genutzt werden kann. Der EFA-Connector kapselt die gesamte EFA-Sicherheitsfunktionalität und bietet einfache Schnittstellen zum Abrufen und Anlegen von Fallakten sowie zum Auslesen und Einstellen von Dokumenten. Ein PVS- oder KIS-Hersteller kann den EFA-Connector einfach in seine Software einbinden und muss lediglich die EFA-Funktionen in die grafische Benutzeroberfläche einbetten und die Anbindung an die interne Dokumentendatenbank und Patientenverwaltung herstellen.

Sobald ein Arzt in seinem System das Datenblatt eines Patienten öffnet wird automatisch im Hintergrund nach Fallakten gesucht. Von den gefundenen Akten wird das Inhaltsverzeichnis ausgelesen und die dort verzeichneten Dokumente werden zusammen mit den lokal verfügbaren Daten angezeigt. Ärzte können so Daten mit einem Mausklick aus einer EFA auslesen oder in eine EFA einstellen.

Umsetzungsschritt 2 (beim Hersteller): CDA-Unterstützung (optional)

Einige der Primärsystem-Hersteller unterstützen den HL7 v3 CDA-Standard, um beispielsweise Arztbriefe nach dem Leitfaden des Herstellerverbands bvitg (vormals VHitG) zu erstellen. Mit Hilfe dieses Standards können viele Funktionen der EFA-Box noch einfacher genutzt und in bestehende Systeme integriert werden:

- neue Fallakten können über CDA-Dokumente beschrieben werden, die an die Fallakte gesandt werden. Der Arzt schreibt quasi einen Arztbrief an die EFA-Box, in dem er die der EFA zugrunde liegenden Diagnosen auflistet und die Mitbehandler benennt. Eine Arzt-Software, die bereits jetzt strukturierte Arztbriefe unterstützt, verfügt implizit über alle Bausteine, um diese Funktionalität der EFA-Box zu nutzen.

- Veränderungen am Kreis der Behandler werden ebenfalls über CDA-Dokumente beschrieben, die an die EFA-Box geschickt werden. Der Vorteil hiervon ist, dass aus dem entsprechenden Dokument gleich auch die vom Patienten zu unterschreibende Einwilligung generiert werden kann.

- In der EFA-Box ist ein spezielles CDA-Dokument abgelegt, dass quasi das aktuelle Inhaltsverzeichnis der EFA mit Verweisen auf alle in der EFA abgelegten Dokumente abbildet. Anstatt in der EFA nach Dokumenten zu suchen oder durch die Ordnerstruktur der EFA zu browsen, kann eine Arzt-Software auch einfach dieses Inhaltsverzeichnis abrufen. Dadurch, dass dieses Dokument strukturiert und kodiert ist (z. B. sind alle Diagnosen als ICD-10 verfügbar), kann sein Inhalt sehr einfach visualisiert oder in eine bestehende Nutzeroberfläche integriert werden.

Umsetzungsschritt 3: Individuelle Anpassung der EFA (optional)

Ärzte in einem Versorgungsnetz können eigene, fachspezifische Erweiterungen für Fallakten definieren, die auf CDA-Inhalte abgebildet werden. Beispiele hierfür sind ein Verzeichnis von durchgeführten Untersuchungen oder eine Liste der dem Patienten verordneten Medikamente. Die EFA-Box verarbeitet diese Informationen nicht, beinhaltet aber Funktionen, mit denen solche Inhalte angelegt und fortgeschrieben werden können (sofern sie den syntaktischen Vorgaben des CDA-Standards entsprechen).

Technische Umsetzung (Beispiel): Über die Fallakte soll von der Klinik ein Behandlungsplan vorgegeben und gepflegt werden. Hierzu wird in das zur Anlage der Fallakte erstellte CDA-Dokument ein Abschnitt aufgenommen, der nach der Vorgabe von IHE für eine kodierte »Care Plan Section« strukturiert ist. Dieser Abschnitt wird in der EFA-Box abgespeichert und kann von allen Nutzern als Teil des oben angesprochenen EFA-Inhaltsverzeichnisses ausgelesen werden. Die Klinik kann die Inhalte der »Care Plan Section« erweitern oder verändern, in dem sie die Erweiterung bzw. Änderungen in einem CDA-Dokument beschreibt und dieses an die EFA-Box sendet. Die EFA-Box wendet die angegebenen Änderungen auf die aktuelle Version der »Care Plan Section« an und erstellt eine neue Version des Behandlungsplans.

Umsetzungsschritt 4: Sichere Anbindung

Anmerkung: Zusammen mit der elektronischen Gesundheitskarte wird schrittweise eine so genannte Telematikinfrastruktur eingeführt, über die alle Leistungserbringer des deutschen Gesundheitswesens auf Anwendungen der Gesundheitskarte und weitere Gesundheitsdatendienste zugreifen können. Die elektronische Fallakte wird aktuell durch die Deutsche Krankenhausgesellschaft und die gematik als erster solcher Gesundheitsdatendienst auf die Telematikinfrastruktur migriert. Hierdurch wird eine sichere Anbindung von Niedergelassenen an einen EFA-Provider ohne Mehraufwand mit Hilfe des gematik-Konnektors (im Prinzip ein spezieller Router mit eingebauten Firewalls) möglich.

Viele der niedergelassenen Ärzte in der Region nutzen KV SafeNet zur Abrechnung mit der Kassenärztlichen Vereinigung. Diese Technologie wird auch von der Klinik als EFA-Provider unterstützt und kann damit von den Niedergelassenen auch zur Kommunikation mit der EFA-Box genutzt werden.

Die anderen Ärzte greifen über eine mit Hilfe von Software-Zertifikaten abgesicherte TLS-Verbindung auf die EFA-Box zu. Um keine Risiken durch korrumpierte Zertifikate einzugehen, ist eine zusätzliche Authentifizierung über den Heilberufsausweis erforderlich, d.h. zusätzlich zur Anmeldung am lokalen System muss sich der Arzt auch noch an der EFA anmelden (was er allerdings vorher gegenüber dem Portal auch machen musste).

3.5 Szenario 5: Single Sign-On und Policy Push

Anmerkung: Das nachfolgend beschriebene Szenario ist über die EFA-Sicherheitsdienste umsetzbar, wird aber durch die Standard-Konfiguration einer EFA-Box nicht abgedeckt. Eine Umsetzung erfordert daher das Aufsetzen weiterer Instanzen der EFA-Sicherheitsdienste außerhalb der EFA-Box.

Die gemeinsame Nutzung der Sicherheitsdienste der Fallakte erlaubt es den Ärzten des Grundversorgers und der kardiologischen Spezialklinik, wechselseitig auf IT-Dienste und Ressourcen zuzugreifen, ohne dass man hierzu immer wieder ein neues Kennwort eingeben müsste. Auch die Zugriffsrechte orientieren sich an den Erfordernissen der übergreifenden Behandlungsketten bei Verlegungen, so dass nach einer kurzen »Einschwingphase« mittlerweile auch für den IT-Betrieb kaum noch Mehraufwände anfallen.

Aus Kostengründen wollen beide Kliniken bestimmte Laboraufträge extern vergeben. Der Abruf der Ergebnisse soll elektronisch über ein durch das KIS ansprechbares Portal des Labors erfolgen. Aus Datenschutzgründen werden Laboranforderungen immer einer Abteilung zugeordnet, und nur bestimmte Mitarbeiter der einzelnen Abteilungen sollen berechtigt sein, Laborergebnisse abzurufen. Der Zugriff auf die IT-Dienste des Labors soll dabei für die Ärzte so einfach und komfortabel erfolgen wie der Zugriff auf Daten der über die EFA vernetzten Kliniken.

Umsetzungsschritt 1: Single Sign-On

Bestandteil der EFA-Sicherheitsdienste ist ein so genanter Identity Provider, der Nachweise über erfolgreiche Authentifizierungen ausstellt und Identitätsmerkmale von Nutzern gegenüber Diensten und Portalen bestätigen kann. Hierüber soll ein Single Sign-On realisiert werden, in dass auch das Portal des Labors eingebunden ist.

Technische Umsetzung (Beispiel): Alle Mitarbeiter der Klinik melden sich über Nutzername und Kennwort am KIS an. Das KIS kann Informationen zum angemeldeten Nutzer als SAML-Assertion bereitstellen und mit einer TLS-Sitzung zwischen KIS und EFA Identity Provider verknüpfen. Hiermit kann auf Basis der lokalen Anmeldung vom EFA Identity Provider eine so genannte EFA Identity Assertion bereitgestellt werden, die auch für externe Dienste verifizierbar ist.

Das externe Labor setzt sein Portal so auf, dass eine Anmeldung über eine EFA Identity Assertion erfolgen kann. Dieses kann über Standardprotokolle und -produkte umgesetzt werden und erfordert lediglich, dass das Signaturzertifikat des EFA Identity Providers gegenüber dem Portal des Labors als vertrauenswürdig bekannt gegeben wird.

Hiermit können sich die Ärzte wie gehabt am KIS anmelden und mit der im KIS erfolgten Authentifizierung auch auf das Portal des Labors zugreifen. Insbesondere muss das Labor keine Nutzeraccounts für alle Mitarbeiter der Klinik pflegen, sondern kann anhand der übermittelten Identity Assertions prüfen, ob es sich um einen Klinikmitarbeiter handelt und welchem Fachbereich dieser zugeordnet ist.

Umsetzungsschritt 2: Policy Push

Klinik und Labor halten es für wenig praktikabel, wenn die in der Klinik festgelegten Rechte zum Zugriff auf Labordaten immer mit dem Berechtigungsmanagement des Labor-Portals synchronisiert werden müssen. Es soll daher eine Lösung umgesetzt werden, mit der die in der Klinik definierten Berechtigungen möglichst einfach um Rechte zum Zugriff auf externe Labordaten erweitert werden und dann in der Klinik gepflegt und im Portal des Labors durchgesetzt werden.

Technische Umsetzung (Beispiel): Zugriffe aus der Klinik werden im Labor-Portal über einen dedizierten Port geleitet. Mit diesem Port ist eine WS SecurityPolicy verknüpft, die definiert, dass zum Zugriff auf das Portal neben einer Identity Assertion auch eine Policy Assertion mitgegeben werden muss. Die WS SecurityPolicy verweist dabei auf einen in der Klinik betriebenen EFA-Sicherheitsdienst, der zu jedem authentifizierten Nutzer eine Berechtigungsregel liefern kann, in der die Rechte dieses Nutzers zum Zugriff auf externe Dienste beschrieben sind. Diese in der Klinik definierte Regel wird vom Portal des Labors ausgewertet und durchgesetzt. Hierdurch muss das Labor keine Berechtigungen für Mitarbeiter der Klinik pflegen, sondern erwartet von der Klinik, dass diese bei jedem Zugriff auf das Portal durch die Klinik zusammen mit der Anfrage übermittelt werden.

A Vorbedingungen für die elektronische Kommunikation

Die erste Herausforderung besteht in vielen E-Health-Projekten darin, dass die Krankenhaus-IT ungenügend auf die elektronische Kommunikation mit niedergelassenen Ärzten eingestellt ist. In den nachfolgenden Abschnitten werden typische Probleme und mögliche Lösungsansätze beschrieben. Als Bezugspunkt werden die in den Szenarien aufgeführten Beispiele verwendet.

A.1 Einpflegen eindeutiger Arzt-Identifizierer

Problemstellung

In allen Krankenhäusern gibt zwar ein zentrales elektronisches Adressbuch mit den Kontaktdaten der Ärzte in der Region, dieses wird jedoch oftmals eher ad hoc gepflegt und enthält zumeist auch keine Informationen, um einen Arzt in der elektronischen Kommunikation eindeutig zu identifizieren. Externe Ärzte können sich also zwar mit ihrem Heilberufsausweis an dem in der EFA-Box enthaltenen Identity Provider anmelden (siehe A.2), es gibt aber keine Möglichkeit, diese Anmeldung mit dem eigenen Datenbestand im Adressbuch zu verknüpfen (d. h. man kann nicht abgleichen, ob ein über das Portal angemeldeter Arzt derjenige ist, der einen bestimmten Patienten eingewiesen hat oder von diesem als Hausarzt benannt wurde).

Die fehlende Verknüpfung von Daten der elektronischen Kommunikation und der im Adressbuch vorhandenen Daten der »konventionellen« Kommunikation bildet die so genannte Telematik-ID. Die Telematik-ID ist eine auf dem Heilberufsausweis eines Arztes elektronisch gespeicherte Zahl, mit der ein Arzt eindeutig identifiziert werden kann. Um mit Niedergelassenen elektronisch kommunizieren zu können, müssen daher alle Adressdatensätze um die Telematik-ID der anzubindenden Ärzte ergänzt werden. Sofern Niedergelassene nicht als Person, sondern als Organisation (Praxis) mit dem Krankenhaus kommunizieren, muss zusätzlich auch die Telematik-ID der Praxis in das Adressbuch eingepflegt werden.

Lösungsbeispiel

Da auch die Niedergelassenen in der elektronischen Kommunikation wenig geübt sind, wird ein Nutzungsleitfaden erstellt. In diesem sind einige elementare Verhaltensregeln festgeschrieben, zu deren Einhaltung sich die Ärzte per Unterschrift verpflichten müssen, bevor sie über das Portal Patientendaten abrufen können. Ärzte können das entsprechende Formular von der Webseite des Krankenhauses herunterladen und müssen dieses mit ihrem Heilberufsausweis elektronisch signieren und dann per E-Mail an die Klinik zurücksenden. In der Klinik werden die signierten Formulare von der IT-

Abteilung archiviert und die in der Signatur enthaltene Telematik-ID wird manuell in das Adressbuch eingepflegt. Sofern in der Signatur auch weitere Adressdaten vorhanden sind, werden auch diese mit dem Adressbuch abgeglichen.

A.2 Authentifizierung von Niedergelassenen

Problemstellung

Damit niedergelassene Ärzte elektronische Dienste des Krankenhauses nutzen können, müssen sie eindeutig identifiziert und authentifiziert werden können. Zur Identifizierung ist eine eindeutige ID erforderlich (siehe A.1). Zusätzlich muss zur Authentifizierung ein geheimes Merkmal des Arztes überprüft werden, das nur der Arzt kennt bzw. besitzt oder nutzen kann. Ein typisches Beispiel ist ein geheimes Kennwort, das bei der Anmeldung überprüft wird.

Für das Krankenhaus als Dienstanbieter haben geheime Kennwörter jedoch drei gravierende Nachteile:

- Kennwörter sind unsicher, wenn sie nicht häufig gewechselt werden. Sie müssen daher durch zusätzliche Maßnahmen (z. B. VPN-Tunnel zwischen Arztpraxis und Krankenhaus) abgesichert werden, wodurch zusätzliche Kosten entstehen.

- Das Krankenhaus muss für alle kooperierenden Ärzte Kennwörter pflegen. Dieser Aufwand ist nicht zu unterschätzen, insbesondere wenn man bedenkt, dass Ärzte ihre Kennwörter vergessen können und es dann Prozesse zur sicheren Zuweisung eines neuen Kennworts geben muss.

- In einigen Regionen (z. B. Kammerbezirk Nordrhein) hat bereits die Ausgabe von elektronischen Heilberufsausweisen (HBA) an die niedergelassenen Ärzte begonnen. Mit der Einführung der Anwendungen zur Gesundheitskarte werden alle Praxen zusätzlich einen elektronischen Organisationsausweis (SMC-B) erhalten. Mit beiden Ausweisen ist eine sichere Authentifizierung möglich, d. h. alle anderen Lösungen werden mit Verfügbarkeit von HBA und SMC-B an Relevanz und Akzeptanz verlieren.

Kennwörter sollten daher nur genutzt werden, wenn die entsprechende sichere Infrastruktur (z. B. in Kombination mit einem VPN) bereits besteht. Alternativen sind Einmal-Passwörter (z. B. RSA SecurID) und Chipkarten wie z. B. der HBA und die SMC-B.

Lösungsbeispiel 1: Nutzung des Heilberufsausweises

Der Heilberufsausweis (HBA) ist eine SmartCard, die aktuell von den Landesärztekammern an alle Ärzte ausgegeben wird[4]. Der HBA verfügt nicht nur über eine qualifizierte Signatur für die elektronische Unterschrift, sondern auch über weitere digitale Zertifikate für die Authentifizierung und Verschlüsselung.

Der in die EFA-Box eingebaute Identity Provider unterstützt eine Anmeldung über einen HBA. Ein Arzt kann sich damit aus seinem Arztsystem heraus sehr einfach durch Stecken des HBA und Eingabe der zugehörigen PIN gegenüber der EFA-Plattform authentifizieren. Sofern die Authentifizierung über ein Web-Portal erfolgen soll, muss zuvor ein entsprechendes Browser-Plugin installiert werden.

Lösungsbeispiel 2: Nutzung der SMC-B

Eine alternative Umsetzung der Authentifizierung ist über die SMC-B möglich. Diese Option ist deutlich komfortabler, da sie z. B. auch die Authentifizierung von Praxispersonal ohne eigenen HBA erlaubt. Der Nachteil ist jedoch, dass hierzu Erweiterungen an dem Praxis-IT-System des Arztes erforderlich sind.

Bei der Anmeldung über die SMC-B wird das so genannte Guarantor-Token-Verfahren genutzt. Der Arzt (bzw. ein Praxismitarbeiter) meldet sich zunächst an seinem lokalen System an. Das Praxissystem identifiziert und authentifiziert die angemeldete Person und stellt ein so genanntes Guarantor Token aus. In diesem ist in einem standardisierten Format kodiert, wer die Person ist und welche Rolle sie hat (z. B. Arzt oder Arztgehilfe). Das Guarantor Token wird anschließend in der Arztpraxis mit der SMC-B digital signiert. Das Arztsystem verbürgt damit die Richtigkeit der Angaben.

Im nächsten Schritt wird das Guarantor Token an den in der EFA-Box eingebauten Identity Provider geschickt. Der Identity Provider prüft die Signatur auf dem Guarantor Token und erstellt aus den im Token enthaltenen Daten einen Authentisierungsnachweis in dem von der EFA-Plattform geforderten Format. Dieser Nachweis wird an das Arztsystem zurück geschickt und kann nun zum Zugriff auf an die EFA-Plattform angebundene Dienste genutzt werden.

[4] Siehe z. B. http://www.aekno.de/page.asp?pageID=5285

A.3 Verwendung einer eindeutigen Patienten-ID

Um auf eine Fallakte zuzugreifen, muss ein Arzt diese zunächst einmal auffinden und identifizieren. Dies ist nicht so einfach, da Fallakten nach »außen« immer nur über nutzerspezifische Pseudonyme – so genannte Admission Codes – sichtbar sind. Damit ein Arzt eine Fallakte eines Patienten finden kann, muss er somit den Admission Code angeben können, der ihm für diesen Patienten zugeordnet ist. Dies erfolgt über einen spezifischen Dienst (Admission Token Service), der aus der ID eines Arztes bzw. einer Gesundheitseinrichtung und der ID des Patienten den Admission Code berechnet.

Das ganze Verfahren funktioniert aber nur dann, wenn bei der Erteilung einer Berechtigung für diesen Arzt und beim Abruf des Admission Codes durch diesen Arzt immer die gleiche Patienten-ID verwendet wird. Dies ist trivial, wenn der Arzt die Akte selber angelegt hat, da er in diesem Fall selber festlegt, welche ID für den Patienten verwendet werden soll. Wenn die Akte jedoch durch einen anderen Arzt angelegt wurde, hat dieser die ID des Patienten festgelegt – und dies ist potenziell nicht die ID, unter der dieser Patient auch bei anderen Ärzten bekannt ist.

Die EFA bietet drei Optionen zur Lösung dieses Problems. Zwei davon – die Nutzung der Gesundheitskarte als Identifizierungsmerkmal und die Verwaltung verschiedener IDs eines Patienten über einen Master Patient Index – wurden in diesem Dokument bereits skizziert.

Die dritte Option ist die Verwendung so genannter Record Discovery Token (RDT). Ein RDT ist eine auf einen Träger (z. B. ein Überweisungsformular) aufgebrachte Zahl, die bei der Vergabe einer Berechtigung erzeugt wird. Ein Arzt kann diese Zahl zusammen mit seiner ID an die EFA-Box senden und erhält von der EFA-Box einen Verweis auf die entsprechende Fallakte. Dieser Verweis ist so kodiert, dass der Arzt einmalig ohne Admission Code nur auf Basis seiner Identitätsdaten auf die Fallakte zugreifen kann, sofern er zur Nutzung dieser Fallakte berechtigt wurde. Im Rahmen dieser einmaligen Nutzung kann er nun entweder

- die bei der Anlage der EFA genutzte Patienten-ID abrufen und in seinem IT-System vermerken. Mit Hilfe dieser ID kann er anschließend den für weitere Zugriffe benötigten Admission Code erzeugen lassen.

- Die für ihn erteilte Berechtigung um die von ihm verwendete Patienten-ID ergänzen. Die EFA-Box erzeugt auf Basis dieser Angaben einen weiteren Admission Code und verknüpft ihn mit der Fallakte, so dass der Arzt zukünftig seine intern genutzte Patienten-ID auch für den Zugriff auf die EFA nutzen kann.

B Abkürzungen

CDA	Clinical Document Architecture (HL7 v3 Standard zur Kodierung strukturierter medizinischer Dokumente)
eCR	electronic CaseRecord (engl. Bezeichnung für EFA)
EFA	elektronische Fallakte
eGK	elektronische Gesundheitskarte
HBA	Heilberufsausweis
IHE	Integrating the Healthcare Enterprise (Forum für Anwender und Hersteller zur Profilierung von Standards für das Gesundheitswesen)
KIS	Krankenhausinformationssystem
MPI	Master Patient Index (Verzeichnis der genutzten IDs für einen Patienten)
PVS	Praxisverwaltungssystem
SMC-B	Secure Module Card (»Ausweis« für Gesundheitseinrichtungen)
XACML	eXtensible Access Control Markup Language (Standard zur regelbasierten Kodierung von Zugriffsberechtigungen)
XDS	Cross-Enterprise Document Sharing (IHE-Standard für elektronische Akten)

C EFA-Spezifikation

Anmerkung: Die nachfolgende Liste führt nur die Teile der EFA-Spezifikation auf, die die Inhalte dieses Dokuments vertiefen.
Alle EFA-Spezifikationen sind über www.fallakte.de frei verfügbar.

eCR in a Box: Specification Overview. Version 1.0, September 2011.

eCR in a Box: Content Modules. Version 1.0, September 2011.

eCR Application Architecture – Services and Interfaces. Version 1.2, März 2008.

eCR Security Architecture v1.2 – Services and Interfaces, Version 1.2.0.5, April 2008.

Übergreifendes Sicherheitskonzept für Umsetzung und Betrieb elektronischer Fallakten. Version 1.2, März 2008.