Erweiterung des Konzeptes einer Patientenakte nach § 291a SGB V um eine Schnittstelle für die medizinische Forschung

Dissertation

zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades

"Doctor rerum naturalium"

der Georg-August-Universität Göttingen

im Promotionsprogramm in Computer Science (PCS)

der Georg-August University School of Science (GAUSS)

vorgelegt von

Krister Helbing

aus Hamburg

Göttingen, 2012

Betreuungsausschuss:

Prof. Dr. Otto Rienhoff, Abt. Medizinische Informatik, Universitätsmedizin Göttingen

Prof. Dr. Ulrich Sax, Geschäftsbereich Informationstechnologie, Universitätsmedizin Göttingen

Prof. Dr. Dieter Hogrefe, Institut für Informatik, Universität Göttingen

Mitglieder der Prüfungskommission:

Referent: Prof. Dr. Otto Rienhoff, Abt. Medizinische Informatik, Universitätsmedizin Göttingen

Korreferent: Prof. Dr. Ulrich Sax, Geschäftsbereich Informationstechnologie, Universitätsmedizin Göttingen

Korreferent: Prof. Dr. Klaus Pommerening, Institut für Medizinische Biometrie, Epidemiologie und Informatik (IMBEI), Universitätsmedizin Mainz

Weitere Mitglieder der Prüfungskommission:

Prof. Dr. Jens Grabowski, Institut für Informatik, Universität Göttingen

Prof. Dr. Dieter Hogrefe, Institut für Informatik, Universität Göttingen

Prof. Dr. Konrad Rieck, Institut für Informatik, Universität Göttingen

Tag der mündlichen Prüfung: 11. Januar 2013

Zusammenfassung

Ein zentrales Thema der medizinischen Informatik ist der institutionsübergreifende Austausch von Patientendaten zwischen den Akteuren des Gesundheitswesens. Die Notwendigkeit einer einheitlichen nationalen Telematikinfrastruktur für einen institutionsübergreifenden Austausch wurde auch von der Politik anerkannt. Dementsprechend wurde 2003 mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG) der erste Grundstein gelegt. Eine der Anwendungen, die laut Gesetzgebung (§ 291a SGB V) über die Telematikinfrastruktur umgesetzt werden sollte, ist die sogenannte elektronische Patientenakte. Diese Anwendung sollte es dem Patienten ermöglichen, seine Versorgungsdaten in einer eigenen Dokumentation zu führen und mit den Systemen seiner Behandler elektronisch zu kommunizieren.

Bei der Gesetzgebung wurde der Fokus sehr eng gefasst, um aus Datenschutzgründen eine enge Zweckbindung der elektronischen Patientenakte sicher zu stellen. Wichtige Themen wie die Partizipation der Bürger und Patienten an der medizinischen Forschung wurden ausgeklammert. Werden die Prozesse der elektronischen Datenerfassung in der Versorgung und in der medizinisch-klinischen Forschung (z. B. den Universitätskliniken) betrachtet, so fällt auf, dass relevante Daten für die Versorgung und die Forschung häufig identisch sind. Da die Systeme von Forschung und Versorgung aber getrennt voneinander betrieben werden, kommt es zu Doppelerfassungen. Diese Doppelerfassungen sind für einen Anwender, der Daten in beide Systeme eintragen muss, schwer nachvollziehbar - auch die gewünschte Partizipation der Patienten an Forschungsvorhaben ist so kaum möglich.

Die grundlegende Idee dieser Arbeit ist es, eine Schnittstelle zwischen einer elektronischen Patientenakte und der medizinischen Forschung gemäß den Vorgaben der nationalen Telematikinfrastruktur zu konzipieren. Damit soll dem oben geschilderten Problem der Doppelerfassung von Patientendaten entgegengewirkt werden, indem mit Hilfe dieser Schnittstelle ein Austausch von Patientendaten über eine elektronische Patientenakte zwischen den Systemen der Versorgung und Forschung ermöglicht wird.

Zu diesem Zweck wurden zunächst die Systeme der Versorgung und der Forschung analysiert und ein Kommunikationsmodell sowie Datenschutzanforderungen für die Kommunikation zwischen einer elektronischen Patientenakte und den Systemen der Forschung formuliert. Auf Grundlage des Kommunikationsmodells und der Datenschutzanforderungen wurden sowohl eine Fach- als auch eine Sicherheitsarchitektur für die Schnittstelle zwischen einer elektronischen Patientenakte und den Systemen der Forschung beschrieben. Als Ergebnis konnte herausgestellt werden, dass die Anbindung der IT-Systeme der medizinischen Forschung über eine elektronische Patientenakte sicher und datenschutzkonform umgesetzt werden kann.

Abschließend wird der entstandene Ansatz mit bisherigen Lösungen zur Nutzung von Versorgungsdaten für die medizinische Forschung kritisch verglichen und die Stärken einer in der nationalen Telematikinfrastruktur integrierte Löschung gegenüber alleinstehenden Insellösungen hervorgehoben. Es wird herausgestellt, dass die grundlegenden Konzepte stehen, aber noch erheblicher Aufwand erbracht werden muss, um ein auf nationaler Ebene verfügbares System bereitzustellen. Vorschläge für die weiteren Arbeiten zu einem funktionierenden System sowie weitere Potentiale der Ergebnisse dieser Arbeit werden in einem Ausblick aufgezeigt.

Abstract

A central topic of medical informatics is the exchange of patient data between the different actors in the health care system. The German Government has recognized the need for a unified, national telematics infrastructure for cross-institutional data exchange. In 2003, the passing of the German Bill on the modernization of public health care [GMG] marked the first step.

According to Article 291a SGB V of the Bill, one of the applications that this telematics infrastructure is supposed to enable is the electronic patient record. This application shall enable patients to access data collected during their routine medical care and communicate electronically with the systems used by their clinicians.

The scope of the law was kept narrow in order to limit the use and dissemination of data in the electronic patient record, for privacy reasons. Important topics, such as patients' participation in medical research, were left out. Looking at the process of electronic data capture both in a routine care and a medical-clinical research environment (for example, in university hospitals), it appears that the data relevant to care and research are often identical. Yet, as the systems for research and routine care are operated separately, the information is recorded twice. This duplication of data seems illogical to a user who has to key the same data into both systems. It does not promote inclusion of patients in research studies either.

The goal of this thesis is to develop the conceptual design of an interface between an electronic patient record and the medical research systems, according to the specifications of the national telematics infrastructure. This interface should resolve the problem of double data entry by enabling the interchange of patient data between systems used in routine care and for research via the electronic patient record.

First, both systems of routine care and medical research are analyzed and a communication model, as well as data protection requirements for the communication between the electronic patient record and the systems of research, drawn up. Then, based on the communication model and the data protection requirements, both a technical framework and a security framework for this interface are described. As a result it is argued that a connection of the IT systems for medical research via the electronic patient record can be realized in a secure way while still maintaining data protection standards.

Finally, the solution is critically examined by comparing it to other, existing approaches for the use of routine care data for medical research. The advantages of a solution integrated into the national telematics infrastructure as compared to an isolated solution are shown. The author concludes that the theories are validated in a scenario with limited scope, but there still are significant challenges to make it nationally available.

Proposals for further work towards a functioning system as well as other opportunities, based on the results of this thesis, are described.

Danksagung

An dieser Stelle möchte ich allen danken, die mich während des langen Prozesses meiner Promotion tatkräftig unterstützt haben. Mein besonderer Dank gilt meinem Erstbetreuer Prof. Dr. Otto Rienhoff für die kreativen Gespräche bei der Auslotung meines Themas und für die fachliche Unterstützung bei der Ausarbeitung des Themas. Meinem Zweitbetreuer Prof. Dr. Ulrich Sax bin ich ebenfalls zu großem Dank verpflichtet. Er stand mir besonders in der Abschlussphase regelmäßig für Diskussionen und Fragen zur Verfügung. Auch beim dritten Mitglied meines Betreuungsausschusses Prof. Dr. Dieter Hogrefe, möchte ich mich herzlich bedanken, der immer wieder einen neuen Blickwinkel in die Diskussion eingebracht hat.

Für die Teilnahme am Experten-Review und die wertvollen Kommentare danke ich Herrn Dr. Johannes Drepper, Herrn Dr. Thomas Ganslandt und Herrn Prof. Dr. Klaus Pommerening.

Bedanken möchte ich mich auch bei meinen Kollegen und Kommilitonen für die zahlreichen Diskussionen und Anregungen. Besonderer Dank gilt auch denen, die es gewagt haben dieses umfangreiche Dokument Korrektur zu lesen.

Außerdem möchte ich mich bei den Kollegen aus dem Forschungs- und Entwicklungsprojekt zur elektronischen Patientenakte gemäß § 291a SGB V[1] für die anregenden Diskussionen und Kommentare bedanken.

Abschließend möchte ich mich noch bei meinen Eltern, meiner Schwester und meiner Lebensgefährtin für die umfangreiche Unterstützung während meiner Promotion bedanken.

[1] Das FuE Projekt zur »Elektronischen Patientenakte« gemäß § 291a SGB V wurde gefördert durch das Bundesministerium für Gesundheit (BMG) aufgrund eines Beschlusses des Deutschen Bundestages.

Inhaltsverzeichnis

1. Einleitung

Mit der elektronischen Erhebung und Verarbeitung von Versorgungsdaten und der Einführung von elektronischen Patientenakten kamen auch die Überlegungen auf, diese elektronisch erfassten Daten für wissenschaftliche Auswertungen zu nutzen. So wurden schon Ende des letzten Jahrhunderts Versorgungsdaten aus den Systemen der Versorgung für Forschungszwecke genutzt [1-6]. Während sich diese Ansätze meistens auf lokale Auswertungen bezogen, wurde 2003 im Rahmen einer Studie des Health Technology Assessment Program [7] des National Institute for Health Research in London [8] untersucht, inwieweit Versorgungsdaten für randomisierte kontrollierte Studien genutzt werden können. Darin wurde bestätigt, dass Versorgungsdaten randomisierte kontrollierte Studien unterstützen können [9]. 2005 wurde in einem Artikel von John Powell et. al festgestellt, dass elektronische Patientenakten (ePA) durch entsprechende Schnittstellen zwischen Forschungs- und Versorgungssystemen unter Berücksichtigung entsprechender Datenschutzmaßnahmen zu einer erheblichen Verbesserung der Effizienz in der klinischen Forschung führen würde; zum Beispiel im Bereich der Hypothesenbildung bzw. der Planung von Studien oder die Rekrutierung sowie der Aufbau von epidemiologischen Registern [10]. Auch auf europäischer Ebene wurde das Thema der Nutzung von Routinedaten für die Forschung immer präsenter, so dass es 2006 auf der Medical Informatics Europe (MIE2006) einen Workshop gab, der sich mit der Frage beschäftigte, wie qualitativ hochwertige Forschung mit Versorgungsdaten betrieben werden kann, und entsprechende Regeln aufstellte [11]. 2007 und 2008 fanden zwei Workshops vom European Institute for Health Records in Brüssel statt, an denen Leistungserbringer, Rechtsexperten, Vertreter der Regierung, Vertreter von Patientengruppen, IT- und Pharmaindustrie die Möglichkeiten und Herausforderungen von elektronischen Patientenakten für die Versorgung und Forschung in Europa diskutierten. Als Ergebnis dieser Workshops wurde u. a. herausgestellt, dass Software-Tools für die Interoperabilität und die Integration zwischen den elektronischen Patientenakten und den electronic data capture Systemen (EDC) der Forschung dringend benötigt werden. Besonders wurde herausgestellt, dass bei allen Maßnahmen der Schutz des Patienten und seiner Daten im Vordergrund stehen muss [12].

In Deutschland wurde 2009 von Prokosch und Ganslandt in ihrem Artikel „Perspectives of Medical Informatics“ als eine von drei Herausforderungen die Verknüpfung von elektronischen Patientenakten und Datenbanken in der klinischen Forschung gesehen, um die Rekrutierung von Patienten und die Datenerfassung für klinische Studien zu verbessern [13].

Auch in den USA wurde das Thema Nutzung von Versorgungsdaten für die medizinische Forschung (auch als Secondary Use bezeichnet) diskutiert. 2006 wurde bei einem Workshop auf dem American Medical Informatics Association (AMIA) Symposium das Thema Datenintegration und Secondary Use als eine Herausforderung im Bereich der Clinical Research Informatics herausgestellt [14]. Im gleichen Jahr hat die AMIA einen Expertenausschuss organisiert, der die Herausforderungen und Möglichkeiten von „Secondary Use“ von Versorgungsdaten diskutiert hat [15]. In den USA wurden auch erste Überlegungen angestellt, wie über Patienten geführte Akten für die medizinische Forschung genutzt werden können [16].

Auch im Bereich der Pharmaindustrie wurde das Potential des „Secondary Use“ von elektronischen Patientenakten erkannt [17] und u. a. auch das im letzten Jahr gestartete EU Projekt „Electronic Health Records for Clinical Research“ (EHR4CR) [18] unterstützt.

In Deutschland hat die Politik die Notwendigkeit einer stärkeren Vernetzung von Forschung und Versorgung bereits 1999 durch das Bundesministerium für Bildung und Forschung (BMBF) erkannt und zum Leitbild der vom BMBF ins Leben gerufenen Kompetenznetze in der Medizin erhoben [19]. Diese Netze haben das Ziel, die Ergebnisse aus der Forschung unmittelbar in die Versorgung zurückfließen zu lassen. Das bedeutet, dass nicht nur Wissenschaftler miteinander vernetzt, sondern auch Patienten und Versorgung stark mit eingebunden werden. Die organisatorische Vernetzung sowohl innerhalb der medizinischen Forschung als auch zwischen Versorgung und Forschung konnte durch die Kompetenznetze in der Medizin erheblich verbessert werden. Eine einheitliche technische Lösung, die den sicheren Datenaustausch zwischen IT-Systemen innerhalb der Forschung bzw. von und zu den Systemen der Versorgung ermöglicht und auch den Patienten mit einbindet, fehlt bisher jedoch. Auch wenn in Deutschland die Systeme der Versorgung über eine nationale Telematikinfrastruktur (TI) untereinander vernetzt werden sollen [20-22], ist eine Anbindung der Systeme der Forschung momentan nicht vorgesehen und nach aktueller Gesetzgebung ausgeschlossen [23].

1.1. Problemstellung und Motivation

In der medizinischen Forschung und in der Versorgung werden häufig dieselben Daten eines Patienten erfasst. Beispielweise wurde in einem Projekt herausgestellt, dass es eine 75%ige Überschneidung der Daten der Routineversorgung und der einer Studie gibt [24]. Da die IT-Systeme von Forschung und Versorgung nicht integriert sind, kommt es häufig zu Doppelerfassungen [25]. Es gibt Ansätze im Bereich des Secondary Use, die Versorgungsdaten für Forschungszwecke nutzen und so beispielsweise die Rekrutierung unterstützen [26-29]. oder auch Daten aus der Versorgung für Studienvorhaben nutzen [30]. Diese Ansätze können auf ein regionales System beschränkt sein [31,32] oder auch auf institutionsübergreifenden Systemen aufbauen. Ein Beispiel für den zweiten Ansatz ist das Versorgungsmodul[2] der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), welches eine institutionsübergreifende Erfassung von Versorgungsdaten mit zentraler Auswertung für die Forschung anbietet [33-35]. Doch ist das Versorgungsmodul als eine losgelöste Anwendung zu sehen [36], in die die Ärzte neben ihrer normalen Dokumentation zusätzlich Daten zum Patienten erheben und somit eine Doppelerfassung entsteht. Auch berücksichtigen die oben genannten Systeme den Patienten nicht als aktiven Teilnehmer, so dass die Kommunikation mit dem Patienten immer über separate Wege stattfinden muss.

In der Versorgung wird die technische Vernetzung der heterogenen IT-Systeme über eine nationale Telematikinfrastruktur angegangen. Über diese nationale Telematikinfrastruktur sollen Anwendungen wie z. B. eine elektronische Patientenakte angeboten werden [22]. Mit Hilfe dieser elektronischen Patientenakte soll eine direkte Kommunikation mit den Systemen der Leistungserbringer unter der Kontrolle des Patienten möglich sein [37]. Hier entsteht eine Plattform, die einen institutions- und fallübergreifenden Austausch von medizinischen Daten eines Patienten ermöglicht. Eine elektronische Patientenakte in Verbindung mit der oben beschriebenen Telematikinfrastruktur könnte durch die Anbindung an einen medizinischen Forschungsverbund einen direkten Austausch zwischen den Systemen der Leistungserbringer und dem System des Forschungsverbundes ermöglichen und zudem den Patienten in die Kommunikation einbeziehen. Dieser Ansatz würde eine Integration der

[2] In der ersten Version der Datenschutzkonzepte der TMF auch Konzept A [33]

Systeme der Leistungserbringer, wie bei oben aufgeführten lokalen Ansätzen und dem institutionsübergreifenden Ansatz des Versorgungsmoduls, ermöglichen und den Patienten in die Kommunikation über seine ePA aktiv einbinden

Eine Nutzung der Telematikinfrastruktur für die Wissenschaft, wie sie schon von Rienhoff 2007 thematisiert wurde [38] oder auch ein sicherer Datenaustausch zwischen Forschung und Versorgung über die Telematikinfrastruktur ist bisher nicht vorgesehen. Dies liegt an der gesetzlichen Grundlage (dem § 291a SGB V), die eine Nutzung der mit Hilfe der Telematikinfrastruktur gesammelten Daten für andere Zwecke als die Versorgung ausschließt. Da die Motivation dieser Gesetzgebung nicht der Ausschluss der medizinischen Forschung, sondern der Missbrauch der Daten der Patienten ist, soll in dieser Arbeit gezeigt werden, wie über eine Schnittstelle zwischen den Systemen der Versorgung und der Forschung Daten der Patienten sicher ausgetauscht werden können.

1.2. Fragestellung und Zielsetzung

Ziel dieser Dissertation ist es, ein Konzept für einen sicheren Datenaustausch zwischen der medizinischen Versorgung und der medizinischen Forschung über eine patientengeführte ePA zu beschreiben. Diese ePA soll als eine der geplanten freiwilligen Anwendungen der Telematikinfrastruktur (im Folgenden auch ePA nach § 291a bzw. § 291a SGB V genannt) eine Anbindung an die Systeme der Leistungserbringer haben. Die Lösung soll möglichst Anpassungen der ePA bzw. der Komponenten, mit denen sie über die Telematikinfrastruktur zugänglich gemacht wird (ePA-System genannt), und der Systeme der Forschung (im Folgenden Forschungssystem genannt) vermeiden. Alle neuen Anforderungen sollen möglichst durch die in dieser Arbeit zu spezifizierende Schnittstelle zwischen dem ePA-System und dem Forschungssystem (im Folgenden Forschungsschnittstelle genannt) umgesetzt werden. Bei diesem Ansatz wird angenommen, dass die in der Literatur und den Spezifikationen beschriebenen Funktionen des ePA-Systems als auch die des Forschungssystems vorhanden sind und die Systeme datenschutzkonform umgesetzt wurden. Die Forschungsschnittstelle soll als eine Erweiterung des ePA-Systems konzipiert werden und die Konzepte des ePA-Systems in Bezug auf die Kommunikation und die Sicherheit übernehmen.

Durch diese Lösung soll ein Mehrwert für den Patienten und die Leistungserbringer aus Forschung und Versorgung entstehen. Wie in Abbildung 1 dargestellt, soll der Patient in seiner ePA Daten aus der Versorgung und der Forschung speichern und Daten aus beiden Domänen sowohl für seine Versorgung als auch Forschungsvorhaben, an denen er teilnimmt, zur Verfügung stellen können und somit einen Mehrwert für die Leistungserbringer, die Studienärzte, die Forscher und seine Versorgung erzielen. Um einen Mehrwert für den Patienten zu generieren, soll die ePA nicht nur als Datenspeicher, sondern auch als Instrument für den Patienten dienen, über das er sich informieren bzw. informiert werden kann. Zusätzlich ist vorgesehen, dass der Patient auch eigene Daten (z. B. aus Home-Care-Geräten, Schmerztagebüchern, Ernährungsverhalten etc.) über seine ePA der Forschung und Versorgung zur Verfügung stellen kann.

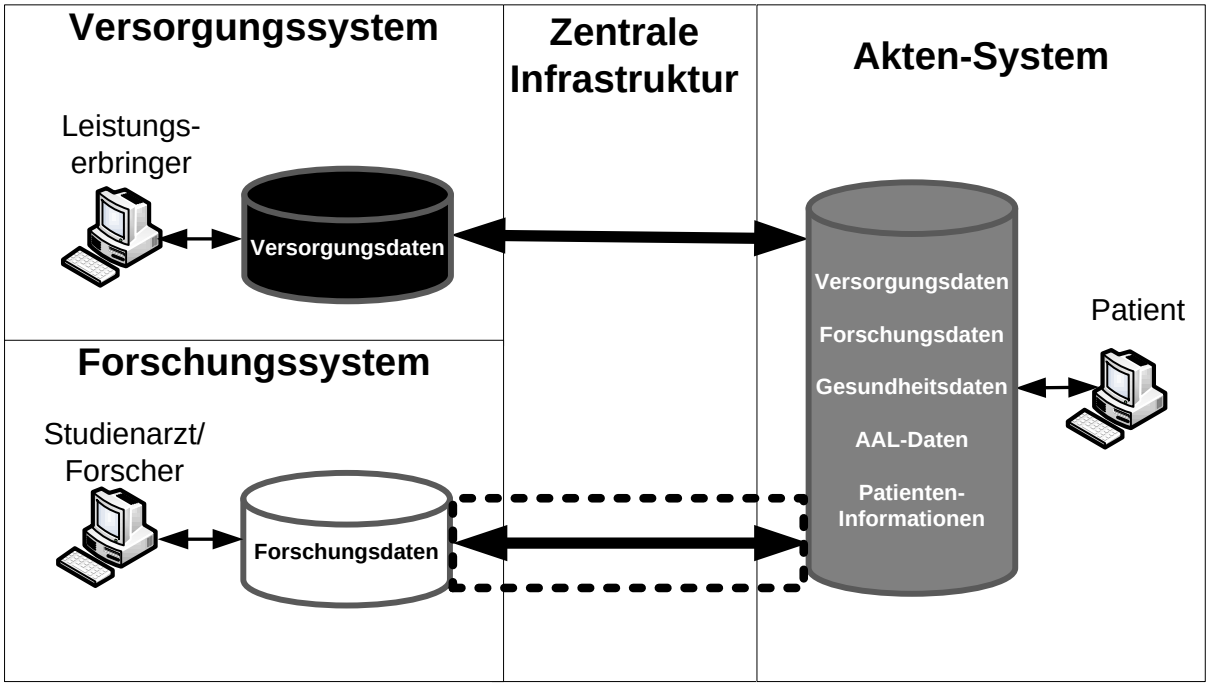

Abbildung 1: Grundidee der Arbeit zur Nutzung einer elektronischen Patientenakte unter der Hoheit des Patienten für die medizinische Versorgung und Forschung.

Im Fokus der Arbeit steht der eingerahmte Teil (gestricheltes Rechteck) der Abbildung 1, also die Anbindung des Forschungssystems über eine Schnittstelle an das ePA-System. Hierbei wird der sichere Datenaustausch zwischen den Systemen betrachtet. Um diese Schnittstelle genauer zu spezifizieren und eine datenschutzkonforme Umsetzung zu beschreiben, sollen folgende Forschungsfragen in der Arbeit untersucht werden:

- **Forschungsfrage 1**: Bei welchen Anwendungsfällen eines medizinischen Forschungsverbunds kann die Kommunikation zwischen den Leistungserbringern aus Forschung und Versorgung und dem Patienten über eine ePA nach § 291a SGB V verbessert werden?

Es ist davon auszugehen, dass der oben skizzierte Ansatz nicht für alle Anwendungsfälle eines Forschungsverbundes die Kommunikation zwischen den Leistungserbringern aus Forschung und Versorgung und dem Patienten über eine ePA nach § 291a SGB V verbessern kann (z. B. wenn der Patient gar nicht in die Kommunikation eingebunden werden muss). Daher soll zunächst untersucht werden, wie ein Forschungsverbund aufgebaut ist und welche Anwendungsfälle für eine Kommunikation über eine ePA nach § 291a SGB V geeignet sind. Auf Grundlage dieser Anwendungsfälle soll dann das Forschungssystem definiert und auch nur in diesem Rahmen im weiteren Verlauf der Arbeit betrachtet werden.

- **Forschungsfrage 2**: Wie erfolgt die Kommunikation zwischen der ePA und den Systemen der Versorgung und wie kann das Forschungssystem an das bestehende ePA-System über eine Forschungsschnittstelle angebunden werden? Welche Voraussetzungen und Anforderungen sind dabei zu beachten?

Nachdem durch die Untersuchung der ersten Forschungsfrage das Forschungssystem definiert wurde, ist es notwendig, das ePA-System genauer zu analysieren. Hierbei soll identifiziert werden, welche Komponenten das ePA-System bereitstellt, wie der Austausch zwischen dem ePA-System und den Systemen der Leistungserbringer erfolgt und welche Komponenten für die Anbindung des Forschungssystems an die IT-Infrastruktur einer ePA nach § 291a benötigt werden. Zusätzlich soll herausgestellt werden, welche Anforderungen

sich aufgrund der Konzepte des ePA-Systems in Bezug auf die Kommunikation und den Zugriff auf die ePA für das ePA-, das Forschungssystem und die Forschungsschnittstelle ergeben, wenn über diese Konzepte eine Kommunikation zwischen den IT-Systemen eines Forschungsverbundes und der ePA realisiert werden soll.

- **Forschungsfrage 3**: Wie sieht ein Kommunikationsmodell aus, über das die Kommunikationsvorgänge der ausgewählten Anwendungsfälle eines medizinischen Forschungsverbundes mit Hilfe einer ePA nach § 291a umgesetzt werden können?

Nachdem das Forschungssystem und das ePA-System definiert wurden und die Anforderungen seitens des ePA-Systems in Bezug auf die Kommunikation und den Zugriff auf die ePA durch das Forschungssystem herausgestellt werden konnten, soll nun untersucht werden, wie ein generisches Kommunikationsmodell aussehen kann, über das die Kommunikationsvorgänge aller ausgewählten Anwendungsfälle mit Hilfe einer ePA nach § 291a umgesetzt werden können. Hierbei geht es nicht nur um die generischen Kommunikationsvorgänge, sondern auch um die Anforderungen, die sich aufgrund einer solchen Umsetzung an das ePA-, das Forschungssystem und die Forschungsschnittstelle ergeben. Ziel ist es, die Kommunikation über ein Modell zu vereinfachen und dieses Modell dann als Grundlage für eine Umsetzung der Forschungsschnittstelle zu nutzen.

- **Forschungsfrage 4**: Wie kann eine datenschutzkonforme Umsetzung des Kommunikationsmodells über eine Forschungsschnittstelle als eine Erweiterung des ePA-Systems erreicht werden?

Ziel dieser Arbeit ist die Konzeption einer Schnittstelle für die Kommunikation zwischen den IT-Systemen eines Forschungsverbundes und einer ePA, die durch eine Anpassung des ePA-Systems umgesetzt werden soll. In Anlehnung an die Spezifikation des ePA-Systems soll in dieser Arbeit eine mögliche datenschutzkonforme Umsetzung der Forschungsschnittstelle in Form einer Fach- und Sicherheitsarchitektur beschrieben werden.

1.3. Aufbau der Arbeit

In diesem Abschnitt wird der Aufbau der Arbeit beschrieben und der Zusammenhang zwischen den Forschungsfragen und den einzelnen Kapiteln verdeutlicht (siehe auch Abbildung 2):

- Im Kapitel 2 wird ein Überblick über die in der Literatur beschriebenen Ansätze zur Nutzung von Versorgungsdaten für die medizinische Forschung gegeben. Das Ergebnis dieses Kapitels ist eine Übersicht der gängigen Ansätze zur Nutzung von Versorgungsdaten für die Forschung sowie eine Einordnung und Abgrenzung des in dieser Arbeit verfolgten Ansatzes.
- Kapitel 3 dient der Beschreibung des methodischen Vorgehens sowie einiger Grundlagen.
- Im Kapitel 4 wird die erste Forschungsfrage untersucht, indem das Forschungssystem auf Grundlage der Datenschutzkonzepte der TMF [33,34] beschrieben und eine Auswahl der weiter zu betrachtenden Komponenten getroffen wird. Am Ende dieses Kapitels sollen die relevanten Module und deren Anwendungsfälle eines Forschungsverbundes in Bezug auf ihre Eignung zur Anbindung an eine ePA bewertet und ausgewählt worden sein.

- Kapitel 5 bezieht sich auf die zweite Forschungsfrage, indem das ePA-System genauer spezifiziert wird. Hierzu werden in diesem Kapitel das Forschungs- und Entwicklungsprojekt elektronische Patientenakte gemäß § 291a SGB V und die für diese Arbeit relevante Teilergebnisse des Projektes vorgestellt und untersucht. Als Ergebnis dieses Kapitels wird feststehen, welche Komponenten für die Anbindung des Forschungssystems an die IT-Infrastruktur einer ePA nach § 291a benötigt werden. Ebenfalls wird es eine Liste von Anforderungen an das ePA-, das Forschungssystem und die Forschungsschnittstelle geben, die für die Anbindung eines Forschungssystems erfüllt werden müssen.
- Kapitel 6 bezieht sich auf die dritte Forschungsfrage. Es wird die Kommunikation der ausgewählten Anwendungsfälle und Module des Forschungsverbundes beschrieben und auf dieser Grundlage analysiert, wie diese Kommunikation mit Hilfe einer ePA umgesetzt werden kann. Ziel ist es, Kommunikationsmuster zwischen den Komponenten und Akteuren zu identifizieren, aus denen eine minimale Anzahl generischer Kommunikationsmuster abgeleitet werden kann, die dann in ihrer Gesamtheit das Kommunikationsmodell für die Kommunikation zwischen einer ePA nach § 291a und den Modulen eines Forschungsverbundes bilden. Neben dem Kommunikationsmodell sollen auch Datenschutzanforderungen herausgearbeitet werden, die bei der Umsetzung des Kommunikationsmodells berücksichtigt werden müssen.
- Im Kapitel 7 wird auf die vierte Forschungsfrage eingegangen, indem beschrieben wird, wie das Kommunikationsmodell unter Berücksichtigung der Datenschutzanforderungen über eine Erweiterung der IT-Infrastruktur des ePA-Systems umgesetzt werden kann. Hierzu werden als erstes die aus Sicht der Forschung relevanten Datenschutzanforderungen zusammengefasst und aus diesen Anforderungen Architekturentscheidungen abgeleitet. Anschließend wird die Architektur beschrieben und gezeigt, wie hierüber die generischen Kommunikationsmuster umgesetzt werden können.
- Im Kapitel 8 wird die vierte Forschungsfrage noch einmal vertieft, indem im Rahmen einer Facharchitektur die Schnittstellen und das Verhalten der einzelnen Komponenten der Forschungsschnittstelle als Grundlage für eine Implementierung beschrieben werden.
- Im Kapitel 9 wird auf die Aspekte der vierten Forschungsfrage in Bezug auf eine datenschutzkonforme Umsetzung der Forschungsschnittstelle im Rahmen der Beschreibung einer Sicherheitsarchitektur eingegangen.
- Im Kapitel 10 werden die Ergebnisse dieser Arbeit in Bezug auf die Forschungsfragen 1-4 diskutiert und in Bezug auf die anderen Ansätze zur Nutzung von Versorgungsdaten für die medizinische Forschung bewertet.
- Im Kapitel 11 werden Forschungsthemen aufgegriffen, die während der Untersuchung der Forschungsfragen 1-4 aufgetaucht sind aber nicht weiter vertieft werden konnten, und es wird vorgeschlagen, wie diese Themen in Bezug auf die Arbeit weiter vertieft werden sollten.

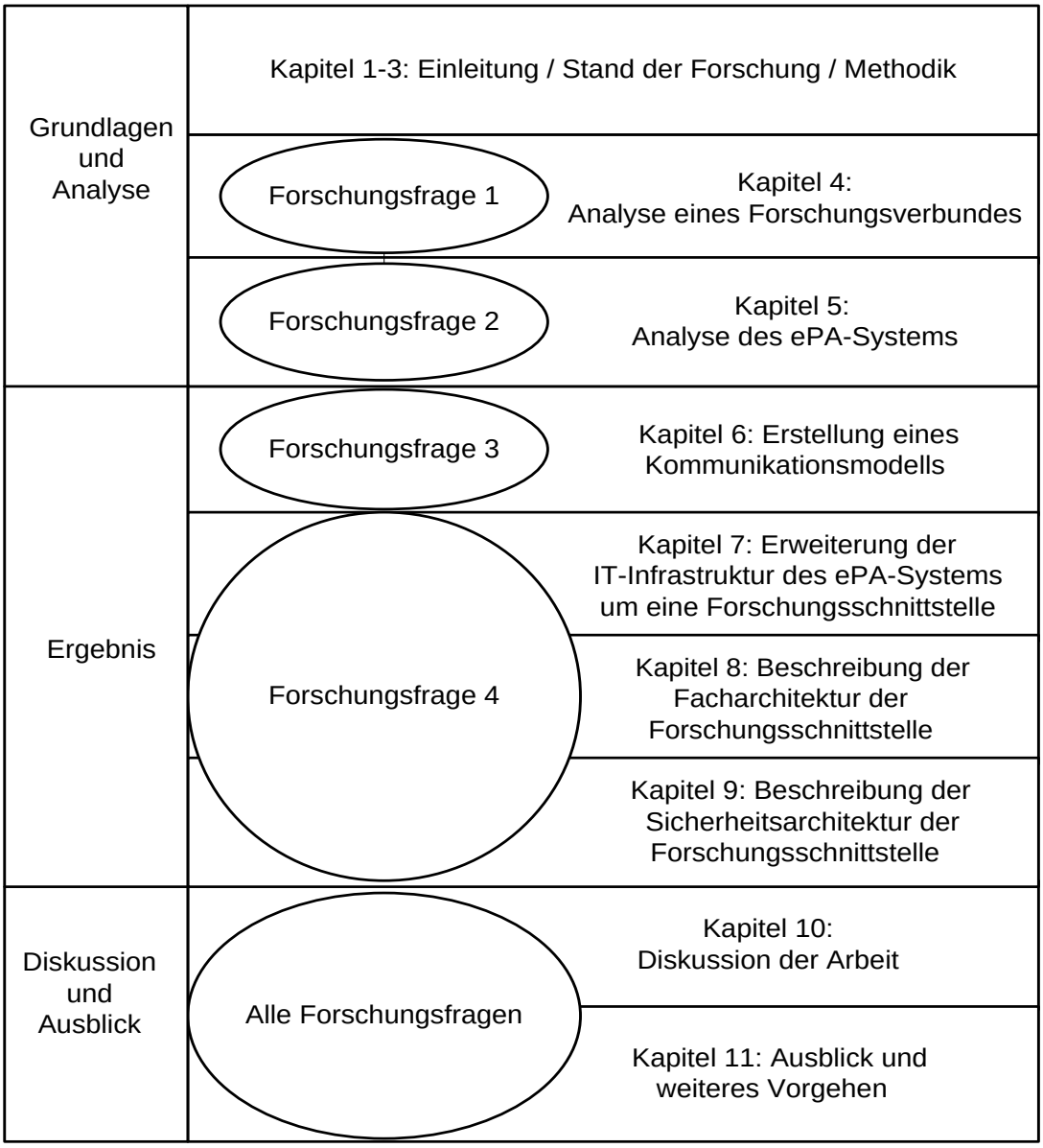

Abbildung 2: Aufbau der Arbeit mit Zuordnung der Forschungsfragen zu den einzelnen Kapiteln der Arbeit

2. Aktueller Stand der Forschung zur Nutzung von Versorgungsdaten für die Forschung

In diesem Kapitel wird ein Überblick über den aktuellen Stand zum Thema „Nutzung von Versorgungsdaten für die medizinische Forschung“ gegeben. Außerdem wird auf den aktuellen Stand zu den Themen „elektronische Patientenakte unter der Datenhoheit des Patienten und Secondary Use[3]“, „die elektronische Gesundheitskarte und die Telematikinfrastruktur in Deutschland“ und das „Forschungs- und Entwicklungsprojekt elektronische Patientenakte gemäß § 291a SGB V“ eingegangen, da diese Themen eine wichtige Grundlage für diese Arbeit bilden.

Grundlage für die Ergebnisse dieses Kapitels ist eine Literaturrecherche. Ein wichtiges Ergebnis dieser Recherche ist, dass die Anwendungsbereiche zur Nutzung von Versorgungsdaten für die medizinische Forschung (z. B. die Rekrutierung) durch unterschiedliche Architekturansätze umgesetzt werden können. Aus diesem Grund werden zum einen die unterschiedlichen Architekturansätze (siehe Abbildung 3, Nr. 1-5) für die Nutzung von Versorgungsdaten für die medizinische Forschung beschrieben, als auch die unterschiedlichen Anwendungsbereiche, die über diese Architekturen abgedeckt werden. Ziel ist es, den in dieser Arbeit beschriebenen Architekturansatz von den bestehenden Ansätzen abzugrenzen und somit das Innovative dieser Arbeit herauszustellen (siehe Abschnitt 2.7). Des Weiteren dienen die Ergebnisse dieses Kapitels für eine Diskussion der Vor- und Nachteile der in dieser Arbeit beschriebenen Architektur im Vergleich zu den bereits bestehenden Architekturansätzen. Der Fokus der Diskussion liegt hierbei auf der unterschiedlichen Umsetzung der in Abschnitt 2.3 beschriebenen Anwendungsbereiche zum Thema Secondary Use von Versorgungsdaten (siehe Kapitel 10).

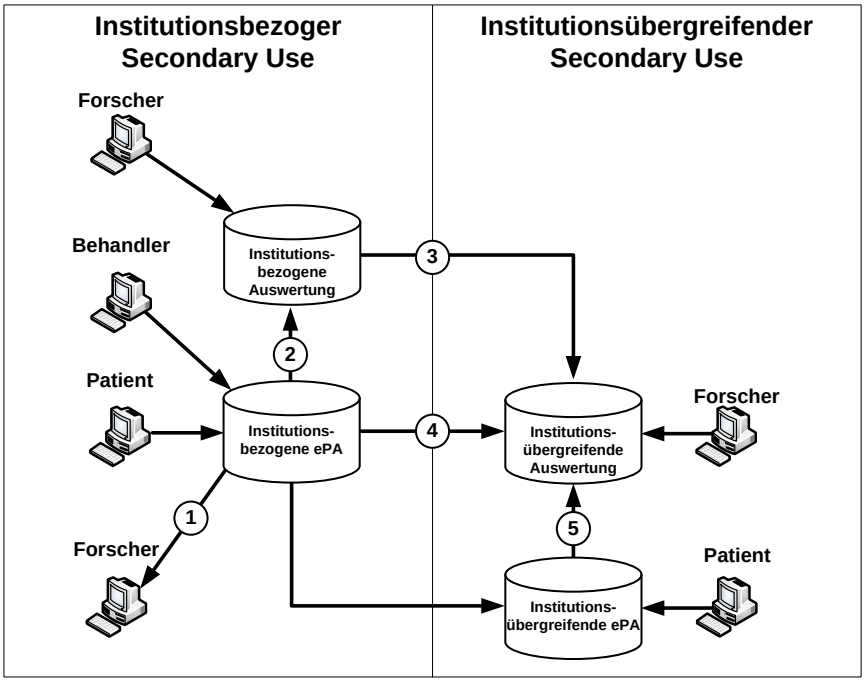

Abbildung 3: Übersicht der unterschiedlichen institutionsbezogenen und -übergreifenden Ansätze des (Secondary Use)

[3] Secondary Use und die Nutzung von Versorgungsdaten für die medizinische Forschung werden synonym verwendet.

2.1. Elektronische Akten im Gesundheitssystem

Die während der Literaturrecherche identifizierten Artikel enthalten sowohl englische als auch deutsche Definitionen von elektronischen Patientenakten. Für die Lesbarkeit bzw. Vergleichbarkeit werden in dieser Arbeit nur deutsche Begriffe für die elektronische Patientenakte verwendet. Grundlage hierfür ist die Definition von elektronischen Akten im Gesundheitswesen des bundesweiten Arbeitskreises EPA/EFA [4] [39]. Eine Zusammenfassung der Definitionen und Zuordnung der deutschen und englischen Begriffe befindet sich in der Tabelle 20 im Anhang A1.1. Im Folgenden werden die einzelnen unterschiedlichen Akten, die in diesem Kapitel verwendet werden, in drei Kategorien zusammengefasst:

- Institutionsbezogene elektronische Patientenakte: Dies kann eine fallübergreifende und fallbezogene elektronische Patientenakte sein, die Daten der Patienten einer Institution zugänglich macht. Unter diese Kategorie fallen die institutionelle elektronische Fallakte und die institutionelle elektronische Patientenakte (iEPA) (im Englischen Electronic Medical Record - EMR -, Electronic Patient Record - EPR -).
- Einrichtungsübergreifende elektronische Patientenakte: Diese Akte stellt die Daten der Patienten (fallbezogen oder fallübergreifend) mehreren Institutionen in elektronischer Form zur Verfügung. Dieser Kategorie gehören die einrichtungsübergreifende elektronische / medizinische Fallakte (EFA) und die einrichtungsübergreifende elektronische Patientenakte (eEPA) (im Englischen Electronic Health Record - EHR -, Electronic Patient Record - EPR-).
- Elektronische Patientenakte unter der Datenhoheit des Patienten: Hierbei handelt es sich um eine einrichtungsübergreifende elektronische Patientenakte, bei der der Patient entscheiden kann, wer Zugriff auf die Inhalte dieser Akte hat. Zu dieser Kategorie gehören die persönliche elektronische Patientenakte (pEPA) oder die elektronische Gesundheitsakte (EGA) (im Englischen Personal Electronic Health Record - PHR - oder Personally Controlled Health Record - PCHR-).

Der Begriff der elektronischen Patientenakte (ePA) wird in dieser Arbeit als Oberbegriff für die drei Kategorien verstanden.

2.2. Unterschiedliche Architekturansätze zur Nutzung von Versorgungsdaten für die Forschung

In den letzten Jahren sind zum Thema „Secondary Use“ von Versorgungsdaten für die medizinische Forschung eine Reihe von Projekten gestartet worden. Neben dem in der Einleitung erwähnten Projekt EHR4CR sind noch weitere EU-Projekte ins Leben gerufen worden, wie z. B. das Projekt TRANSFoRm (Translational Research and Patient Safety in Europe) und das Projekt PONTE (Efficient Patient Recruitment for Innovative Clinical Trials of Existing Drugs to other Indications) [40,41] oder DebugIT (Detecting and Eliminating Bacteria Using Information Technology) [42]. In Frankreich wurde das Thema in dem Projekt RE-USE (Retrieve from EHR Useful clinical data for Secondary Exploitation) vertieft [43]. In den USA ist unter anderen das Projekt Stanford Translational Research Integrated Database Environment (STRIDE) [44-47] umgesetzt worden. In den UK wurden das electronic Primary Care Research Network (ePCRN) [48-50] und das FARSITE (Feasibility Assessment and Recruitment System for Improving Trial Efficiency) Projekt [51,52] etabliert. Diese und

[4] EFA steht für elektronische Fallakte

weitere in der Literatur beschriebene Projekte können in zwei unterschiedliche Ansätze unterteilt werden. Der erste Ansatz geht von einer institutionsbezogenen elektronischen Patientenakte aus. Der zweite Ansatz geht von einer einrichtungsübergreifenden elektronischen Patientenakte bzw. einer elektronischen Patientenakte unter der Datenhoheit des Patienten aus, aus der die Daten für die Forschung gewonnen werden (siehe auch Abbildung 3). Während der zweite Ansatz über eine zentrale Patientenakte oder Gesundheitsakte immer eine institutionsübergreifende Auswertung der Daten vorsieht (siehe Nr. 5, Abbildung 3), kann der erste Ansatz der Datengewinnung aus einer institutionsbezogenen Patientenakte entweder eine lokale (siehe Nr. 1 und 2, Abbildung 3) oder institutionsübergreifende Auswertung verfolgen (siehe Nr. 3 und 4, Abbildung 3).

Im Folgenden werden die einzelnen aus der Literaturanalyse erhobenen Ansätze zur Nutzung von Versorgungsdaten für die Forschung genauer beschrieben (die Ansätze sind mit den Nummern 1-5 auf der Abbildung 3 markiert):

1. Daten werden in einer institutionsbezogenen elektronischen Patientenakte gesammelt und direkt für Forschungszwecke genutzt. Beispiele sind hier die Rekrutierung für Studien [27-29,53,54] oder das Anzeigen von Überlebensstatistiken [55].
2. Daten werden aus einer institutionsbezogenen elektronischen Patientenakte in ein lokales Data Warehouse (DW) oder eine Auswertungssoftware geladen und dort ausgewertet. Beispiele sind hier die Übertragung von Routinedaten aus einem Krankenausinformationssystem (KIS) in ein lokales Data Warehouse [31,32], die Überprüfung der Behandlungsqualität von Diabetes-Patienten anhand der Medikation aus einer institutionsbezogenen elektronischen Patientenakte [56] oder die Gewinnung von Daten aus einem Krankenhausinformationssystem für monozentrische Studien [25,57]. Es gibt auch Beispiele, bei denen der Patient selbsterfasste Daten (zur Lebensqualität) beisteuert [58].
3. Daten werden aus einem lokalen Data Warehouse in ein institutionsübergreifendes Metadata Warehouse übertragen bzw. es wird ein virtuelles institutionsübergreifendes DW erstellt. Beispiele sind das electronic Primary Care Research Network [48-50,59] oder die standortübergreifende Forschungsplattform für das Deutsche Prostatakarzinom-Konsortium [60-62], die ein übergreifendes Data Warehouse einsetzt. Außerdem ist das Shrine Projekt zu nennen, bei dem ein zentraler Service zum Einsatz kommt, um die lokalen Data Warehouses eines Krankenhausverbundes institutionsübergreifend abfragen [63]. Weitere Beispiele sind das Childhood Arthritis & Rheumatism Research Alliance (CARRA) Registry of pediatric rheumatic diseases and Harvard Inflammatory Bowel Disease Longitudinal Data Repository [64] und das EHR4CR Projekt [18,43,65,66].
4. Daten werden aus einer institutionsbezogenen elektronischen Patientenakte in eine institutionsübergreifende Datenbank für wissenschaftliche Auswertungen überführt. Beispiele sind hier die Nutzung von elektronischen Patientenakten zur Gewinnung von Phänotypdaten für genomweite Assoziationsstudien [67], die Übertragung von Daten aus einem Krankenhausinformationssystem an Register [68,69] sowie die Übertragung von Routinedaten in eine institutionsübergreifende Forschungsdatenbank [70] z. B. zum Zwecke der Rekrutierung [71]. Ein weiteres Szenario ist die Zusammenführung von Daten aus mehreren institutionsbezogenen elektronischen Patientenakten in ein gemeinsames DW zum Zwecke der Identifizierung von Patientenkohorten [44,45]. Weitere Beispiele sind die Übertragung von Daten aus mehreren Versor-

gungssystemen an eine Studiendatenbank [24,43,72-74] oder das Senden von unerwünschten Arzneimittelwirkungen aus einer ePA an eine zentrale Datenbank der Food and Drug Administration (FDA) [75].

5. Versorgungsdaten werden aus einrichtungsübergreifenden elektronischen Patientenakten bzw. einer elektronischen Patientenakte unter der Datenhoheit des Patienten in eine Datenbank für wissenschaftliche Auswertungen überführt. Ein Beispiel hierfür ist die Identifizierung von Kindern und Jugendlichen, die ein Risiko für Dyslipidämie aufweisen, auf Grundlage der Daten aus einer institutionsübergreifenden ePA und die Überführung und Auswertung dieser Daten in einer Statistik Software [76]. Ein weiteres Beispiel ist das central Hampshire electronic health record pilot project, bei dem Daten aus einer institutionsübergreifenden ePA in eine Datenbank zum Zwecke des Qualitätsmanagements des Behandlungsprozesses in einer Einrichtung und eines einrichtungsübergreifenden Vergleiches [77,78] überführt werden. In anderen Projekten wird die Rekrutierung mit Hilfe von Daten aus einer institutionsübergreifenden Patientenakte umgesetzt [51,52]. Die institutionsübergreifende ePA kann auch um die Funktionalitäten einer Studiendatenbank erweitert werden und die Daten werden dann in anonymisierter Form in eine Auswertedatenbank übertragen [79]. Bei einigen Projekten werden die Ergebnisse den Behandlern in Form von Tools wieder in der ePA zur Verfügung gestellt (beispielsweise zur Überprüfung, ob Patienten ein Risiko haben Dyslipidämie zu bekommen [76]) oder zur Überprüfung, ob bei einer Krankheit eines Patienten ein Zusammenhang mit anderen Krankheiten besteht [80].

2.3. Anwendungsbereiche zur Nutzung von Versorgungsdaten für die Forschung

Mit den oben aufgeführten fünf Ansätzen wird eine Vielzahl von Anwendungsbereichen abgedeckt, die im Folgenden beschrieben werden:

2.3.1. Feasibility, Identifizierung und Rekrutierung von Patienten

Bei diesem Anwendungsbereich geht es zum einen um die Feasibility, also das Überprüfen, wie viele Patienten in einem Zentrum mit bestimmten Einschlusskriterien für eine Studie durchschnittlich behandelt werden und zukünftig ggf. rekrutiert werden können, als auch um die Identifizierung und Rekrutierung von Patienten. Die Identifizierung bzw. Rekrutierung von Patienten für weitere Forschungsvorhaben wird mit vielen Ansätzen verfolgt. So wird in mehreren Projekten eine Rekrutierungsfunktion in das KIS integriert [26-29]. Es wurde auch ein BMBF Projekt ins Leben gerufen, bei dem die Rekrutierungsfunktion im KIS an mehreren Standorten in Deutschland untersucht und eingeführt wird [53,54]. Im electronic Primary Care Research Network (ePCRN) werden über einen zentralen Service einzelne ePAs oder DWs für die Identifizierung von Patienten für Studien abgefragt. Bei diesen Abfragen werden keine Daten übertragen, sondern nur die Anzahl der Patienten, die für die Studien potentiell interessant sind [48,50]. Dieses Vorgehen wird auch im EHR4CR Projekt verfolgt, in dem sowohl die Protocol Feasibility als auch die Rekrutierung unterstützt werden soll [18,43,65,66]. In UK wurde eine große nationale Datenbank mit anonymisierten Daten aus Versorgungsystemen aufgebaut [70], die dann beispielsweise für die Rekrutierung von Patienten verwendet wird [71]. Ein weiteres Projekt aus den UK ist das FARSITE Projekt [51,52], bei dem anonymisierte Daten aus einer institutionsübergreifenden elektronischen Patientenakte (Salfort Integrated Record [81]) in ein e-LAB [82,83] überführt und dort für die Rekrutierung eingesetzt werden. Aus den USA ist beispielweise das Stride Projekt zu nennen, in dem ein Data Warehouse mit Patientendaten aus mehreren Krankenhäusern

aufgesetzt wurde, um die Identifizierung von Patientenkohorten zu ermöglichen [44-47]. Eine weitere Möglichkeit, Patienten für Forschungsvorhaben zu rekrutieren, kann über eine elektronische Gesundheitsakte (im Englischen Personal Health Records - PHR - genannt) umgesetzt werden, in der dem Patienten passende Studien angezeigt werden. Zu nennen sind hier die elektronischen Gesundheitsakte IndivoX, die eine clinical-trials matching app enthält, mit der Patienten passende Studien in ihrer EGA angezeigt bekommen [84]. In einem weiteren Projekt aus den USA, werden elektronische Gesundheitsakte eingesetzt, um Brustkrebspatientinnen Teilnahmemöglichkeiten an Studien vorzuschlagen [85]. Die Rekrutierung der Patienten erfolgt nicht immer auf der Grundlage von strukturierten Daten. Es gibt auch Projekte, in denen die Daten mit der Hilfe von Natural language processing aufbereitet werden [86].

2.3.2. Behandlungsunterstützung

Bei diesem Anwendungsbereich geht es darum, auf Grundlage von bestehenden Patientendaten diese Daten dem Behandler für eine Unterstützung der Behandlung aufzubereiten, zum Beispiel durch die direkte Integration in das Krankenhausinformationssystem zum Anzeigen von Überlebensstatistiken von Krebskranken [55] oder die Nutzung von Daten aus einer elektronischen Patientenakte in einem Analyse-Tool des Behandlers, um das Herzinfarktrisiko zu berechnen [87].

Eine weitere Unterstützung bekommt der Behandler bei der Identifizierung von Kindern und Jugendlichen, die ein Risiko für Dyslipidämie aufweisen, auf Grundlage der AHLTA (Armed Forces Health Longitudinal Technology Application) - eine einrichtungsübergreifende Patientenakte, die von den medizinischen Versorgungseinrichtungen der U.S. Militärs genutzt wird [76] - oder bei Hinweisen auf einen Zusammenhang zwischen verschiedenen Krankheiten (Komorbidität) auf Grundlage einer institutionsübergreifenden Patientenakte [80].

2.3.3. Qualitätsmanagement

Bei diesem Anwendungsbereich geht es darum Versorgungsdaten auszuwerten, um die Qualität der Behandlung zu bewerten und ggf. zu verbessern. Ein Beispiel hierfür ist die Nutzung einer institutionsübergreifenden elektronischen Patientenakte für die Auswertung der Behandlungsprozesse und Behandlungsergebnisse in den einzelnen Versorgungseinrichtungen und untereinander [77,78]. Ein weiteres Beispiel ist die Überprüfung der Behandlungsqualität von Patienten mit Diabetes Typ 2 auf Grundlage der Medikationsdokumentation in einer elektronischen Patientenakte in einem Krankenhaus [56]. Des Weiteren ist ein Projekt zu nennen, indem Daten aus einem KIS zur Dokumentation von Prostatatumoren auch für das Qualitätsmanagement genutzt werden [88].

2.3.4. Gewinnung von Phänotypdaten

Bei diesem Anwendungsbereich geht es um die Gewinnung und Zuordnung von Phänotypdaten zur Nutzung in genomweiten Assoziationsstudien [67,89–92]. Hier wurde beispielsweise ein Netzwerk zwischen 5 Kliniken ausgebaut, um mit Hilfe von elektronischen Patientenakten genomweite Assoziationsstudien durchzuführen. Dabei geht es um die Verknüpfung von Phänotypdaten aus den elektronischen Patientenakten mit genetischen Daten aus Biobanken. Ziel ist es, aufgrund der Phänotypdaten genetische Merkmale zu finden, die im Zusammenhang mit bestimmten Krankheiten stehen, beispielsweise die Identifizierung von Diabetes Typ 2 oder periphere arterielle Verschlusskrankheit.

Es gibt auch einen Vorschlag, Daten aus elektronischen Gesundheitsakten zur Phänotyp-datengewinnung zu nutzen, indem der Patient diese Daten für die Forschung freigibt [93].

2.3.5. Nutzung von Versorgungsdaten für Register und Studien

Hierbei können Daten aus den Versorgungsdaten für ein Register oder eine Studie gewonnen werden oder die Daten teilweise aus der Versorgung gewonnen und durch spezielle Studiendaten erweitert werden.

So wurden beispielsweise in den USA aus einer lokalen elektronischen Patientenakte Daten exportiert und in ein EDC System importiert. Diese Daten wurden sowohl für prospektive Studien als auch für retrospektive Studien genutzt [30]. Im Klinikum in Münster werden Daten aus dem lokalen Krankenhausinformationssystem exportiert und an ein Krebsregister geschickt [69] oder für eine monozentrische Prostatakrebs-Studie genutzt [25]. In Frankreich wurden Daten in einem Krankenhausinformationssystem erfasst und an ein Nationales Register für interventional vascular radiology procedures übertragen [68]. Ein weiteres Beispiel ist das ArchiMed System aus Österreich - eine Datenbank, die monozentrische Studien unterstützt und mit einem Interface zur Übernahme von Routinedaten aus einem Krankenhausinformationssystem versehen ist [57,94]. Ein weiteres Projekt wurde in München durchgeführt, das die Übertragung von Patientendaten aus einem KIS in eine Studiendatenbank im Rahmen einer multizentrischen Studie zum Thema Brustkrebs als Ziel hatte [74]. Außerdem ist die STARBRITE[5] Proof-of-Concept Study zu nennen, bei der Daten in einem KIS erfasst und in eine Studiendatenbank für eine multizentrische Studie übertragen wurden [24]. Im Rahmen des RE-USE Projektes in Frankreich werden Daten in einer elektronischen Patientenakte für eine multizentrische Studie ausgefüllt. Der Ausbau der Formulare wird aus dem EDC-System des Forschungsprojektes bereitgestellt und in der ePA dargestellt. Durch ein Mapping mit den Daten in der elektronischen Patientenakte und den Formularen können die Formulare teilweise mit Routinedaten aus der ePA vorausgefüllt werden. Die Daten werden dann in der ePA gespeichert und an das EDC-System geschickt [43]. In Michigan werden mit Hilfe eines „Honest Broker“ Daten für eine Studie, die die Komorbidität zwischen klinischer Depression und interventional cardiac catheterization Events untersuchen soll, aus mehreren institutionsübergreifenden Systemen in eine Studien-datenbank überführt [72,73,95]. Im EHR4CR sollen an mehreren europäischen Krankenhäusern Daten aus den lokalen KIS in eine multizentrische Studiendatenbank überführt werden [18,43,65,96].

2.3.6. Selbstdokumentation

Bei diesem Anwendungsbereich geht es um die Nutzung von Daten für medizinische Auswertungen, die der Patient selbst erhoben hat.

Hier wurden beispielsweise in Münster Daten zur Lebensqualität von Patienten elektronisch mit mobilen Geräten selbst erhoben und in ein Krankenhausinformationssystem überführt. Dort werden sie für die Behandlung genutzt und zusätzlich mit weiteren klinischen Informationen zu den Patienten für wissenschaftliche Auswertungen exportiert [58,97]. In UK wurde eine institutionsübergreifende Patientenakte um die Funktionalität einer Studiendatenbank erweitert. Hierbei können u. a. auch Daten von Patienten eingetragen

[5] Strategies for Tailoring Advanced Heart Failure Regimens in the Outpatient Setting: Brain Natriuretic Peptide versus the Clinical Congestion Score

werden, um die Lebensqualität von Krebspatienten zu erfassen [79]. In einem sozialen Netzwerk für Diabetes wurde eine elektronische Gesundheitsakte zur Eingabe von Daten durch den Patienten und anschließender Auswertung des Blutzuckerspiegels integriert [98]. In eine elektronischen Gesundheitsakte namens Indivo wurde ein Umfragemodul integriert, über das Forscher direkt Informationen von Patienten abfragen können [99].

2.3.7. Meldung von unerwünschten Arzneimittelwirkungen

Bei diesem Anwendungsbereich geht es darum, in der Versorgung auftretende unerwünschter Arzneimittelwirkungen zu erfassen und zu melden. Diese Nebenwirkungen können innerhalb von Studien auftreten oder auch innerhalb der Versorgung. In Boston wurde beispielsweise eine ePA für das Versenden von unerwünschten Arzneimittelwirkungen erweitert. Die Daten werden in der ePA ausgefüllt. Hierbei wird der Report teilweise mit den Daten aus der ePA vorausgefüllt und an eine Datenbank der FDA geschickt [75]. Im EHR4CR Projekt ist ebenfalls die Integration eines Reportings unerwünschter Arzneimittelwirkungen in die Krankenhausinformationssysteme mehrerer europäischer Krankenhäusern vorgesehen [18,43,65,96].

2.4. Elektronische Patientenakten unter der Datenhoheit des Patienten und Secondary Use

In dieser Arbeit wird der Einsatz einer elektronischen Patientenakte unter der Hoheit des Patienten für die Kommunikation von Daten zwischen der Versorgung und der medizinischen Forschung untersucht. Aus diesem Grund wird im Folgenden zunächst auf die am Markt befindlichen patientengeführten elektronischen Patientenakten eingegangen, um eine Übersicht zu schaffen, welche Akten momentan am Markt sind und potentiell für den in dieser Arbeit beschriebenen Ansatz genutzt werden können. Anschließend wird auf den Einsatz von elektronischen Patientenakten unter der Hoheit des Patienten für die Forschung und die Kommunikation mit dem Patienten eingegangen, um zum einen zu zeigen, was in diesem Bereich schon existiert und zum anderen die bestehenden Ansätze von den Zielen dieser Arbeit abzugrenzen (siehe 2.7).

2.4.1. Elektronische Patientenakten unter der Datenhoheit des Patienten auf dem nationalen und internationalen Markt

In Deutschland sind die Gesundheitsakten seit Anfang dieses Jahrhunderts auf dem Markt. So wird beispielweise die Careon seit 2001 in Deutschland angeboten [100,101]. Auch die Gesundheitsakte Akteonline.de konnte ab 2001 von verschiedenen Kliniken des Universitätsklinikums Münster genutzt werden. Sie wurde allerdings mittlerweile für den Endnutzer eingestellt [102–104]. Vita-x ist eine Gesundheitsakte der CompuGroup, die jetzt unter dem Namen CGM Life Gesundheitsakte in Deutschland angeboten wird [105,106]. Sie war auch in der Modellregion Trier im Einsatz [107]. Lifesensor ist eine Gesundheitsakte der Firma InterComponentWare AG (ICW), die Mitte 2011 eingestellt wurde [108]. ICW stellt die Akte nicht mehr für Privatkunden bereit, stellt aber die Komponenten z. B. für die Metropolregion Rhein Neckar zur Verfügung [109,110]. In der Metropolregion Rhein Neckar wird eine pEPA angeboten [111–115].

Microsoft HealthVault wurde 2007 in den USA gestartet [116] und kommt dort in mehreren Projekten zum Einsatz [117,118]. In Deutschland wurde diese elektronische Gesundheitsakte von 2010 bis Juni 2012 von Siemens bzw. Atos als Assingo vertrieben [119–121] und wird jetzt wieder direkt von Microsoft angeboten [122]. Google Health ist eine webbasierte

Gesundheitsakte, die 2008 von Google ins Leben gerufen, weltweit angeboten und dann Ende 2011 eingestellt wurde [123–125]. Dossia ist eine elektronische Gesundheitsakte, die auf der Indivo Plattform aufsetzt [126] und den Arbeitnehmern mehrerer Firmen (z. B. Intel, at&t oder Walmart) zur Verfügung gestellt wird [127].

2.4.2. Einsatzmöglichkeiten elektronischer Patientenakten unter der Datenhoheit des Patienten für die Forschung und Kommunikation mit dem Patienten

1994 wurde in einem Manuskript „Guardian Angel: Patient-Centered Health Information Systems" vorgeschlagen, eine lebenslange elektronische Patientenakte unter der Kontrolle des Patienten zu implementieren, die es ihm ermöglichen soll, u. a. auch Daten Forschern zur Verfügung zu stellen [128,129]. Die Idee wurde in den USA weiterverfolgt und es entstand eine elektronische Gesundheitsakte namens PING [130], die in ihrer Weiterentwicklung den Namen Indivo bekam [99]. Neben der Idee, Informationen über die elektronische Gesundheitsakte für die Forschung zu gewinnen, wurden auch Konzepte umgesetzt, den Patienten über neue Forschungsergebnisse zu informieren [99,131]. Hier wurde auch die Repräsentation von unterschiedlichen Sichten der Daten für verschiedene Rollen (Patient, Leistungserbringer oder Forscher) anhand der Berechnung des Cardiac Risk in einer elektronischen Gesundheitsakte erprobt [87]. Auch eine clinical-trials matching app wurde auf der Basis von Indivo entwickelt, mit der Patienten passende Studien in ihre elektronische Gesundheitsakte angezeigt bekommen [84].

Im Rahmen der Plattform BreastCancerTrials.org wurde eine elektronische Gesundheitsakte eingesetzt, um Brustkrebspatientinnen mögliche Studien vorzuschlagen [85].

Auch Bonander und Gates beschreiben in ihrem Artikel „Public Health in an Era of Personal Health Records: Opportunities for Innovation and New Partnerships" Möglichkeiten zum Einsatz von elektronischen Gesundheitsakten für die Forschung. Es wird vorgeschlagen, dass Patienten anonymisierte Daten aus ihren elektronischen Gesundheitsakten für public health monitoring einsetzen. Es wird auch vorgeschlagen, dass der Patient Informationen über seine elektronische Gesundheitsakte bekommen soll und selbsterfasste Daten z. B. zum Blutdruck aus seiner elektronischen Gesundheitsakte für die Forschung zur Verfügung gestellt werden sollen [132].

Auch Beispiele für eine direkte Kommunikation mit dem Patienten über seine elektronische Gesundheitsakte werden in der Literatur beschrieben. So wird beispielsweise im Artikel "Electronic Patient Messages to Promote Colorectal Cancer Screening: A Randomized, Controlled Trial" die Umsetzung für eine Erinnerung an eine Krebsvorsorgeuntersuchung über eine elektronische Gesundheitsakte beschrieben [133].

Die oben erwähnte eEPA der Metropolregion Rhein Neckar [111–115] soll eine Schnittstelle zu einem Data Warehouse bekommen, so dass die Daten der Patienten in der Metropolregion Rhein Neckar in diesem DW ausgewertet werden können [112]. Dieser Ansatz bezieht sich allerdings ausschließlich auf die Region Rhein Neckar.

2.5. Die elektronische Gesundheitskarte und die Telematikinfrastruktur in Deutschland

Der in dieser Arbeit verfolgte Ansatz setzt auf eine Nutzung der elektronischen Gesundheitskarte (eGK) und der Telematikinfrastruktur. Im Folgenden wird kurz auf die Grundlagen der eGK und der Telematikinfrastruktur sowie auf den aktuellen Stand des Projektes eingegangen.

Im Jahr 2003 wurde in Deutschland das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung verabschiedet, das die Erweiterung der Krankenkassenkarte zu einer elektronischen Gesundheitskarte durch die Krankenkassen beinhaltete. Durch die Gesundheitskarte sollen die Behandlungsqualität sowie die Transparenz im Gesundheitswesen verbessert und der Patient besser in die Behandlung eingebunden werden. Über eine sichere Kommunikationsinfrastruktur (im folgenden Telematikinfrastruktur genannt) sollen Pflichtanwendungen - sie sind für alle Patienten verpflichtend - wie das elektronische Rezept als auch freiwillige Anwendungen - der Patient kann entscheiden, ob er diese Anwendungen nutzen möchte - wie der elektronische Arztbrief oder die elektronische Patientenakte [21] umgesetzt werden. Die Daten für die Anwendungen können auf der elektronischen Gesundheitskarte (eGK) des Patienten selbst gespeichert oder auf einem Server abgelegt werden. Im zweiten Fall dient die eGK dann als Schlüssel für den Zugriff auf die Daten des Servers [134]. Zur Umsetzung dieser Telematikinfrastruktur und Einführung der elektronischen Gesundheitskarte wurde am 11. Januar 2005 die gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH ins Leben gerufen [135]. „*Die gematik hat den gesetzlichen Auftrag, die elektronische Gesundheitskarte und die Telematikinfrastruktur als Plattform einer vernetzten Versorgung einzuführen*“ [136]. Neben der elektronischen Gesundheitskarte für den Patienten ist auch ein sogenannter elektronischer Heilberufsausweis (HBA) für die Leistungserbringer (Ärzte, Apotheker und Vertreter anderer Heilberufe) vorgesehen [137], mit dem die Leistungserbringer auch Dokumente signieren können und sich gegenüber der Telematikinfrastruktur bzw. der eGK als Leistungserbringer ausweisen können [138]. Für die Nicht-Heilberufler, die auch einen Zugriff auf die Telematikinfrastruktur haben sollen, sowie die Konnektoren, die von den einzelnen Leistungserbringerorganisationen für die Kommunikation mit der Telematikinfrastruktur eingesetzt werden, sind ebenfalls Smartcards vorgesehen - die sogenannten Secure Module Card (SMC) [22]. Für Nicht-Heilberufler kommen SMC-As zum Einsatz, für Konnektoren SMC-Bs.

Nach einem Politikwechsel wurde 2010 eine Konsolidierung der bisherigen Arbeiten zur eGK und Telematikinfrastruktur durchgeführt. Die Nutzungsanwendungen wurden deutlich reduziert und man verständigte sich darauf, vier Anwendungen primär zu verfolgen. Diese Anwendungen sind das Versichertenstammdatenmanagement, das Notfalldatenmanagement, die Arzt-zu-Arzt-Kommunikation und die elektronische Fallakte [138]. Neben dieser Priorisierung auf die vier Anwendungen wurde auch ein Großteil der bisher veröffentlichten Spezifikationen (z. B. das Datenschutz- und Sicherheitskonzept) abgekündigt [139]. Die Krankenkassen wurden gesetzlich dazu verpflichtet, bis Ende 2011 10% aller eGKs und ab 2013 nur noch die elektronische Gesundheitskarte an ihre Versicherten auszugeben [138]. Da die gematik ihre bisherigen Spezifikationen im Bereich Datenschutz und Datensicherheit abgekündigt hat, wird in dieser Arbeit nicht im Detail auf die Anforderungen seitens der gematik eingegangen. Vielmehr werden die Annahmen aus dem Forschungs- und Entwicklungsprojekt (FuE) ePA Projekt bezüglich einer sicheren Telematikinfrastruktur, die die grundlegenden Mechanismen der gematik berücksichtigen (z. B. Smartcards, Public-Key-Infrastruktur - PKI - etc.), einbezogen.

2.6. Forschungs- und Entwicklungsprojekt elektronische Patientenakte gemäß § 291a SGB V

Das Bundesministerium für Gesundheit (BMG) hat 2009 ein Forschungs- und Entwicklungsprojekt ins Leben gerufen (im Folgenden auch FuE-ePA-Projekt genannt), welches die Umsetzbarkeit einer elektronischen Patientenakte nach den gesetzlichen Vorgaben des § 291a SGB V untersuchen und ein entsprechendes Konzept zur Umsetzung einer solchen Akte vorlegen soll. Ein Teilaspekt dieser Untersuchung beinhaltete auch die Nutzung einer ePA nach § 291a für einen besseren und sicheren Datenaustausch zwischen der Versorgung und der medizinischen Forschung. Neben den technischen Herausforderungen einer Vernetzung zwischen medizinischer Forschung und Versorgung gibt es auch gesetzliche Einschränkungen im § 291a SGB V, die momentan eine Nutzung der mit der eGK verwalteten Daten, unter die auch die Daten einer ePA nach § 291a fallen, für andere Zwecke als die Versorgung ausschließen und somit auch eine Nutzung der Daten für die medizinische Forschung untersagen [23]. Aus diesem Grund soll ein Vorschlag erarbeitet werden, der einen sicheren Datenaustausch zwischen Forschung und Versorgung ermöglicht und somit als Diskussionsgrundlage in Bezug auf eine Änderung des § 291a zu Gunsten der Forschung dienen kann. Diese Dissertation entsteht auf Grundlage dieses Projektes.

Die beteiligten Partner sind neben der Abteilung Medizinische Informatik der Universitätsmedizin Göttingen die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), die Fraunhofer Institute für Sichere Informationstechnologie (SIT) und für Offene Kommunikationssysteme (FOKUS)[6]. Zusätzlich sind die Bundesärztekammer, die Deutsche Krankenhausgesellschaft e. V. und die gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH als Kooperationspartner an dem FuE-ePA-Projekt beteiligt.

Der Schwerpunkt der Arbeit der Abteilung Medizinischen Informatik und somit auch dieser Dissertation liegt in der Konzeption einer datenschutzkonformen Anbindung einer ePA an die medizinische Forschung. Die Konzeption der ePA für die Versorgung sowie die prototypische Implementierung der gesamten IT-Komponenten wird durch die Fraunhofer Institute durchgeführt. Die in diesem Projekt erarbeiteten Ergebnisse zur Konzeption einer ePA für die Versorgung werden im Kapitel 5 beschrieben.

2.7. Abgrenzung der Arbeit zu anderen Projekten

Im Bereich des Secondary Use von Versorgungsdaten gibt es lokale und institutionsübergreifende Ansätze, über die verschiedenste Anwendungsfälle umgesetzt werden. Der Einsatz von patientengeführten elektronischen Patientenakten für die Forschung ist noch wenig erforscht. Besonders in Bezug auf die deutsche Telematikinfrastruktur und die Möglichkeiten des Einsatzes einer ePA für die Forschung gibt es noch keine Arbeiten. Dies wird auch am § 291a SGB V liegen, der eine Nutzung der Daten außerhalb der Versorgung ausschließt. In den USA werden die patientengeführten elektronischen Patientenakten sowohl für die Gewinnung von Daten für die Forschung vorgesehen, als auch um den Patienten über Forschungsergebnisse und neue Studien zu informieren. In Deutschland soll in der Metropolregion Rhein Neckar eine persönliche,

[6] Projektverantwortliche: Jörg Caumanns (Fraunhofer FOKUS), Levona Eckstein (Fraunhofer SIT) und Sebastian Semler (TMF e.V.).

einrichtungsübergreifende Patientenakte aufgebaut werden, aus der Daten in ein Data Warehouse überführt werden können. Dieser Ansatz soll allerdings nur auf eine Region beschränkt werden und bezieht somit die nationale Telematikinfrastruktur nicht mit ein.

Der in dieser Arbeit verfolgte Ansatz soll einen Austausch von Patientendaten zwischen der Forschung und der Versorgung über eine elektronische Patientenakte unter der Datenhoheit des Patienten ermöglichen. Dabei soll der Patient aktiv entscheiden, welche Daten über seine ePA übertragen werden sollen, und selbst auch als Datenlieferant sowie als Empfänger von Daten aktiv in die Kommunikation einbezogen werden. Auch wenn ähnliche Konzepte schon in den USA publiziert wurden, wird in dieser Arbeit der Fokus auf das deutsche Gesundheitswesen und die deutschen Forschungsinfrastrukturen gelegt. D. h. die Ergebnisse dieser Arbeit sind auf die nationalen IT-Infrastrukturen und Datenschutzanforderungen ausgelegt. Zudem wird zum ersten Mal ein Konzept entwickelt, das die Nutzung einer nationalen Telematikinfrastruktur für den Datenaustausch zwischen Forschung und Versorgung mittels einer elektronischen Patientenakte unter der Datenhoheit des Patienten zum Ziel hat. Damit sollen die bestehenden bzw. im Aufbau befindlichen IT-Infrastrukturen der Versorgung und der Forschung in Deutschland sicher und datenschutzkonform über eine patientengeführte elektronische Patientenakte verbunden und somit ein direkter Austausch zwischen den oben genannten IT-Infrastrukturen aus der Forschung und der Versorgung ermöglicht werden.

2.8. Abgrenzung der Fragestellung

Auch wenn im vorhergehenden Abschnitt der Ansatz der Arbeit zu anderen Projekten abgegrenzt wurde, so sind die zu betrachtenden Fragestellungen hierzu immer noch sehr vielschichtig. Der Fokus der Arbeit liegt auf dem sicheren und datenschutzkonformen Austausch von Daten. Weitere Punkte, die bei dem Ansatz berücksichtigt werden müssen, aber nicht Bestandteil dieser Arbeit sind, werden im Folgenden kurz aufgeführt:

Die rechtlichen Rahmenbedingungen des § 291a SGB V schließen eine Nutzung der mithilfe der eGK verwalteten medizinischen Daten für andere Zwecke als die der medizinischen Versorgung der Versicherten aus. Damit wird auch eine Nutzung der Daten einer ePA für die versorgungsnahe Forschung ausgeschlossen. Daher ist die in dieser Arbeit beschriebene Lösung zur Anbindung der versorgungsnahen Forschung an eine ePA als ein Vorschlag zu sehen, wie ein datenschutzkonformer Austausch pseudonymisierter medizinischer Daten unter Kontrolle des Versicherten aussehen könnte. Auf dieser Basis kann dann eine mögliche Anpassung der rechtlichen Rahmenbedingungen geprüft werden. Eine rechtliche Betrachtung und mögliche gesetzliche Anpassungen werden in dieser Arbeit nicht berücksichtigt.

Als IT-Infrastruktur eines Forschungsverbundes werden die in den Datenschutzkonzepten der TMF [33,34] beschriebenen IT-Komponenten und Anwendungsfälle betrachtet. Da das Thema Biobanken für sich schon sehr komplex ist, wird hierauf in dieser Arbeit nicht weiter eingegangen, d. h. es werden nur Systeme für Phänotypdaten berücksichtigt.

Ein großes Forschungsfeld im Bereich der elektronischen Kommunikation von Patientenakten im Gesundheitswesen ist die semantische Interoperabilität der Daten. In dieser Arbeit wird nur die sichere Kommunikation von Daten betrachtet; auf den Aufbau der Daten sowie deren semantische Interoperabilität wird nicht weiter eingegangen. Hierbei sind strukturierte

textuelle Daten gemeint; die Pseudonymisierung von Bilddaten ist ein komplexes Thema und wird hier ebenfalls nicht weiter behandelt.

Es wird nur auf die Kommunikation zwischen der ePA und den Leistungserbringern bzw. der ePA und den Modulen der Forschung eingegangen. Wie die Daten über die ePA zwischen Versorgung und Forschung weitergeleitet werden (vollautomatisch, immer durch den Patienten, durch Anfragen der Leistungserbringer bzw. der Module der Forschung etc.), ist nicht Bestandteil der Betrachtung.

Auch wenn es durch die Verbindung der ePA mit der Forschung mögliche neue Anwendungsfälle bzw. Szenarien geben kann, wird der Fokus der Arbeit auf die Umsetzung der bereits bestehenden Anwendungsfälle eines Forschungsverbundes über eine ePA gelegt.

Es wird keine Schutzbedarfsanalyse der Forschungsschnittstelle oder des Gesamtsystems durchgeführt. Diese Schutzbedarfsanalyse muss im Rahmen einer weiteren Arbeit erfolgen.

Ein wichtiger Aspekt ist die verständliche Darstellung der Daten, so dass ein Patient bzw. Proband überhaupt selbst entscheiden kann, welche Daten bzw. Berechtigungen er für wen vergibt. Dieses Thema ist sehr komplex und wird in dieser Arbeit nicht weiter verfolgt. Es muss aber eine Voraussetzung für den ePA-Hersteller sein, diese Anforderungen zu erfüllen.

Der Bürger soll die Kommunikation mit der Forschung über einen eigenen Client durchführen. Es werden Anforderungen an den Client bzw. das Aktensystem gestellt, diese Anforderungen werden aber nicht in dieser Arbeit konzeptionell betrachtet.

Die Konzeption geht bis zur Fach- und Sicherheitsarchitektur; eine Implementierung ist nicht Teil dieser Arbeit. Im Rahmen des Projektes und im Rahmen von studentischen Arbeiten wurden anhand der Spezifikation Teile davon prototypisch umgesetzt.

Es werden keine Anforderungen zum Thema Datenqualität oder weitere Regeln (beispielsweise Good Clinical Practice Regeln -GCP-) zum Erheben und zur Verarbeitung von Forschungsdaten wie z. B. ein Audit-Trail betrachtet.

3. Methodik und Grundlagen

In diesem Kapitel wird zunächst auf die Methodik und das Vorgehen zum Herleiten des Kommunikationsmodells sowie der Fach- und Sicherheitsarchitektur der Forschungsschnittstelle eingegangen. Anschließend wird das Vorgehen bei der Überprüfung der Ergebnisse der Arbeit durch einen Experten-Review beschrieben. Abschließend wird auf das Vorgehen bei der Literaturrecherche, das Zusammenspiel mit den Ergebnissen aus dem FuE-ePA Projekt und die Implementierung eingegangen.

3.1. Vorgehen und Methodik bei der Analyse der Module und Anwendungsfälle eines medizinischen Forschungsverbundes

In dieser Arbeit wird das Forschungssystem auf die IT-Infrastruktur von Forschungsverbünden eingegrenzt, die sich an den Vorgaben der Datenschutzkonzepte der TMF orientieren. Die Datenschutzkonzepte der TMF [33,34] wurden aus zwei Gründen als Grundlage für die Analyse eines medizinischen Forschungsverbundes ausgewählt: Zum einen haben die Konzepte einen generischen Charakter und können somit auf mehrere Forschungsverbünde angewendet werden. Zum anderen sind sie mit allen deutschen Landesdatenschutzbeauftragten abgestimmt und bilden somit aus Sicht des Datenschutzes einen Konsens, wie medizinische Forschungsverbünde in Deutschland datenschutzkonform umgesetzt werden können. Die Datenschutzkonzepte der TMF haben nicht den Anspruch alle Anwendungsfälle eines Forschungssystems vollständig zu erfassen. Daher wird die Analyse der generischen Datenschutzkonzepte der TMF durch eine Analyse der Datenschutzkonzepte bestehender medizinischer Forschungsverbünde ergänzt. Auf Grundlage dieser beiden Analysen wird abschließend noch eine Priorisierung der Komponenten eines medizinischen Forschungsverbundes in Bezug auf die Eignung zur Anbindung an eine ePA nach § 291a vorgenommen, um die Komplexität des Forschungssystems zu reduzieren.

3.1.1. Analyse der generischen Datenschutzkonzepte

Um eine Übersicht über alle IT-Komponenten eines medizinischen Forschungsverbundes zu erlangen, werden die generischen Datenschutzkonzepte der TMF und der Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - in Bezug auf die IT-Komponenten und die möglichen Anwendungsfälle analysiert. Hier werden beide Versionen untersucht, da die zweite Version noch nicht final ist und die erste Version momentan noch als aktuelle Empfehlung der TMF gilt. Dennoch gibt es viele neue Aspekte in der zweiten Version, die in dieser Arbeit aufgegriffen werden sollen. Grundsätzlich werden die Inhalte der zweiten Version als aktuell angesehen. Sollten Anwendungsfälle in der 1. Version beschrieben worden sein und in der 2. Version nicht, so werden diese Anwendungsfälle ergänzt. Bei allgemeingültigen Datenschutzanforderungen (siehe Kapitel 7.1), die sowohl Grundlage der ersten als auch in der zweiten Version sind, wird die erste Version zitiert, da diese Version schon publiziert und mit den Datenschutzbeauftragten der Länder abgestimmt ist.

Als Ergebnis dieser Analyse wird eine Übersicht aller Module bzw. IT-Komponenten eines medizinischen Forschungsverbundes und deren Anwendungsfälle erwartet. Eine Beschreibung aller in der Analyse identifizierten Module bzw. IT-Komponenten eines medizinischen Forschungsverbundes befindet sich in den Unterkapiteln Kapitel 4.2.1-4.2.4. Die identifizierten Anwendungsfälle werden zunächst für alle Module in Tabellenform erfasst (siehe Tabelle 1). Hier wird für jeden Anwendungsfall das zugehörige Modul, der Name des

Anwendungsfalls, die Information, ob ein Patientenbezug besteht, und die Quelle(n), in der / denen der Anwendungsfall beschrieben wird, erfasst[7].

Modul	Anwendungsfall	Patientenbezug	Quelle
Name des Moduls	Name des Anwendungsfalls	Begründung, warum der Anwendungsfall einen Patientenbezug hat oder nicht.	Quelle(n), in der / denen der Anwendungsfall beschrieben wurde.

Tabelle 1: Beispiel der Dokumentation der IT-Komponenten und Anwendungsfälle eines medizinischen Forschungsverbundes

Für die Arbeit sind nur Anwendungsfälle mit Patientenbezug interessant, da nur für diese Anwendungsfälle eine Kommunikation über die Forschungsschnittstelle mit Hilfe der ePA erfolgen soll. Als Patientenbezug wird verstanden, dass der Patient aktiv mitwirkt, d. h. alle Anwendungsfälle, bei denen der Patient Informationen bereitstellt oder bekommt. Alle Anwendungsfälle, die keinen Patientenbezug haben, werden in der Tabelle 21 im Anhang A1.4 grau hinterlegt und im weiteren Verlauf der Arbeit nicht weiter berücksichtigt.

Da in den generischen Datenschutzkonzepten zwar alle Module bzw. IT-Komponenten beschrieben werden, die Konzepte aber nicht den Anspruch haben, alle Anwendungsfälle zu beschreiben und auch nicht jede mögliche Umsetzung, wird die Tabelle 21 durch eine Analyse der Datenschutzkonzepte der medizinischen Forschungsverbünde ergänzt.

3.1.2. Analyse bestehender medizinischer Forschungsverbünde

Um die Ergebnisse aus der Analyse der generischen Datenschutzkonzepte zu erweitern, werden Datenschutzkonzepte der medizinischen Forschungsverbünde, die im Zeitraum von 2002 bis Ende 2011 entstanden sind, analysiert. Ziel ist es, zum einen weitere Anwendungsfälle der einzelnen IT-Komponenten und unterschiedliche Umsetzungen zu identifizieren. Zum anderen soll analysiert werden, welche Module wie häufig eingesetzt werden, um das Ergebnis dieser Analyse als eine Bewertung für die Auswahl der relevanten Module mit einzubeziehen.

Grundlage für die Analyse der Datenschutzkonzepte (DSK) der letzten 10 Jahre sind die in der Arbeitsgruppe Datenschutz (AG DS) der TMF vorgestellten DSKs [140]. Es werden nur Datenschutzkonzepte berücksichtigt, für die entweder eine Befürwortung von einem Landesbeauftragten für den Datenschutz (LfD) oder für die ein Votum der TMF AG DS vorliegt.

Die AG DS führt seit 2004 kontinuierliche datenschutzrechtliche Beratung von Projekten durch [141]. Seit 2004 sind auch die Protokolle der AG DS verfügbar, aus denen hervorgeht, welche Datenschutzkonzepte vorgestellt und befürwortet wurden. Zudem gibt es eine Übersicht bis zum 24.06.2008, in der der Beratungs- und Implementationsstand zu Datenschutzkonzepten in der medizinischen Verbundforschung von 2001-2008 zusammengefasst wird [142].

Die Datenschutzkonzepte der Verbünde der TMF, die vor 2004 entstanden sind, sowie deren Befürwortung wird in der oben erwähnten Übersicht aufgeführt.

[7] Anwendungsfälle, die während der Analyse identifiziert wurden und noch nicht in den Datenschutzkonzepten der TMF enthalten waren, wurden an die Autoren des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - weitergeleitet und dann in eine spätere Version des Leitfadens aufgenommen.

Für den Zeitraum zwischen 2002 und 2008 wurden die Datenschutzkonzepte von der Geschäftsstelle der TMF zur Verfügung gestellt. Von 2008 bis Ende 2011 werden alle DSKs berücksichtigt, die in der TMF AG DS vorgestellt wurden und als Konzept vorlagen.

Eine Übersicht aller in der AG DS vorgestellten Datenschutzkonzepte befindet sich in der Tabelle 19 und der Tabelle 20 im Anhang A1.3. Die Tabellen enthalten für jeden in der AG DS vorgestellten Forschungsverbund einen Eintrag mit dem Namen des Forschungsverbundes, dem Datum der Erstvorstellung des Datenschutzkonzeptes in der AG DS sowie Angaben, ob ein Konzept vorhanden ist und dieses Konzept befürwortet wurde (siehe Tabelle 2). Sind Einträge in der Tabelle grau hinterlegt, so haben die Forschungsverbünde die Kriterien nicht erfüllt und deren Datenschutzkonzepte wurden nicht weiter untersucht.

Verbund	Erstvorstellung	Konzept vorhanden	Befürwortet durch (Quelle)
Name des Forschungsverbundes	Datum, an dem das Datenschutzkonzept zum ersten Mal in der AG DS vorgestellt wurde.	Angabe, ob das Konzept vorhanden ist oder nicht.	Ob und durch wen das Datenschutzkonzept befürwortet wurde sowie die Angabe der Quelle (Protokoll, Web-Recherche, Auskunft des Sprechers der AG DS).

Tabelle 2: Beispiel der Auflistung der in der AG DS vorgestellten Datenschutzkonzepte der medizinischen Forschungsverbünde

Neben den Datenschutzkonzepten wurden auch die Patienteneinwilligungen und die Patientenaufklärungsbögen analysiert (sofern diese zugänglich waren), da hier häufig die Kommunikation zwischen dem Forschungsverbund (Kontaktaufnahme durch den Forschungsverbund, Möglichkeiten des Rückzugs der Einwilligungserklärung etc.) und dem Patienten geregelt wird.

3.1.3. Priorisierung der Module

Während der Analyse stellte sich heraus, dass die detaillierte Analyse aller Module eines Forschungsverbundes im Rahmen dieser Arbeit aus Komplexitätsgründen nicht geleistet werden kann, so dass nur die Anbindung eines Moduls eines medizinischen Forschungsverbundes über die Forschungsschnittstelle betrachtet werden soll. Da die Module untereinander „kompatibel“ sind und auch gleiche Datenschutzmechanismen zum Einsatz kommen, wird hier davon ausgegangen, dass die in dieser Arbeit zu spezifizierende Forschungsschnittstelle ohne extreme Anpassungen um weitere Module eines Forschungsverbundes ergänzt werden kann.

Die Auswahl des Moduls eines medizinischen Forschungsverbundes, das über die Forschungsschnittstelle an die ePA angebunden werden soll, erfolgt durch eine Priorisierung der einzelnen Module nach den folgenden Faktoren:

- **Die Anzahl des Einsatzes des Moduls in den analysierten Forschungsverbünden:** Ein wichtiger Punkt ist die Häufigkeit des Einsatzes eines Moduls, um die Relevanz der Anbindung des Moduls für die medizinischen Forschungsverbünde zu berücksichtigen. Daher werden häufiger umgesetzte Module priorisiert. Je häufiger ein Modul im Einsatz ist, desto mehr Leistungserbringer und Patienten können von der Anbindung profitieren.

- **Die Anzahl der relevanten Anwendungsfälle:** Ziel der Arbeit ist es, den Patienten über seine ePA besser in die Prozesse eines Forschungsverbundes einzubinden. Daher werden Module höher priorisiert, die viele Anwendungsfälle mit Patientenbezug vorweisen.
- **Die Anzahl der Anwendungsfälle, bei denen der Patient eigene Daten über seine ePA bereitstellt:** Ein wichtiges Ziel der Arbeit ist nicht nur, den Patienten aktiver in die Informationsflüsse einzubeziehen, sondern es ihm auch zu ermöglichen, Daten über sich zu erfassen und für die Forschung bereitzustellen. Aus diesem Grund werden Module priorisiert, die Anwendungsfälle vorsehen, bei denen der Patient eigene Daten bereitstellt.
- **Die Anzahl der Anwendungsfälle, bei denen ein Austausch mit der Versorgung stattfindet:** Ein weiteres Ziel der Arbeit ist es, den Austausch zwischen der Versorgung und der Forschung über eine ePA zu verbessern. Es werden also Module höher priorisiert, bei denen viele Anwendungsfälle einen Austausch zwischen Forschung und Versorgung vorsehen.

Die einzelnen Punkte sind gleich gewichtet. Die Ergebnisse der Auswertung der Kriterien werden summiert. Das Modul mit den meisten Punkten hat somit die höchste Priorität und wird damit weiter verfolgt. Im Abschnitt 4.4 werden die einzelnen Module zusammenfassend bewertet. Hierzu werden für jedes Modul die einzelnen Punkte in Form einer Tabelle (siehe auch Tabelle 3) zusammengefasst.

Anwendungs-fall	**Bereitstellung von Daten durch den Forschungs-verbund**	**Bereitstellung von Daten durch den Patienten**	**Austausch Versorgung**	**Bereitstellung selbst erhobener Daten**
Name des Anwendungs-falls	Aufzählung von Informationen, die den Patienten von einem Forschungs-verbund während des Anwendungs-falls bereitgestellt werden.	Aufzählung von Informationen, die dem Forschungs-verbund während des Anwendungs-falls durch den Patienten bereit-gestellt werden.	Beschreibung der Möglichkeiten des Austausches von Daten zwischen dem Modul und der Versorgung während dieses Anwendungsfalls.	Aufzählung von durch den Patienten erho-benen Informationen, die dem Forschungs-verbund während des Anwendungsfalls durch den Patienten bereitgestellt werden.

Tabelle 3: Beispiel der Dokumentation der Auswahlkriterien eines Moduls eines medizinischen Forschungsverbundes

3.2. Erheben und Umsetzen von Anforderungen an die Systeme

Während der Arbeit werden Anforderungen an die Forschungsschnittstelle gestellt. Diese Anforderungen werden mit dem Präfix A durchnummeriert. Im Anhang A3.5 in der Tabelle 49 werden alle Anforderungen zusammengefasst. Diese Tabelle enthält sowohl die Nummer und den Namen der Anforderung sowie den Namen des Systems, für das die Anforderung gilt, als auch eine kurze Beschreibung der Anforderung und einen Verweis darauf, in welchem Kapitel auf die Anforderung eingegangen wird und eine entsprechende Umsetzung erfolgt (vergleiche auch Tabelle 4).

An.-Nr.	Anforderungsname	System	Kurzbeschreibung	Umgesetzt in Abschnitt
A01	Anforderungs- und Bereitstellungsobjekte unterstützen	Forschungs-schnittstelle	Die Forschungsschnittstelle muss Anforderungs- und Bereitstellung-objekte unterstützen.	Kapitel 7

Tabelle 4: Beispiel einer Zusammenfassung einer Anforderung der Forschungsschnittstelle

In den Kapiteln, in denen die Anforderungen wieder aufgenommen werden, wird ein entsprechender Verweis auf die Nummer der Anforderung vorgenommen und begründet, wie diese Anforderung umgesetzt wird. Können die Anforderungen nicht direkt durch die Forschungsschnittstelle erfüllt werden, so werden Voraussetzungen an die Systeme formuliert. Diese Voraussetzungen werden ebenfalls in Tabellenform zusammengefasst (siehe Tabelle 50 und Tabelle 51).

3.3. Methodik und Vorgehen bei der Erstellung des Kommunikationsmodells

Ziel ist es, eine Schnittstelle zwischen dem ePA-System und dem Forschungssystem zu konzipieren, über die eine datenschutzkonforme Kommunikation zwischen den Systemen erfolgen kann. Hierzu soll ein Kommunikationsmodell hergeleitet und beschrieben werden, über welches die Kommunikation aller identifizierten Anwendungsfälle zwischen dem ausgewählten Modul des Forschungsverbundes und der ePA abgebildet werden können. Außerdem soll analysiert werden, welche Datenschutzanforderungen bei einer Kommunikation zwischen dem ausgewählten Modul eines Forschungsverbundes und der ePA berücksichtigt werden müssen. Neben dem Kommunikationsmodell werden also auch Anforderungen aus den Anwendungsfällen abgeleitet, die durch die Forschungsschnittstelle, das Forschungssystem oder das ePA-System erfüllt werden müssen. Diese Anforderungen werden wie im Abschnitt 3.2 beschrieben erfasst und umgesetzt. Auf Grundlage des Kommunikationsmodells und der herausgestellten Anforderungen an die Forschungsschnittstelle werden dann die IT-Komponenten der Forschungsschnittstelle beschrieben und gezeigt, wie über diese Komponenten im Zusammenspiel mit dem ePA- und dem Forschungssystem die Kommunikationsmuster des Kommunikationsmodells unter den herausgearbeiteten Anforderungen umgesetzt werden können (siehe Kapitel 7).

Zunächst werden Annahmen getroffen und Voraussetzungen für die Anbindung einer ePA nach § 291a an das ausgewählte Modul eines Forschungsverbundes festgelegt.

Auf Grundlage dieser Annahmen und Voraussetzungen wird im Sinne einer Blackbox ein bestimmtes Verhalten der Forschungsschnittstelle angenommen. Mit diesem Hintergrund wird die Forschungsschnittstelle in die Gesamtarchitektur eingeordnet (siehe Abschnitt 6.1).

Anschließend wird für jeden identifizierten Anwendungsfall des ausgewählten Moduls eines Forschungsverbundes die Kommunikation zwischen dem Patienten und den Akteuren des Moduls analysiert. Es wird immer nur eine mögliche Umsetzung eines Anwendungsfalls betrachtet. Sollte es mehrere Umsetzungen geben, wird immer die Umsetzung ausgewählt, die eine direkte Kommunikation zwischen dem Patienten und dem Forschungsverbund ermöglicht. Als Beispiel sei hier die Aktualisierung der Kontaktdaten eines Patienten genannt. Die neuen Kontaktdaten können entweder vom Patienten dem behandelnden Arzt mitgeteilt werden und der Arzt teilt die Daten wiederum dem Forschungsverbund mit, oder die Daten werden direkt vom Patienten dem Forschungsverbund mitgeteilt. In diesem Fall würde die zweite Variante aufgrund der direkteren Kommunikation zwischen dem Patienten und dem Forschungsverbund gewählt werden.

Bei der Beschreibung der Kommunikation der einzelnen Anwendungsfälle wird herausgestellt, welche Informationen dem Patienten und welche Informationen dem Forschungsverbund nach Ablauf der Kommunikation vorliegen (siehe Tabelle 5). Diese Informationen werden mit Infoxx fortlaufend beschriftet.

Im nächsten Schritt wird untersucht, wie die Kommunikation zwischen dem Patienten und den Akteuren des ausgewählten Moduls eines Forschungsverbundes über eine ePA nach § 291a umgesetzt werden kann. Bei der Beschreibung der Kommunikation werden die Kommunikationsmuster der ePA berücksichtigt, die in das Anfordern und Bereitstellen von Informationen unterteilt sind (vergleiche Kapitel 5.5). Die Kommunikation eines Anwendungsfalls ist immer erfolgreich mit Hilfe einer ePA umgesetzt, wenn den Akteuren die gleichen Informationen vorliegen, wie bei der Kommunikation des zugrunde liegenden Anwendungsfalls. D. h. der Patient und der Hauptakteur[8], der an der Kommunikation beteiligt ist, können die gleichen Informationen über die Forschungsschnittstelle austauschen, wie sie die Informationen andernfalls auf dem herkömmlichen Wege ausgetauscht hätten.

Bei der Umsetzung der Anwendungsfälle des ausgewählten Moduls eines Forschungsverbundes mit Hilfe einer ePA sollen folgende Fragen berücksichtigt werden:

- Gibt es eine Optimierung der Kommunikation zwischen dem Patienten und dem Hauptakteur. Eine Optimierung der Kommunikation wird erzielt, wenn weniger Akteure an der Kommunikation beteiligt sind. Im Idealfall kommunizieren der Patient und der Hauptakteur direkt.
- Können durch eine Kommunikation mit der ePA Medienbrüche vermieden werden?
- Welche zusätzlichen Anforderungen ergeben sich an das ePA-System, das Forschungssystem und die Forschungsschnittstelle durch die Anpassung der Kommunikation für die Anwendungsfälle?

Bei der Kommunikation mit Hilfe der ePA wird immer davon ausgegangen, dass sie so direkt wie möglich zwischen dem Patienten und dem initiierenden Akteur erfolgt. Sollte es Gründe geben, die eine direkte Kommunikation verhindern, so werden diese Gründe auf Grundlage des ursprünglichen Anwendungsfalls erläutert.

Für jeden Anwendungsfall wird beschrieben, ob sich aufgrund der direkten Kommunikation zwischen der ePA und den Datenbanken des Versorgungsmoduls neue Anforderungen an das ePA-System, das Forschungssystem oder die Forschungsschnittstelle ergeben.

Die Kommunikation wird für jede IT-Komponente des ausgewählten Moduls eines Forschungsverbundes zusammengefasst und hieraus werden generische Kommunikationsmuster abgeleitet, die dann das Kommunikationsmodell beschreiben. Hierbei werden immer der Anwendungsfall, der empfangende und bereitstellende Akteur sowie das empfangende und bereitstellende System aufgeführt (vergleiche Tabelle 5). Jedes Kommunikationsmuster wird fortlaufend mit I-xx gekennzeichnet.

[8] Der Hauptakteur ist derjenige, der die Informationen für den Patienten bereitstellt bzw. vom Patienten bekommt.

Nr.	Anwendungsfall	Empfänger	Bereitsteller	Empfangendes System	Bereitstellendes System	Informationsaustausch
I-1	Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler	Patient	Verwalter Patientenliste	ePA	Patientenliste	Info01
I-2	Kontaktieren eines Patienten über den Verwalter der Patientenliste	Patient	Verwalter Patientenliste	ePA	Patientenliste	Info03

Tabelle 5: Beispielhafte Zusammenfassung der Kommunikation zwischen einer ePA und der Patientenliste.

Aufgrund des vom ePA-System unterstützten Prinzips des Anforderns und Bereitstellens können pro Anwendungsfall auch zwei Kommunikationsvorgänge entstehen, die dann durch zwei Kommunikationsmuster umgesetzt werden. Zum Beispiel fordert der Patient im Rahmen des Auskunftsrechtes seine Informationen vom Forschungsverbund an (erste Kommunikation) und der Forschungsverbund stellt dem Patienten daraufhin die Informationen bereit (zweite Kommunikation). Die Kommunikationsmuster werden für die IT-Komponenten des ausgewählten Moduls eines Forschungsverbundes anschließend zu generischen Kommunikationsmustern zusammengefasst. Kommunikationsmuster können immer zu einem generischen Kommunikationsmuster zusammengefasst werden, wenn die Akteure und die Systeme gleich sind und sich nur die auszutauschenden Informationen unterscheiden.

Die generischen Kommunikationsmuster und die Anforderungen an die Systeme sind dann die Grundlage für die Beschreibung der Umsetzung der Kommunikation zwischen einer ePA und dem ausgewählten Modul eines Forschungsverbundes über die Forschungsschnittstelle im Kapitel 7.

3.4. Formale Beschreibung des Verhaltens sowie der Kommunikation zwischen den IT-Komponenten

Die Kommunikation der Anwendungsfälle der ePA, des Versorgungsmoduls und der Umsetzung der generischen Kommunikationsmuster des Kommunikationsmodells werden zum einen strukturiert textuell dokumentiert (siehe Tabelle 6) und zum anderen in Form von Unified Modeling Language (UML) Sequenzdiagrammen abgebildet [143] (siehe Abbildung 4).

Bezeichner	Bezeichner z. B. UC-1-1
Name	Name des Anwendungsfalls, für den die Kommunikation beschrieben wird.
Kurzbeschreibung	Kurze Beschreibung des Anwendungsfalls.
Primärer Akteur	Akteur, der die Kommunikation initiiert.
Andere Akteure	Weitere an der Kommunikation beteiligte Akteure.
Systeme	An der Kommunikation beteiligte Systeme.
Vorbedingungen	Bedingungen, die vor dem Ablauf der Kommunikation erfüllt sein müssen.
Nachbedingungen	Bedingungen, die nach dem Ablauf der Kommunikation erfüllt sind.
Hauptszenario	Textuelle Beschreibung der einzelnen Schritte der Kommunikation.

Beziehungen zu anderen Use Cases	Verweise auf andere Anwendungsfälle, die in Beziehung zu diesem Anwendungsfall stehen.
Bereitstellen von Daten durch den Forschungsverbund	Informationen, die dem Patienten nach Ablauf der Kommunikation vom Forschungsverbund zur Verfügung gestellt wurden (nur bei der Beschreibung der Kommunikation des Versorgungsmoduls).
Bereitstellen von Daten durch den Patienten	Informationen, die dem Forschungsverbund nach Ablauf der Kommunikation vom Patienten zur Verfügung gestellt wurden (nur bei der Beschreibung der Kommunikation des Versorgungsmoduls).

Tabelle 6: Beispiel für eine textuelle Beschreibung einer Kommunikation eines Anwendungsfalls.

Die folgende Abbildung zeigt die verwendete UML-Notation für die Beschreibung der Sequenzdiagramme.

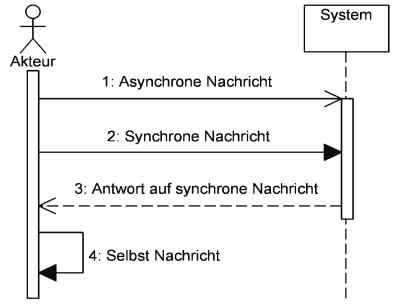

Abbildung 4: UML-Notation für Sequenzdiagramme

Die Beschreibung des Verhalten der IT-Komponenten beim Aufrufen bzw. Durchführen von Operationen wird im Rahmen der Facharchitektur neben einer textuellen Beschreibung auch in Form von UML-Aktivitätsdiagrammen [143] beschrieben (Beispiel siehe Abbildung 5).

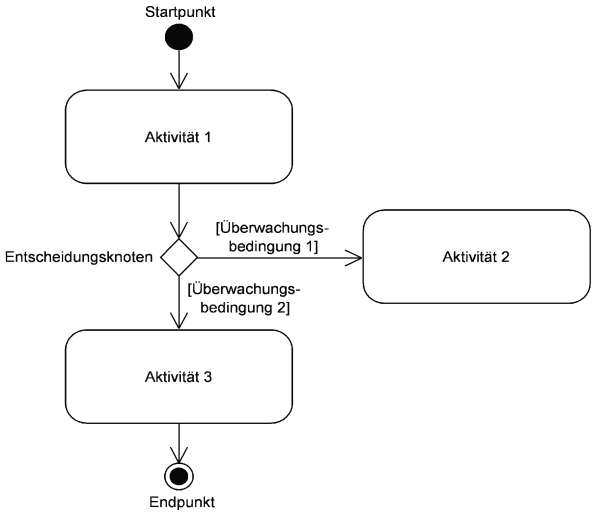

Abbildung 5: UML-Notation für Aktivitätsdiagramme

3.5. Vorgehen bei der Herleitung der Fach- und Sicherheitsarchitektur

Grundsätzlich wird angenommen, dass die bestehenden Komponenten des ePA-Systems genutzt werden (dies betrifft Fach- und Sicherheitsarchitektur). Nur wenn es aufgrund von Anforderungen seitens des Forschungssystems nicht vereinbar ist, werden spezielle Lösungen erarbeitet. Diese Lösungen werden dann auch im Hinblick auf eine Widerspruchsfreiheit überprüft.

Nachdem das Kommunikationsmodell definiert wurde, wird beschrieben, wie die herausgestellten Datenschutzanforderungen des ausgewählten Moduls eines Forschungsverbundes für jedes Kommunikationsmuster des Modells im Zusammenspiel der IT-Komponenten der Forschungsschnittstelle und der IT-Komponenten des ePA-Systems umgesetzt werden können.

Es werden aus dem „Teil A: Bereitstellung von Behandlungs- und Forschungsdaten in klinisch fokussierten Forschungsnetzen der Generischen Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin“ [33] Datenschutzanforderungen an das Versorgungsmodul herausgestellt und mit entsprechenden Zitaten aus dem Datenschutzkonzept belegt. Aus diesen Datenschutzanforderungen und den in den vorherigen Kapiteln herausgestellten Datenschutz- und technischen Anforderungen werden Architekturentscheidungen abgeleitet und ggf. neue Voraussetzungen an die Systeme gestellt. Anschließend werden die Komponenten der Forschungsschnittstelle auf Grundlage der Architekturentscheidungen beschrieben. Bei dieser Beschreibung wird darauf eingegangen, wie die restlichen technischen Anforderungen an die Forschungsschnittstelle durch die Komponenten umgesetzt werden, und beschrieben, wie die Forschungsschnittstelle mit der ePA-Kommunikationskomponente kommuniziert.

Anschließend wird sowohl textuell als auch in Form eines Sequenzdiagrammes beschrieben, wie jedes Kommunikationsmuster über die beschriebenen Komponenten der Forschungsschnittstelle umgesetzt werden kann. Die Ergebnisse dieses Vorgehens sind in Kapitel 7 zu sehen.

Aufbauend auf der Beschreibung der Komponenten der Forschungsschnittstelle und den Kommunikationsmustern wird die Facharchitektur der Forschungsschnittstelle im Kapitel 8 beschrieben. Da die Forschungsschnittstelle und die Schnittstelle zwischen der ePA und den Systemen der Versorgung (LE-Schnittstelle) als ein Gesamtkonzept implementiert werden sollen, wird sich bei der Beschreibung der IT-Komponenten der Forschungsschnittstelle, deren Kommunikation und Schnittstellen an die Methodik und den Aufbau der im FuE-Projekt-EPA entstandenen Facharchitektur der LE-Schnittstelle orientiert [144].

Es sollen die Schnittstellen und Hilfsobjekte der LE-Schnittstelle verwendet werden. Es werden die Hilfsobjekte der LE-Schnittstelle und der Kommunikation untersucht (siehe auch 8.2). Danach wird die Umsetzung der generischen Kommunikationsmuster über die von der LE-Schnittstelle verwendeten Operationen beschrieben. Hierzu wird für jedes generische Kommunikationsmuster analysiert, welche IT-Komponenten welche Informationen austauschen und wie diese Informationen über die Operationen der LE-Schnittstelle ausgetauscht werden können. Hierbei wird auch festgelegt, wer Dienstanbieter (also die Operationen bereitstellt) und wer Dienstnutzer (also die Operationen aufruft) ist. Die Operationen werden dann zu Schnittstellen zusammengefasst. Auf dieser Grundlage wird das Verhalten der einzelnen Komponenten vom Aufrufen bzw. beim Aufruf der Operation

beschrieben und festgelegt, welche Module die einzelnen Komponenten der Forschungsschnittstelle umsetzen müssen (siehe Anhang A4).

Der Übergabepunkt zwischen der im Kapitel 8 beschriebenen Facharchitektur und dem detailliertem Verhalten der Komponenten im Anhang A4 ist eine Zusammenfassung der Operationen für die einzelnen Schnittstellen der Komponenten. Die Operationen der Schnittstellen werden wie im nachfolgenden Beispiel (siehe Abbildung 6) beschrieben durch einen Namen, eine RLUS-Operation (Details zu RLUS sind im Abschnitt 5.6.1 beschrieben) und den entsprechenden zu verwendenden Semantic Signifier (Details zu den Semantic Signifiern sind im Abschnitt 5.4.3 beschrieben) jeweils durch einen Doppelpunkt getrennt zusammengefasst.

- **Anfordern einer PID durch den Forschungs-Client-MDAT:** RLUS-List(Parameter): SemSigGetPID

Abbildung 6: Beispielhafte Darstellung einer RLUS-Operation

Auf Grundlage der Sicherheitsarchitektur der LE-Schnittstelle wird anschließend untersucht, inwieweit die Konzepte der Sicherheitsarchitektur der LE-Schnittstelle übernommen werden können bzw. angepasst werden müssen. Anpassungen werden dann vorgenommen, wenn die Konzepte der Sicherheitsarchitektur die Datenschutzanforderungen des ausgewählten Moduls eines Forschungsverbundes nicht erfüllen. Sollten Sicherheitskonzepte angepasst werden, so wird immer beschrieben, wie diese Anpassungen über die generischen Kommunikationsmuster umgesetzt werden können. Die Analyse bezieht sich auf die Vertrauens- und Kommunikationsbeziehungen, Authentifizierung und Sicherung der Kommunikation, die Autorisierung und die Verschlüsselung.

3.6. Vorgehen bei der Überprüfung durch die Reviewer

Die Überprüfung der Ergebnisse der Arbeit erfolgte durch einen Experten-Review. Hierzu wurden strukturierte Kommentierungsbögen erstellt. Diese Bögen sind in vier Themen untergliedert, wobei sich die ersten beiden Themen auf die Grundlagen für das Kommunikationsmodell beziehen und der dritte und vierte Bogen auf die Herleitung und die Umsetzung des Kommunikationsmodells.

1) Auswahl der Anwendungsfälle des Moduls eines Forschungsverbundes:

Während die Literatur den Aufbau, die Komponenten sowie die Anwendungsfälle eines Forschungsverbundes beschreibt, so gibt es keine Aussagen darüber, welche Anwendungsfälle des ausgewählten Moduls eines Forschungsverbundes für die Kommunikation mit einer ePA nach § 291a von Bedeutung sein könnten. Dies kann darauf zurückgeführt werden, dass die ePA nach § 291a momentan noch als theoretisches Konstrukt zu betrachten ist, über das selbst noch wenig publiziert wurde und eine Nutzung der Daten der ePA für die medizinische Forschung momentan nicht zulässig ist. Daher bezieht sich die erste Frage an die Reviewer auf die Auswahl der Anwendungsfälle des ausgewählten Moduls eines Forschungsverbundes.

Über die Forschungsschnittstelle sollen alle Kommunikationsvorgänge von Anwendungsfällen unterstützt werden, die auch einen Patientenbezug haben. Ein Anwendungsfall hat einen Patientenbezug, wenn der Patient bei diesem Anwendungsfall Informationen bekommt oder bereitstellt. Die Berücksichtigung aller Anwendungsfälle mit Patientenbezug ist insofern

wichtig, da aus diesen Anwendungsfällen Kommunikationsmuster und Anforderungen an die Forschungsschnittstelle, das ePA-System und das Forschungssystem abgeleitet werden. Sie stellen somit eine wichtige Grundlage der Arbeit da und sollten möglichst vollständig sein. Eine Auflistung aller Anwendungsfälle befindet sich in der Tabelle 21 im Anhang A1.4.

Anhand dieser Auflistung der Anwendungsfälle sollen die Reviewer die folgende Frage beantworten:

- Sind alle Anwendungsfälle des Versorgungsmoduls mit Patientenbezug für die Anbindung einer ePA nach § 291a berücksichtigt worden?

2) Umsetzung der Kommunikation der Anwendungsfälle des Moduls eines Forschungsverbundes:

Die Kommunikationsvorgänge der Anwendungsfälle des Moduls eines Forschungsverbundes dienen als Grundlage für die Herleitung des Kommunikationsmodells und die sich daraus an die einzelnen Systeme ergebenden Anforderungen. Daher ist die Richtigkeit der Kommunikation der Anwendungsfälle essentiell, um nicht aus einer falsch beschriebenen Kommunikation auch falsche Schlussfolgerungen für die Herleitung des Kommunikationsmodells zu ziehen. Die Datenschutzkonzepte der TMF empfehlen keine konkrete Kommunikation für jeden Anwendungsfall, sondern geben nur die Rahmenbedingungen vor. Daher kann die Umsetzung der einzelnen Anwendungsfälle in Bezug auf die Kommunikation unterschiedlich ausfallen, solange die beschriebenen Rahmenbedingungen in Bezug auf den Datenschutz berücksichtigt sind. Auch die überprüften Datenschutzkonzepte können hier nicht als Basis genommen werden, da zum einen nicht alle Kommunikationen der Anwendungsfälle im Detail beschrieben wurden und zum anderen nur 3 der 16 Datenschutzkonzepte öffentlich zugänglich sind. Daher werden für jeden ausgewählten Anwendungsfall folgende Fragen an die Reviewer gestellt:

- Sind bei der Beschreibung der Kommunikation der ausgewählten Anwendungsfälle alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?
- Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten Informationen aufgeführt?

3) Herleitung der Kommunikationsmuster für das Kommunikationsmodell sowie die Ableitung der Anforderungen an die Systeme:

Die Kommunikationsmuster werden aufgrund des in der Analyse herausgestellten Informationsaustausches zwischen dem Patienten und dem Hauptakteur hergeleitet. Ziel ist es immer, eine möglichst direkte Kommunikation zwischen dem Patienten und dem Hauptakteur umzusetzen. Die Kommunikation einiger der Anwendungsfälle wird allerdings aufgrund spezieller Datenschutzanforderungen nicht direkt umgesetzt. Zum Beispiel kann der Verwalter der Versorgungsdatenbank den Patienten nicht direkt kontaktieren, da der Verwalter die identifizierenden Daten des Patienten nicht kennen darf. Diese speziellen Anforderungen aus den Anwendungsfällen müssen identifiziert werden und ggf. durch Anforderungen an das ePA-, das Forschungssystem oder die Forschungsschnittstelle abgedeckt werden. Die Reviewer sollen überprüfen, ob alle wichtigen Datenschutzanforderungen berücksichtigt worden sind und ob diese Datenschutzanforderungen durch neue Anforderungen an das ePA-System, das Forschungssystem oder die Forschungs-

schnittstelle vollständig abgedeckt sind. Entsprechend werden den Reviewern für jeden Anwendungsfall folgende Fragen gestellt:

- Wurden alle Datenschutzanforderungen, die sich aus dem Kontext der Anwendungsfälle ergeben, identifiziert?
- Werden die identifizierten Datenschutzanforderungen aus dem Kontext der Anwendungsfälle durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

4) Umsetzung der Datenschutzanforderungen des Versorgungsmoduls durch das Kommunikationsmodell:

Im Kapitel 7 soll aufzeigt werden, dass die generischen Kommunikationsmuster des Kommunikationsmodells unter Berücksichtigung der herausgearbeiteten Datenschutzanforderungen über eine Erweiterung der Infrastruktur des ePA-Systems umgesetzt werden können. Hierbei sollen nicht nur die während der Analyse herausgestellten Anforderungen berücksichtigt werden, sondern auch die grundlegenden Datenschutzanforderungen, die an den Betrieb eines Versorgungsmoduls gestellt werden (siehe Abschnitt 7.1 „Datenschutzanforderungen an die Forschungsschnittstelle“). Wichtig ist hierbei, dass die Datenschutzanforderungen vollständig erfasst wurden. Während durch den oberen Kommentierungsbogen schon die speziellen Datenschutzanforderungen aus den Anwendungsfällen überprüft worden sind, soll hier zunächst die Vollständigkeit der grundlegenden Datenschutzanforderungen an den Betrieb eines Versorgungsmoduls überprüft werden. Diese Anforderungen werden zwar indirekt in den Datenschutzkonzepten der TMF genannt, allerdings gibt es keine explizite Auflistung dieser Anforderungen, so dass die Vollständigkeit der grundlegenden Datenschutzanforderungen durch entsprechende Literaturverweise schwer belegt werden kann. Aus diesem Grund wird folgende Frage an die Reviewer gestellt:

- Sind die Anforderungen an einen datenschutzkonformen Betrieb des Versorgungsmoduls vollständig aufgeführt?

Anschließend werden aus den Datenschutzanforderungen die Architekturentscheidungen abgeleitet und beschrieben, wie die generischen Kommunikationsmuster über diese Architektur umgesetzt werden können. Hierbei besteht der Anspruch, dass während jeder Kommunikation die herausgestellten Datenschutzanforderungen eingehalten werden. Ein Nachweis soll durch die Reviewer erfolgen, in dem sie die folgende Frage beantworten:

- Sind bei der Beschreibung der Umsetzung der generischen Kommunikationsmuster des Kommunikationsmodells über eine Erweiterung der Infrastruktur des ePA-Systems alle herausgearbeiteten Datenschutzanforderungen berücksichtigt worden?

Der gesamte Fragebogen befindet sich im Anhang A6.1. Die Ergebnisse des Reviews wurden ausgewertet und bei Anmerkungen der Reviewer werden diese Anmerkungen an entsprechender Stelle in die Arbeit eingearbeitet. Eine Tabelle mit den Ergebnissen des Reviews und den Verweisen auf die Einarbeitung in der Kapitel der Arbeit befindet sich im Anhang A6.2.

3.7. Literaturrecherche

Sowohl für den aktuellen Stand der Forschung im Bereich der Nutzung von Versorgungsdaten für die medizinische Forschung (siehe Kapitel 2), als auch für die Beschreibung des Forschungs- (siehe Kapitel 4) und des ePA-Systems (siehe Kapitel 5) wurde eine Literaturrecherche durchgeführt.

3.7.1. Aktueller Stand der Forschung zur Nutzung von Versorgungsdaten

Durch diese Literaturrecherche wurde der aktuelle Stand der Forschung zur Nutzung von Versorgungsdaten für die Forschung analysiert und der aktuelle Stand zur gematik-Infrastruktur und eGK recherchiert. Für die Literaturrecherche wurden Pubmed [145], Google Scholar [146] und besonders für die nationalen Themen (elektronische Gesundheitskarte und Telematikinfrastruktur) Springerlink [147] verwendet. Die Suchbegriffe wurden in vier Kategorien unterteilt: Versorgungsystem und ePA-System, Forschungssystem, Secondary Use, Elektronische Gesundheitskarte und Telematikinfrastruktur. Während die ersten drei Kategorien nur englische Begriffe enthalten und für Pubmed und Google Scholar verwendet wurden, enthält die vierte Kategorie nur deutsche Begriffe und wurde für Springerlink und Google Scholar verwendet. Für Pubmed wurden MeSH[9] (Medical Subject Headings) Terms verwendet, sofern diese Terms vorhanden und präzise genug formuliert waren. Eine Übersicht aller Suchbegriffe befindet sich in der Tabelle 18 im Anhang A1.2.

3.7.2. Aufbau eines Forschungssystems

Die Analyse des Forschungssystems bezieht sich auf Forschungsverbünde, die sich an den Vorgaben der generischen Datenschutzkonzepte der TMF orientieren. Um den Aufbau eines medizinischen Forschungsverbundes zu beschreiben, wurden die generischen Datenschutzkonzepte der TMF sowie konkrete Datenschutzkonzepte von medizinischen Forschungsverbünden analysiert. Details zur Analyse sind im Abschnitt 3.1 beschrieben. An dieser Stelle wird nochmal darauf hingewiesen, dass der Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - noch in der Überarbeitung ist. In dieser Arbeit wurde mit der Version 0.11a gearbeitet. Auch wenn keine prinzipiellen Änderungen mehr erwartet werden, so kann es noch Anpassungen an den Begrifflichkeiten (der Module, Pseudonyme etc.) geben, die dann von denen in der Arbeit abweichen.

3.7.3. Aufbau des ePA-Systems

Die Ergebnisse zu Kapitel 5 werden durch eine Literaturrecherche der Spezifikationen des FuE-ePA-Projektes gewonnen. Ziel der Literaturrecherche ist es, eine Übersicht aller Anforderungen aus den Spezifikationen des FuE-ePA-Projektes zu erlangen, um deren Relevanz für die Forschungsschnittstelle bewerten zu können und die relevanten Anforderungen bei der Konzeption der Forschungsschnittstelle zu berücksichtigen.

Da das Projekt zum Zeitpunkt der Erstellung dieser Arbeit noch nicht abgeschlossen war, wurde der Stand der Spezifikationen vom 18.12.2011 für die Literaturrecherche genommen. Das Projekt ist in sechs Arbeitspakete aufgeteilt, in denen mehrere Dokumente entstanden sind. Diese Dokumente wurden in folgende drei Klassen unterteilt:

[9] Ist ein Vokabular Thesaurus zum Indexieren von Artikel in Pubmed.

- **Grundlagen und Analyse:** Dies sind Dokumente, die als Grundlage für die Spezifikationen der ePA zu sehen sind. Auf diese Dokumente wird in der Arbeit nicht direkt eingegangen, da die wichtigen Ergebnisse dieser Dokumente direkt oder indirekt in die Spezifikationen eingegangen sind. Diese Dokumente werden teilweise herausgezogen, wenn bestimmte Details, die für diese Arbeit wichtig sind, nicht in der Spezifikation, sondern in den Grundlagen erklärt werden.
- **Spezifikation:** Sind Dokumente, die das Verhalten der ePA bzw. der LE-Schnittstelle und die Kommunikation zwischen der ePA und den Leistungserbringersystemen spezifizieren. Diese Dokumente sind eine wichtige Grundlage für die Konzeption und Spezifikation der Forschungsschnittstelle. Daher werden diese Dokumente im Detail betrachtet. Die Ergebnisse dieser Analyse sind im Kapitel 5 zusammengefasst. Die Spezifikationen werden als Projektergebnis veröffentlicht und sind dann neben anderen Dokumenten aus diesem Projekt auf der Webseite des Projektes (www.epa291a.de) frei zugänglich. Auf die Dokumente für die Anbindung der Forschung wird hier nicht eingegangen, da diese Ergebnisse dieser Arbeit sind und daher nicht analysiert werden müssen.
- **Prototyp:** Dies sind Dokumente, die die Implementierung spezieller Szenarien für den Prototyp beschreiben. Auf diese Dokumente wird nicht eingegangen, da es sich hier um die Anwendung der Spezifikationen handelt und somit keine neuen Erkenntnisse für die Konzeption der Forschungsschnittstelle gewonnen werden können.
- **Veröffentlichungen:** Sind Dokumente, die zum Zeitpunkt der Literaturrecherche öffentlich zugänglich sind. Diese Dokumente werden bevorzugt verwendet, da sie final sind und somit am besten zitiert werden können. Diese Dokumente sind allerdings eher allgemein gehalten und überschaubar, so dass sie die Spezifikationen nicht ersetzen, sondern nur ergänzen können.
- **Projektinterne Dokumente:** Sind Dokumente, die nicht veröffentlicht werden sollen. Auf diese Dokumente wird nicht eingegangen, da sie nicht veröffentlicht werden sollen und somit Aussagen daraus nicht verifiziert werden können.

Eine Übersicht aller Spezifikationen ist im Anhang A1.5 zu finden.

3.8. Zusammenhang zwischen dem FuE-ePA-Projekt und der Dissertation

Neben den oben genannten Spezifikationen zur LE-Schnittstelle fließen auch die Ergebnisse dieser Arbeit im Rahmen von Spezifikationen der Forschungsschnittstelle bzw. Dokumenten zum Thema Grundlagen und Analyse in das FuE-ePA-Projekt mit ein. Eine Auflistung dieser Dokumente und der Zusammenhang mit den Kapiteln dieser Arbeit ist in der Tabelle 23 im Anhang A1.6 zu finden. Hierbei können sich die Inhalte der Dokumente leicht von denen der Arbeit unterscheiden, da sich die Arbeit nur auf das Versorgungsmodul konzentriert und das Versorgungsmodul im Detail untersucht. Die Arbeiten im Projekt konzentrieren sich auf die Anbindung des Nationales Register für angeborene Herzfehler [148]. Das Kommunikationsmodell sowie die Fach- und die Sicherheitsarchitektur sind auf beide Bereiche anwendbar.

Bevor die Spezifikationen des FuE-ePA-Projektes für die Forschungsschnittstelle veröffentlich werden, durchlaufen sie einen Reviewing-Prozess. Hierzu wird die Spezifikation an die Projektpartner zur Kommentierung geschickt. Kommentare werden eingearbeitet und nochmals mit den Projektpartnern abgestimmt. Das Dokument wird vom BMG geprüft und für

die Veröffentlichung freigegeben. Nach der Freigabe wird das Dokument auf der Webseite des Projektes (www.epa291a.de) veröffentlicht.

Auch an dieser Stelle wird nochmal darauf hingewiesen, dass nicht alle Spezifikationen in der endgültigen Version vorlagen und es noch kleine Änderungen z. B. an den Begrifflichkeiten geben kann. Inhaltlich sind keine prinzipiellen Änderungen mehr zu erwarten. Es wird im Literaturverzeichnis vermerkt, mit welcher Version der einzelnen Spezifikationen gearbeitet wurde.

3.9. Prototyp Entwicklung

Auch wenn es nicht Ziel dieser Arbeit ist, die hier entwickelten Konzepte zu implementieren, so wurden Teile der Forschungsschnittstelle innerhalb des FuE-ePA-Projektes sowie durch studentische Arbeiten umgesetzt. Im Rahmen des FuE-ePA-Projektes wurden die grundlegenden Komponenten und die Pseudonymisierung implementiert. Diese Implementierung wurde im Rahmen eines Praktikums getestet. Im Rahmen einer Bachelorarbeit wurde der Prototyp der Forschungsschnittstelle um die Autorisierung erweitert. Damit konnte gezeigt werden, dass das Konzept zur Abbildung von Autorisierungsregeln auf der Grundlage von Patienteneinwilligung (siehe Abschnitt 9.4) über den Prototypen umsetzbar ist. Ebenfalls wird die angepasste Form des Verschlüsselungskonzeptes im Abschnitt 9.5 gerade im Rahmen einer Projektarbeit umgesetzt.

4. Module und Anwendungsfälle eines medizinischen Forschungsverbundes

Ziel dieses Kapitels ist es, das Forschungssystem genauer zu spezifizieren, indem die IT-Komponenten eines medizinischen Forschungsverbundes und deren Anwendungsfälle vorgestellt werden und eine Auswahl der weiter zu betrachtenden Komponenten getroffen wird. Hierzu wurde eine Analyse der generischen Datenschutzkonzepte der TMF sowie von Datenschutzkonzepten bestehender Forschungsverbünde durchgeführt

Am Ende dieses Kapitels sind die relevanten Module und deren Anwendungsfälle eines Forschungsverbundes in Bezug auf eine Eignung zur Anbindung an eine ePA bewertet und ausgewählt worden. Auf Grundlage dieses Ergebnisses wird dann im Kapitel 6 die Anbindung der ausgewählten Module an eine ePA unter Berücksichtigung der Umsetzbarkeit der Anwendungsfälle beschrieben.

4.1. Zusammenfassung der Ergebnisse der Analyse

Es wurde die generischen Datenschutzkonzepte Version 1 [33] und 2 [34] der TMF analysiert. Das erste Konzept hat das Modell A und B beschrieben. Diese Konzepte wurden in der zweiten Version zum Versorgungsmodul (Modell A) bzw. zum Forschungsmodul (Modell B) umbenannt. Neu hinzugekommen sind im zweiten Konzept auch das Studienmodul sowie das Biobankenmodul, wobei beim Biobankenmodul nur eine Übersicht gegeben wird und größtenteils auf das hierfür gesonderte publizierte Datenschutzkonzept für Biobanken [149] verwiesen wird. Im weiteren Verlauf werden die Module eines medizinischen Forschungsverbundes wie sie in Abbildung 7 dargestellt und in der zweiten Version der TMF Datenschutzkonzepte beschrieben sind betrachtet. Insgesamt besteht ein medizinischer Forschungsverbund aus fünf Modulen (Versorgungs-, Studien-, Forschungs- Biobankenmodul und dem Identitätsmanagement). Das Biobankenmodul wurde dabei nicht weiter betrachtet (siehe auch Abgrenzung). Die anderen Module können je nach Anwendungszweck als Register oder Bilddatenbank realisiert werden.

Für die vier Module (Versorgungs-, Studien-, Forschungsmodul und Identitätsmanagement) wurden in der 1. und 2. Version der generischen Datenschutzkonzepte sowie der Analyse der Datenschutzkonzepte bestehender Forschungsverbünde insgesamt 39 Anwendungsfälle identifiziert (10 Identitätsmanagement, 13 Versorgungsmodul, 8 Studienmodul, 8 Forschungsmodul), von denen 23 Anwendungsfälle einen Patientenbezug hatten (5 Identitätsmanagement, 8 Versorgungsmodul, 6 Studienmodul, 4 Forschungsmodul) (siehe auch Tabelle 21 im Anhang A1.4).

Bei der Analyse der Datenschutzkonzepte bestehender Forschungsverbünde wurden insgesamt 38 Datenschutzkonzepte von Forschungsverbünden vorgestellt. Von sechzehn Forschungsverbünden lag ein befürwortetes Datenschutzkonzept vor. (siehe auch Tabelle 19 und Tabelle 20 im Anhang A1.3).

4.2. Übersicht der Module eines medizinischen Forschungsverbundes

Der Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - sieht vier eigenständige Module vor, die man beliebig miteinander kombinieren kann. Das sind das Versorgungs-, das Studien-, Forschungs- und das Biobank-Modul, die immer eine oder mehrere Datenbanken enthalten (siehe Abbildung 7). Das Identitätsmanagement hat die Aufgabe, die Identitäten des Patienten bzw. Probanden und ggf. seiner Proben über alle Module zusammenzuführen (siehe Abbildung 7). Daher ist es nicht als ein eigenständiges Modul zu sehen und wird immer in Kombination mit einem oder mehreren Modulen betrieben. Es gibt Module (z. B. das Studienmodul), die in einigen Einsatzszenarien auch einen Betrieb ohne ein zentrales Identitätsmanagement vorsehen [34]. Diese Szenarien werden aus Komplexitätsgründen nicht betrachtet und somit wird bei der weiteren Analyse vorausgesetzt, dass jedes Modul mit einem zentralen Identitätsmanagement betrieben wird. Es wird auch nur das jeweilige Modul mit dem Identitätsmanagement betrachtet. Eine Kombination und ein Austausch zwischen den Modulen werden nicht betrachtet.

Da die Arbeit nur Phänotypdaten berücksichtig, wird das Biobank Modul nicht analysiert. Im Leitfaden wurde herausgestellt, dass Bilddatenbanken und Register durch eine Studiendatenbank, eine Versorgungsdatenbank oder eine Forschungsdatenbank umgesetzt werden können. Aus diesem Grund werden sie auch nicht gesondert analysiert. Auch wenn die eben genannten IT-Komponenten nicht in Bezug auf ihre Anwendungsfälle analysiert werden, wird deren Funktionalität kurz beschrieben, um das Gesamtbild eines medizinischen Forschungsverbundes zu vermitteln.

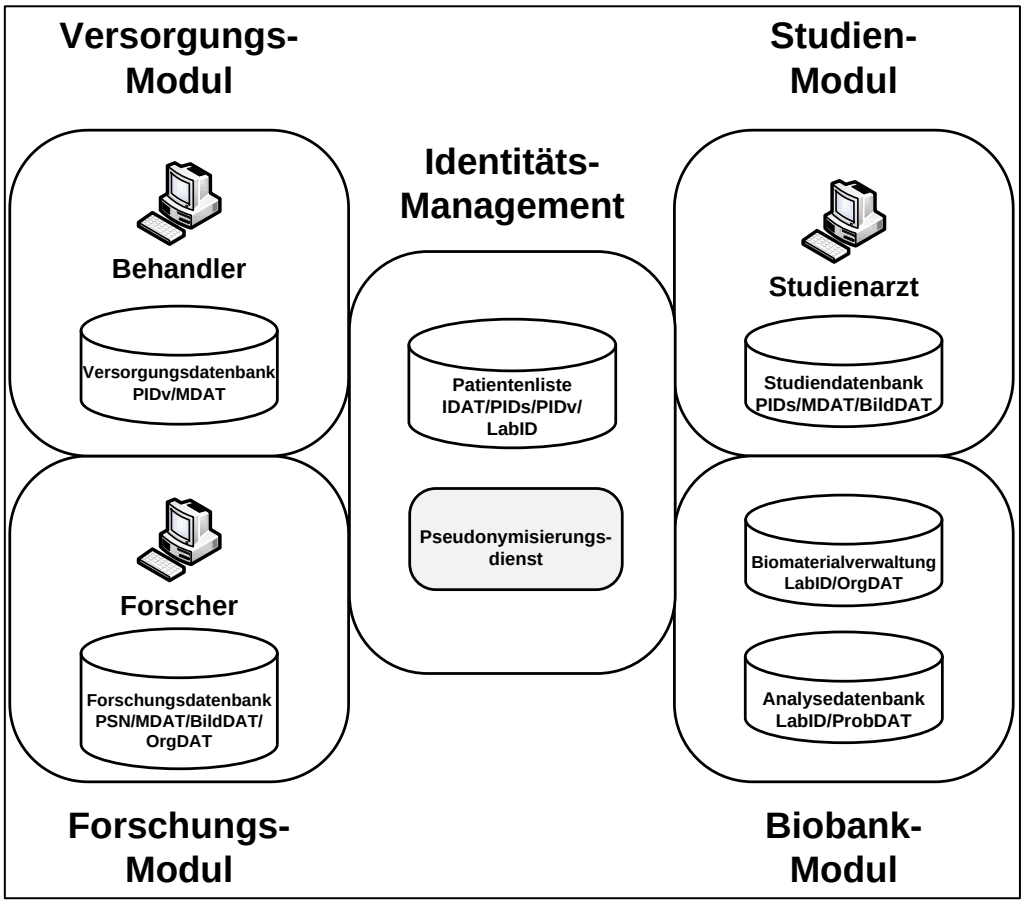

Abbildung 7: Übersicht aller Module eines medizinischen Forschungsverbundes (angelehnt an Abb. in [34] auf Seite 68)

4.2.1. Identitätsmanagement

Das Identitätsmanagement hat zum Ziel, die medizinischen Daten eines Patienten in den einzelnen IT-Komponenten eines Forschungsverbundes korrekt zuzuordnen und dabei die Identität dieses Patienten vor Unberechtigten zu verbergen. Das Identitätsmanagement eines Forschungsverbundes besteht aus einer (zentralen) Patientenliste. Ist eine Langzeitaufbewahrung der Daten in einer Forschungsdatenbank vorgesehen, so wird das Identitätsmanagement durch einen Pseudonymisierungsdienst erweitert [34]. Im Folgenden erfolgt eine Beschreibung der beiden Komponenten:

Die **Patientenliste** ermöglicht die Registrierung eines Patienten im Forschungsverbund. Sie speichert die Identitätsdaten (IDAT) dieser Person und vergibt einen eindeutigen netzübergreifenden Patientenidentifikator (PID). Die Patientenliste ermöglicht zusätzlich die Verwaltung und Zuordnung des PID zu den einzelnen Pseudonymen (z. B. dem Subject Identification Code - SIC -, die ID zur Identifizierung von Proben - LabID -, Patientenidentifikator des Studienmoduls - PIDs -) des Patienten in den unterschiedlichen Projekten und Systemen (Studiendatenbank, Versorgungsdatenbank und ggf. Biomaterialverwaltung). Somit können die pseudonymisierten Daten eines Patienten unabhängig vom Zeitpunkt, von der Einrichtung und vom System immer eindeutig dem Patienten zugeordnet werden und ggf. projektübergreifend zusammengeführt werden. Dieses Verfahren ermöglicht es, Patienten mit chronischen oder langwierigen Erkrankungen über einen längeren Zeitraum von unterschiedlichen Einrichtungen in unterschiedlichen Forschungsprojekten zu behandeln und zu beobachten [34].

Der **Pseudonymisierungsdienst** ist ein Instrument zur Übertragung von medizinischen Forschungsdaten in eine nachhaltige, netzweite Forschungsdatenbank. Der Pseudonymisierungsdienst kommt zum Einsatz, um das Pseudonym des Patienten (PID) in ein Pseudonym der zweiten Stufe (PSN) zu transformieren und die Daten dann unter dem PSN in der Forschungsdatenbank abzulegen. Das PSN wird durch eine symmetrische Verschlüsselung erzeugt. Der Schlüssel ist nur dem Pseudonymisierungsdienst bekannt (z. B. ein symmetrischer Schlüssel auf einer SmartCard). Dadurch, dass nur der Pseudonymisierungsdienst Zugriff auf den symmetrischen Schlüssel hat, kann auch nur er das PSN wieder in eine PID transformieren. Dieses Verfahren hat den Vorteil, dass die Daten des Patienten mit einem neuen Pseudonym versehen sind (dem PSN), das an keiner Stelle mit den identifizierenden Daten des Patienten abgelegt wurde und trotzdem durch den Einsatz einer weiteren Vertrauensstelle in vorher definierten Anwendungsfällen (z. B. der Rekrutierung oder dem Informieren eines Patienten über Forschungsergebnisse siehe Anhang A2.2) die Identität des Patienten aufgelöst werden und der Patient kontaktiert werden kann [33,34].

Während der Analyse der Datenschutzkonzepte der medizinischen Forschungsverbünde, stellte sich heraus, dass elf der sechzehn Forschungsverbünde eine Patientenliste eingesetzt haben. Drei haben einen zentralen Pseudonymisierung-Service eingesetzt, der nur ein Pseudonym erzeugt und an die Zentren zurückgibt, aber keine identifizierenden Daten des Patienten speichert. Zwei der analysierten Forschungsverbünde haben kein zentrales Identitätsmanagement im Einsatz und führen eine dezentrale Pseudonymisierung durch. Auf die Funktionen der Patientenliste konnte teilweise direkt aus den teilnehmenden Zentren zugegriffen werden. In einigen Fällen wurde sie auch in der Studienzentrale oder bei einem Treuhänder als eine lokale Datenbank gehalten und die Anmeldungen des Patienten wurden papierbasiert an die Studienzentrale oder den Treuhänder geschickt.

Für den weiteren Verlauf der Arbeit wird eine aus den teilnehmenden Zentren direkt zugreifbare Patientenliste vorausgesetzt, die die oben beschriebenen Eigenschaften besitzt. Sie soll in der Lage sein, die identifizierenden Daten und mehrere Pseudonyme eines Patienten aus unterschiedlichen Systemen bzw. Forschungsprojekten zu verwalten (VF00).

Die Patientenliste kann auch zusätzliche Funktionen haben wie z. B. das Erstellen von Serienbriefen zwecks Kontaktierung der Patienten oder das Verwalten von Einwilligungserklärungen. Bei der Betrachtung der Anwendungsfälle und im weiteren Verlauf der Arbeit wird davon ausgegangen, dass diese Funktionen durch die Patientenliste für bestimmte Anwendungsfälle umgesetzt werden (z. B. beim Kontaktieren eines Patienten) (VF01).

Die Analyse der Forschungsverbünde ergab, dass sieben der sechzehn medizinischen Forschungsverbünde einen Pseudonymisierungsdienst vorsehen. In sechs der Fälle wurde der Pseudonymisierungsdienst in Verbindung mit einer Forschungsdatenbank verwendet. In einem Fall wurde er als zusätzliche Sicherheitsmaßnahme in Verbindung mit einem Versorgungsmodul verwendet. Der Einsatz des Pseudonymisierungsdienstes wird im weiteren Verlauf der Arbeit nur in Verbindung mit einer Forschungsdatenbank betrachtet.

Insgesamt wurden bei der Analyse des Identitätsmanagements zehn Anwendungsfälle identifiziert, von denen fünf einen Patientenbezug haben Eine Beschreibung dieser fünf Anwendungsfälle ist im Anhang A2.3 zu finden.

4.2.2. Studienmodul

Das Studienmodul enthält eine oder mehrere Studiendatenbanken. Eine **Studiendatenbank** ermöglicht die Durchführung von Forschungsvorhaben mit einer klar definierten Fragestellung und einem festgelegten Zeitraum. Eine Studiendatenbank kann Daten einer oder mehrerer, auch multizentrischer, klinischer Studien oder epidemiologischer Studien zentral sammeln und verwalten.

Sie enthält pseudonymisierte bzw. anonymisierte, (meist) strukturierte medizinische Informationen zu einem Patienten, die zu mehreren Zeitpunkten (Visiten) erfasst werden können. Das Pseudonym des Patienten (PIDs oder SIC[10]) kann entweder dezentral oder in den Zentren erstellt werden. Im Rahmen dieser Arbeit wird davon ausgegangen, dass es eine zentrale Patientenliste gibt, die die Pseudonyme für die Studiendatenbank erzeugt und verwaltet.

Dank der pseudonymisierten Datenhaltung ist ein Zugriff auf die Daten der Studiendatenbank (z. B. zur wissenschaftlichen Auswertung durch einen Biometriker) für Personen ohne Behandlungszusammenhang möglich. Der **Studienarzt** hat in der Studiendatenbank nur Zugriff auf die Daten der Patienten, die er eingetragen hat. Ihm sind auch nur die Zuordnungen zu den Pseudonymen seiner eingetragenen Patienten bekannt [34,150].

Die Analyse der Forschungsverbünde ergab, dass fünf der sechzehn medizinischen Forschungsverbünde eine Studiendatenbank vorsehen.

[10] Der SIC wird verwendet, wenn ein Studienteilnehmer in jeder einzelnen Studie mit einem unterschiedlichen Pseudonym geführt werden soll. Der PIDs wird eingesetzt, wenn ein Studienteilnehmer in allen Studien des Studienmoduls unter dem gleichen Pseudonym geführt werden soll.

Insgesamt wurden acht Anwendungsfälle für eine Studiendatenbank beschrieben, von denen sechs einen Patientenbezug haben. Eine Beschreibung der Anwendungsfälle befindet sich im Anhang A2.1.

4.2.3. Versorgungsmodul

Das Versorgungsmodul kapselt immer eine oder mehrere Versorgungsdatenbanken. Das Ziel einer **Versorgungsdatenbank** ist es, strukturiert medizinische Daten zu einem Patienten zu erfassen, die sowohl in der Behandlung als auch für Forschungszwecke verwendet werden können. Im Gegensatz zu einer Studiendatenbank muss bei der Versorgungsdatenbank keine explizit formulierte klinische Forschungsfrage im Vordergrund stehen. Mit der Versorgungsdatenbank werden beispielweise Beobachtungsstudien, die Dokumentation von Heilversuchen oder gesundheitsökonomische Studien realisiert.

In der Versorgungsdatenbank werden ausschließlich pseudonymisierte Daten gespeichert. Die zugehörigen identifizierenden Daten werden in einer separat geführten Patientenliste gehalten. Ein behandelnder **Arzt** hat nur Zugriff auf die Daten der Patienten, die bei ihm in Behandlung sind. Da dieser Zugriff mit identifizierenden Daten des Patienten erfolgen darf und sollte, werden die medizinischen Daten aus der Versorgungsdatenbank und die identifizierenden Daten aus der Patientenliste separat abgerufen und beim Arzt zusammengeführt. Das Abrufen und Zusammenführen der Daten erfolgt über ein temporäres Zugriffticket (TKT). Das Pseudonym des Patienten (PIDv = Pseudonym für Versorgungsdatenbank) bleibt dem Behandelnden verborgen. Für wissenschaftliche Auswertungen erfolgt ein pseudonymisierter bzw. anonymisierter Export aus der Versorgungsdatenbank. Da der PIDv aus Datenschutzgründen nicht offenbart werden darf, wird er weder beim pseudonymen Export noch für Studien verwendet. Für den Export wird ein neues Einmal-Pseudonym (EX-PIDs) generiert, und in einer Zuordnungsliste zu dem PIDv der Patienten gespeichert [33,34].

Die Analyse der Forschungsverbünde ergab, dass acht der sechzehn medizinischen Forschungsverbünde eine Versorgungsdatenbank vorsehen.

Es wurden dreizehn Anwendungsfälle des Versorgungsmoduls identifiziert, von denen acht Anwendungsfälle einen Patientenbezug haben. Eine detaillierte Beschreibung der Anwendungsfälle befindet sich im Anhang A2.4.

4.2.4. Forschungsmodul

Das Forschungsmodul kann aus einer oder mehreren Forschungsdatenbanken bestehen. Die **Forschungsdatenbank** „..dient dazu, medizinische Daten hoher Qualität langfristig, auch für zukünftige Forschungsprojekte, zur Verfügung zu stellen. *Daraus ergibt sich, dass, im Unterschied zu dem Studienmodul,"…"der Verwendungszweck sowie die Lebensdauer der Daten nicht explizit angegeben werden können. Die Einsatzmöglichkeiten eines Forschungsmoduls sind sehr weit gefasst. Das können gesundheitsökonomische oder epidemiologische Studien sein, aber auch die Ermittlung von Fallzahlen bzw. von Patienten für klinische Studien kann ermöglicht werden. Im Gegensatz zu dem Versorgungsmodul ist ein unmittelbarer Behandlungsbezug der gespeicherten Daten nicht notwendigerweise gegeben. Mit Hilfe eines Forschungsmoduls können große Kollektive abgebildet werden, die über einen längeren Zeitraum beobachtet werden, ohne dass die Vertraulichkeit der Information angetastet wird. Eine direkte Verknüpfung der Identitätsdaten mit den medizinischen Daten einer Forschungsdatenbank ist generell ausgeschlossen, da kein zur*

unmittelbaren Identifikation eines Patienten führendes Merkmal - wie z. B. der PID des Versorgungsmoduls - als Ordnungskriterium in einer Forschungsdatenbank geführt wird. Das Forschungsmodul kann medizinische Daten zu einem Patienten aus mehreren Studien oder Systemen verwalten und bietet Forschern somit einen Datenpool, der sich zur Generierung neuer Fragestellungen oder für Sekundärauswertungen eignet“ [34, Seiten 53-54].

Die Analyse der Forschungsverbünde ergab, dass sechs der sechzehn medizinischen Forschungsverbünde eine Forschungsdatenbank vorsehen.

Insgesamt wurden acht Anwendungsfälle für eine Forschungsdatenbank beschrieben, von denen vier einen Patientenbezug haben. Eine Beschreibung der vier Anwendungsfälle befindet sich im Anhang A2.2.

4.2.5. Biobankmodul

Das Biobankmodul wird in medizinischen Forschungsverbünden in der Regel durch zwei voneinander getrennte Datenbanken realisiert. Diese beiden Datenbanken sind die Biomaterialverwaltung bzw. Probenbank und die Analysedatenbank.

In der **Biomaterialverwaltung** werden die einzelnen Proben der an einer Studie oder einem Forschungsvorhaben teilnehmenden Patienten verwaltet. Neben dem Lagerort werden hier auch Informationen zu den Biomaterialien selbst hinterlegt (OrgDAT). Jede Probe wird mit einem Pseudonym versehen, der sogenannten LabID (ID zur Identifizierung von Proben). Diese LabID entspricht aus Datenschutzgründen nicht dem Pseudonym des Patienten, was dazu führt, dass an geeigneter Stelle (z. B. in den Studienzentren oder in der Patientenliste) eine Zuordnung von diesen beiden Pseudonymen stattfinden muss. Die LabID kann entweder dezentral von den Studienzentren oder zentral von Patientenliste erzeugt und vergeben werden.

Die **Analysedatenbank** enthält Ergebnisse zu Auswertungen einzelner Proben (ProbDAT), die aus Datenschutzgründen in einer gesonderten Datenbank gehalten werden müssen. Die Auswertungen einer Probe werden mit deren LabID abgelegt, so dass man hier eine Beziehung zwischen Auswertung und Probe erhält [149,151].

Wie schon in der Abgrenzung erwähnt, wird das Thema Biomaterialbank aus Komplexitätsgründen nicht betrachtet und wurde hier nur aus Gründen der Verständigkeit im Sinne einer Definition und Abgrenzung zu den anderen Modulen mit aufgeführt.

Im Rahmen der Analyse der Forschungsverbünde wurde das Thema Biomaterialbank nicht berücksichtigt.

4.3. Unterschiedliche Einsatzmöglichkeiten der Module

Im Folgenden wird auf die unterschiedlichen Einsatzmöglichkeiten der Module eingegangen.

4.3.1. Register

Ein medizinisches Register ist eine standardisierte Dokumentation von Patienten zu einer grob definierten und erweiterbaren Fragestellung. Bis auf Ausnahmefälle ist es notwendig, die erhobenen Daten eines Registers in einen Bezug zur Quellpopulation setzen zu können. Register können zu folgenden Zwecken eingesetzt werden [152]:

- Beschreibung epidemiologischer Zusammenhänge und Unterschiede
- Unterstützung von Qualitätssicherung und -verbesserung
- Unterstützung klinischer Forschung
- Evaluation und Monitoring der Patientensicherheit
- Evaluierung der Wirksamkeit in der Versorgungsroutine
- Ökonomische Evaluation
- Mindestmengenforschung
- Unterstützung der Versorgungsplanung

Die Analyse der medizinischen Forschungsverbünde ergab, dass zehn der sechzehn Verbünde ein Register betreiben. Die Umsetzung des Registers wurde je nach Anwendungszweck über eine Studien-, Versorgungs-, oder Forschungsdatenbank realisiert. Aus diesem Grund werden Register in diesem Dokument nicht als gesonderte Komponente bzw. gesondertes Modul betrachtet.

4.3.2. Bilddatenbank

Eine **Bilddatenbank** hält pseudonymisierte Bilder zu den einzelnen Patienten eines Forschungsverbundes vor. Diese Bilder werden meistens im Rahmen von Studien erhoben und an zentralen Stellen ausgewertet, um hier eine möglichst einheitliche Auswertung zu gewährleisten. Auf Grund der besonderen Anforderungen an die Bildübertragung und Verarbeitung werden die Bilder meistens in einer speziell dafür aufgebauten Bilddatenbank abgelegt. Die Bilder können unter dem Pseudonym des Patienten geführt werden oder bekommen ein eigenes Pseudonym. Bekommen die Bilder ein eigenes Pseudonym, so muss dieses Pseudonym in einer medizinischen Datenbank oder in der Patientenliste dem Pseudonym des Patienten zugeordnet werden [34,150].

In den analysierten Forschungsverbünden wurden Bilder sowohl über eine zentrale Bilddatenbank verwaltet als auch in den einzelnen Versorgungs-, Studien- bzw. Forschungsdatenbanken.

Die Bilddatenbank wird in dieser Arbeit nicht gesondert betrachtet, da sie je nach Anwendungsbereich wie eine Versorgungsdatenbank, Studiendatenbank oder Forschungsdatenbank betrieben wird bzw. die Bilder Teil einer solchen Datenbank sind.

4.4. Bewertung der IT-Komponenten und Definition des Forschungssystems

Die Patientenliste bildet immer mit einer oder mehreren Versorgungsdatenbanken, Studiendatenbanken oder Forschungsdatenbanken ein Versorgungs-, Studien-, bzw. Forschungsmodul. Daher muss sie weiter in der Arbeit betrachtet werden. Im Folgenden findet eine Bewertung und anschließende Auswahl einer der drei medizinischen Datenbanken statt, die dann mit der Patientenliste in Bezug auf ihre Kommunikation im Kapitel 6 analysiert werden soll.

4.4.1. Auswahl der IT-Komponenten

Die Priorisierung der Komponenten nach dem im Abschnitt 3.1.3 beschriebenen Vorgehen und den vier Auswahlkriterien:

- Häufigkeit des Einsatzes
- Anzahl der Anwendungsfälle mit Patientenbezug
- Anwendungsfälle mit Austausch zwischen Forschung und Versorgung
- Anwendungsfälle mit Selbstdokumentation

hat ergeben, dass die Studiendatenbank insgesamt 13 Punkte erhalten hat, das Versorgungsmodul insgesamt 18 und das Forschungsmodul insgesamt 10 Punkte erhalten hat (siehe Tabelle 7). Somit hat das Versorgungsmodul mit 18 Punkten die höchste Priorität in Bezug auf die Auswahlkriterien und wird im weiteren Verlauf der Arbeit genauer als Forschungssystem betrachtet. Die Details zur Priorisierung der Module befinden sich im Anhang A2.5.

Auswahlkriterien	**Studiendaten-bank**	**Versorgungs-modul**	**Forschungs-datenbank**
Häufigkeit des Einsatzes	5	8	6
Anzahl der Anwendungsfälle mit Patientenbezug	5	7	4
Anwendungsfälle mit Austausch zwischen Forschung und Versorgung	2	2	0
Anwendungsfälle mit Selbstdokumentation	1	1	0
Summe	13	18	10

Tabelle 7: Vergleich der Bewertung der Studien-, Versorgungs- und Forschungsdatenbank in Bezug auf die Auswahlkriterien

4.4.2. Definition des Forschungssystems

Das Forschungssystem, das über die Forschungsschnittstelle an die ePA angeschlossen wird, besteht aus einer **Patientenliste** und einer **Versorgungsdatenbank**, die jeweils von einem unabhängigen Systemverwalter (der **IDAT-Verwalter** für die Patientenliste und der **MDAT-Verwalter** für die Versorgungsdatenbank) administriert werden. Die Patientenliste enthält nur die identifizierenden Daten der Patienten und deren Pseudonyme. Die Versorgungsdatenbank enthält die medizinischen Daten des Patienten und deren Pseudonyme. So bleibt dem MDAT-Verwalter die Identität der Patienten verborgen und dem IDAT-Verwalter die medizinischen Daten. Direkten Zugriff auf beide Datenbanken und somit die Möglichkeit der Zuordnung der medizinischen Daten zu den Identitäten der Patienten hat nur der **Behandler** (siehe Abbildung 8). Eine Auflistung aller Akteure des Versorgungsmoduls befindet im Anhang A2.6.

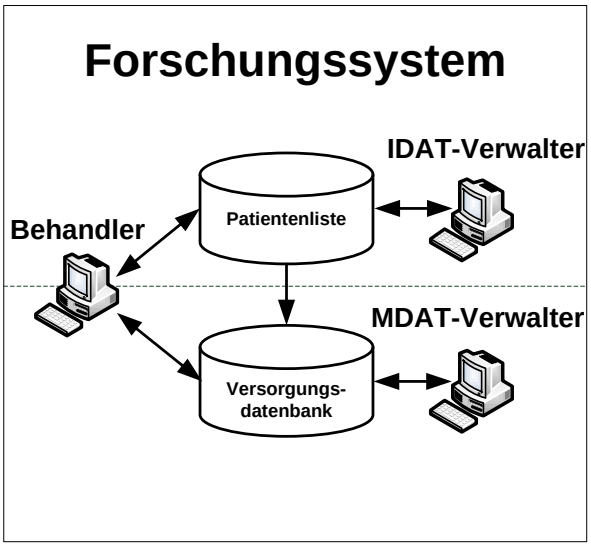

Abbildung 8: Das Forschungssystem mit den zugreifenden Akteuren und den einzelnen Datenbanken

5. Die elektronische Patientenakte nach § 291a

Nachdem in den vorherigen Kapiteln der Arbeit ein Grundverständnis über die elektronischen Patientenakten vermittelt und die in Deutschland von der gematik im Aufbau befindliche Telematikinfrastruktur eingegangen wurde, soll in diesem Kapitel das Forschungs- und Entwicklungsprojekt elektronische Patientenakte gemäß § 291a SGB V vorgestellt und die für diese Arbeit relevante Teilergebnisse des Projektes untersucht werden. Ziel ist es, die Rahmenbedingungen seitens des ePA-Systems für die Anbindung des Forschungssystems herauszustellen.

Es wird zunächst das ePA-System beschrieben. Dabei wird auf die Definition einer elektronische Patientenakte nach § 291a, die Akteure einer ePA, die IT-Komponenten einer elektronische Patientenakte, den Zugriff auf die Daten einer ePA und die Kommunikationsmuster einer elektronischen Patientenakte sowie die Sicherheitsarchitektur eingegangen. Anschließend wird auf Grundlage der Beschreibung des ePA-Systems analysiert, welche Komponenten für die Anbindung an das Forschungssystem relevant sind, und herausgestellt, welche Voraussetzungen und Anforderungen an das ePA-System, die Forschungsschnittstelle und das Forschungssystem im Hinblick auf eine Kommunikation zwischen dem ePA- und dem Forschungssystem formuliert werden müssen.

Als Ergebnis dieses Kapitels wird feststehen, welche Komponenten für die Anbindung eines Forschungssystems an die IT-Infrastruktur einer ePA nach § 291a benötigt werden und welche Rahmenbedingungen für eine Kommunikation zwischen dem ePA- und dem Forschungssystem erfüllt sein müssen. Ebenfalls wird es eine Liste von Anforderungen an das ePA-, das Forschungssystem und die Forschungsschnittstelle geben, die für die Anbindung eines Versorgungsmoduls erfüllt werden müssen.

5.1. Die elektronische Patientenakte nach § 291a

In dem Forschungs- und Entwicklungsprojekt zur elektronischen Patientenakte gemäß § 291a SGB V [153] wird die ePA als eine einrichtungs- und fallübergreifende elektronische Krankenakte definiert, deren Geltungsbereich sich über die gesamte Lebensdauer des Patienten aufspannen kann und in der Datenhoheit des Patienten ist. Ein Patient kann je nach Fähigkeiten und Interesse unterschiedliche Aktentypen auswählen. Es kann sich hierbei um eine sogenannte **Basisakte** handeln, auf die der Patient nicht direkt (über einen Client von Zuhause) zugreifen kann, sondern nur bei seinem Leistungserbringer. Dort kann der Patient allerdings entscheiden, ob und welche Daten er dem Leistungserbringer zugänglich macht [144]. Diese Ausprägung entspricht der Definition einer persönlichen elektronischen Patientenakte (pEPA) nach Haas wie sie nachfolgend definiert wird:

> *„Fallübergreifende Akte unter der Datenhoheit der Patientin bzw. des Patienten. Die Entscheidung über die konkrete Nutzung (Zweckbestimmung) erfolgt im Einzelfall durch die Patientin bzw. den Patienten, indem diese die Informationen bei Bedarf einer behandelnden Ärztin oder einem behandelnden Arzt zur Verfügung stellen. Die Patientin bzw. der Patient kann Rechte auch an eine Ärztin bzw. einen Arzt ihres/seines Vertrauens delegieren. Sinn der pEPA ist, als Quelle für die Speisung der zweckbestimmten Patientenakten in der Verantwortung der Ärztinnen und Ärzte zu dienen.“ [39, Seite 16]*

Eine weitere Variante der ePA, die sogenannte **Komfortakte**, ermöglicht zusätzlich eine Selbstdokumentation des Patienten und weitere Einträge aus dem Bereich Gesundheit und

Fitness. Sie kann vom Patienten in eigener Verantwortung über einen Zugang von Zuhause (den Bürger-Client) geführt werden [144]. Diese Ausprägung entspricht der Definition einer elektronischen Gesundheitsakte nach Haas:

> *„Von den Patientinnen bzw. den Patienten ausgewählte Daten und Dokumente aller ihrer Behandlungen über alle Gesundheitsversorgungseinrichtungen hinweg, ärztlich- oder patientengeführt oder hybrid und rein patientenmoderiert, ergänzt um beliebige eigene Eintragungen der Patientin und des Patienten." [39, Seite 16]*

Neben den beschriebenen Akten-Varianten wird auch noch eine **Patientenakte für eine spezielle Anwendung** betrachtet, die nur für eine bestimmte Anwendung ausgelegt ist (z. B. eine Diabetesakte). Die Akte verfügt (wie die Komfortakte) über einen Bürger-Client, der die Einsichtnahme in die Inhalte der Akte und die Vergabe von Zugriffrechten ermöglicht. Abhängig von den Anwendungsfällen, die eine solche Akte unterstützen soll, kann sie dem Bürger auch das Eintragen von selbsterfassten Daten über den Bürger-Client ermöglichen (z. B. das Anlegen und Pflegen eines Diabetestagebuchs) [144].

5.2. Akteure einer ePA nach § 291a

Im FuE-ePA-Projekt werden bezüglich des Informationsaustausches zwischen dem Versorgungssystem und dem ePA-System die zwei Akteure Leistungserbringer und Bürger betrachtet:

- Leistungserbringer: „*Eine Person im Bereich der Versorgung oder Versorgungsforschung, die zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 SGB V gehört. Als Leistungserbringer werden folgende Akteure bezeichnet: Ärzte, Zahnärzte, Studienärzte und Apotheker sowie berufsmäßig tätige Gehilfen und Personen, die bei den Ärzten zur Vorbereitung auf den Beruf tätig sind*." [154, Seite 11]
- Bürger: „*Mit dem Begriff Bürger ist der Besitzer der ePA gemeint*." …" *Zugleich werden hierunter auch die vom Bürger zur Wahrnehmung der Aktenhoheit Berechtigten verstanden.*" [144, Seite 4]

5.3. IT-Komponenten einer elektronische Patientenakte nach § 291a

Die Gesamtarchitektur zur Anbindung einer ePA nach § 291a SGB V eines Bürgers an die Systeme der Leistungserbringer unterteilt sich in die folgenden drei Bereiche (siehe auch Abbildung 9): Die Komponenten zur Kommunikation zwischen Versorgungsystem und Aktensystem (ePA-LE-Client, LE-Postfach-Komponente und ePA-Kommunikationskomponente) werden als Leistungserbringerschnittstelle (LE-Schnittstelle) bezeichnet. Das Aktensystem mit der LE-Schnittstelle wird als ePA-System definiert. Als Versorgungssystem werden die Systeme der Leistungserbringer bezeichnet. Der ePA-LE-Client gehört zur LE-Schnittstelle, wird aber innerhalb des Versorgungssystems als Zugangskomponente zur zentralen Infrastruktur betrieben und daher in der Beschreibung dem Versorgungssystem zugeordnet.

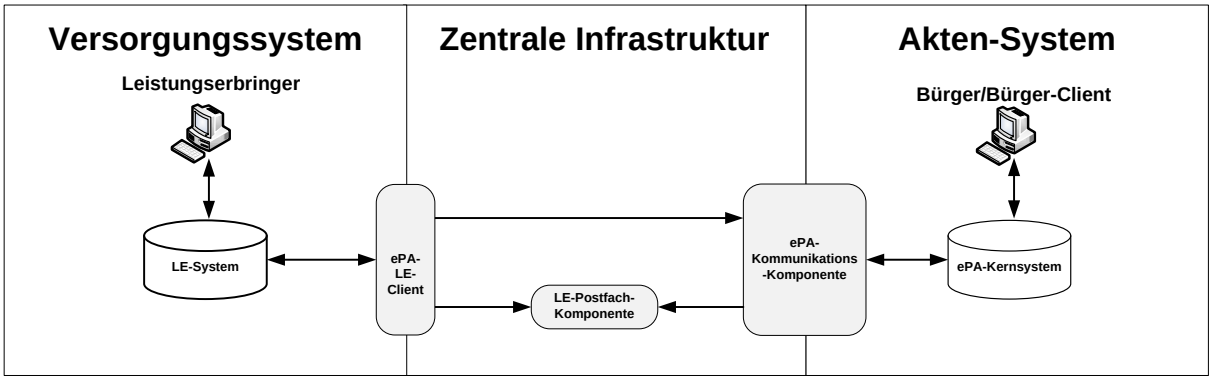

Abbildung 9: Übersicht der Architektur zur Einbindung einer ePA nach § 291a über eine zentrale Infrastruktur.

5.3.1. Versorgungssystem

Das Versorgungssystem ist das lokale System des Leistungserbringers und kann je nach Einrichtung die Stand-Alone-Anwendung eines niedergelassenen Arztes bis hin zu einer komplexen Client-Server-Umgebung mit unterschiedlichen Anwendungen sein, wie sie in großen Krankenhäusern zu finden ist. Abstrakt betrachtet werden im Versorgungssystem immer die folgenden zwei Komponenten betrieben:

- **Leistungserbringersystem (LE-System):** Der Begriff Leistungserbringersystem ist als Oberbegriff für die Systeme der Leistungserbringer zu verstehen. Je nach Leistungserbringer und Rolle kann dies z. B. ein Arztinformationssystem für den niedergelassenen Arzt oder ein Krankenhausinformationssystem für den Stationsarzt sein.
- **ePA-LE-Client**: Dieser Client kann entweder eine Komponente des Leistungserbringersystems sein oder losgelöst vom Leistungserbringersystem betrieben werden. Die Aufgabe des ePA-LE-Clients besteht darin, die Kommunikation zur ePA-Kommunikationskomponente und zum ePA-LE-Postfach zu kapseln. Über den Client können sowohl Informationen aus der ePA angefordert, als auch für die ePA bereitgestellt werden. Für die Kommunikation mit den Diensten in der Telematikinfrastruktur verfügt der ePA-LE-Client über eine Kommunikationskomponente, deren Identität in der Telematikinfrastruktur registriert ist und somit von den Diensten der Telematikinfrastruktur authentifiziert werden kann [144].

5.3.2. Zentrale Infrastruktur

Im Forschungs- und Entwicklungsprojekt zur ePA gemäß § 291a wird angenommen, dass es eine zentrale Infrastruktur gibt (wie z. B. die Telematikinfrastruktur des deutschen Gesundheitswesens), die entsprechende Dienste und Komponenten für einen sicheren Datenaustausch bereitstellt (z. B. eine PKI und SmartCards für die Akteure, Details siehe Sicherheitsarchitektur der LE-Schnittstelle [155]). Zusätzlich werden folgende Komponenten für die Kommunikation zwischen einer ePA und den Leistungserbringersystemen innerhalb der zentralen Infrastruktur benötigt:

- **LE-Postfach-Komponente:** Diese Komponente befindet sich in der Telematikinfrastruktur und nimmt Informationen für den Leistungserbringer aus der ePA des Bürgers entgegen. Diese Informationen können dann aus dem Leistungserbringer-Postfach über den ePA-LE-Client in das Leistungserbringersystem übernommen werden. Die Notwendigkeit einer solchen Komponente besteht zum einen darin, dass aus Sicherheitsgründen aus der Telematikinfrastruktur nicht auf die Systeme der

Leistungserbringer zugegriffen werden darf, d. h. eine Kommunikation mit einem Leistungserbringersystem muss immer vom ihm initiiert werden. Zum anderen wird davon ausgegangen, dass die Systeme der Leistungserbringer nicht permanent verfügbar sind. Diese Komponente ist optional. Entscheidet sich ein Leistungserbringer gegen ein LE-Postfach, so ist keine vom Bürger über seine ePA initiierte Kommunikation möglich, da die ePA das System aus den oben genannten Gründen dann nicht erreichen kann [144].

- **ePA-Kommunikationskomponente:** Diese Komponente kapselt die Kommunikation über die Telematikinfrastruktur für das ePA-Kernsystem. Ihre Aufgabe besteht darin, seitens der Telematikinfrastruktur eine standardisierte Schnittstelle bereitzustellen, über die das ePA-Kernsystem mit der LE-Postfach-Komponente und dem ePA-LE-Client Nachrichten austauschen kann. Die Schnittstelle zur Anbindung dieser Komponente an das ePA-Kernsystem wird nicht vorgegeben und kann vom Hersteller des ePA-Kernsystems beliebig umgesetzt werden. Neben der Kommunikation hat die ePA-Kommunikationskomponente zusätzlich die Aufgabe, Informationen zwischen zu speichern, falls das ePA-Kernsystem nicht verfügbar ist [144].

5.3.3. Akten-System

Das Akten-System besteht aus zwei Komponenten:

- **ePA-Kernsystem:** Dieses System verwaltet die medizinischen Informationen des Bürgers und unterstützt den Bürger beim Austausch von medizinischen Informationen mit dem Leistungserbringer. Bis auf einige Basisanforderungen ist die Ausgestaltung dem Hersteller des ePA-Kernsystems überlassen [144]. Dementsprechend kann es auch viele unterschiedliche Komponenten geben, die speziell auf die Bedürfnisse des Bürgers abgestimmt sind und ihn bei seinem Gesundheitsmanagement unterstützen (z. B. die Erfassung der Ernährung, ein Medikationsplan, Schmerztagebücher, Blutzuckermessungen etc.).
- **ePA-Bürger-Client:** Dieser Client ermöglicht es dem Bürger auf das ePA-Kernsystem zuzugreifen (z. B. von Zuhause) und Funktionen der Aktenführung, -nutzung sowie seine Aktenhoheit wahrzunehmen. Zu den Funktionen können u. a. die Vergabe von Zugriffsrechten, die Bearbeitung von Anforderungen eines Leistungserbringers sowie das Einsehen oder Eintragen von Informationen aus der bzw. in die Akte gehören. Diese Komponente ist optional und unterliegt der herstellerspezifischen Implementierung [144].

5.4. Zugriff auf die Daten einer ePA

Die ePA nach § 291a ist so konzipiert, dass die Leistungserbringer nicht volle Einsicht in die ePA bekommen und in ihr suchen können, sondern in ihren Leistungserbringersystemen spezielle Anforderungen formulieren müssen (z. B. alle Arztbriefe des letzten Jahres, siehe auch Abschnitt 5.4.3 zu Semantic Signifier), die dann als Anforderung an die ePA gesendet werden und von der ePA nach entsprechender Überprüfung der Autorisierungsrichtlinien (siehe auch Autorisierung) entsprechend bereitgestellt werden. Welche Inhalte von der ePA unterstützt werden (z. B. Arztbriefe, Laborbefunde, Basisdokumentation, Schmerztagebücher etc.), wird dem Leistungserbringersystem von der ePA während des ersten Kommunikationsvorganges mitgeteilt (siehe Abschnitt 5.4.2 zur Capability List), so dass der Leistungserbringer auch nur Informationen auswählen und anfordern kann, die von der ePA unterstützt werden. Auf die gleiche Art und Weise kann der Bürger auch Informationen für seine ePA vom Leistungserbringer anfordern (siehe auch Abschnitt 5.4.1 zur Anforderungs- und Bereitstellungsobjekten).

5.4.1. Anforderungs- und Bereitstellungsobjekt

Für den Austausch von Informationen zwischen der ePA und dem System der Leistungserbringer werden sogenannte Anforderungs- und Bereitstellungsobjekte eingesetzt. Anforderungsobjekte dienen dazu, eine Informationsanforderung an die ePA bzw. den Bürger oder das Leistungserbringersystem bzw. den Leistungserbringer zu formulieren [156]. Ein Anforderungsobjekt kommt z. B. zum Einsatz, wenn ein Leistungserbringer bei der Anamnese die Basisdokumentation des Patienten aus seiner ePA Daten einsehen möchte. Dann erstellt das Leistungserbringersystem ein Anforderungsobjekt, das die Informationen enthält, dass der Leistungserbringer die aktuelle Basisdokumentation des Patienten einsehen möchte. Dieses Anforderungsobjekt wird dann an die ePA des Patienten geschickt und dort von der ePA ausgewertet.

Bereitstellungsobjekte kapseln die Informationen, die der ePA bzw. dem Leistungserbringersystem bereitgestellt werden sollen [156]. Ein Bereitstellungsobjekt würde z. B. zum Einsatz kommen, wenn die ePA die im oberen Beispiel angeforderte Basisdokumentation für den Leistungserbringer bereitstellt. Dann wird die Basisdokumentation in ein Bereitstellungsobjekt gekapselt und dem Leistungserbringersystem zugesendet.

Beide Objekte werden als Informationsobjekte bezeichnet. Im Anhang A3.1 wird der logische Aufbau der Anforderungs- und Bereitstellungsobjekte im Detail beschrieben.

5.4.2. Capability List

Im FuE-ePA-Projekt wird angenommen, dass die unterschiedlichen Hersteller der ePA-Kernsysteme unterschiedliche Funktionen bzw. Akten-Varianten anbieten. Daher ist es erforderlich, dass dem Leistungserbringer vor dem Nutzen der ePA eines Patienten mitgeteilt wird, welche Funktionen (Kommunikationsmuster, Semantic Signifier) die ePA des Patienten unterstützt. Aus diesem Grund wurde ein Konformitätsprofil, die sogenannte Capability List, eingeführt, die das System des Leistungserbringers vor der eigentlichen Kommunikation herunterladen kann, um den Leistungsumfang der entsprechenden ePA zu erfahren. Neben diesen Informationen wird auch das öffentliche Schlüsselmaterial der Akte in der Capability List mitgeschickt, mit dem die Daten, die an die ePA geschickt werden sollen, verschlüsselt werden [157]. Der genaue Aufbau einer Capability List wird im Anhang A3.1 beschrieben.

5.4.3. Semantic Signifier

Da der Leistungserbringer keinen direkten Zugriff auf die ePA des Patienten hat und somit die ePA nicht durchsuchen und für ihn relevante Informationen aussuchen kann, muss er eine andere Möglichkeit haben, Informationen aus der ePA zu bekommen. Um den Informationsbedarf eines Leistungserbringers bzw. Bürgers zu formulieren und die Daten in der ePA eines Patienten bzw. dem Arztinformationssystems des Leistungserbringers zu identifizieren und anschließend zu übertragen, wird im FuE-Projekt auf die von der Object Management Group (OMG) [158] herausgegebenen Retrieve, Locate, and Update Service (RLUS) Spezifikation [159] gesetzt.

> *„Grundlegende Idee dieser Spezifikation ist es, auf Ebene des Nachrichtentransports, eine möglichst generische Schnittstelle zum Austausch von (medizinischen) Datenobjekten zu definieren. Die Ausgestaltung der über diese Schnittstelle angebotenen Operationen ist dabei losgelöst von einem konkreten Informationsmodell, d. h. grundsätzlich können beliebige Inhalte in beliebigen Strukturen transportiert werden. Um den die Schnittstelle nutzenden Systemen auf Anwendungsebene dennoch umfassende Informationen über Inhalt und Struktur der ausgetauschten Datenobjekte zu geben, sieht RLUS die Verwendung sogenannter Semantic Signifier vor.“ [160, Seite 1]*

Ein Semantic Signifier beschreibt also nicht nur die Inhalte eines medizinischen Datenobjektes, sondern auch die Struktur, in der diese Inhalte zwischen den Systemen kommuniziert werden sollen. Über einen Semantic Signifier kann ein Leistungserbringer bestimmte Informationen anfordern (z. B. die im obigen Beispiel genannte Basisdokumentation eines Patienten). Die Informationen werden von dem bereitstellenden System (in diesem Fall der ePA des Patienten) anhand der durch den Semantic Signifier vorgegebenen Inhalte und der Datenstruktur aufbereitet. Anschließend werden die Informationen dem anfordernden System (im diesem Fall dem Arztinformationssystem des Leistungserbringers) bereitgestellt und von dem anfordernden System übernommen. Damit dieses Verfahren funktioniert, müssen die Systeme für jeden Semantic Signifier ein Mapping auf ihre interne Datenstruktur von der durch die vom Semantic Signifier beschriebene Struktur vornehmen [160]. Es können also nur Daten zwischen den Systemen ausgetauscht werden, für die ein Semantic Signifier existiert. Zudem muss dieser Semantic Signifier von beiden Systemen unterstützt werden (welcher Semantic Signifier die ePA eines Patienten unterstützt, wird in der Capability List hinterlegt, siehe Abschnitt 5.4.2).

Im FuE-ePA-Projekt werden die Semantic Signifier sowohl für medizinische Datenobjekte als auch für Hilfsobjekte eingesetzt.

Die nachfolgende Tabelle beschreibt die einzelnen Bestandteile eines Semantic Signifier:

Bezeichner	Der Bezeichner dient zur einfachen Referenzierung eines Semantic Signifiers. Er steht grundsätzlich stellvertretend für das beschriebene inhaltliche Konzept.
Beschreibung / Bedeutung	Detaillierte Beschreibung des inhaltlichen Konzepts / Bedeutung (Semantik), des durch diesen Semantic Signifier repräsentierten Objekttypen (vollständiges Fachkonzept).
Datenstruktur	Beschreibt die normative Datenstruktur für Instanzobjekte dieses Semantic Signifiers. Dazu können neben Implementierungsleitfäden und Schemata auch Vorgaben zur Validierung (z. B. Schematron-Regeln) und zum Rendering (z. B. XSLT[11]-Skripte) der Instanzobjekte gehören.

Tabelle 8: Logische Bestandteile des Semantic Signifier [160, Seiten 4-5]

5.4.4. Adressierung der ePA

Im FuE-Projekt wurde festgelegt, dass es keinen zentralen Verzeichnisdienst für die Patientenakten geben soll. Vielmehr soll der Patient die Lokalisierungsinformationen direkt an den Leistungserbringer weitergeben. Als Lokalisierungsinformation dient die sogenannte ePA-ID oder auch die synonym verwendete Akten-ID [144].

Dieses Vorgehen hat gegenüber einem zentralen Verzeichnisdienst, den jeder Leistungserbringer abfragen könnte, den Vorteil, dass ein Patient selbst im Sinne einer Autorisierung entscheiden kann, wem er die Existenz seiner ePA offenbart und die Lokalisierungsinformationen (ePA-ID) zugänglich macht. Der Bürger ist somit in der Lage, gezielt den Nutzerkreis seiner ePA auszuwählen [161].

Die ePA-ID kann vor Ort beim Leistungserbringer von der eGK des Bürgers ausgelesen werden. Hier muss der Bürger diese Informationen durch die Eingabe einer PIN explizit freigeben. Sollte der Bürger über eine ePA mit Bürger-Client verfügen, so kann er die ePA-ID dem Leistungserbringer auch über ein Anforderungsobjekt bereitstellen. Zusätzliche Voraussetzung ist, dass der Leistungserbringer über ein LE-Postfach verfügt [161].

5.4.5. Zentraler und dezentraler Speicher

Im FuE-ePA-Projekt wird es dem Bürger bzw. den ePA-Herstellern überlassen, ob sie ihre ePA als Online-Akte oder als USB-Akte anbieten. Wie in der Abbildung 10 skizziert, werden beide Varianten durch die LE-Schnittstelle unterstützt, in dem im ePA-LE-Client entweder eine Verbindung zu einer USB-Akte oder zu einer Online-Akte aufgebaut wird [162]. Eine USB-Akte hat den Vorteil, dass sie auch „physisch“ in der Hoheit des Patienten ist. Sie hat allerdings auch den Nachteil, dass der Austausch von Daten mit dem Leistungserbringer nur beim Leistungserbringer vor Ort in Anwesenheit des Patienten und seiner USB-Akte stattfinden kann. Eine Online-Akte ermöglicht den Austausch von Daten zwischen dem Leistungserbringer und dem Patienten auch in dessen Abwesenheit.

[11] Extensible Stylesheet Language Transformations

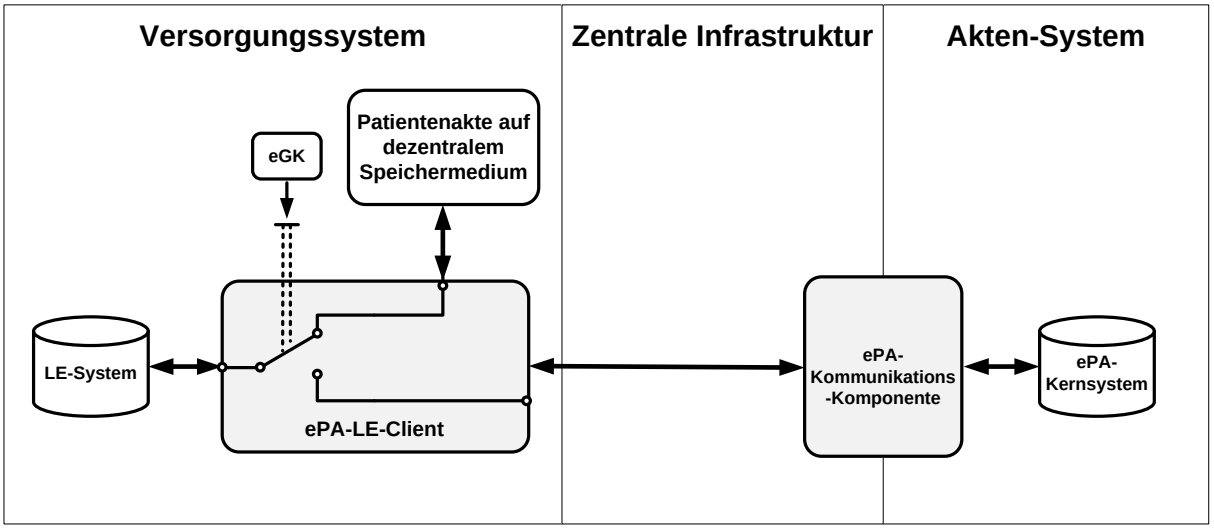

Abbildung 10: Nutzung einer ePA von zentralen oder dezentralen Speicher (angelehnt an Abb. auf Seite 5 in [162, Seite 5])

5.5. Kommunikationsmuster einer elektronische Patientenakte nach § 291a

Die Anwendungsfälle einer elektronischen Patientenakte können je nach Einsatzszenario sehr unterschiedlich sein und der Versuch, alle Anwendungsfälle einer ePA zu den unterschiedlichsten medizinischen Szenarien zu analysieren, hätte den Rahmen des FuE-ePA-Projektes gesprengt. Werden die Inhalte abstrahiert und nur noch die Akteure (Leistungserbringer und Bürger) und deren Kommunikation betrachtet, so bleibt eine überschaubare Menge an Kommunikationsmustern erhalten. In dem Forschungs- und Entwicklungsprojekt zur elektronischen Patientenakte gemäß § 291a wurden sechs Kommunikationsmuster definiert [163], über die diverse Anwendungsfälle umgesetzt werden können.

Bei dem Kommunikationsmuster wird zwischen einer synchronen und einer asynchronen Kommunikation unterschieden. Synchrone Kommunikation bedeutet, dass auf eine Anforderung unmittelbar eine Antwort auf diese Anforderung erfolgt. Asynchron bedeutet, dass zwischen der Anforderung und der entsprechenden Bereitstellung der Daten ein unbestimmter Zeitraum verstreichen kann. Im Folgenden werden die einzelnen Kommunikationsmuster beschrieben [163]:

- **Kommunikationsmuster 1 - Anfordern von Daten durch einen Leistungserbringer:** Der Leistungserbringer kann über sein Arztinformationssystem Daten aus der ePA des Bürgers anfordern. Dies kann z. B. eine Übersicht für einen Diabetespatienten sein, die das Gewicht, den Blutzuckerwert und die Medikation enthält. Die Anforderung wird in das Postfach des Bürgers gelegt und dann vom Bürger verworfen oder bearbeitet. Eine genaue Beschreibung des Ablaufes wird im Anhang A3.2.1 textuell und in Form eines Sequenzdiagrammes auf Grundlage von [163] beschrieben.
- **Kommunikationsmuster 2 - Anfordern von Daten durch einen Bürger:** Auch der Bürger kann über seine ePA Informationen aus den Systemen seiner behandelnden Ärzte (Leistungserbringer) anfordern. Diese Information kann z. B. das Ergebnis einer Laboruntersuchung sein, nachdem die Ergebnisse telefonisch besprochen wurden. Die Anforderung von Daten durch einen Bürger von seinem Leistungserbringer wird von der ePA an das LE-Postfach geschickt. Der Leistungserbringer kann die Anforderung dann aus dem Postfach abrufen und verwerfen oder bearbeiten. Eine genaue Beschreibung des Ablaufes wird im Anhang A3.2.2 textuell und in Form eines Sequenzdiagrammes auf Grundlage von [163] beschrieben.

- **Kommunikationsmuster 3 - Bereitstellen von Daten durch einen Bürger:** Der Bürger kann dem Leistungserbringer Informationen aus seiner ePA nach einer entsprechenden Anforderung (siehe Kommunikationsmuster 1) des Leistungserbringers bereitstellen. Er kann aber auch ohne entsprechende Anforderung dem Leistungserbringer Daten aus seiner ePA bereitstellen. Diese Daten können z. B. regelmäßig durchgeführte Blutzuckermesswerte sein, die dem Arzt regelmäßig zur Kontrolle übermittelt werden. Eine genaue Beschreibung des Ablaufes bei der Bereitstellung von Daten durch den Bürger erfolgt im Anhang A3.2.3 textuell und in Form eines Sequenzdiagrammes auf Grundlage von [163] beschrieben.
- **Kommunikationsmuster 4 - Bereitstellen von Daten durch einen Leistungserbringer:** Der Leistungserbringer kann der ePA des Bürgers Daten ohne eine vorherige Anforderung schicken (z. B. bei einem Arztbesuch) oder auf eine Anforderung des Bürgers reagieren (siehe Kommunikationsmuster 2). Die Anforderung muss nicht immer über das ePA-System erfolgen. Sie kann durch den Bürger z. B. auch per Telefon oder Fax etc. erfolgt sein. Der Ablauf der Bereitstellung von Daten durch einen Leistungserbringer an die ePA eines Bürgers wird im Anhang A3.2.4 textuell und in Form eines Sequenzdiagrammes auf Grundlage von [163] beschrieben.
- **Kommunikationsmuster 5 - Anfordern von Bereitstellungsobjekten durch einen Leistungserbringer mit unmittelbarer Zustellung:** Dieses Kommunikationsmuster ist eine Kombination der Kommunikationsmuster 1 und 3. Hier erfolgt allerdings nach der Anforderung durch den Leistungserbringer eine direkte Bereitstellung durch die Akte, ohne dass der Bürger hier noch eingreifen muss. Voraussetzung ist, dass der ePA eine entsprechende Ad-hoc oder Vorab-Autorisierungsrichtlinie vorliegt [162]. Da der Ablauf des Kommunikationsmusters 5 nur einer Ausführung der Schritte des 1. und 3. Kommunikationsmusters hintereinander entspricht, wird dieses Kommunikationsmuster nicht noch einmal beschrieben.
- **Kommunikationsmuster 6 - Zustellen von Bereitstellungsobjekten durch einen Leistungserbringer mit unmittelbarer Verarbeitung:** Dieses Kommunikationsmuster unterscheidet sich nur geringfügig vom Kommunikationsmuster 4. Während beim Kommunikationsmuster 4 die Bereitstellung erst durch den Bürger überprüft und dann in die ePA übernommen wird, wird bei diesem Kommunikationsmuster die Bereitstellung automatisch in die ePA übernommen. Voraussetzung ist, dass der ePA eine entsprechende Ad-hoc oder Vorab-Autorisierungsrichtlinie vorliegt [162]. Da sich dieses Kommunikationsmuster nur bei der Übernahme der Bereitstellung in die ePA vom Kommunikationsmuster 4 unterschiedet, die Kommunikation zwischen den Komponente aber die gleiche ist, wird es nicht nochmal getrennt beschrieben.

5.6. Operationen und Nachrichtentransport der LE-Schnittstelle

Im nachfolgenden Abschnitt werden die Operationen der LE-Schnittstelle, der Nachrichtenaufbau und die Abbildung eines Anforderungsobjektes bei einer asynchronen und synchronen Kommunikation auf die Nachrichtenstruktur beschrieben. Hierbei handelt es sich nur um eine Übersicht. Eine detaillierte Beschreibung ist in der Facharchitektur der LE-Schnittstelle zu finden [144].

5.6.1. Operationen der LE-Schnittstelle

Im FuE-ePA-Projekt werden die Schnittstellen der IT-Komponenten der LE-Schnittstelle über die RLUS Spezifikation aufgeführten Operationen umgesetzt [159], die von der Object Management Group [158] verfasst wurde. Der Standard sieht die folgenden sechs Kern-Operationen vor [159]:

- Mit der **Get-Operation** können einzelne Informationsobjekte abgerufen werden.
- Die **List-Operation** ermöglicht im Gegensatz zur Get-Operation das Abrufen mehrerer Informationsobjekte.
- Durch die **Locate-Operation** kann eine Liste von Adressen der Dienste angefragt werden, von denen ein bestimmtes Informationsobjekt abgerufen werden kann.
- Die **Put-Operation** dient dazu, ein Informationsobjekt einem anderen Dienst bereitzustellen.
- Mit der **Discard-Operation** können Informationsobjekte von einem Dienst gelöscht werden.
- Durch die **Describe-Operation** kann das Schema eines Semantic Signifier abgerufen werden.

Die LE-Schnittstelle nutzt allerdings nur die List-Operation, um Objekte abzurufen und die Put-Operation, um Objekte bereitzustellen. In der Facharchitektur der LE-Schnittstelle besitzt jede Operation immer einen Request- und einen Response-Teil [144], wie es in der nachfolgenden Tabelle 9 am Beispiel des PutRLUSGenericRequest dargestellt wird. Eine Beschreibung aller RLUS-Operation befindet sich im Anhang A3.3.

Operationsparameter / -element	**Beschreibung**
xs:any	XML-Dokument
RLUStypes:RLUSPutRequestSrcStruct	Informationen zum Aufrufkontext (Semantic Signifier, SourceIdentity, CBR-Context)
writeCommandEnum	Definiert die gewünschte Aktion im Zielsystem.

Tabelle 9: Beschreibung des PutRLUSGenericRequest [144, Seite 37]

5.6.2. Aufbau der Nachrichten

Das FuE-ePA-Projekt setzt bei der Kommunikation auf eine serviceorientierte Architektur auf der Basis von SOAP (Simple Object Access Protocol) [164]. Die RLUS-Operationen werden dabei im SOAP-Body eingetragen (siehe Abbildung 11) [144].

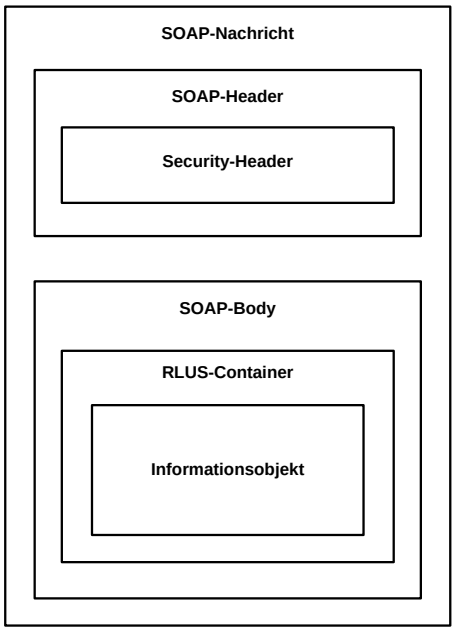

Abbildung 11: Nachrichtenaufbau (angelehnt an Abb. auf Seite 35 in [144])

5.6.3. Synchrone und asynchrone Kommunikation

Wie im Abschnitt 5.5 herausgestellt wurde, kann über die LE-Schnittstelle eine synchrone und eine asynchrone Kommunikation umgesetzt werden. In Abbildung 12 ist zu sehen, dass bei einer asynchronen Kommunikation die Elemente eines Informationsobjektes erst auf ein XML-Schema abgebildet, in eine RLUS-Operation eingebettet und dann in den Body der SOAP-Nachricht überführt werden. Dies ist dadurch begründet, dass nach der Kommunikation der Kommunikationskontext noch erhalten bleiben muss. Im Fall einer synchronen Kommunikation werden die Elemente des Informationsobjektes in die RLUS-Operation und in den SOAP-Header abgebildet (Abbildung 13). Dadurch können in Informationen direkt durch den Kommunikationspartner aus den SOAP-Headern verarbeitet werden, so dass sie nicht wie bei der asynchronen Kommunikation persistiert werden müssen [156].

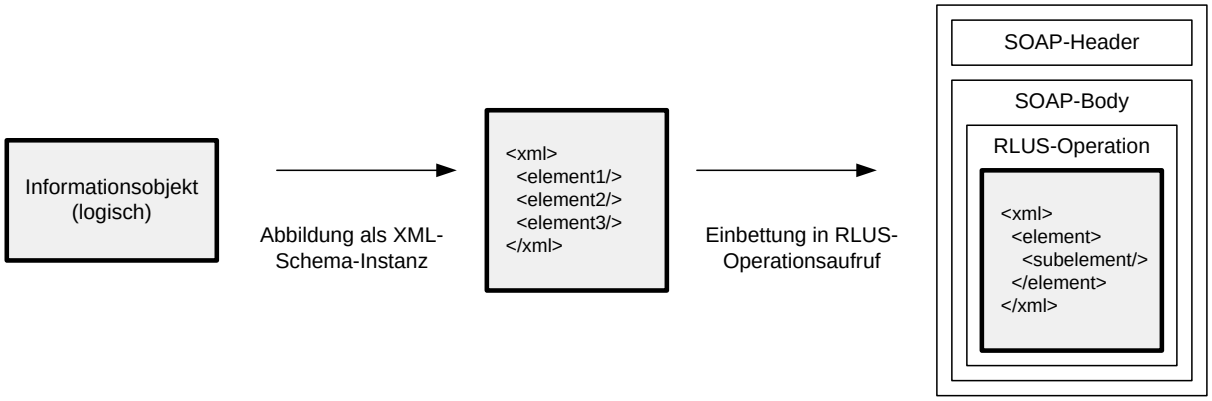

Abbildung 12: Abbildung eines Anforderungsobjektes bei einer asynchronen Kommunikation [156, Seite 6]

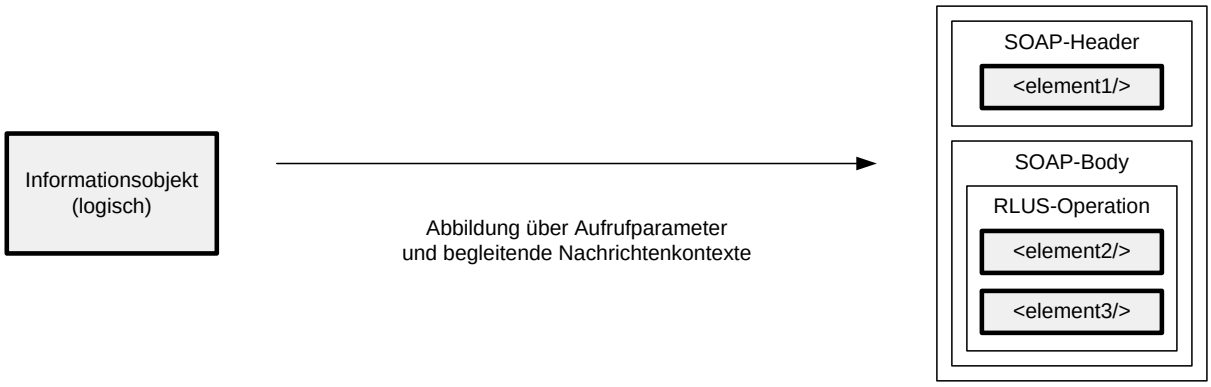

Abbildung 13: Abbildung eines Anforderungsobjektes bei einer synchronen Kommunikation [156, Seite 7]

5.7. Sicherheitsarchitektur

Die Sicherheitsarchitektur der LE-Schnittstelle sieht drei Zonen vor (siehe auch Abbildung 14). In der dezentralen Zone befinden sich die Systeme der Leistungserbringer sowie der Access Token Service, der für die Ausstellung von Autorisierungstoken für die Ad-Hoc Autorisierung verantwortlich ist, und der Guarantor Token Service, der für die Authentifizierung der Mitarbeiter einer Leistungserbringerorganisation verantwortlich ist und eine Guarantor Assertion ausstellt. In der zweiten Zone (zentrale Infrastruktur) befinden sich neben dem LE-Postfach und der ePA-Zugangskomponente der Identity Provider, der als zentraler Authentifizierungsdienst dient und bei denen sich jeder Nutzer der ePA vor einen entsprechenden Zugriff authentifizieren muss (mittels HBA oder Guarantor Assertion). Des Weiteren befinden sich ein zentraler PKI-Dienst zur Überprüfung der X.509-Zertifikate sowie ein Verzeichnisdienst zum Abrufen weiterer Attribute der Leistungserbringer bzw. der Leistungserbringerinstitutionen in der zentralen Infrastruktur. Die genauen Details der Sicherheitsarchitektur der LE-Schnittstelle können hier [155] nachgelesen werden.

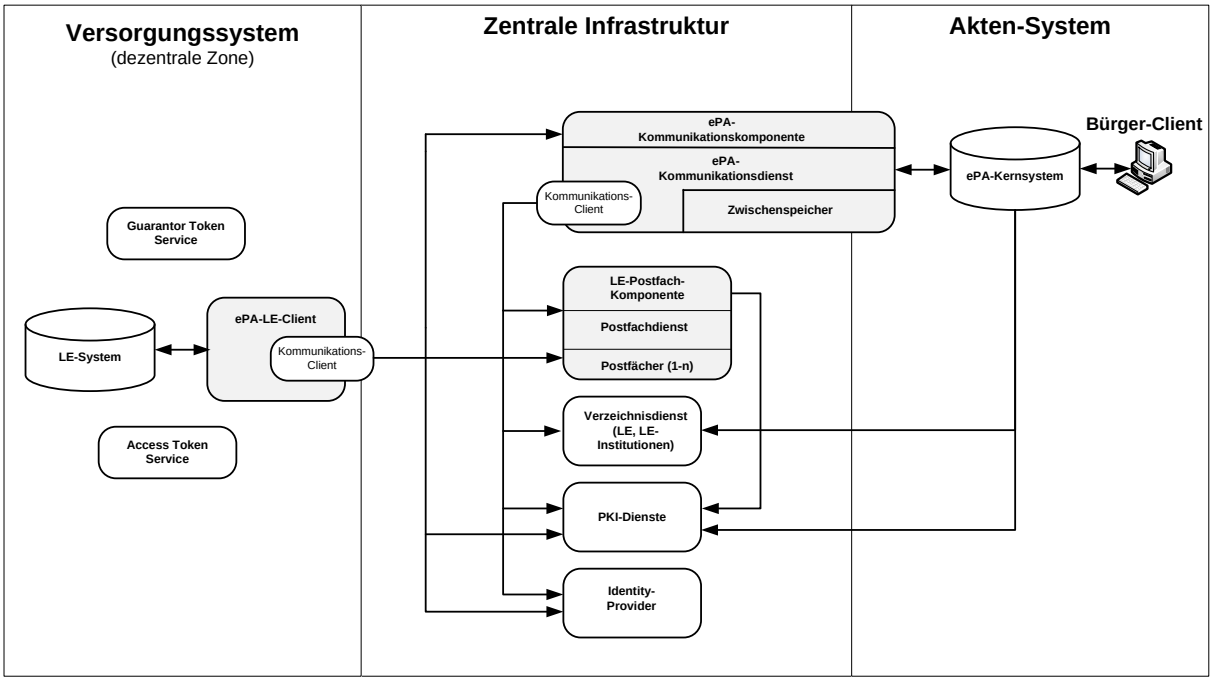

Abbildung 14: Systemüberblick mit den Sicherheitsdiensten der LE-Schnittstelle (angelehnt an Abb. auf Seite 4 in [155])

5.7.1. Vertrauens- und Kommunikationsbeziehungen der LE-Schnittstelle

Die LE-Schnittstelle unterscheidet zwei Möglichkeiten der Kommunikation zwischen den Komponenten (siehe Abbildung 15) [155]:

- **Trusted Client**: Ein Client befindet sich in einer vertrauten Sicherheitszone und baut eine Verbindung zu einem Service in einer anderen Sicherheitszone auf. Im Fall der LE-Schnittstelle ist der ePA-LE-Client ein Trusted Client, der aus der dezentralen Zone der Leistungserbringerorganisation eine Verbindung zu dem LE-Postfachdienst bzw. der ePA-Kommunikationskomponente aufbaut.
- **Dedicated Service**: Ein Service baut eine Verbindung zu einem anderen Service in derselben Sicherheitszone auf. Bei der LE-Schnittstelle baut z. B. die ePA-Kommunikationskomponente eine Verbindung über einen Dedicated Service zum LE-Postfachdienst aufbaut.

Die Abbildung 15 stellt die Vertrauensbeziehungen (durch Pfeile mit gepunkteter Linie dargestellt) und Kommunikationsbeziehungen (durch Pfeile mit durchgezogener Linie dargestellt) der IT-Komponenten der LE-Schnittstelle über die einzelnen Sicherheitszonen dar. Das ePA-Kernsystem vertraut der ePA-Kommunikationskomponente, die ePA-Kommunikationskomponente vertraut dem zentralen Identity Provider in der zentralen Infrastruktur. Der Identity Provider vertraut wiederum dem Guarantor Token Service. Auch der LE-Postfachdienst vertraut dem Identity Provider. Somit kann sich ein Leistungserbringer mit einer durch den Guarantor Token Service erstellten Authentifizierungsnachweis (Guarantor Assertion) beim Identity Provider authentisieren und vom Identity Provider einen Authentifizierungsnachweis anfordern (Identity Assertion). Diesen Authentifizierungsnachweis kann er wiederum nutzen kann, um sich gegenüber der ePA-Kommunikationskomponente bzw. dem LE-Postfachdienst zu authentisieren (der genaue Ablauf zum Erstellen einer Guarantor Assertion und einer Identity Assertion wird in der Sicherheitsarchitektur der LE-Schnittstelle [155] beschrieben).

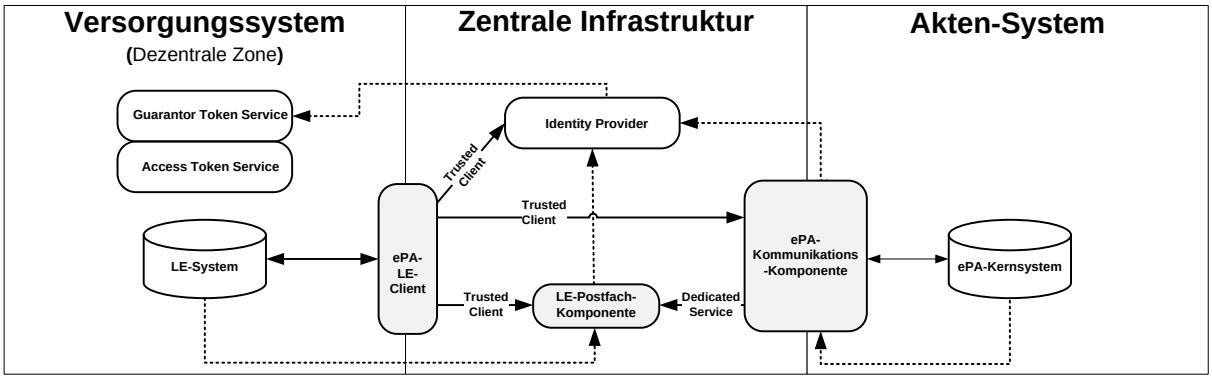

Abbildung 15: Vertrauens- und Kommunikationsbeziehungen der LE-Schnittstelle (angelehnt an Abb. auf Seite 10 in [155])

Im FuE-ePA-Projekt wird eine Session-basierte Sicherung der Kommunikation zwischen den Clients und Diensten eingesetzt (vergleiche auch Sicherheitsarchitektur der LE-Schnittstelle Kapitel 2.8 [155]). Beim Aufbau der Session kommen zwei unterschiedliche Möglichkeiten zur Sicherung der Kommunikation zum Einsatz, zum einen das SymmetricBinding und zum anderen das AsymmetricBinding.

Ein AsymmetricBinding wird eingesetzt, wenn sowohl der Client als auch der Server Sicherheits-Token für die Sicherung der Kommunikation bereitstellen. Im Falle der LE-

Schnittstelle kommen die X509 Zertifikate des Clients und des Servers als Sicherheits-Token zum Einsatz. D. h. der Client und der Server nutzen jeweils ihren privaten Schlüssel (Client=InitiatorToken und Server=RecipientToken) für die Signatur der Nachricht und die öffentlichen Schlüssel des Partners für die Verschlüsslung der Nachricht [165,166] (siehe auch Abbildung 16). Ein AsymmetricBinding kommt immer zum Einsatz, wenn der Client und der Server sich in der gleichen Sicherheitszone befinden [155].

Befinden sich Client und Server in unterschiedlichen Sicherheitszonen, so kommt ein SymmetricBinding für die Sicherung der Kommunikation zum Einsatz, bei dem nur das X509 Zertifikat des Servers eingesetzt wird. Das bedeutet, dass der Client einen temporären symmetrischen Schlüssel (ProtectionToken) generiert, diesen symmetrischen Schlüssel mit dem öffentlichen Schlüssel des Servers verschlüsselt und dem Server übermittelt. Client und Server nutzen diesen Schlüssel, um die auszutauschenden Nachrichten zu verschlüsseln und zu signieren. Damit der Server den Client auch authentifizieren kann, sendet der Client noch ein SupportingToken mit [165,166] (siehe auch Abbildung 16). Im Falle der LE-Schnittstelle ist der SupportingToken die IdentityAssertion [155], die die Identität des Leistungserbringers eindeutig nachweist.

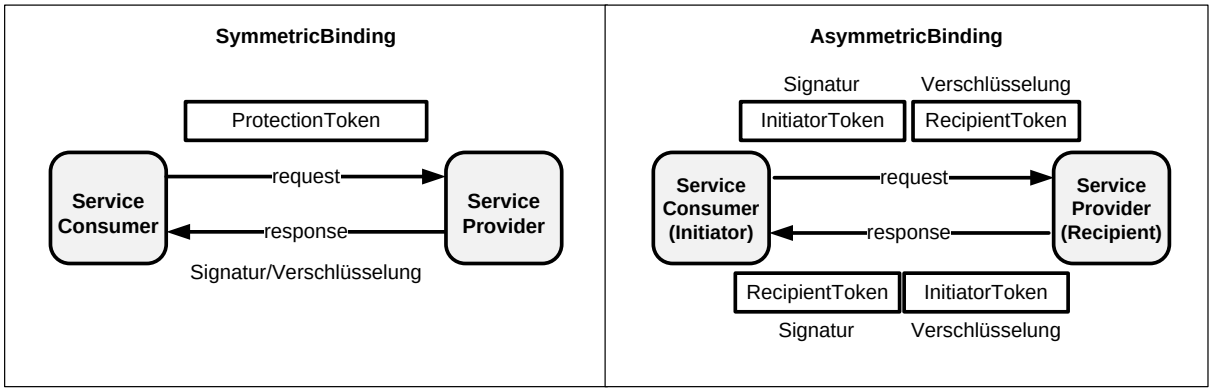

Abbildung 16: Message Protection Bindings (angelehnt an Abb. auf Seite 57 in [155])

5.7.2. Autorisierungskonzept der LE-Schnittstelle

Die Autorisierung der Leistungserbringer findet in der ePA statt. Das Autorisierungskonzept der ePA sieht zwei Möglichkeiten zur Vergabe von Autorisierungsrichtlinien durch den Bürger vor. Das ist zum einen die Möglichkeit, „Vorab-Autorisierungsrichtlinien“ in der ePA zu hinterlegen, und zum anderen die Möglichkeit, eine „Ad-hoc Autorisierung“ beim Leistungserbringer durchzuführen [161]. Die beiden Varianten werden im Folgenden kurz erläutert:

- **Vorab-Autorisierungsrichtlinien** kann der Bürger über seinen Bürger-Client in seiner ePA hinterlegen und verwalten. Diese Autorisierungsrichtlinien werden dann bei jeder Anfrage bzw. Bereitstellung durch einen Leistungserbringer ausgewertet und entsprechend wird die Aktion durchgeführt oder verweigert. Z. B. kann der Bürger für seinen Hausarzt Vorab-Autorisierungsrichtlinien hinterlegen, so dass der Hausarzt auch ohne die Anwesenheit des Bürgers bzw. seiner eGK auf die Daten in der ePA zugreifen kann. Auch hier kann der Bürger entscheiden, dass der Hausarzt nur auf Teile seiner ePA zugreifen kann (z. B. nur auf die Basisdokumentation und das Diabetestagebuch). Alle anderen Dokumente muss der Bürger dann vor Ort per Ad-hoc-Autorisierung für den Hausarzt freigeben. Beim Anlegen der Akte wird ein Basissatz an Vorab-Autorisierungsrichtlinien (Basiskonfiguration) hinterlegt, der einen Betrieb der ePA (im Sinne des Bürgers) auch ohne weitere Konfiguration der Vorab-Autorisierungsrichtlinien durch den Bürger ermöglicht.

- Eine **Ad-hoc Autorisierung** durch den Bürger kommt zum Einsatz, wenn der Bürger beim Leistungserbringer vor Ort ist und diesem Zugriff auf Daten aus seiner ePA ermöglichen möchte, auf die der Leistungserbringer momentan keine Zugriffsberechtigung in Form einer Vorab-Autorisierungsrichtlinie hat. Dies kann z. B. der Fall sein, wenn der Patient einen Arzt besucht, den er bisher noch nicht kannte oder der Patient bestimmte Daten nur in seiner Anwesenheit dem Leistungserbringer aushändigen möchte. Diese Ad-hoc Autorisierungsrichtlinie wird dann mit der Anforderung des Leistungserbringers an die ePA geschickt und dort ausgewertet. Diese Art der Autorisierung wird immer nur mit synchronen Kommunikationsmustern eingesetzt (auf die synchronen Kommunikationsmuster wird im Abschnitt 5.5 eingegangen).

5.7.3. Verschlüsselungskonzept der LE-Schnittstelle

Im FuE-ePA-System ist eine nutzerzentrierte Verschlüsselung der medizinischen Datenobjekte vorgesehen. D. h. es wird für jede Akte ein asymmetrisches Schlüsselpaar angelegt [167]. Der öffentliche Schlüssel kann von der ePA (pubAS) durch die Leistungserbringer abgerufen werden. Der private Schlüssel der ePA (prkAS) wird mit einem symmetrischen Schlüssel (symkeyAS1) gesichert (siehe auch Abbildung 17). Dieser Schlüssel wird mit der eGK des Bürgers gesichert. Weitere Kopien des symmetrischen Schlüssels (symkeyASn) werden mit den öffentlichen Schlüsseln der zugriffsberechtigten Nutzer verschlüsselt (z. B. pubHBA, oder pubSMC). Bei einer Bereitstellung durch die Leistungserbringer an die ePA wird das medizinische Datenobjekt (MDO) mit einem zufällig generierten symmetrischen Schlüssel (symkeyMDO) verschlüsselt, dieser symmetrischen Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel der ePA (pubAS) verschlüsselt. Sowohl das verschlüsselte medizinische Datenobjekt als auch der mit dem pubAS gesicherte symmetrische Schlüssel werden dann dem ePA-Kernsystem zugestellt. Beim Abrufen der Daten durch den Patienten wird dann mit Hilfe der eGK der private Aktenschlüssel entschlüsselt und somit kann der Patient auf die medizinischen Daten zugreifen. Beim Abrufen der Daten durch einen berechtigten Leistungserbringer wird nicht nur das verschlüsselte medizinische Datenobjekt sondern auch der durch den öffentlichen Schlüssel des HBAs des Leistungserbringers gesicherte private Aktenschlüssel verschickt, den der Leistungserbringer dann entschlüsseln kann. Mit dem Ergebnis der Entschlüsselung erhält der Leistungserbringer Zugriff auf den privaten Aktenschlüssel und somit auf das mitgesendete MDO. Da der private Aktenschlüssel mitgeschickt und entschlüsselt wird, muss dieser Vorgang in einer abgesicherten Umgebung erfolgen (z. B. im Konnektor). Weitere Voraussetzungen und Anforderungen dieses Systems werden im Dokument “Verschlüsselte Datenhaltung - Beschreibung eines alternativen Verschlüsselungsmodells-“ beschrieben [167].

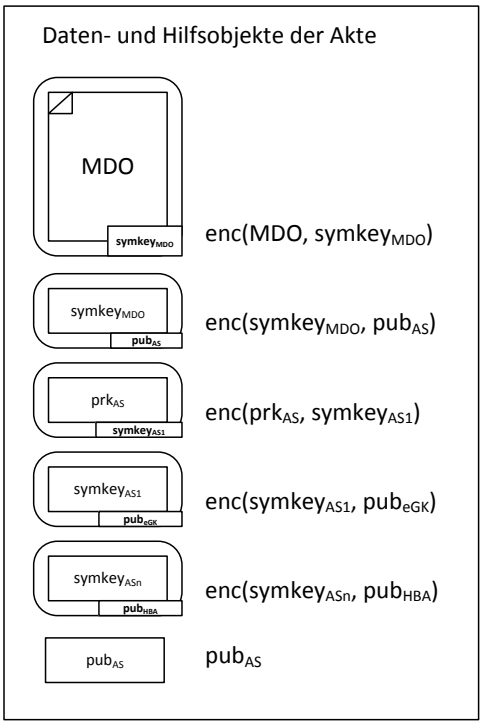

Abbildung 17: Übersicht der Hilfsobjekt für die Verschlüsselung im ePA-Kernsystem [167, Seite 2]

Der genaue Ablauf beim Bereitstellen von medizinischen Datenobjekten durch den Leistungserbringer für die ePA und der Ablauf beim Abrufen von medizinischen Datenobjekten von der ePA durch einen Leistungserbringer wird im Anhang A3.4 auf Grundlage von [167] beschrieben.

5.8. Analyse der Anforderungen an das ePA-, das Forschungssystem und die Forschungsschnittstelle

In diesem Abschnitt soll analysiert werden, welche IT-Komponenten des ePA-Systems für die Kommunikation mit der Forschungsschnittstelle benötigt werden und welche Anforderungen bzw. Voraussetzungen sich daraus an das ePA-System, die Forschungsschnittstelle und das Forschungssystem ergeben. Außerdem werden Rahmenbedingungen festgelegt, unter denen eine Kommunikation zwischen dem ePA- und dem Forschungssystem möglich ist. Bei der Analyse soll berücksichtigt werden, dass sowohl am Forschungssystem, als auch am ePA-System so wenige Anpassungen wie möglich erfolgen und somit die Anforderungen möglichst von der Forschungsschnittstelle umgesetzt werden sollen.

5.8.1. Auswahl der IT-Komponente für die Kommunikation mit der Forschungsschnittstelle

Die ePA-Kommunikationskomponente kapselt die Kommunikation über die Telematikinfrastruktur für das ePA-Kernsystem. Da sich die Forschungsschnittstelle auch innerhalb der Telematikinfrastruktur befinden soll, ist es nur logisch, die ePA-Kommunikationskomponente für die Kommunikation zwischen der ePA und der Forschungsschnittstelle zu nutzen. Dies bedeutet, dass das Forschungssystem mit Hilfe der Forschungsschnittstelle über die ePA-Kommunikationskomponente mit dem ePA-Kernsystem kommuniziert. Da möglichst wenige Anpassungen an dem bestehenden ePA-System vorgenommen werden sollen, muss die Forschungsschnittstelle die Operationen und Nachrichten der Kommunikationskomponente unterstützen (A00).

5.8.2. Aktensystem (Komfort-, Spezial- oder Basisakte)

Für die Kommunikation zwischen einer ePA und dem Versorgungsmodul wird eine Komfortakte bzw. eine Patientenakte für eine spezielle Anwendung vorausgesetzt, da hier eine direkte Kommunikation zwischen dem Forschungsverbund und dem Patienten über seine ePA erfolgen soll, was wiederum einen direkten Zugang des Patienten auf seine ePA verlangt. D. h. es werden in dieser Arbeit nur die Systeme mit einem Bürger Client betrachtet (Rahmenbedingung 1). Prinzipiell ist auch eine Anbindung über eine Basisakte möglich, bei der bestimmte Dokumente automatisch weitergeleitet oder Nachrichten vom Arzt abgerufen und an den Probanden weitergeleitet werden und der Arzt die Kommunikation zwischen dem Patienten und dem Forschungsverbund vermittelt. Diese Betrachtung würde allerdings den Rahmen dieser Arbeit sprengen. Es sollte daher in einer weiteren Arbeit untersucht werden, wie auch Patienten bzw. Probanden an diesem System partizipieren können, wenn sie nur über eine Basisakte verfügen bzw. keinen Bürger-Client bedienen wollen oder können, und ob sich daraus weitere Anforderungen an die Systeme ergeben. Spezielle Anforderungen an die Forschungsschnittstelle oder das Forschungssystem ergeben sich daraus nicht.

5.8.3. Zentrale und dezentrale Speicher

Bei der Betrachtung in dieser Arbeit wird davon ausgegangen, dass der Patient über eine Online-Akte verfügt, die über die ePA-Kommunikationskomponente mittels der Forschungsschnittstelle für das Versorgungsmodul erreichbar ist. Diese Anforderungen könnten auch durch eine ePA erfüllt werden, die über einen dezentralen Speicher umgesetzt wird. Es müsste allerdings sichergestellt werden, dass der Patient über die ePA-Kommunikationskomponente Daten an die Forschungsschnittstelle schicken und empfangen kann. D. h. hier müsste es eine Möglichkeit geben, von Zuhause eine Verbindung zwischen dem dezentralen Speicher und der ePA-Kommunikationskomponente aufzubauen, um die Kommunikation mit der Forschungsschnittstelle zu ermöglichen. Momentan wird diese Funktion nicht unterstützt.

Eine zweite Möglichkeit wäre, die Kommunikation nur beim Arztbesuch über die Anbindung an die Telematikinfrastruktur der Arztpraxis zu ermöglichen. Diese Möglichkeit wäre z. B. mit dem Szenario der Basisakte, die vom Arzt geführt wird, gut kombinierbar. Diese Aspekte sollten in einer weiteren Arbeit (vielleicht auch mit den oben genannten Punkten) untersucht werden. Hierbei sollten die Ergebnisse des Projekts zwischen Fraunhofer und Med-O-Card berücksichtigt werden [168]. Aus den oben genannten Gründen wird vorerst vorausgesetzt, dass der Patient über eine Online-Akte verfügt (Rahmenbedingung 2). Spezielle Anforderungen an die Forschungsschnittstelle oder das Forschungssystem ergeben sich daraus nicht.

5.8.4. Zugriff auf die Daten einer ePA

Der Zugriff auf die ePA wurde in fünf Unterpunkten beschrieben, deren Bedeutung für die Kommunikation zwischen dem ePA- und dem Forschungssystem im Folgenden analysiert wird:

- **Anforderungs-, Bereitstellungsobjekte und Semantic Signifier:** Da festgelegt wurde, dass die Kommunikation mit dem Forschungssystem über die ePA-Kommunikationskomponente erfolgen soll und auch möglichst wenig Änderungen an dem bestehenden ePA-System vorgenommen werden sollen, ist es nur konsequent, für die Kommunikation mit dem Forschungssystem auch Anforderungs- und Bereitstellungsobjekte zu verwenden und Semantic Signifiern einzusetzen. Das bedeutet, dass die Forschungsschnittstelle sowohl Anforderungs- und Bereitstellungsobjekte

(A01), als auch Semantic Signifier (A02) unterstützen muss. Außerdem muss sie die Erstellung von Bereitstellungs-, und Anforderungsobjekten übernehmen, die Nutzlast aus diesen Objekten extrahieren und dem Forschungssystem bereitstellen (A03). Das Forschungssystem muss die Nutzlast nach den inhaltlichen und strukturellen Vorgaben der Semantic Signifier aufbereiten bzw. die empfangenen Daten richtig in die Datenbanken des Forschungssystems schreiben (VF02). Das Forschungssystem muss also für jeden einzusetzenden Semantic Signifier das Mapping auf die interne Datenstruktur des Forschungssystems von der durch die vom Semantic Signifier beschriebene Struktur vornehmen. Besondere Anforderungen an das ePA-System ergeben sich nicht, da die Forschungsschnittstelle und das Forschungssystem somit Anforderungs- und Bereitstellungsobjekte als auch Semantic Signifier unterstützen.

- **Adressierung der ePA:** Es wurde festgelegt, dass das ePA-Kernsystem und das Forschungssystem über die ePA-Kommunikationskomponente kommunizieren. Die ePA-Kommunikationskomponente adressiert die ePA eines Patienten über die ePA-ID. Diese Form der Adressierung sollte im Sinne möglichst weniger Anpassungen am ePA-System beibehalten werden. Andersherum sollte auch das Forschungssystem so wenig wie möglich angepasst werden. Dort werden die Daten des Patienten über sein Pseudonym zugeordnet. Um trotzdem die Daten des gleichen Patienten im Forschungs- und im ePA-System zuordnen zu können, muss die Forschungsschnittstelle während der Kommunikation ein entsprechendes Mapping der Identitäten des Patienten im Forschungs- und ePA-System durchführen (A04). Spezielle Anforderungen an das ePA- und das Forschungssystem ergeben sich nicht.
- **Kommunikationsmuster**: Für die Umsetzung der Kommunikation der Anwendungsfälle des Versorgungsmoduls über eine ePA werden nur asynchrone Kommunikationsmuster benötigt, da bei keinem Anwendungsfall eine direkte Antwort erwartet wird. D. h. die Forschungsschnittstelle unterstützt nur asynchrone Kommunikationsmuster für die Kommunikation von Informationen zwischen der ePA und den Datenbanken des Versorgungsmoduls (Rahmenbedingung 3) (mit Ausnahme des Abrufen von Hilfsobjekten wie der Capability List und den Schlüsselobjekten).
- **Capability List:** Die Capability List enthält das öffentliche Schlüsselmaterial der ePA, die unterstützten Kommunikationsmuster und die unterstützten Semantic Signifier. Diese Informationen sind für die Kommunikation zwischen dem ePA- und dem Forschungssystem relevant und müssen somit vor der Kommunikation abgerufen und ausgewertet werden. Da die Forschungsschnittstelle die Kommunikation für das Forschungssystem kapselt, muss sie auch die Capability List abrufen und auswerten (A05).
- **Autorisierung:** Da die Kommunikation zwischen dem ePA-System und dem Forschungssystem nur über asynchrone Kommunikationsmuster erfolgt, wird bei der Kommunikation mit dem ePA-System keine Ad-Hoc Autorisierung eingesetzt. Somit muss die ePA auch für die Kommunikation mit dem Forschungssystem keine Ad-Hoc Autorisierung unterstützen (Rahmenbedingung 4). Sie sollte allerdings eine Vorab-Autorisierung unterstützen, so dass die Kommunikation auch ohne das ständige Eingreifen des Bürgers erfolgen kann. Das ist aber nicht zwingend notwendig. Da die Vorab-Autorisierung im ePA-Kernsystem erfolgt, ergeben sich keine Anforderungen an das Forschungssystem oder die Forschungsschnittstelle und auch keine neuen Anforderungen an das ePA-System.

6. Kommunikationsmodell für die Anbindung eines Versorgungsmoduls an eine ePA

In diesem Kapitel wird die Kommunikation der ausgewählten Anwendungsfälle des Versorgungsmoduls beschrieben und auf dieser Grundlage analysiert, wie diese Kommunikation mit Hilfe einer ePA umgesetzt werden kann. Ziel ist es, Kommunikationsmuster zwischen den Komponenten und Akteuren herzuleiten, aus denen dann eine minimale Anzahl generischer Kommunikationsmuster abgeleitet werden kann. Diese Kommunikationsmuster bilden dann in ihrer Gesamtheit das Kommunikationsmodell für die Kommunikation zwischen einer ePA nach § 291a und dem Versorgungsmodul. Neben dem Kommunikationsmodell sollen auch Datenschutzanforderungen herausgearbeitet werden, die bei der Umsetzung des Kommunikationsmodells berücksichtigt werden müssen. Die Ergebnisse dieses Kapitels dienen als Grundlage für das Kapitel 7, in dem dann beschrieben wird, wie das Kommunikationsmodell unter Berücksichtigung der Datenschutzanforderungen über eine Erweiterung der IT-Infrastruktur des ePA-Systems umgesetzt werden kann.

Zunächst werden Annahmen und Voraussetzungen an bzw. für die Anbindung einer ePA nach § 291a an ein Versorgungsmodul definiert und die Forschungsschnittstelle in die Gesamtarchitektur eingeordnet.

In einem nächsten Schritt wird für jeden Anwendungsfall der Patientenliste und der Versorgungsdatenbank die Kommunikation zwischen dem Patienten und den Akteuren des Versorgungsmoduls bzw. der Patientenliste analysiert. Die Anwendungsfälle der Patientenliste und des Versorgungsmoduls können in Bezug auf die Kommunikation unterschiedlich umgesetzt werden. Es wird immer die Umsetzung des Anwendungsfalls beschrieben, bei der die direkteste Kommunikation zwischen dem Patienten und dem Forschungsverbund stattfindet. Es wird nur auf die Kommunikation des Anwendungsfalls eingegangen. Weitere Details zu den Anwendungsfällen können in den Datenschutzkonzepten der TMF [33,34] nachgelesen werden.

Abschließend wird untersucht, wie die Kommunikation zwischen dem Patienten und den Akteuren der Versorgungsdatenbank und der Patientenliste über eine ePA nach § 291a umgesetzt werden kann, welche Kommunikationsmuster und welche Anforderungen sich an die Systeme ergeben. Die Kommunikationsmuster werden am Ende der Analyse zu generischen Kommunikationsmustern zusammengefasst. Die Anforderungen werden in einer Liste zusammengefasst.

6.1. Annahmen und Voraussetzungen an bzw. für die Anbindung einer ePA nach § 291a an ein Versorgungsmodul

In diesem Abschnitt werden Annahmen und Voraussetzungen für die Anbindung einer ePA an ein Versorgungsmodul genannt und gezeigt, wie sich die Forschungsschnittstelle unter diesen Annahmen und Voraussetzungen in die Gesamtarchitektur einordnen lässt.

6.1.1. Allgemeine Voraussetzungen für die Kommunikation über eine Forschungsschnittstelle

Im Folgenden werden Voraussetzungen genannt, die bei einer Anbindung eines Versorgungsmoduls an eine ePA nach § 291a erfüllt werden müssen:

- **Voraussetzung 1**: Die ePA ist eine freiwillige Anwendung [169] und ist somit immer nur optional. Das bedeutet, dass Anwendungsfälle des Versorgungsmoduls auch weiterhin ohne eine ePA funktionieren müssen, damit auch Patienten ohne eine ePA nach § 291a weiter an einem Versorgungsmodul teilnehmen können.
- **Voraussetzung 2**: Ein Forschungsverbund kann sich entscheiden, nur einige der hier vorgeschlagenen Anwendungsfälle über eine ePA umzusetzen. Es können z. B. nur die Anwendungsfälle, die eine Kommunikation zwischen dem Forschungsverbund und den Patienten verbessern, umgesetzt werden.
- **Voraussetzung 3**: Es wird angenommen, dass eine Kommunikation zwischen der ePA eines Patienten und den Datenbanken eines Forschungsverbundes erst nach der Anmeldung eines Patienten am Versorgungsmodul stattfinden kann. Die nötigen Informationen für die Kommunikation (z. B. die Adresse der ePA oder die notwendigen Adressen der Datenbanken des Forschungsverbundes) sollen während des Anmeldeprozesses ausgetauscht werden. Diese Informationen werden in der Patientenliste (VF03) und in der ePA gespeichert (VE00).
- **Voraussetzung 4**: Über die ePA sollen nicht nur medizinische Daten an die Versorgungsdatenbank des Versorgungsmoduls übertragen werden. Sie soll auch eine Kommunikation zur Patientenliste ermöglichen und somit auch die Kommunikation von identifizierenden Daten und allgemeinen Informationen zwischen dem Patienten und dem Versorgungsmodul ermöglichen (A06).
- **Voraussetzung 5**: Die Kommunikation von Anwendungsfällen des Versorgungsmoduls, die im direkten Bezug zur Versorgung des Patienten stehen, also das Einstellen und Abrufen von Versorgungsdaten, soll direkt zwischen den Leistungserbringersystemen und der ePA erfolgen. Das bedeutet, dass die Behandler vorhandene Daten über ihre Arztinformationssysteme aus der ePA anfordern und neue Daten der ePA bereitstellen können. Medizinische Daten, die für Forschungsfragen interessant sind, können dann aus der ePA über die Forschungsschnittstelle an die Versorgungsdatenbank übertragen werden (A07).

6.1.2. Angenommenes Verhalten der Forschungsschnittstelle

Die Forschungsschnittstelle wird in diesem Kapitel als eine Blackbox betrachtet. Eine detaillierte Ausgestaltung der Forschungsschnittstelle mit ihren einzelnen IT-Komponenten und Interaktionen mit den Komponenten des Forschungs- bzw. ePA-Systems wird erst im Kapitel 7 auf Grundlage der hier hergeleiteten Kommunikationsmuster und Anforderungen stattfinden. Es wird hier also ein bestimmtes Verhalten der Forschungsschnittstelle

festgelegt, welches im Kapitel 7 aufgegriffen und entsprechend beschrieben wird, wie dieses Verhalten der Forschungsschnittstelle unter Berücksichtigung der Datenschutzanforderungen für alle Kommunikationsmuster umgesetzt werden kann. An dieser Stelle wird erst einmal angenommen, dass das hier festgelegte Verhalten der Forschungsschnittstelle datenschutzkonform ist. Es wird folgendes Verhalten von der Forschungsschnittstelle vorausgesetzt:

1. Um die Anforderung A06 umzusetzen wird angenommen, dass die Forschungsschnittstelle eine direkte Anbindung zwischen einer ePA eines Patienten und der Patientenliste ermöglicht. Da die Identität des Patienten in der ePA und in der Patientenliste bekannt ist (siehe Anforderung VF03), muss bei dieser Kommunikation keine Pseudonymisierung stattfinden. Die Schnittstelle kann die Informationen also direkt weiterleiten.
2. Um die Anforderung A07 umzusetzen wird angenommen, dass die Forschungsschnittstelle eine direkte Kommunikation zwischen einer ePA und einer Versorgungsdatenbank ermöglicht. Da die Daten des Patienten in der Versorgungsdatenbank pseudonymisiert und in der ePA mit identifizierenden Daten vorliegen, muss die Forschungsschnittstelle während der Kommunikation zwischen der ePA und dem Versorgungsmodul die Pseudonymisierung bzw. Depseudonymisierung vornehmen (A08).
3. Um eine Kommunikation von Daten eines Patienten zwischen der ePA und der Versorgungsdatenbank zu ermöglichen, müssen die Daten dem gleichen Patienten in der ePA und in der Versorgungsdatenbank zugeordnet werden können (vergleiche auch Kapitel 5.8.4 bzw. A04).

6.1.3. Einordnung der Forschungsschnittstelle in die Gesamtarchitektur

In der nachfolgenden Abbildung (Abbildung 18) wird die Einordnung der Forschungsschnittstelle in die Gesamtarchitektur dargestellt. Diese Abbildung berücksichtigt die Architektur des ePA-Systems (siehe Abbildung 9), des Versorgungsmoduls (siehe Abbildung 8) und die oben genannten Annahmen und Voraussetzungen.

Wie in der Abbildung 18 zu sehen ist, können der Verwalter der Patientenliste, der Verwalter der Versorgungsdatenbank und der Behandler wie gehabt auf die Datenbanken des Versorgungsmoduls zugreifen. Somit können die Voraussetzungen 1 und 2 aus dem Abschnitt 6.1.1, die einen Betrieb des Versorgungsmoduls ohne ePA bzw. die Umsetzung nur einiger Anwendungsfälle mit Hilfe der ePA fordern, erfüllt werden. Die vierte Voraussetzung ist ebenfalls erfüllt, da durch die Forschungsschnittstelle sowohl die Patientenliste als auch die Versorgungsdatenbank angebunden werden. Auch die fünfte Voraussetzung ist durch dieses Architekturbild erfüllt. Der Patient und der Behandler können direkt über die ePA bzw. das Arztinformationssystem Daten im Rahmen der Versorgung austauschen. Daten, die für Forschungsfragen interessant sind, werden von der ePA über die Forschungsschnittstelle an die Versorgungsdatenbank übertragen.

Die dritte Voraussetzung betrifft nicht direkt die Gesamtarchitektur. Diese Voraussetzung wird im Anwendungsfall UC-1-1 „Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler“ wieder aufgenommen.

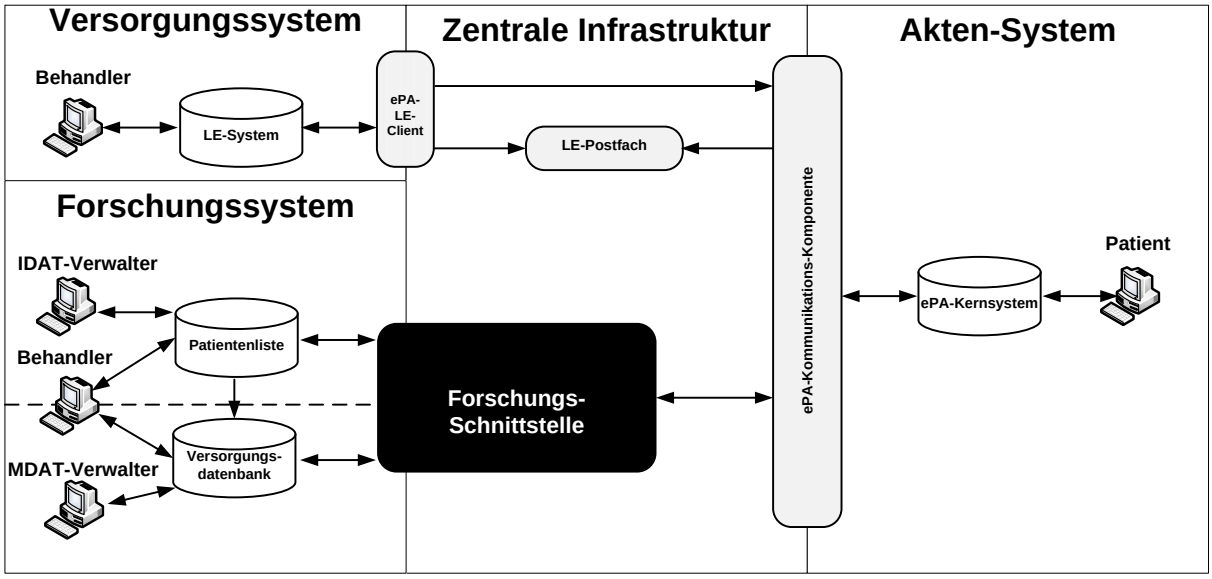

Abbildung 18: Einordnung der Forschungsschnittstelle in die Gesamtarchitektur

6.2. Anbindung einer Patientenliste an eine ePA

Im Folgenden wird die Kommunikation der ausgewählten Anwendungsfälle der Patientenliste analysiert und beschrieben, wie diese Kommunikation über die oben skizzierte Architektur mit Hilfe einer ePA umgesetzt werden kann und welche Anforderungen sich daraus an das ePA-System, die Patientenliste und die Forschungsschnittstelle ergeben.

6.2.1. Anmeldung eines Patienten an einem Forschungsverbund

Die Anmeldung eines Patienten beim Versorgungsmodul weicht etwas von der Anmeldung eines Patienten an einer Studiendatenbank ab. Grund hierfür ist die Notwendigkeit, das Pseudonym (PIDv) des Patienten dem behandelnden Arzt nicht zu offenbaren. Da der Behandler den Patienten im Gegensatz zum Studienarzt nicht mit seinem Pseudonym, sondern mit seinen identifizierenden Daten im Versorgungsmodul aufruft (siehe Anwendungsfall UC-3-1 Erfassung und Zugriff auf Daten im Behandlungsprozess) ist die Offenbarung des Pseudonyms gegenüber dem Behandler auch nicht notwendig.

Ablauf: Bei der Anmeldung des Patienten am Versorgungsmodul teilt der Patient dem Behandler seine identifizierenden bzw. Kontaktdaten mit. Der Behandler trägt die Daten des Patienten in die Patientenliste ein. Die Patientenliste bestätigt dem Behandler die Anmeldung. Der Behandler übergibt dem Patienten Informationen zum Versorgungsmodul und zum Forschungsverbund. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.3.1 [33,34].

Austausch von Informationen: Der Patient erhält somit bei diesem Anwendungsfall Informationen über den Forschungsverbund, Patienteninformationen, Bestätigung der Anmeldung (Info01) und übermittelt dem Forschungsverbund seine identifizierenden bzw. seine Kontaktdaten (Info02).

Analyse: Da die ePA vor der Anmeldung noch nicht für die Kommunikation mit der Patientenliste konfiguriert ist (vergleiche Voraussetzung 3), können die identifizierenden Daten des Patienten (Info02) nicht über die ePA bereitgestellt werden. Somit bleibt die Kommunikation wie gehabt. Um eine Kommunikation mit der ePA nach der Anmeldung zu ermöglichen, müssen neben den identifizierenden Daten und den Kontaktdaten auch die

Daten zur Kommunikation mit einer ePA in der Patientenliste hinterlegt werden (siehe auch VF03). Ebenfalls werden in dem Anwendungsfall nach der Anmeldung Informationen über den Forschungsverbund, eine für den Patienten angefertigte Kopie der Patienteninformationen und eine Bestätigung der Anmeldung dem Patienten durch den Behandler übergeben (Info01). Nach einer erfolgreichen Anmeldung des Patienten an einem Forschungsverbund kann die Patientenliste nun mit Hilfe der hinterlegten Daten zur Kommunikation mit der ePA des Patienten eine Anmeldebestätigung an die ePA des Patienten schicken. Diese Nachricht muss sowohl die Informationen zur Kommunikation mit den medizinischen Datenbanken für das ePA-System als auch Informationen für den Patienten über den Forschungsverbund, Ansprechpartner etc. enthalten (I-1). Dadurch, dass die Informationen für den Patienten direkt aus der Patientenliste an die ePA des Patienten geschickt werden, kann hier ein Medienbruch verhindert werden. Die Kommunikation zwischen dem Patienten und dem Forschungsverbund wird hier nicht verbessert, da die Informationen vorher schon dem Patienten direkt vom Behandler übergeben werden. Die ePA muss in der Lage sein, die Informationen für die Kommunikation mit den Datenbanken eines Forschungsverbundes zu verwalten (siehe auch VE00), um im Rahmen des Forschungsvorhabens mit den Datenbanken des Forschungsverbundes kommunizieren zu können. Spezielle Anforderungen an die Forschungsschnittstelle ergeben sich nicht. Es wurden keine speziellen Datenschutzanforderungen identifiziert, die sich aus der direkten Kommunikation mit einer ePA nach § 291a ergeben.

6.2.2. Kontaktieren eines Patienten

Das Kontaktieren eines Patienten kann je nach Art der Informationen entweder durch den Verwalter der Patientenliste oder durch den behandelnden Arzt erfolgen. Im Rahmen des Versorgungsmoduls sind beide Varianten vorstellbar. Im Folgenden wird das Kontaktieren durch den Verwalter der Patientenliste beschrieben und analysiert. Das Kontaktieren durch einen behandelnden Arzt wird im Anwendungsfall der Versorgungsdatenbank „Informieren eines Patienten über Forschungsergebnisse“ (6.3.5) beschrieben.

Ablauf: Zum Kontaktieren des Patienten ruft der Verwalter der Patientenliste die Kontaktdaten des Patienten aus der Patientenliste ab. Der Verwalter der Patientenliste erstellt die Nachricht mit den Kontaktdaten und übermittelt die Nachricht an den Patienten (meistens per Brief, sollten viele Patienten kontaktiert werden, per Serienbrief). Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.3.2 [33,34].

Austausch von Informationen: Bei diesem Anwendungsfall werden dem Patienten allgemeine Ergebnisse aus Studien, Informationen über neue Forschungsprojekte, persönliche Nachrichten an den Patienten, Newsletter, eine aktualisierte Liste der Ärzte, die am Expertenforum teilnehmen etc. übermittelt (Info03). Der Patient stellt dem Forschungsverbund bei diesem Anwendungsfall keine Informationen bereit.

Analyse: Bei der Übermittlung der Informationen an den Patienten (Info03) sind nur der Verwalter der Patientenliste und der Patient beteiligt. Hier gibt es in Bezug auf die Kommunikation kein Optimierungspotential. Allerdings kann durch eine direkte Kommunikation zwischen der ePA und der Patientenliste ein Medienbruch verhindert werden. Das geschieht beispielsweise, wenn der Forschungsverbund Patienten Erinnerungen an Visiten oder zum Ausfüllen von Fragebögen nicht wie üblich über einen Serienbrief, sondern direkt über die ePA schickt. Der Verwalter der Patientenliste schickt direkt eine Nachricht von der

Patientenliste an die ePA des Patienten (I-2). Der Patient muss für die Kontaktierung eingewilligt haben. Diese Einwilligung kann auch abgestuft erfolgt sein, d. h. er möchte z. B. über neue Forschungsprojekte informiert werden, aber nicht über individuelle Forschungsergebnisse. Es muss eine Überprüfung der Einwilligung erfolgen, bevor ein Patient kontaktiert wird. Da diese Funktionalität in mehreren Anwendungsfällen gefordert wird (siehe Anwendungsfälle UC-2-3 und UC-2-5) und auch die Versorgungsdatenbank betrifft, wird hier festgelegt, dass diese Prüfung zentral durch die Forschungsschnittstelle erfolgen soll (A09). Das hat den Vorteil, dass nicht jede Datenbank Informationen zu den Einwilligungen der Patienten abbilden und überprüfen muss. Spezielle Anforderungen an das ePA- und an das Forschungssystem ergeben sich nicht. Die spezielle Datenschutzanforderung zur Überprüfung des Einwilligungsstatus wird von der Forschungsschnittstelle umgesetzt.

6.2.3. Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten

Der Patient kann sich direkt beim Forschungsverbund bzw. dem Verwalter der Patientenliste melden und seine Kontaktdaten aktualisieren lassen oder der Behandler stellt bei einer Visite fest, dass die Kontaktdaten des Patienten nicht mehr aktuell sind. Der Patient bzw. der Arzt übermittelt diese Kontaktdaten dem Verwalter der Patientenliste, der dann eine Aktualisierung dieser Daten in der Patientenliste durchführt. Im Folgenden wird die erste Variante betrachtet.

Ablauf: Bei diesem Anwendungsfall übermittelt der Patient dem Verwalter der Patientenliste die neuen Kontaktdaten und der Verwalter der Patientenliste aktualisiert die Kontaktdaten des Patienten in der Patientenliste. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.3.3[12].

Austausch von Informationen: Dem Patienten werden bei diesem Anwendungsfall keine Informationen übermittelt. Der Patient übermittelt dem Forschungsverbund seine identifizierenden bzw. seine Kontaktdaten (Info04).

Analyse: Bei der Übermittlung der Informationen durch den Patienten (Info04) sind nur der Patient und der Verwalter der Patientenliste beteiligt, d. h. hier besteht schon eine direkte Kommunikation zwischen dem Patienten und dem Verwalter der Patientenliste, so dass die Aktualisierung der Kontaktdaten durch einen Patienten direkt durch eine Übertragung der Informationen aus der ePA an die Patientenliste erfolgen kann (I-3). Dadurch, dass dem Patienten nun die Option ermöglicht wird, über seine ePA der Patientenliste Daten zu schicken, muss weiterhin sichergestellt werden, dass die Patientenliste nur Daten erhält, die auch für diesen Anwendungsfall notwendig sind. D. h. die Forschungsschnittstelle muss sicherstellen, dass der Patient der Patientenliste über seine ePA nur seine Kontaktdaten bzw. identifizierenden Daten bereitstellen kann (A10). Der Vorteil der Umsetzung dieses Anwendungsfalls über eine ePA liegt hier in der medienbruchfreien Kommunikation. Der Verwalter der Patientenliste und der Patient kommunizieren schon direkt miteinander, so dass hier die Kommunikation nicht vereinfacht werden kann. Neue Anforderungen an das ePA- oder das Forschungssystem ergeben sich nicht.

[12] Der Anwendungsfall war in der Version des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - noch nicht aufgenommen und stammt aus der Analyse der Datenschutzkonzepte der medizinischen Forschungsverbünde. Daher gibt es an dieser Stelle keine Quelle aus den TMF Datenschutzkonzepten.

6.2.4. Recht des Patienten auf Auskunft über die Daten in der Patientenliste

Bei diesem Anwendungsfall wird nur das Auskunftsrecht in Bezug auf die Patientenliste betrachtet. Der Patient hat die Möglichkeit sein Auskunftsrecht über seinen behandelnden Arzt oder direkt über den Forschungsverbund wahrzunehmen. Im Folgenden wird die zweite Variante beschrieben, da hier eine direktere Kommunikation zwischen dem Patienten und dem Forschungsverbund stattfindet.

Ablauf: Bei diesem Anwendungsfall kontaktiert der Patient gemäß seinem Recht den Ansprechpartner des Forschungsverbundes und verlangt Auskunft. Der Ansprechpartner des Forschungsverbundes fordert die Daten des Patienten beim Verwalter der Patientenliste an. Der Verwalter der Patientenliste ruft die Daten aus der Patientenliste und leitet die Daten an den Ansprechpartner des Forschungsverbundes weiter. Der Ansprechpartner des Forschungsverbundes händigt die Daten dem Patienten aus. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.3.4 [33,34].

Austausch von Informationen: Dem Patienten werden bei diesem Anwendungsfall die in der Patientenliste über ihn gespeicherten Daten bereitgestellt (z. B. identifizierende Daten des Patienten, den Einwilligungsstatus, seine Adresse, sein behandelndes Zentrum etc.) (Info05). Der Patient übermittelt dem Forschungsverbund eine Anfrage nach Auskunft (Info06).

Analyse: Bei diesem Anwendungsfall erfolgt die Kommunikation zwischen dem Patienten und dem Ansprechpartner des Forschungsverbundes. Der Ansprechpartner des Forschungsverbundes dient dem Patienten in diesem Anwendungsfall als Ansprechpartner. Er hat die Aufgabe, den Patienten eindeutig zu identifizieren und zu überprüfen, welche Daten angefordert werden müssen, um dem Recht des Patienten nach Auskunft nachzukommen. Er muss die entsprechenden Anfragen an den oder die Datenbank-Verwalter weiterleiten und überreicht dem Patienten anschließend das Ergebnis dieser Anfrage. Des Weiteren muss der Ansprechpartner des Forschungsverbundes einschätzen, ob diese Daten dem Patienten mit oder ohne weitere Erklärungen durch medizinisches Fachpersonal ausgehändigt werden können. Wird nun eine Optimierung durch eine direkte Kommunikation zwischen einer ePA und der Patientenliste eines Forschungsverbundes angestrebt, so muss sichergestellt werden, dass diese Aufgaben des Ansprechpartners des Forschungsverbundes trotzdem erfüllt werden und ggf. entsprechende Anforderungen an die Systeme gestellt werden. Unter diesen Voraussetzungen kann der Patient über seine ePA eine direkte Auskunftsanfrage an den Verwalter der Patientenliste stellen (I-4) (Info06) und der Verwalter der Patientenliste kann die über den Patienten gespeicherten Daten direkt aus der Patientenliste an die ePA des Patienten schicken (I-5) (Info05). Da es sich hier um Kontaktdaten und ggf. organisatorische Daten handelt (z. B. an welchen Projekten der Patient teilnimmt), können diese Daten dem Patienten ohne weitere Erklärung durch medizinisches Fachpersonal zugänglich gemacht werden. Die Zuordnung der Daten zum Patienten, die sonst durch den Ansprechpartner des Forschungsverbundes erfolgt, wird nun durch die Forschungsschnittstelle umgesetzt (wie im Kapitel 6.1.2 unter Punkt 3 beschrieben). Durch entsprechende Authentifizierungsmechanismen in der ePA und der Zuordnung der Identität des Patienten in der ePA zu der Identität im Versorgungsmodul kann eindeutig festgestellt werden, dass die Anfrage des Patienten authentisch ist. Da bei der direkten Kommunikation zwischen der Patientenliste und der ePA der Ansprechpartner des Forschungsverbundes wegfällt, gibt es keine Instanz mehr, die im Sinne einer Autorisierung zuordnet, welche Daten der Patient im Rahmen des Auskunftsrechts einsehen darf. Diese

Funktion ist in diesem Kontext nicht notwendig, da vorher festgestellt wurde, dass der Patient alle über ihn in der Patientenliste gespeicherten Daten ohne weitere Voraussetzungen bekommen kann. Neben der Optimierung der Kommunikation ist durch die direkte Kommunikation mit der ePA auch ein medienbruchfreier Austausch der Informationen möglich. Weitere Anforderungen an die Forschungsschnittstelle, das Forschungssystem oder das ePA-System ergeben sich nicht.

6.2.5. Rückzug der Einwilligung für die Teilnahme an einem Forschungsverbund

Der Patient kann sich bezüglich des Rückzugs seiner Einwilligungserklärung an seinen behandelnden Arzt oder direkt an den Forschungsverbund wenden. Es wird die zweite Variante ausgewählt, da hier eine direktere Kommunikation zwischen dem Patienten und dem Forschungsverbund stattfindet. Im Folgenden wird der Rückzug der Einwilligung über einen Forschungsverbund verbunden mit der Löschung aller Daten des Patienten aus der Patientenliste und der Versorgungsdatenbank beschrieben und analysiert.

Ablauf: Der Patient kontaktiert zum Rückzug seiner Einwilligung den Ansprechpartner des Forschungsverbundes. Der Ansprechpartner des Forschungsverbundes beauftragt den Verwalter der Patientenliste mit dem Löschen der Daten des Patienten in der Patientenliste. Der Verwalter der Patientenliste führt den Löschvorgang der Daten des Patienten in der Patientenliste durch. Die Patientenliste übermittelt dem Verwalter der Versorgungsdatenbank einen Löschauftrag mit dem Pseudonym, unter dem der Patient in der Versorgungsdatenbank geführt wird. Die Patientenliste löscht die Daten des Patienten. Die Patientenliste bestätigt dem Verwalter der Patientenliste die Löschung. Der Verwalter der Patientenliste leitet die Bestätigung der Löschung an den Ansprechpartner des Forschungsverbundes weiter. Der Verwalter der Versorgungsdatenbank löscht die Daten zu dem Pseudonym in der Versorgungsdatenbank. Der Verwalter der Versorgungsdatenbank leitet die Bestätigung an den Ansprechpartner des Forschungsverbundes weiter. Der Ansprechpartner des Forschungsverbundes händigt die Bestätigung der Löschung dem Patienten aus[13]. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.3.5 [33,34].

Austausch von Informationen: Der Patient übermittelt dem Forschungsverbund bei diesem Anwendungsfall den Auftrag zur Löschung seiner Daten (Info07). Dem Patienten wird die Bestätigung der Löschung übermittelt ggf. wird er auf eine Anonymisierung der Daten hingewiesen, sofern die Daten wegen gesetzlicher o. ä. Aufbewahrungs- und Archivierungspflichten nicht gelöscht werden konnten (Info08).

Analyse: Der Rückzug einer Einwilligungserklärung betrifft immer die Patientenliste. Beim Rückzug der Einwilligung für den Forschungsverbund müssen alle Daten des Patienten aus der Patientenliste gelöscht werden. Beim Rückzug aus einem Forschungsvorhaben muss das Pseudonym des Patienten, unter dem er im Forschungsvorhaben geführt wurde, aus der Patientenliste entfernt werden. Aus diesem Grund wird in dieser Arbeit festgelegt, dass der Rückzug jeder Einwilligungserklärung über die ePA zentral an die Patientenliste erfolgt und von dort weiter geleitet wird. Die ursprüngliche Kommunikation sieht vor, dass der Patient sich an den Ansprechpartner des Forschungsverbundes wendet, und der Ansprechpartner des Forschungsverbundes die Löschung beim Verwalter der Patientenliste beauftragt. Auch

[13] Wegen gesetzlicher o. ä. Aufbewahrungs- und Archivierungspflichten können u. U. nicht alle Daten gelöscht werden. Evtl. muss in diesen Fällen eine Anonymisierung anstatt einer Löschung vorgenommen werden.

hier kann eine direkte Kommunikation unter den im Abschnitt 6.2.4 genannten Voraussetzungen zwischen dem Patienten und dem Verwalter der Patientenliste ohne den Ansprechpartner des Forschungsverbundes erfolgen. Dabei muss ebenfalls nur eine Authentifizierung des Patienten über die ePA erfolgen. Eine Autorisierung ist nicht notwendig, da der Patient jederzeit das Recht hat, alle über ihn im Forschungsverbund gespeicherten Daten löschen zu lassen. Der Patient schickt hierzu über seine ePA den Auftrag zur Löschung seiner Daten aus dem gesamten Forschungsverbund oder aus einem Forschungsvorhaben an den Verwalter der Patientenliste (I-6) (Info07). Wenn der Patient den Rückzug aus allen Forschungsvorhaben beantragt, wird ein Löschungsauftrag der Daten des Patienten im Versorgungsmodul mit dem entsprechenden Pseudonym des Patienten an den Verwalter der Versorgungsdatenbank weitergeleitet. Danach werden die Daten in der Versorgungsdatenbank gelöscht und dem Verwalter der Patientenliste wird eine Bestätigung des Löschvorganges geschickt. Anschließend löscht der Verwalter der Patientenliste die Daten des Patienten in der Patientenliste. Sollte nur der Rückzug aus einem Forschungsvorhaben beantragt werden, löscht der Verwalter der Patientenliste nach der Bestätigung des Löschvorgangs in der Versorgungsdatenbank nur das Pseudonym, unter dem der Patient in der Patientenliste für das Forschungsvorhaben geführt wird. In beiden Fällen schickt der Verwalter der Patientenliste dem Patienten abschließend die Bestätigung des gesamten Löschvorganges an seine ePA (I-7) (Info08).

Neben der Optimierung der Kommunikation ist durch die direkte Kommunikation mit der ePA auch ein medienbruchfreier Austausch der Informationen zwischen dem Patienten und dem Forschungsverbund möglich. Die ePA muss dem Patienten die Möglichkeit bieten, dass er seinen Rückzug der Einwilligung differenziert formulieren kann (z. B. Rückzug aus einem Forschungsvorhaben oder Rückzug aus dem ganzen Forschungsverbund) (VE01). Spezielle Anforderungen an die Forschungsschnittstelle ergeben sich nicht. Es wurden keine weiteren speziellen Datenschutzanforderungen identifiziert, die sich aus der direkten Kommunikation mit einer ePA nach § 291a ergeben.

6.2.6. Zusammenfassung der Kommunikation

In der nachfolgenden Tabelle sind die für jeden Anwendungsfall der Patientenliste analysierten Informationsflüsse zusammenfassend dargestellt:

Nr.	Anwendungsfall	Empfänger	Bereitsteller	Empfangendes System	Bereitstellendes System	Informationsaustausch
I-1	Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler	Patient	Verwalter Patientenliste	ePA	Patientenliste	Info01
I-2	Kontaktieren eines Patienten über den Verwalter der Patientenliste	Patient	Verwalter Patientenliste	ePA	Patientenliste	Info03
I-3	Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten	Verwalter Patientenliste	Patient	Patientenliste	ePA	Info04

Nr.	Anwendungsfall	Empfänger	Bereitsteller	Empfangendes System	Bereitstellendes System	Informationsaustausch
I-4	Recht des Patienten auf Auskunft über die Daten in der Patientenliste	Verwalter Patientenliste	Patient	Patientenliste	ePA	Info06
I-5	Recht des Patienten auf Auskunft über die Daten in der Patientenliste	Patient	Verwalter Patientenliste	ePA	Patientenliste	Info05
I-6	Rückzug der Einwillligung für die Teilnahme an einem Forschungsverbund	Verwalter Patientenliste	Patient	Patientenliste	ePA	Info07
I-7	Rückzug der Einwilligung für die Teilnahme an einem Forschungsverbund	Patient	Verwalter Patientenliste	ePA	Patientenliste	Info08

Tabelle 10: Zusammenfassung der Kommunikationsmuster der Patientenliste

Aus der Zusammenfassung der Informationsflüsse ergeben sich zwei generische Kommunikationsmuster:

1. **Informationen aus einer Patientenliste einer ePA bereitstellen:** Der Verwalter der Patientenliste stellt über die Patientenliste der ePA des Patienten Informationen für den Patienten bereit. Durch dieses generische Kommunikationsmuster können die Kommunikationsvorgänge I-1, I-2, I-5 und I-7 umgesetzt werden.
2. **Informationen aus einer ePA einer Patientenliste bereitstellen:** Der Patient stellt über seine ePA dem Verwalter der Patientenliste Informationen für die Patientenliste bereit. Über dieses generische Kommunikationsmuster können die Kommunikationsvorgänge I-3, I-4 und I-6 umgesetzt werden.

6.3. Anbindung einer Versorgungsdatenbank an eine ePA

Nachdem alle Anwendungsfälle der Patientenliste analysiert wurden, wird jetzt die Kommunikation der ausgewählten Anwendungsfälle der Versorgungsdatenbank analysiert und beschrieben, wie diese Kommunikation über die in der Abbildung 18 skizzierte Architektur mit Hilfe einer ePA umgesetzt werden kann und welche Anforderungen sich daraus an das ePA-System, die Versorgungsdatenbank und die Forschungsschnittstelle ergeben.

6.3.1. Aufnahme in die Versorgungsdatenbank

Dieser Anwendungsfall wird durch eine Kombination der Anwendungsfälle „Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler“ (siehe Abschnitt 6.2.1) und „Erfassung und Zugriff auf Daten im Behandlungsprozess“ (siehe Abschnitt 6.3.2) umgesetzt und muss hier nicht weiter analysiert werden.

6.3.2. Erfassung und Zugriff auf Daten im Behandlungsprozess bzw. durch einen Patienten

Es können sowohl der Behandler als auch der Patient Daten in die Versorgungsdatenbank eintragen. Im Folgenden wird die Kommunikation bei der Erfassung und Zugriff auf Daten durch den Behandler im Behandlungsprozess und anschließend die Erfassung und der Zugriff durch den Patienten von Zuhause beschrieben und anschließend beide Varianten gemeinsam analysiert:

Ablauf (Erfassung und Zugriff auf Daten durch den Behandler im Behandlungsprozess): Der Behandler übermittelt die identifizierenden Daten des Patienten an die Patientenliste. Die Patientenliste generiert ein temporäres Pseudonym auch Ticket (TKT) genannt. Die Patientenliste übermittelt dem Behandler das TKT. Die Patientenliste übermittelt das TKT und das Pseudonym des Patienten an die Versorgungsdatenbank. Die Versorgungsdatenbank ordnet das Pseudonym dem Datensatz des Patienten zu. Der Behandler ruft mit dem TKT den Datensatz des Patienten aus der Versorgungsdatenbank ab. Die Versorgungsdatenbank übermittelt dem Behandler den Datensatz des Patienten. Der Behandler befragt bzw. untersucht den Patienten. Der Patient beantwortet dem Behandler die Fragen. Der Behandler trägt die neuen Daten des Patienten in der Versorgungsdatenbank ein. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.4.1 [33,34].

Austausch von Informationen (Erfassung und Zugriff auf Daten durch den Behandler im Behandlungsprozess): Dem Patienten werden bei diesem Anwendungsfall keine Informationen mitgeteilt. Dem Behandler werden die aktuellen Daten des Patienten aus der Versorgungsdatenbank angezeigt. Der Behandler teilt dem Forschungsverbund medizinische Daten des Patienten z. B. Befunde, Bilder, Medikation, vom Patienten bereitgestellte Daten wie z. B. Blutzuckerwerte, Lebensqualität etc. mit (Info09).

Ablauf (Erfassung und der Zugriff durch den Patienten von Zuhause): Der Patient übermittelt seine identifizierenden Daten an die Patientenliste. Die Patientenliste generiert ein temporäres Pseudonym (TKT). Die Patientenliste übermittelt dem Patienten das TKT. Die Patientenliste übermittelt das TKT und das Pseudonym des Patienten an die Versorgungsdatenbank. Die Versorgungsdatenbank ordnet es anhand des Pseudonyms dem Datensatz des Patienten zu. Der Patient ruft mit dem TKT den Datensatz des Patienten aus der Versorgungsdatenbank ab. Die Versorgungsdatenbank übermittelt dem Patienten seine Daten. Der Patient trägt die neuen Daten in der Versorgungsdatenbank ein. Die Versorgungsdatenbank löscht das TKT zu dem Patienten wieder. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.4.1[33,34].

Austausch von Informationen (Erfassung und der Zugriff durch den Patienten von Zuhause): Der Patient teilt dem Forschungsverbund medizinische Daten (z. B. Blutzuckerwerte, Lebensqualität etc.) mit (Info10). Dem Patienten werden die bisher vom Patienten eingetragenen Daten im Versorgungsmodul angezeigt (Info11).

Analyse (beider Varianten): Durch die Anbindung einer ePA an das Versorgungsmodul kann die Bereitstellung und Anforderung von medizinischen Daten des Patienten im Rahmen der Behandlung über die ePA-Infrastruktur umgesetzt werden (wie in der Voraussetzung 5 beschrieben). Der Patient kann über seinen Bürgerclient selbst erhobene Daten für die Versorgung (z. B. Daten zur Lebensqualität) bereitstellen. Der behandelnde Arzt kann Daten

aus der ePA abrufen bzw. dem Patienten über sein Arztinformationssystem Daten für die ePA bereitstellen, die der Patient anderen Behandlern über seine ePA verfügbar machen kann.

Sind die Daten auch für die wissenschaftliche Auswertung interessant bzw. vorgesehen, so können diese Daten vom Patienten über die ePA an die Versorgungsdatenbank geschickt werden (I-8) (Info09 und Info10). Die bisher vom Patienten in die Versorgungsdatenbank eingetragenen Daten müssen dem Patienten nicht übertragen und angezeigt werden (Info11), da sich diese Daten auch in der ePA befinden und auch nur dort angezeigt und bearbeitet werden. Die Versorgungsdatenbank enthält immer nur Kopien des Datenbestandes der ePA des Patienten.

Durch die oben geschilderte Nutzung der ePA in Verbindung mit dem Versorgungsmodul ist es sinnvoll, dass Daten, die für die Versorgung und die Forschung vorgesehen sind, gleich automatisch durch die ePA an das Versorgungsmodul weitergeleitet werden. Der Patient könnte diese Daten auch manuell weiterleiten, allerdings erscheint das etwas unkomfortabel. Die ePA sollte es ermöglichen, Regeln zu hinterlegen, in denen eine automatische Weiterleitung der Daten aus der Versorgung an das Versorgungsmodul definiert werden können (VE02). Hierbei ist zu beachten, dass durch die direkte Anbindung der ePA an die Versorgungsdatenbank nur Daten für Forschungsvorhaben, in die der Patient eingewilligt hat, ausgetauscht werden dürfen. Daher muss die Forschungsschnittstelle sicherstellen, dass der Patient der Versorgungsdatenbank nur Daten bereitstellt, die auch im Rahmen des Forschungsvorhabens benötigt werden und für die eine Einwilligung des Patienten vorliegt (A11).

Eine Optimierung der Kommunikation erfolgt bei diesem Anwendungsfall nicht. Allerdings kann durch die direkte Einbindung der Arztinformationssysteme eine zusätzliche Erfassung im Versorgungsmodul verhindert werden und somit eine medienbruchfreie Kommunikation zwischen den beiden Systemen erfolgen. Anforderungen an das Forschungssystem ergeben sich nicht.

6.3.3. Vergabe von Zugriffsrechten

Dieser Anwendungsfall muss in Verbindung mit einer ePA nicht weiter betrachtet werden, da wie oben festgelegt wurde, die Kommunikation der medizinischen Daten für die Behandlung direkt über die ePA erfolgt und die ePA dem Patienten die Möglichkeit anbietet, Zugriffsrechte individuell zu vergeben. Der Zugriff auf die Daten des Versorgungsmoduls erfolgt somit nur noch für wissenschaftliche Auswertungen und das Expertenforum. Diese Zugriffsrechte werden nicht direkt durch den Patienten gesteuert.

6.3.4. Rekrutierung von Patienten

Im Folgenden wird die Rekrutierung von Patienten mit anschließender Kontaktaufnahme durch den Verwalter der Patientenliste beschrieben und analysiert.

Ablauf: Der Forscher identifiziert potentielle Patienten für ein neues Forschungsvorhaben in der Versorgungsdatenbank und formuliert für diese Patienten eine Rekrutierungsanfrage, die er dem Verwalter der Versorgungsdatenbank übermittelt. Der Verwalter der Versorgungsdatenbank leitet die Liste mit den Pseudonymen der zu rekrutierenden Patienten an den Verwalter der Patientenliste weiter. Der Verwalter der Patientenliste leitet für diese Patienten die Kontaktierung ein (siehe UC-1-2). Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.4.2 [34].

Austausch von Informationen: Der Patient teilt dem Forschungsverbund keine Informationen mit. Dem Patienten werden Informationen zum Forschungsvorhaben und die Anfrage zur Teilnahme vom Forschungsverbund mitgeteilt (Info12).

Analyse: Bei der Übermittlung der Informationen durch den Behandler (Info12) an den Patienten ist ursprünglich vorgesehen, dass die Pseudonyme der zu rekrutierenden Patienten vom Verwalter der Versorgungsdatenbank an den Verwalter der Patientenliste zur Kontaktierung weitergeleitet werden. Durch die Möglichkeit einer direkten Kommunikation zwischen der Versorgungsdatenbank und den ePAs der Patienten kann der Verwalter der Versorgungsdatenbank die Patienten direkt kontaktieren (I-9). Die datenschutzkonforme Depseudonymisierung wird in diesem Fall durch die Forschungsschnittstelle übernommen (Vergleiche Abschnitt 6.1.2). Eine direkte Kommunikation zwischen dem Forscher und dem Patienten ist nicht vorgesehen, so dass mit dem Verwalter der Versorgungsdatenbank immer noch eine Kontrollinstanz vorhanden ist, die die Kontaktierung autorisieren muss (z. B. nach einem Beschluss und Anweisung des Ausschusses Datenschutz). Neben der Optimierung der Kommunikation wird hier auch wieder wie beim Anwendungsfall „Kontaktierung durch den Verwalter der Patientenliste“ ein Medienbruch verhindert (es erfolgt keine Benachrichtigung per Serienbrief).

Eine Kontaktaufnahme zum Zwecke der Rekrutierung bedarf der Einwilligung des Patienten. Daher muss die Forschungsschnittstelle, wie im Anwendungsfall zur Kontaktierung, auch hier überprüfen, ob der Patient eingewilligt hat, dass er zwecks Rekrutierung kontaktiert werden darf (A12). Spezielle Anforderungen an das ePA-System oder das Forschungssystem ergeben sich nicht.

6.3.5. Informieren eines Patienten über Forschungsergebnisse

Bei diesem Anwendungsfall ist eine direkte Kontaktierung des Patienten durch seinen behandelnden Arzt mit anschließender Erklärung der Forschungsergebnisse vorgesehen, die im Folgenden beschrieben wird:

Ablauf: Der Forscher übermittelt dem Ausschuss Datenschutz neue Forschungserkenntnisse und die Pseudonyme (EX-PIDs), unter denen die Patienten im Export des Forschers geführt werden. Der Ausschuss Datenschutz gibt die Depseudonymisierung nach einer erfolgreichen Beratung frei. Hierzu übermittelt der Ausschuss Datenschutz dem Verwalter der Versorgungsdatenbank die EX-PID und eine Vorgangsnummer. Der Verwalter der Versorgungsdatenbank fordert unter Angabe der EX-PID die PID des Patienten von der Versorgungsdatenbank an. Der Verwalter des Versorgungsmoduls leitet die PID und die Vorgangsnummer an den Verwalter der Patientenliste weiter. Der Verwalter der Patientenliste fordert die identifizierenden Daten des Patienten und die Kontaktdaten des behandelnden Arztes zu der PID von der Patientenliste an und übermittelt die identifizierenden Daten des Patienten sowie die Vorgangsnummer an den behandelnden Arzt mit der Bitte, den Ausschuss Datenschutz zu kontaktieren. Der behandelnde Arzt fordert die neuen Forschungserkenntnisse anhand der Vorgangsnummer beim Ausschuss Datenschutz an. Der Ausschuss Datenschutz übermittelt dem behandelnden Arzt die neuen Forschungserkenntnisse zu seinem Patienten. Der behandelnde Arzt informiert den Patienten über die neuen Forschungserkenntnisse. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.4.3 [33].

Austausch von Informationen: Der Patient teilt dem Forschungsverbund keine Informationen mit. Dem Patienten werden neue Forschungserkenntnisse vom Forschungsverbund mitgeteilt (Info13).

Analyse: Bei diesem Anwendungsfall sind der Forscher, der Ausschuss Datenschutz, der Verwalter der Versorgungsdatenbank und der Patientenliste, der behandelnde Arzt und der Patient beteiligt. Eine direkte Kommunikation der neuen Forschungsergebnisse (Info13) durch den Forscher an den Patienten über seine ePA ist in diesem Fall nicht möglich, da eine Genehmigung vom Ausschuss Datenschutz vorliegen muss, bevor ein Patient informiert werden kann. Hierbei sollte nicht nur entschieden werden, ob der Patient informiert werden soll sondern auch, ob diese Informationen über einen Arzt (wegen ethischer Gründe oder gesetzlicher Vorschriften[14]) oder direkt mitgeteilt werden können.

Im ersten Fall kann der Patient direkt vom Verwalter der Versorgungsdatenbank über seine ePA informiert werden, dass Informationen für ihn vorliegen und dass sich sein behandelnder Arzt beim Forschungsverbund melden soll. Neben diesem Schreiben wird dem Patienten auch die Vorgangsnummer mitgeteilt, unter der der Arzt die Informationen abrufen kann (I-10). Die Depseudonymisierung wird über die Forschungsschnittstelle durchgeführt, so dass hier eine direkte und datenschutzkonforme Kommunikation zwischen dem Verwalter der Versorgungsdatenbank und dem Patienten erfolgen kann. Das Abrufen der Daten durch den behandelnden Arzt verläuft dann wie bisher. Dieses Verfahren würde die Kommunikation mit dem Patienten optimieren und hätte den Vorteil, dass der Patient seinen behandelnden Arzt selbst auswählen kann und auch der Patient kontaktiert werden kann, wenn die Informationen über seinen behandelnden Arzt nicht vorhanden bzw. veraltet sind. Bei der Übertragung der Information, dass neue Ergebnisse vorliegen, erfolgt eine optimierte, medienbruchfreie Kommunikation. Die medizinischen Daten (Forschungsergebnisse) werden, wie gehabt, auf dem herkömmlichen Weg kommuniziert. Hier findet weder eine Optimierung der Kommunikation noch eine medienbruchfreie Kommunikation statt.

Im zweiten Fall können die Forschungsergebnisse vom Verwalter der Versorgungsdatenbank direkt an die ePA des Patienten geschickt werden (I-10). Da die Depseudonymisierung über die Forschungsschnittstelle erfolgt, bleiben dem Verwalter der Versorgungsdatenbank die identifizierenden Daten verborgen, obwohl eine direkte Kommunikation mit dem Patienten erfolgt. Hier wird nicht nur die Kommunikation optimiert, sondern auch eine medienbruchfreie Übertragung der medizinischen Daten ermöglicht.

In beiden Fällen muss sichergestellt werden, dass der Patient auch eingewilligt hat, dass er über die Forschungsergebnisse informiert werden darf. Diese Überprüfung wird durch die Forschungsschnittstelle übernommen (Vergleiche Anforderung aus dem Anwendungsfall „Kontaktieren eines Patienten über den Verwalter der Patientenliste“) (A13). Spezielle Anforderungen an das ePA-System oder das Forschungssystem ergeben sich nicht.

[14] Evtl. muss bei gendiagnostischen Ergebnissen ein Humangenetiker eingeschaltet werden.

6.3.6. Recht des Patienten auf Auskunft über die Daten in der Versorgungsdatenbank

Verlangt ein Patient Einsicht in die über ihn in der Versorgungsdatenbank gespeicherten Daten, so kann er sich an den Ansprechpartner des Forschungsverbundes wenden.

Ablauf: Der Patient verlangt Auskunft über seine im Versorgungsmodul gespeicherten Daten vom Ansprechpartner des Forschungsverbundes. Der Ansprechpartner des Forschungsverbundes fordert die Daten des Patienten aus der Patientenliste vom Verwalter der Patientenliste an. Der Verwalter der Patientenliste ruft die Daten des Patienten von der Patientenliste ab und leitet die Daten an den Ansprechpartner des Forschungsverbundes weiter. Der Ansprechpartner des Forschungsverbundes fordert die über den Patienten in der Versorgungsdatenbank gespeicherten Daten vom Verwalter der Versorgungsdatenbank an. Der Verwalter der Versorgungsdatenbank ruft die über dem Patienten gespeicherten Daten aus der Versorgungsdatenbank und leitet die Daten an den Ansprechpartner des Forschungsverbundes weiter. Der Ansprechpartner des Forschungsverbundes händigt die Daten dem Patienten aus. Eine detaillierte Beschreibung der Kommunikation dieses Anwendungsfalls befindet sich im Anhang A2.4.4 [33].

Austausch von Informationen: Der Patient stellt eine Anfrage zur Auskunft an den Forschungsverbund (Info14). Dem Patienten werden alle über ihn in der Versorgungsdatenbank gespeicherten Daten vom Forschungsverbund mitgeteilt (Info15).

Analyse: Bei diesem Anwendungsfall wendet sich der Patient an den Ansprechpartner des Forschungsverbundes, der die Daten zusammenstellt und sie dem Patienten aushändigt (ggf. erfolgt eine medizinische Beratung bzw. Erläuterung der Daten). Auch hier müssen die gleichen Voraussetzungen durch den Wegfall des Ansprechpartners des Forschungsverbundes berücksichtigt werden wie in Abschnitt 6.2.4 Recht des Patienten auf Auskunft. Hier muss allerdings auch eine Autorisierung durchgeführt werden, da dem Patienten ggf. bestimmte medizinische Informationen nicht direkt, sondern nur vom medizinischen Fachpersonal mit entsprechender Erklärung ausgehändigt werden dürfen. In den Fällen, in denen die Informationen nicht aus rechtlichen, ethischen oder anderen Gründen über den behandelnden Arzt mitgeteilt werden müssen, kann die Kommunikation direkt zwischen dem Verwalter der Versorgungsdatenbank und dem Patienten bzw. seiner ePA erfolgen. In dem Fall schickt der Patient über seine ePA eine Auskunftsanfrage an den Verwalter der Versorgungsdatenbank (I-11) (Info14). Der Verwalter der Versorgungsdatenbank selektiert die Daten des Patienten und schickt diese Daten über die Versorgungsdatenbank an die ePA des Patienten (I-12) (Info15). Bei beiden Kommunikationsvorgängen wird die datenschutzkonforme Pseudonymisierung bzw. Depseudonymisierung durch die Forschungsschnittstelle vorgenommen. Hier erfolgt also eine direktere und medienbruchfreie Kommunikation zwischen dem Patienten und dem Verwalter der Versorgungsdatenbank.

Sollten die Informationen nicht direkt abgerufen werden können, weil ggf. die Daten von einem Behandler erläutert und übergeben werden müssen oder der Erhalt der Daten die Studienergebnisse beeinflussen würde (z. B. bei verblindeten Studien) oder mit dem Patienten vereinbart wurde, dass er die Informationen oder Teile davon nicht wissen möchte (z. B. bei Ergebnissen von genetischen Untersuchungen), so bekommt der Patient anstatt der über ihn gespeicherten Daten eine Nachricht, dass er sich für die Einsicht direkt mit dem Forschungsverbund in Verbindung setzen soll. Hier muss durch den Forschungsverbund festgelegt werden, welche Informationen einem Patienten direkt aus der Versorgungsdatenbank bereitgestellt werden können und welche über einen behandelnden Arzt zur Verfügung gestellt werden müssen. Diese Regeln, die vorher vom Ansprechpartner des

Forschungsverbundes berücksichtigt wurden, müssen nun in der Forschungsschnittstelle abgebildet und durchgeführt werden (A14). Spezielle Anforderungen an das ePA-System oder das Forschungssystem ergeben sich nicht.

6.3.7. Rückzug der Einwilligung

Dieser Anwendungsfall wird als eine Variante im Anwendungsfall der Patientenliste zum Rückzug der Einwilligung betrachtet (siehe Abschnitt 6.2.5).

6.3.8. Zusammenfassung der Kommunikation

In der nachfolgenden Tabelle sind die einzelnen identifizierten Informationsflüsse zwischen dem Patienten und dem Behandler bzw. Verwalter der Versorgungsdatenbank zusammenfassend dargestellt:

Nr.	Anwendungs-fall	Empfänger	Bereitsteller	Empfangen-des System	Bereitstellen-des System	Informa-tionsaus-tausch
I-8	Erfassung und Zugriff auf Daten im Behandlungs-prozess	Verwalter Versorgungs-datenbank	Patient	Versorgungs-datenbank	ePA	Info09 u. Info10
I-9	Rekrutierung von Patienten	Patient	Verwalter Versorgungs-datenbank	ePA	Versorgungs-datenbank	Info12
I-10	Informieren eines Patienten über Forschungs-ergebnisse	Patient	Verwalter Versorgungs-datenbank	ePA	Versorgungs-datenbank	Info13
I-11	Recht des Patienten auf Auskunft über die Daten in der Versorgungs-datenbank	Verwalter Versorgungs-datenbank	Patient	Versorgungs-datenbank	ePA	Info14
I-12	Recht des Patienten auf Auskunft über die Daten in der Versorgungs-datenbank	Patient	Verwalter Versorgungs-datenbank	ePA	Versorgungs-datenbank	Info15

Tabelle 11: Zusammenfassung der Kommunikationsmuster der Versorgungsdatenbank

Aus der Zusammenfassung der Informationsflüsse ergeben sich zwei generische Kommunikationsmuster:

1. **Informationen aus einer ePA einer Versorgungsdatenbank bereitstellen:** Der Patient stellt über seine ePA dem Verwalter der Versorgungsdatenbank Informationen für die Versorgungsdatenbank bereit. Durch dieses generische Kommunikationsmuster können die Kommunikationsvorgänge I-8 und I-12 umgesetzt werden.
2. **Informationen aus einer Versorgungsdatenbank einer ePA bereitstellen:** Der Verwalter der Versorgungsdatenbank stellt über die Versorgungsdatenbank der ePA des Patienten Informationen für den Patienten bereit. Über dieses generische Kommunikationsmuster können die Kommunikationsvorgänge I-9 bis I-11 und I-13 umgesetzt werden.

7. Erweiterung der IT-Infrastruktur des ePA-Systems für die Kommunikation zwischen einer ePA und dem Versorgungsmodul

In diesem Kapitel wird beschrieben, wie das Kommunikationsmodell unter Berücksichtigung der Datenschutzanforderungen über eine Erweiterung der IT-Infrastruktur des ePA-Systems umgesetzt werden kann. Hierzu werden als erstes die Datenschutzanforderungen seitens des Versorgungsmoduls zusammengefasst und aus diesen Anforderungen und den in den vorherigen Kapitel herausgearbeiteten Anforderungen an die Forschungsschnittstelle (siehe Tabelle 49 im Anhang A3.5) Architekturentscheidungen abgeleitet. Anschließend wird die Architektur beschrieben und gezeigt, wie über diese Architektur die generischen Kommunikationsmuster umgesetzt werden können. Die beschriebene Umsetzung der Kommunikationsmuster dient dann als Grundlage für die im Kapitel 8 beschriebene Facharchitektur und die im Kapitel 9 beschriebene Sicherheitsarchitektur.

7.1. Datenschutzanforderungen an die Forschungsschnittstelle

In diesem Abschnitt werden neue Datenschutzanforderungen an die Forschungsschnittstelle aus dem „Teil A: Bereitstellung von Behandlungs- und Forschungsdaten in klinisch fokussierten Forschungsnetzen der Generischen Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin“ [33] abgeleitet und die in den bisherigen Kapiteln herausgestellten Datenschutzanforderungen an die Forschungsschnittstelle zusammengefasst. Die technischen Anforderungen an die Forschungsschnittstelle werden direkt bei der Herleitung der Architekturentscheidungen bzw. bei der Beschreibung der Komponenten berücksichtigt.

Bei der Kommunikation der Anwendungsfälle des Versorgungsmoduls mit Hilfe der ePA werden keine weiteren Akteure in die Kommunikation eingebunden und es wird auch keinen weiteren Administratoren Zugriff auf die Daten des Patienten gewährt. Es wird angenommen, dass das ePA-System sicher ist und durch entsprechende Mechanismen (wie z. B. eine nutzerzentrierte Verschlüsselung der Nutzdaten) [155][167] einen unbefugten Zugriff auf die Daten durch Innen- und Außentäter verhindern. Es werden die in der Sicherheitsarchitektur der LE-Schnittstelle vorgeschriebenen Mechanismen übernommen bzw. ggf. leicht angepasst, so dass seitens der ePA die Anforderungen an den Datenschutz und die Datensicherheit schon berücksichtigt sind. D. h., bei der Ableitung des Kommunikationsmodells sind nur die bestehenden Datenschutzanforderungen, die an den Betrieb eines Versorgungsmoduls gestellt werden, zu berücksichtigen. Hier wurden vier grundsätzliche Anforderungen herausgestellt, die mit entsprechenden Zitaten aus dem „Teil A: Bereitstellung von Behandlungs- und Forschungsdaten in klinisch fokussierten Forschungsnetzen der Generischen Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin“ [33] belegt werden.

> *„Anderen Personen als den behandelnden Ärzten und Laborärzten darf die Zusammenführung von identifizierenden Daten und Behandlungsdaten nicht möglich sein.“ [33, Seite 41]*

Aus diesem Zitat und der Tatsache, dass der Patient immer das Recht hat seine Daten einzusehen, ergibt sich folgende Anforderung:

- **Datenschutzanforderung 1:** Die medizinischen Daten des Patienten aus dem Versorgungsmodul dürfen nur ihm und im Behandlungszusammenhang stehenden Personen zusammen mit den identifizierenden Daten des Patienten zugänglich gemacht werden.

  „Die PID wird ausschließlich von der Patientenliste zur Behandlungsdatenbank übertragen, sie wird nicht an den behandelnden Arzt (bzw. dessen Rechner) übermittelt, sie wird ebenso nie an einen Wissenschaftler übertragen.“ [33, Seite 25]

  „Die Patientenliste beinhaltet zusätzlich eine Zufallszahl (entsprechend einem nicht rückrechenbaren Pseudonym), die genau einem individuellen Patienten eindeutig zugeordnet ist (PID). Diese PID findet sich auch in der Behandlungsdatenbank. Sie dient der Zuordnung der Datensätze von Patientenliste und Behandlungsdatenbank. Die PID ist an keiner anderen Stelle gespeichert und ist für keine Prozesse außerhalb des klinischen Datenbestandes verfügbar.“ [33, Seite 39]

Das bedeutet auch, dass die einzigen Akteure, die Zugriff auf die PID haben, die Systembetreuer der Patientenliste und der Versorgungsdatenbank sind. Diese beiden Zitate lassen sich somit in folgender Anforderung zusammenfassen:

- **Datenschutzanforderung 2**: Das Pseudonym des Patienten (PIDv) darf nur zwischen der Versorgungsdatenbank und der Patientenliste kommuniziert und auch nur dort (zwischen)gespeichert werden. Es darf nur den Systemverwaltern der Versorgungsdatenbank bzw. der Patientenliste zugänglich gemacht werden.

  „Der "klinische Datenbestand" wird aus zwei physikalisch voneinander getrennten, an unterschiedlichen Orten untergebrachten und von unabhängigen Systembetreuern verwalteten autonomen Datenbankservern zusammengeführt. Einer der Datenbankserver - die Behandlungsdatenbank - hält ausschließlich MDATw[15], der zweite Datenbankserver - die Patientenliste - hält die (von den MDATw damit vollständig getrennten) IDAT„ [33, Seite 24]

  „Als Systembetreuer wird im generischen Modell für klinisch fokussierte Forschungsnetze die Person bezeichnet die über administrative Zugriffsrechte entweder zu den Daten der Patientenliste oder zu den Daten der Behandlungsdatenbank verfügt. Patientenliste und Behandlungsdatenbank haben je einen Systembetreuer. Es muss gewährleistet sein, dass die Systembetreuer voneinander unabhängig sind.“ [33, Seite 31]

Aus der Trennung der Datenbanken und der Unabhängigkeit der Systemverwalter, können folgende Anforderungen hergeleitet werden:

- **Datenschutzanforderung 3:** Der Patientenliste bzw. ihrem Systemverwalter dürfen die medizinischen Daten der Patienten in der Versorgungsdatenbank nicht zugänglich gemacht werden.

[15] MDATw entspricht dem Begriff MDAT in dieser Arbeit.

- **Datenschutzanforderung 4:** Der Versorgungsdatenbank bzw. ihrem Systemverwalter dürfen die identifizierenden Daten des Patienten in der Patientenliste nicht zugänglich gemacht werden.

Neben den vier grundsätzlichen Datenschutzanforderungen wurden einige zusätzliche Anforderungen an den Datenschutz aufgrund spezieller Anforderungen aus den Anwendungsfällen identifiziert (siehe Abschnitt 6.2 und 6.3). Die im Folgenden aufgeführten Anforderungen sind nicht wie die oben genannten Anforderungen allgemeingültig, sondern gelten nur für bestimmte Anwendungsfälle. Da der Anspruch an die Forschungsschnittstelle gestellt wird, alle für die Kommunikation mit einer ePA identifizierten Anwendungsfälle zu unterstützen, müssen diese Anforderungen auch bei der Umsetzung der Forschungsschnittstelle berücksichtigt werden.

- **Datenschutzanforderung 5:** Die Forschungsschnittstelle muss vor der Kontaktierung eines Patienten überprüfen, ob eine entsprechende Einwilligung des Patienten vorliegt (A09).
- **Datenschutzanforderung 6:** Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Patientenliste nur seine Kontaktdaten bzw. identifizierenden Daten bereitstellen kann (A10).
- **Datenschutzanforderung 7:** Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Versorgungsdatenbank nur Daten bereitstellt, die auch im Rahmen des Forschungsvorhabens benötigt werden und für die eine Einwilligung des Patienten vorliegt (A11).
- **Datenschutzanforderung 8:** Die Forschungsschnittstelle muss überprüfen, ob der Patient für neue Forschungsvorhaben rekrutiert werden möchte (A12).
- **Datenschutzanforderung 9:** Die Forschungsschnittstelle muss überprüfen, ob der Patient über neue Forschungsergebnisse informiert werden möchte (A13).
- **Datenschutzanforderung 10:** Es muss durch den Forschungsverbund festgelegt werden, welche Informationen einem Patienten direkt aus der Versorgungsdatenbank bereitgestellt werden können und welche über einen behandelnden Arzt zur Verfügung gestellt werden müssen. Diese Regeln müssen in der Forschungsschnittstelle abgebildet und überprüft werden (A14).

7.2. Ableitung der Anforderungen in Architekturentscheidungen

Im folgenden Abschnitt werden Architekturentscheidungen aus den oben aufgeführten Datenschutzanforderungen sowie den in den vorherigen Kapiteln gesammelten Anforderungen (siehe Tabelle 49 im Anhang A3.5) beschrieben und begründet. Bei der Begründung der Architekturentscheidungen muss auch das vorher festgelegte Verhalten der Forschungsschnittstelle (siehe Abschnitt 6.1.2) bei deren Ableitung berücksichtigt werden. Dem festgelegten Verhalten der Forschungsschnittstelle entsprechend wird hier auch auf die direkte Kommunikation mit der Versorgungsdatenbank und der Patientenliste eingegangen und beschrieben, wie bei dieser Kommunikation die Zuordnung der Identitäten des Patienten in der ePA und in der Versorgungsdatenbank durch die Forschungsschnittstelle erfolgt (vergleiche Punkt 2 und 3).

Architekturentscheidung 1 - Schutz der medizinischen Daten des Patienten durch Verschlüsselung und Pseudonymisierung: Die Datenschutzanforderung 1 fordert, dass die medizinischen Daten in Verbindung mit den identifizierenden Daten des Patienten nur dem Patienten und dem im Behandlungszusammenhang stehenden Personen zugänglich gemacht werden dürfen. Die Sicherheitsarchitektur der ePA sieht hierfür eine nutzerzentrierte Verschlüsselung der nicht pseudonymisierten medizinischen Daten vor [167]. Dieser Schutz wird beim Verlassen der Telematikinfrastruktur (in Richtung Forschungssystem) aufgehoben, da die Daten entschlüsselt werden, um sie pseudonymisiert in die Versorgungsdatenbank zu übernehmen. Das bedeutet, dass die medizinischen Daten vor dem Verlassen der Telematikinfrastruktur pseudonymisiert werden müssen, um die Identität des Patienten auch nach der Entschlüsselung der Daten zu schützen. Aus demselben Grund dürfen die medizinischen Daten, die aus der Versorgungsdatenbank an eine ePA geschickt werden, erst in der Telematikinfrastruktur (nachdem sie verschlüsselt wurden) depseudonymisiert werden. Da die Nutzdaten innerhalb der Telematikinfrastruktur verschlüsselt sind und somit nicht verändert werden können, muss die Pseudonymisierung und Depseudonymisierung aufgrund von unverschlüsselten Metadaten der Informationsobjekte erfolgen. Die verschlüsselten medizinischen Daten wiederum dürfen weder das Pseudonym des Patienten (PIDv) noch identifizierende Daten des Patienten enthalten. D. h. diese Informationen müssen vor der Verschlüsselung von der Versorgungsdatenbank bzw. dem ePA-Kernsystem entfernt werden (VE03 und VF04).

Architekturentscheidung 2 - Kommunikation zwischen der ePA und der Versorgungsdatenbank: Um eine Kommunikation von Daten eines Patienten zwischen der ePA und der Versorgungsdatenbank zu ermöglichen (wie sie in Anforderung A07 gefordert wird), müssen die Daten dem gleichen Patienten in der ePA und in der Versorgungsdatenbank von der Forschungsschnittstelle zugeordnet werden können (vergleiche Anforderung A04). Bei der Kommunikation zwischen einer ePA und den Leistungserbringersystemen wird für diesen Zweck eine ePA-ID verwendet, die die Adresse der ePA des Patienten darstellt. Sie wird in den Metadaten der Informationsobjekte als Zuordnung der Identität des Patienten im ePA-System genutzt. Die ePA-ID kann nicht für die Kommunikation zwischen der Versorgungsdatenbank und der ePA zum Einsatz kommen, da sie ein identifizierendes Merkmal des Patienten ist und die Datenschutzanforderung 4 fordert, dass der Verwalter der Versorgungsdatenbank keinen Zugriff auf die identifizierenden Daten der Patienten erlangen darf. Somit darf die ePA-ID weder in der Versorgungsdatenbank gespeichert werden, noch darf sie an die Versorgungsdatenbank übertragen werden. Innerhalb des Versorgungsmoduls werden die Daten dem Patienten in den einzelnen Datenbanken über den PIDv zugeordnet. Laut Datenschutzanforderung 2 darf dieses Pseudonym nur zwischen den Datenbanken des Versorgungsmoduls kommuniziert werden. D. h., das Pseudonym sollte den IT-Komponenten des ePA-Systems bzw. der Telematikinfrastruktur nicht offenbart werden und kann somit auch nicht als Identität des Patienten zur Kommunikation zwischen der Versorgungsdatenbank und der ePA genutzt werden.

Die Patientenliste enthält die identifizierenden Daten der Patienten und sie muss auch die ePA-ID der Patienten verwalten können (VF03). Hier gibt es also eine Zuordnung der ePA-ID zur PIDv. Ein Austausch der PIDv durch die ePA-ID bzw. andersherum in den Metadaten der Informationsobjekte sollte allerdings an einer anderen Stelle umgesetzt werden, da die medizinischen Daten der Patientenliste verborgen bleiben sollen (vergleiche Datenschutzanforderung 3). Das könnte zwar dadurch erreicht werden, dass die medizinischen Daten verschlüsselt werden, eine sicherere Variante ist aber ein Austausch der IDs

des Patienten durch eine unabhängige Instanz innerhalb der Telematikinfrastruktur. Diese Instanz (im Folgenden ePA-Forschungsadapter genannt) soll bei der Kommunikation zwischen einer ePA und einer Versorgungsdatenbank die ePA-ID einem pseudonymisierten medizinischen Datenobjekt zuordnen (also eine Depseudonymisierung durchführen, vergleiche auch Anforderung A08) bzw. die ePA-ID aus dem medizinischen Datenobjekt entfernen und durch ein Pseudonym ersetzen (also die Pseudonymisierung durchführen, vergleiche auch Anforderung A08). Da dem ePA-Forschungsadapter die PIDv nicht offenbart werden sollte (vergleiche Datenschutzanforderung 2 - hier würde außerhalb der Patientenliste eine Verknüpfung der PIDv mit dem identifizierenden Merkmal ePA-ID des Patienten entstehen), kommt stattdessen einer Transaktions-ID (TID) als temporäres Pseudonym zum Einsatz, die von der Patientenliste für jede Pseudonymisierung bzw. Depseudonymisierung erzeugt und temporär verwaltet wird. Die Versorgungsdatenbank und der ePA-Forschungsadapter können für Informationsobjekte, die sie versenden, eine TID für eine PIDv bzw. ePA-ID beantragen, um diese TID gegen die ursprüngliche ID des Patienten auszutauschen. Andersherum können sie für Informationsobjekte, die sie empfangen, zu einer TID die entsprechende PIDv bzw. die ePA-ID anfordern, um die Daten dem richtigen Patienten im jeweiligen System wieder zuordnen zu können. Die detaillierte Beschreibung dieser Abläufe ist in den Abschnitten 7.5.1 bzw. 7.5.2 zu finden. Die Zuordnung der IDs des Patienten wird in Abbildung 19 veranschaulicht.

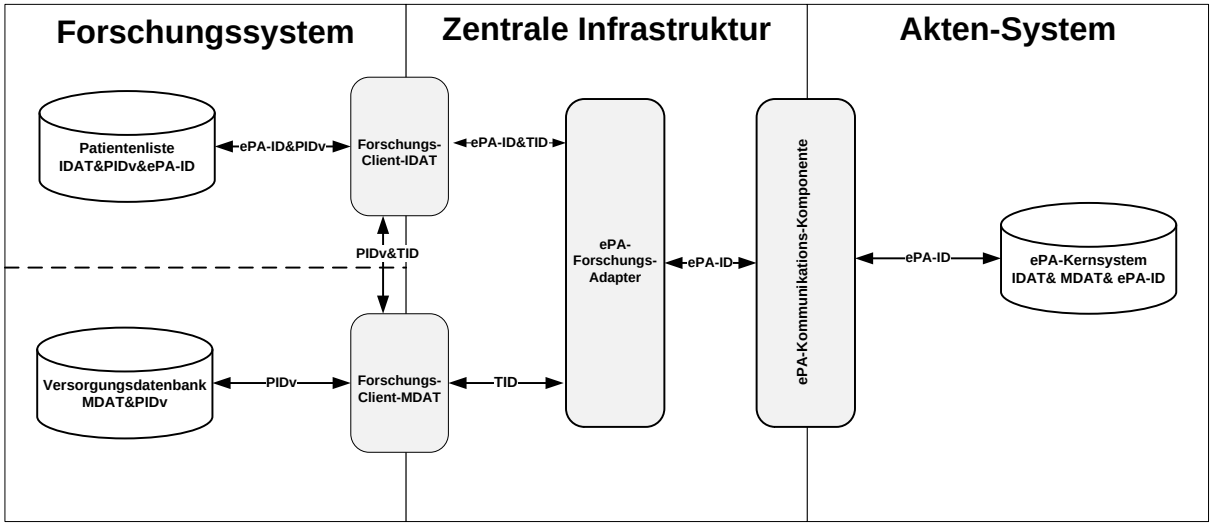

Abbildung 19: Abbildung der Zuordnung der IDs des Patienten über die Forschungsschnittstelle

Architekturentscheidung 3 - Kommunikation zwischen der Patientenliste und der ePA: Es wurde festgelegt, dass auch die Patientenliste mit der ePA kommunizieren soll (vergleiche Anforderung A06). Die Kommunikation zwischen der Patientenliste und der ePA kann direkt (ohne einen Austausch der IDs) über die ePA-ID erfolgen, da die ePA-IDs der Patienten sowohl der Patientenliste als auch der ePA bekannt sind. Somit muss keine Zuordnung der Identitäten durch die Forschungsschnittstelle, wie sie in Anforderung A04 gefordert wird, erfolgen. Die ePA und die Patientenliste kommunizieren ebenfalls über den ePA-Forschungsadapter. Um keine weiteren Anpassungen an der ePA-Kommunikationskomponente vornehmen zu müssen, kommuniziert der Forschungs-Client-IDAT nicht direkt mit der ePA-Kommunikationskomponente, sondern ausschließlich über den ePA-Forschungsadapter.

Architekturentscheidung 4 - Autorisierung des Datenaustausches zwischen der ePA und dem Versorgungsmodul: Aus den Datenschutzanforderungen 5-10 ergibt sich, dass bevor Daten über die Forschungsschnittstelle von der ePA an das Versorgungsmodul und andersherum kommuniziert werden, eine Überprüfung der oben genannten Anforderungen stattfinden muss. D. h. es müssen in der Forschungsschnittstelle (im Sinne einer Autorisierung) Regeln hinterlegt und überprüft werden, über die abgebildet wird, welche Daten aus der ePA vom Versorgungsmodul angefordert bzw. der ePA bereitstellt werden dürfen und welche Daten ein Patient dem Versorgungsmodul aus seiner ePA bereitstellen bzw. aus dem Versorgungsmodul für seine ePA anfordern darf. Da diese Regeln vom Forschungsverbund festgelegt und verantwortet werden müssen, wird festgelegt, dass die Autorisierung zu kommunizierenden Daten durch die Patientenliste umgesetzt werden muss bzw. durch die Komponente, die die Patientenliste in der Telematikinfrastruktur repräsentiert. Die Autorisierung wird von der Patientenliste und nicht von der Versorgungsdatenbank übernommen, da die Patientenliste an jeder Kommunikation beteiligt ist (vergleiche Punkt 2). Die Autorisierung erfolgt bei der Kommunikation zwischen der Patientenliste und der ePA immer bevor die Daten von der Patientenliste für die ePA an den ePA-Forschungsadapter übergeben werden bzw. nachdem die Daten aus der ePA von der Patientenliste vom ePA-Forschungsadapter abgerufen wurden. Bei der Kommunikation zwischen der Versorgungsdatenbank und der ePA erfolgt die Autorisierung immer bei einer Anfrage einer TID bei der Patientenliste. Sollte die Überprüfung der Autorisierungsregeln in der Patientenliste negativ ausfallen, so wird keine TID herausgegeben und die Kommunikation kann nicht fortgesetzt werden. Die detaillierte Umsetzung dieser Autorisierung wird im Kapitel 9 zur Sicherheitsarchitektur beschrieben (siehe Abschnitt 9.4).

7.3. Komponenten der Forschungsschnittstelle

Aufgrund der oben beschrieben Architekturentscheidungen wird festgelegt, dass das Versorgungsmodul über eine Forschungsschnittstelle, bestehend aus einem Forschungs-Client-IDAT, einem Forschungs-Client-MDAT und einem ePA-Forschungsadapter, an das ePA-System angebunden wird (siehe Abbildung 20, grau gestrichelter Rahmen). Im Folgenden wird kurz auf die Funktionalität der einzelnen Komponenten eingegangen:

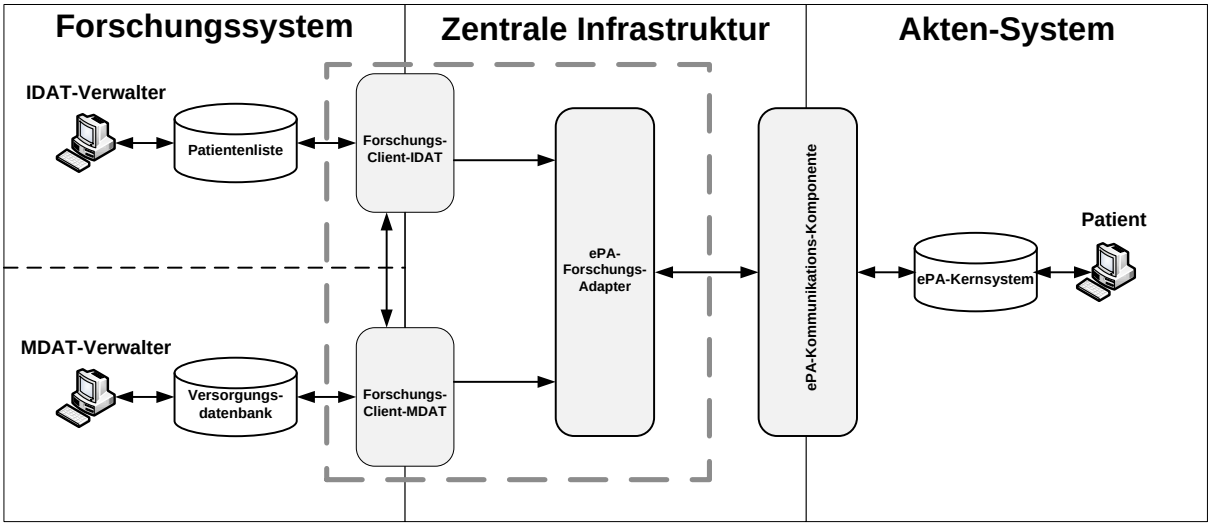

Abbildung 20: Komponenten der Forschungsschnittstelle für die Anbindung eines Versorgungsmoduls an die ePA

- Der **ePA-Forschungsadapter** befindet sich in der Telematikinfrastruktur und nimmt sowohl die Daten vom Forschungs-Client-IDAT als auch -MDAT des Versorgungsmoduls an und leitet diese Daten an die ePA-Kommunikationskomponente weiter. Er nimmt ebenfalls Daten aus der ePA über die ePA-Kommunikationskomponente an und hält diese Daten für den Forschungs-Clients-IDAT oder -MDAT zum Abruf vor. Als unabhängige Komponente übernimmt er die Pseudonymisierung und Depseudonymisierung der Anforderungs- und Bereitstellungsobjekte, bevor er die Daten dem Forschungs-Client-MDAT für die Versorgungsdatenbank bzw. der ePA-Kommunikationskomponente für die ePA des Patienten zur Verfügung stellt. Der ePA-Forschungsadapter kann aufgrund der Vorgaben der Telematikinfrastruktur (siehe dazu auch den Abschnitt zur LE-Postfach-Komponente) keine direkte Verbindung zu den Forschungs-Clients aufnehmen und stellt deswegen immer die Daten für die Forschungs-Clients bereit, die die Forschungs-Clients dann abrufen können. In der Anforderung A01 wurde festgelegt, dass die Forschungsschnittstelle Anforderungs- und Bereitstellungsobjekte unterstützen muss. Daher muss der Forschungsadapter die Kommunikation mit der ePA-Kommunikationskomponente über Anforderungs- und Bereitstellungsobjekte realisieren. Der ePA-Forschungsadapter realisiert auch die Kommunikation mit den Forschungs-Client-IDAT und -MDAT über Anforderungs- und Bereitstellungsobjekte, um hier nicht noch einen weiteren Standard einzuführen, auf den der ePA-Forschungsadapter die Anforderungs- und Bereitstellungsobjekte immer konvertieren müsste.
- **Forschungs-Client-IDAT und -MDAT:** Die Datenbanken des Versorgungsmoduls kommunizieren jeweils über eine Client-Komponente, die den Zugang zur Telematikinfrastruktur ermöglicht. Sowohl die Patientenliste als auch die Versorgungsdatenbank erhalten jeweils einen unabhängigen Client (Forschungs-Client-IDAT und Forschungs-Client-MDAT). Über diesen Client können die Datenbanken des Versorgungsmoduls eine Verbindung zum ePA-Forschungsadapter aufbauen, um Informationen abzurufen oder bereitzustellen. Die Funktionalität dieses Clients ist ähnlich der des ePA-LE-Clients mit dem Unterschied, dass er nur mit dem ePA-Forschungsadapter kommunizieren kann und keine direkte Kommunikation mit der ePA-Kommunikationskomponente ermöglicht. Die Clients können untereinander kommunizieren und zum Zwecke der Pseudonymisierung bzw. Depseudonymisierung den PIDv und eine Transaktions-ID (TID) austauschen. Identifizierende Daten oder medizinische Daten können zwischen den Forschungs-Clients-IDAT und -MDAT nicht ausgetauscht werden. Zusätzlich übernimmt der Forschungs-Client-IDAT noch die Autorisierung, die sich aus der Architekturentscheidung 4 ergibt. Die einzelnen Funktionen der Clients werden in den nachfolgenden Kapiteln zur Umsetzung der Kommunikation genauer beschrieben. Wie oben schon dargestellt, erfolgt die Kommunikation zwischen den Forschungsadaptern und den Forschungs-Clients-IDAT und -MDAT über Anforderungs- und Bereitstellungsobjekte. Es wurde festgelegt, dass die Forschungsschnittstelle die Anforderungs- und Bereitstellungsobjekte erstellen und Semantic Signifier unterstützen muss (siehe auch A02 und A03). Diese beiden Funktionen werden von den Forschungs-Clients-IDAT und -MDAT umgesetzt, da diese beiden Clients die Kommunikation für die Datenbanken des Versorgungsmoduls kapseln sollen und somit die Erstellung der Anforderungs- und Bereitstellungsobjekte sowie deren Interpretation übernehmen müssen.

7.4. Kommunikation mit der Patientenliste

Im nachfolgenden Abschnitt wird beschrieben, wie die beiden, die Patientenliste betreffenden, generischen Kommunikationsmuster unter den oben aufgeführten Anforderungen bzw. den oben beschriebenen Komponenten der Forschungsschnittstelle umgesetzt werden können. Hierbei wird nicht unterschieden, ob es sich um eine Anforderung oder eine Bereitstellung handelt, da dies für die Kommunikation nicht relevant ist. Es wird der Begriff des Informationsobjektes verwendet, was sowohl ein Anforderungs- als auch ein Bereitstellungsobjekt sein kann.

7.4.1. Informationen aus einer Patientenliste einer ePA bereitstellen

Im Folgenden wird die Umsetzung des generischen Kommunikationsmuster „Informationen aus einer Patientenliste einer ePA bereitstellen“ über die oben aufgeführten Infrastruktur-Komponenten beschrieben. Die Beschreibung erfolgt sowohl textuell (siehe Tabelle 12), als auch in Form eines Sequenzdiagrammes (siehe Abbildung 21):

Bezeichner	UC-3-1
Name	Informationen aus einer Patientenliste einer ePA bereitstellen
Kurzbeschreibung	Der Verwalter der Patientenliste möchte dem Patienten Informationen bereitstellen.
Primärer Akteur	Verwalter Patientenliste
Andere Akteure	Patient
Systeme	Patientenliste, Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Der Patient wurde in der Patientenliste angelegt. Die Anbindung an die ePA des Patienten wurde eingerichtet. Der Patient hat eingewilligt, dass er über seine ePA informiert werden darf.
Nachbedingungen	Die Informationen wurden vom Patienten überprüft und in die ePA übernommen.
Hauptszenario	1. Der Verwalter der Patientenliste stellt Informationen für den Patienten aus der Patientenliste zusammen. 2. Die Patientenliste übermittelt diese Informationen an den Forschungs-Client-IDAT. 3. Der Forschungs-Client-IDAT überprüft, ob dem Patienten diese Daten übermittelt werden dürfen (Prüfung der Anforderungen 5-9 im Sinne einer Autorisierung). 4. Nach erfolgreicher Prüfung erstellt der Forschungs-Client-IDAT ein Informationsobjekt. 5. Der Forschungs-Client-IDAT übermittelt das Informationsobjekt an den ePA-Forschungsadapter. 6. Der ePA-Forschungsadapter leitet das Informationsobjekt an die ePA-Kommunikationskomponente weiter. 7. Die ePA-Kommunikationskomponente leitet das Informationsobjekt an das ePA-Kernsystem weiter. 8. Der Patient ruft die Informationen aus der ePA ab. 9. Die ePA zeigt dem Patienten die Informationen an. 10. Der Patient überprüft die Informationen. 11. Der Patient übernimmt die Informationen in seine ePA.
Beziehungen zu anderen Use Cases	UC-3-2

Tabelle 12: Informationen aus einer Patientenliste einer ePA bereitstellen

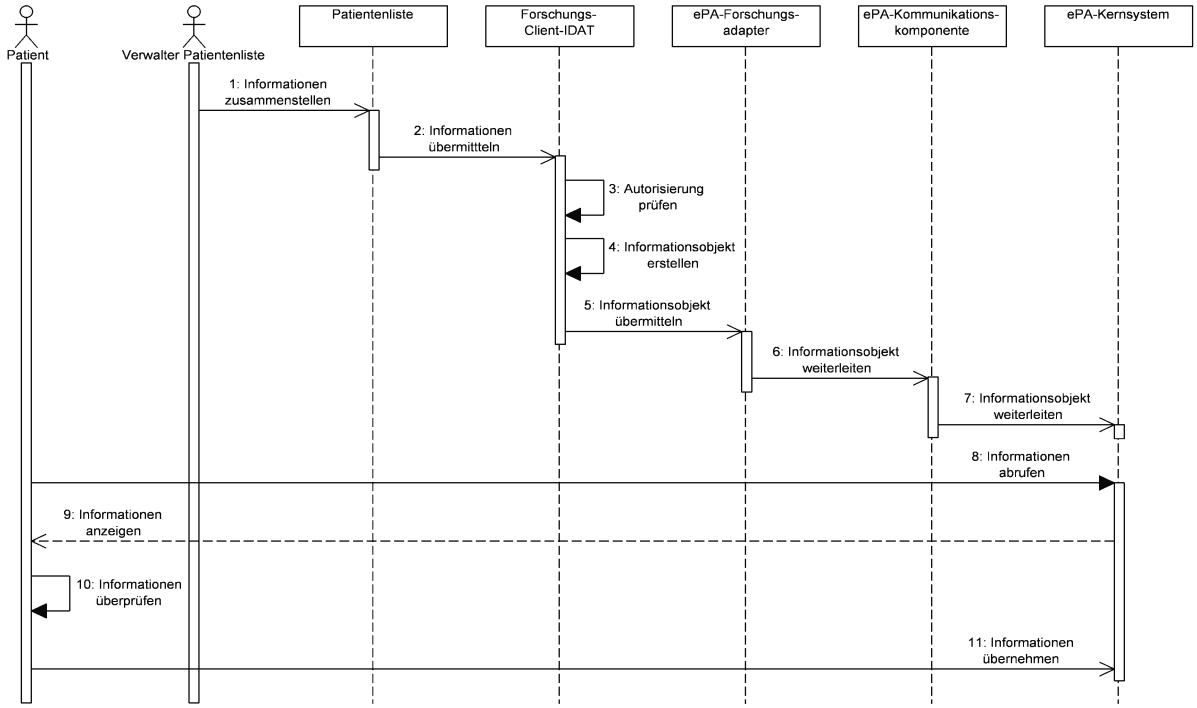

Abbildung 21: Informationen aus einer Patientenliste einer ePA bereitstellen

7.4.2. Informationen aus einer ePA einer Patientenliste bereitstellen

Im Folgenden wird die Umsetzung des generischen Kommunikationsmuster „Informationen aus einer ePA einer Patientenliste bereitstellen“ über die oben aufgeführten Infrastruktur-Komponenten beschrieben. Die Beschreibung erfolgt sowohl textuell (siehe Tabelle 13), als auch in Form eines Sequenzdiagrammes (siehe Abbildung 22):

Bezeichner	UC-3-2
Name	Informationen aus einer ePA einer Patientenliste bereitstellen
Kurzbeschreibung	Der Patient möchte dem Verwalter der Patientenliste Informationen bereitstellen.
Primärer Akteur	Patient
Andere Akteure	Verwalter Patientenliste
Systeme	Patientenliste, Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Der Patient wurde in der Patientenliste angelegt. Die Anbindung an die ePA des Patienten wurde eingerichtet.
Nachbedingungen	Die Informationen wurden vom Verwalter der Patientenliste überprüft und in die Patientenliste übernommen.
Hauptszenario	1. Der Patient stellt Informationen in seiner ePA für das ePA-System zusammen. 2. Das ePA-Kernsystem erstellt ein Informationsobjekt. 3. Das ePA-Kernsystem übermittelt das Informationsobjekt an die ePA-Kommunikationskomponente. 4. Die ePA-Kommunikationskomponente leitet das Informationsobjekt an den ePA-Forschungsadapter weiter. 5. Der Forschungs-Client-IDAT fragt vom ePA-Forschungsadapter neue Informationsobjekte ab. 6. Der ePA-Forschungsadapter übermittelt das Informationsobjekt an den Forschungs-Client-IDAT.

	7. Der Forschungs-Client-IDAT überprüft, ob der Patient diese Daten übermitteln darf (Prüfung der Anforderungen 5-9 im Sinne einer Autorisierung). 8. Der Forschungs-Client-IDAT leitet das Informationsobjekt an die Patientenliste weiter. 9. Der Verwalter der Patientenliste ruft die Informationen aus der Patientenliste ab. 10. Die Patientenliste zeigt die Informationen an. 11. Der Verwalter der Patientenliste überprüft die Informationen. 12. Der Verwalter der Patientenliste übernimmt die Informationen.
Beziehungen zu anderen Use Cases	UC-3-1

Tabelle 13: Informationen aus einer ePA einer Patientenliste bereitstellen

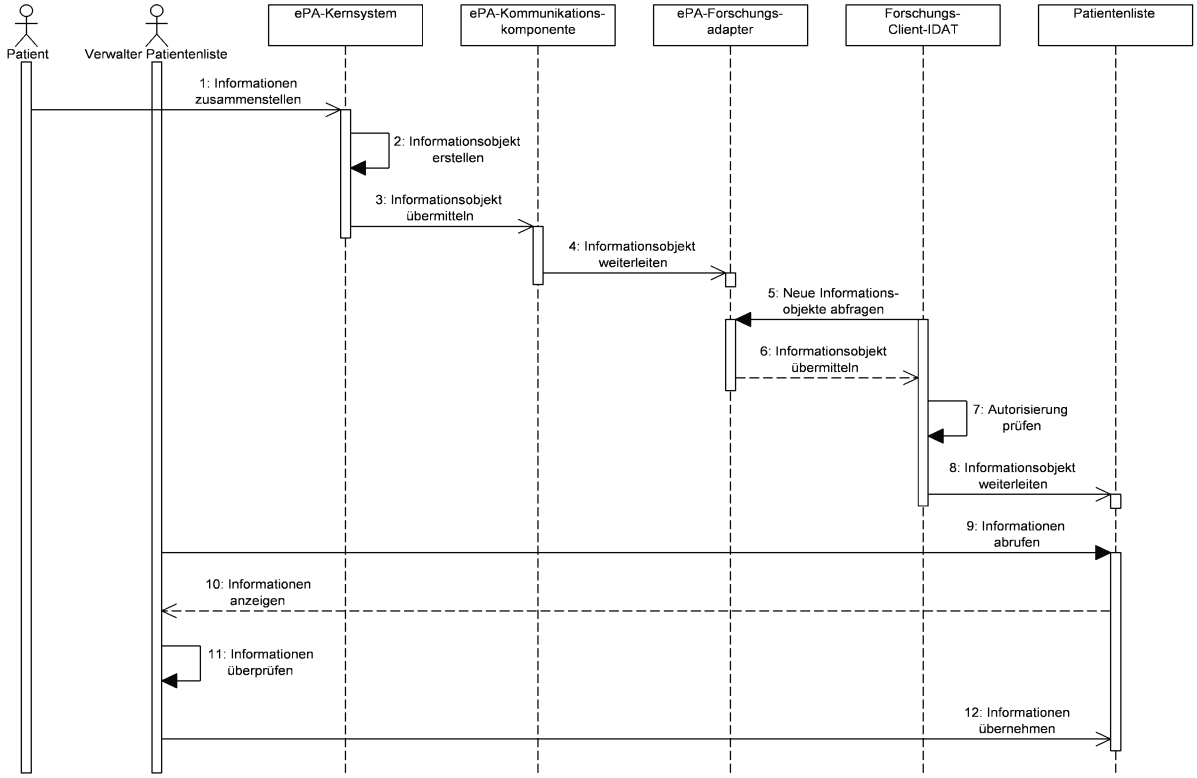

Abbildung 22: Informationen aus einer ePA einer Patientenliste bereitstellen

7.5. Kommunikation mit der Versorgungsdatenbank

Im nachfolgenden Abschnitt wird beschrieben, wie die beiden, die Versorgungsdatenbank betreffenden, generischen Kommunikationsmuster unter den oben aufgeführten Anforderungen bzw. den oben beschriebenen Komponenten der Forschungsschnittstelle umgesetzt werden können. Hierbei wird nicht unterschieden, ob es sich um eine Anforderung oder eine Bereitstellung handelt, da dies für die Kommunikation nicht relevant ist. Es wird der Begriff des Informationsobjektes verwendet, was sowohl ein Anforderungs- als auch ein Bereitstellungsobjekt sein kann.

7.5.1. Daten aus einer ePA einer Versorgungsdatenbank bereitstellen

Im Folgenden wird die Umsetzung des generischen Kommunikationsmuster „Daten aus einer ePA einer Versorgungsdatenbank bereitstellen“ über die oben aufgeführten Infrastruktur-Komponenten beschrieben. Die Beschreibung erfolgt sowohl textuell (siehe Tabelle 14), als auch in Form eines Sequenzdiagrammes (siehe Abbildung 23).

Bezeichner	UC-4-1
Name	Daten aus einer ePA einer Versorgungsdatenbank bereitstellen
Kurzbeschreibung	Der Patient stellt dem Behandler Daten aus seiner ePA über die Forschungsschnittstelle für die Versorgungsdatenbank bereit.
Primärer Akteur	Patient
Andere Akteure	Behandler
Systeme	Patientenliste, Versorgungsdatenbank, Forschungs-Client-MDAT, Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Der Patient wurde in der Patientenliste und der Versorgungsdatenbank angelegt. Die Anbindung an die ePA des Patienten wurde eingerichtet.
Nachbedingungen	Dem Behandler liegen die Informationen aus der ePA in der Versorgungsdatenbank vor.
Hauptszenario	1. Der Patient stellt Informationen im ePA-Kernsystem zusammen. 2. Das ePA-Kernsystem erstellt ein Informationsobjekt mit der Versorgungsdatenbank als Empfänger. 3. Das ePA-Kernsystem übermittelt das Informationsobjekt an die ePA-Kommunikationskomponente. 4. Die ePA-Kommunikationskomponente leitet das Informationsobjekt an den ePA-Forschungsadapter weiter. 5. Der Forschungs-Client-IDAT fragt beim ePA-Forschungsadapter regelmäßig an, ob neue Nachrichten für ihn vorliegen. 6. Auf diese Anfrage übermittelt der ePA-Forschungsadapter eine ePA-ID und fordert eine Transaktions-ID (TID) für diese ePA-ID an. 7. Der Forschungs-Client-IDAT überprüft, ob der Patient autorisiert ist, das Informationsobjekt an die Versorgungsdatenbank zu übermitteln. 8. Nach erfolgreicher Prüfung generiert der Forschungs-Client-IDAT eine TID. 9. Der Forschungs-Client-IDAT speichert die TID und die ePA-ID zwischen. 10. Der Forschungs-Client-IDAT übermittelt TID und ePA-ID an den ePA-Forschungsadapter. 11. Der ePA-Forschungsadapter löscht die ePA-ID aus dem Informationsobjekt für die Versorgungsdatenbank. 12. Der ePA-Forschungsadapter fügt die TID dem Informationsobjekt hinzu. 13. Der Forschungs-Client-MDAT fragt beim ePA-Forschungsadapter regelmäßig an, ob Nachrichten für ihn vorliegen. 14. Der ePA-Forschungsadapter übermittelt dem Forschungs-Client-MDAT das an die Versorgungsdatenbank adressierte Informationsobjekt. 15. Danach fordert der Forschungs-Client-MDAT den PID des Patienten unter Angabe der TID beim Forschungs-Client-IDAT an. 16. Der Forschungs-Client-IDAT löst die TID in die entsprechende ePA-ID aus dem Zwischenspeicher auf. 17. Der Forschungs-Client-IDAT übermittelt die ePA-ID an die Patientenliste und fordert hierzu die PID an. 18. Die Patientenliste löst die ePA-ID in die PID des Patienten auf. 19. Die Patientenliste übermittelt die PID und die TID an den Forschungs-Client-IDAT. 20. Der Forschungs-Client-IDAT leitet den PID mit der TID an den Forschungs-Client-MDAT weiter. 21. Der Forschungs-Client-IDAT löscht die zwischengespeicherte ePA-ID und die TID. 22. Der Forschungs-Client-MDAT ersetzt die TID durch den PID. 23. Die Informationen werden vom Forschungs-Client-MDAT an die Versorgungsdatenbank übermittelt. 24. Die Versorgungsdatenbank ordnet die Informationen dem Patienten anhand der PID zu.

	25. Der Behandler ruft die Informationen zum Patienten von der Versorgungsdatenbank ab. 26. Die Versorgungsdatenbank zeigt dem Behandler die Informationen an. 27. Der Behandler überprüft die Informationen. 28. Der Behandler übernimmt die Informationen in die Versorgungsdatenbank.
Beziehungen zu anderen Use Cases	Keine

Tabelle 14: Daten aus einer ePA einer Versorgungsdatenbank bereitstellen

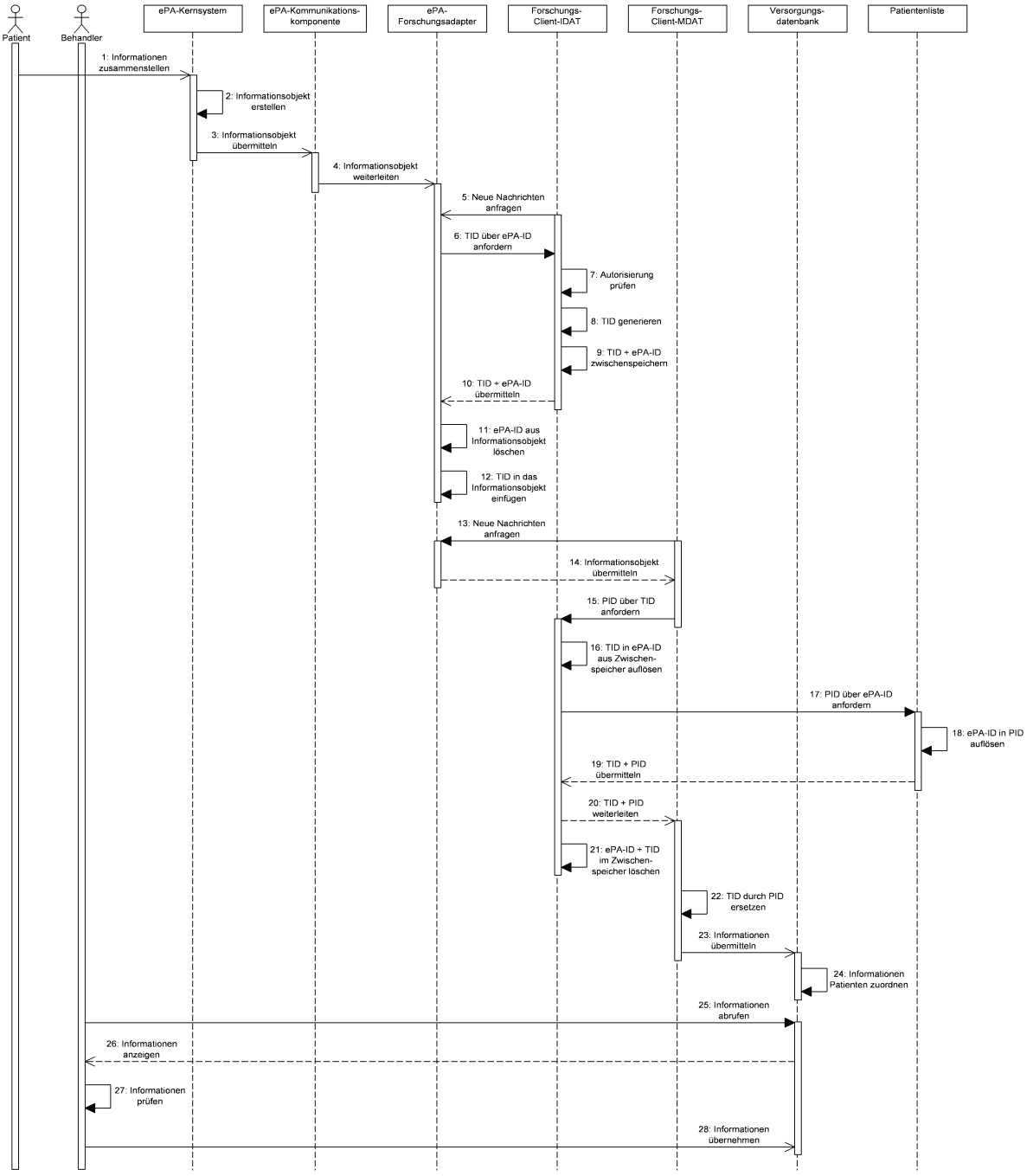

Abbildung 23: Daten aus einer ePA einer Versorgungsdatenbank bereitstellen

7.5.2. Daten aus einer Versorgungsdatenbank an eine ePA bereitstellen

Im Folgenden wird die Umsetzung des generischen Kommunikationsmuster „Daten aus einer Versorgungsdatenbank an eine ePA bereitstellen“ über die oben aufgeführten Infrastruktur-Komponenten beschrieben. Die Beschreibung erfolgt sowohl textuell (siehe Tabelle 15), als auch in Form eines Sequenzdiagrammes (siehe Abbildung 24).

Bezeichner	UC-4-2
Name	Daten aus einer Versorgungsdatenbank an eine ePA bereitstellen
Kurzbeschreibung	Der Behandler stellt dem Patienten Daten aus der Versorgungsdatenbank über die Forschungsschnittstelle für die ePA des Patienten bereit.
Primärer Akteur	Behandler
Andere Akteure	Patient
Systeme	Patientenliste, Versorgungsdatenbank, Forschungs-Client-MDAT, Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikations-komponente, ePA-Kernsystem
Vorbedingungen	Der Patient wurde in der Patientenliste und der Versorgungsdatenbank angelegt. Die Anbindung an die ePA des Patienten wurde eingerichtet. Der Patienten hat eingewilligt, dass der Behandler ihm diese Informationen bereitstellt.
Nachbedingungen	Dem Patienten liegen die Informationen aus der Versorgungsdatenbank in seiner ePA vor.
Hauptszenario	1. Der Behandler stellt die Informationen für den Patienten im Versorgungs-modul zusammen. 2. Das Versorgungsmodul übermittelt die Informationen an den Forschungs-Client-MDAT. 3. Der Forschungs-Client-MDAT fordert vom Forschungs-Client-IDAT eine TID zu der PID des Patienten an. 4. Der Forschungs-Client-IDAT überprüft, ob die Versorgungsdatenbank autorisiert ist, das Informationsobjekt an den Patienten zu übermitteln. 5. Nach erfolgreicher Autorisierung generiert der Forschungs-Client-IDAT eine TID. 6. Der Forschungs-Client-IDAT speichert die TID und die PID zwischen. 7. Der Forschungs-Client-IDAT übermittelt die TID und die PID an den Forschungs-Client-MDAT. 8. Der Forschungs-Client-MDAT erstellt aus den Informationen und der TID ein Informationsobjekt für die ePA des Patienten. 9. Der Forschungs-Client-MDAT übermittelt das Informationsobjekt dem ePA-Forschungsadapter. 10. Der Forschungs-Client-IDAT fragt den ePA-Forschungsadapter regel-mäßig nach neuen Nachrichten an. 11. Der ePA-Forschungsadapter antwortet dem Forschungs-Client-IDAT mit einer Anfrage zur Auflösung einer TID in eine ePA-ID. 12. Der Forschungs-Client-IDAT löst die TID in die PID des Patienten auf. 13. Der Forschungs-Client-IDAT fordert bei der Patientenliste die ePA-ID zu der PID an. 14. Die Patientenliste löst die ePA-ID in die PID auf. 15. Die Patientenliste übermittelt die ePA-ID zu der PID an den Forschungs-Client-IDAT. 16. Der Forschungs-Client-IDAT leitet die ePA-ID zu der TID an den ePA-Forschungsadapter weiter. 17. Der ePA-Forschungsadapter ersetzt im Informationsobjekt die TID durch die ePA-ID. 18. Der ePA-Forschungsadapter übermittelt das Informationsobjekt an die ePA-Kommunikationskomponente. 19. Die ePA-Kommunikationskomponente leitet das Informationsobjekt an

	das ePA-Kernsystem weiter. 20. Der Patient ruft die Informationen aus dem ePA-Kernsystem ab. 21. Das ePA-Kernsystem zeigt dem Patienten die Informationen an. 22. Der Patient überprüft die Informationen. 23. Der Patient übernimmt die Informationen in seine ePA.
Beziehungen zu anderen Use Cases	Keine

Tabelle 15: Daten aus einer Versorgungsdatenbank an eine ePA bereitstellen

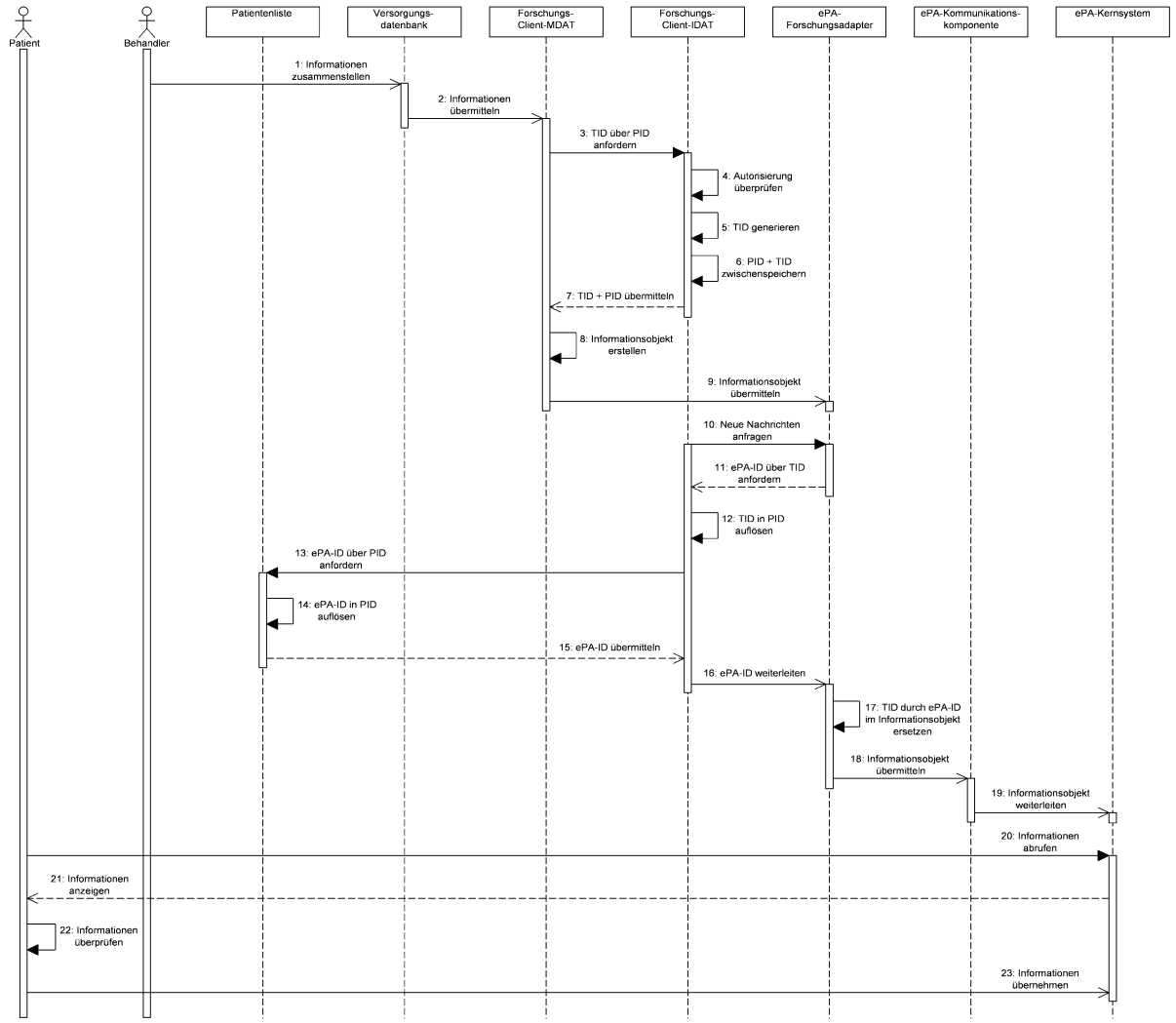

Abbildung 24: Daten aus einer Versorgungsdatenbank an eine ePA bereitstellen

8. Facharchitektur

Nachdem im Kapitel 7 die Komponenten und ihre Kommunikationsbeziehungen beschrieben wurden, wird nun auf dieser Basis dargestellt, welche Schnittstellen und Operationen die einzelnen Komponenten der Forschungsschnittstelle bereitstellen müssen und welches Verhalten die einzelnen Komponenten bei den Operationsaufrufen ausweisen müssen, damit die beschriebene Kommunikation zwischen den Komponenten der Forschungsschnittstelle umgesetzt werden kann. Da im Abschnitt 5.8.1 festgelegt wurde, dass die Nachrichten und Operationen der LE-Schnittstelle verwendet werden sollen (A00), erfolgt die Beschreibung auf Grundlage der im Abschnitt 5.6 aufgeführten Nachrichten und RLUS-Operationen. Im Abschnitt 5.8 wurde festgelegt, dass die Komponenten der Forschungsschnittstelle die Hilfsobjekte (Anforderungs- und Bereitstellungsobjekte sowie die Capability List) der LE-Schnittstelle nutzen sollen. Daher wird analysiert, inwieweit die von der LE-Schnittstelle verwendeten Hilfsobjekte zum Zugriff auf die ePA (siehe Abschnitt 5.4) für die Kommunikation der Forschungsschnittstelle angepasst werden müssen. Die Forschungsschnittstelle und die LE-Schnittstelle sollen als ein Gesamtkonzept implementiert werden. Aus diesem Grund orientiert sich die Beschreibung der IT-Komponenten der Forschungsschnittstelle, deren Kommunikation und Schnittstellen an der Methodik und dem Aufbau der im FuE-ePA-Projekt entstandenen Facharchitektur der LE-Schnittstelle [144].

Zunächst wird ein Systemüberblick beschrieben, um eine Gesamtübersicht und das Zusammenspiel der beiden Schnittstellen zu vermitteln. Anschließend wird dann nur noch auf die Details der Komponenten der Forschungsschnittstelle eingegangen. In diesem Kapitel werden die Schnittstellen der einzelnen Komponenten definiert und die Umsetzung der Kommunikation über die RLUS-Operationen beschrieben. Eine genauere Spezifikation der entsprechenden Komponenten der Forschungsschnittstelle und deren Verhalten beim Aufrufen der Operationen sowie deren einzelne Module werden im Anhang A4 beschrieben.

8.1. Systemüberblick

In der Abbildung 25 wird das Gesamtsystem mit allen Komponenten der LE-Schnittstelle und der Forschungsschnittstelle dargestellt. Die in Rot dargestellten Pfeile illustrieren die Kommunikation der Forschungsschnittstelle. Die blauen Komponenten sind Bestandteil der Forschungsschnittstelle, die grauen Komponenten bilden die LE-Schnittstelle und die weißen Komponenten sind die Systeme aus Forschung und Versorgung sowie das ePA-Kernsystem, die über die Schnittstellen kommunizieren. Im Sinne einer minimalen Anpassung bauen die IT-Komponenten der Forschungsschnittstelle auf den Komponenten der LE-Schnittstelle auf. Der im Abschnitt 7.3 beschriebene ePA-Forschungsadapter ist eine Erweiterung der LE-Postfachkomponente und die ebenfalls in diesem Abschnitt beschriebenen Forschungs-Clients-IDAT und -MDAT sind Erweiterungen des ePA-LE-Clients. D. h. grundlegende Module der Komponenten der LE-Schnittstelle wie der Postfachdienst, das Authentifizierungsmodul, das Validierungsmodul für Informationsobjekte, das Postfachmodul, das Nachrichtenmodul und der Kommunikations-Client werden wiederverwendet und ggf. erweitert.

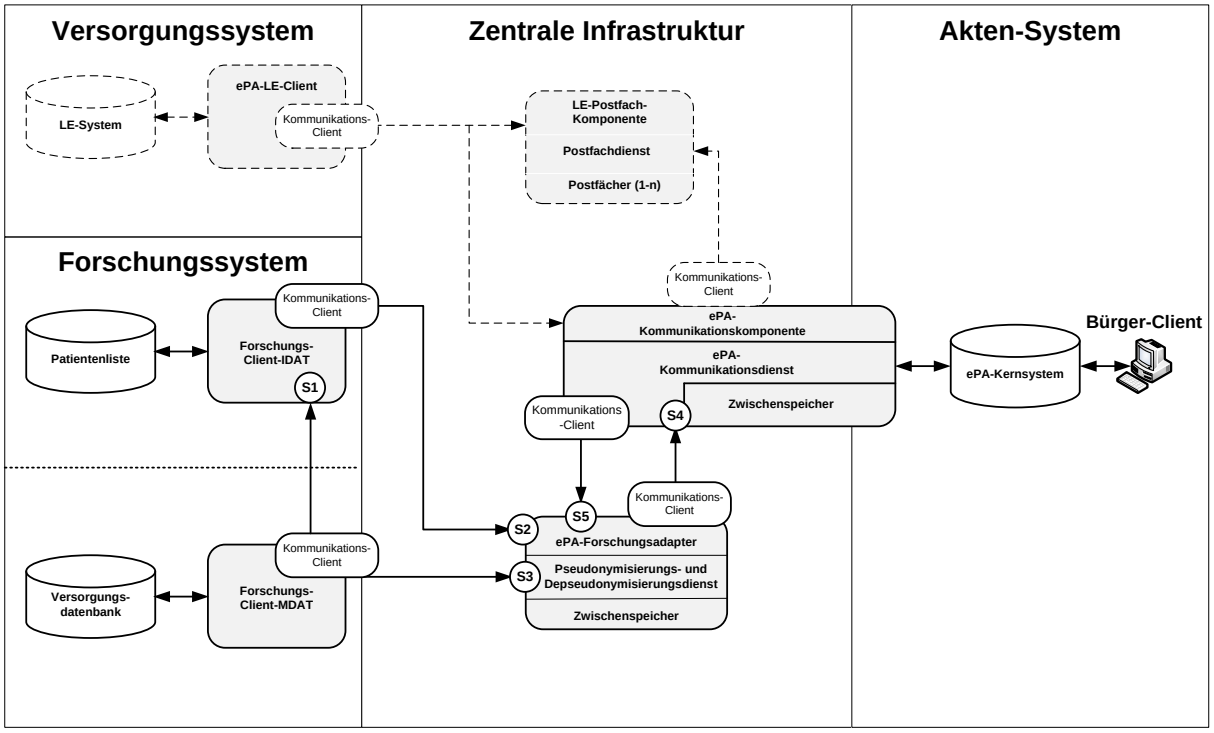

Abbildung 25: Zusammenspiel der Forschungsschnittstelle und der LE-Schnittstelle im Systemüberblick (Angelehnt an die Abbildungen auf den Seiten 18 und 21 in [144])

8.2. Hilfsobjekte

Für die Forschungsschnittstelle sollen die Hilfsobjekte der LE-Schnittstelle zum Einsatz kommen. Diese Hilfsobjekte der LE-Schnittstelle sind die Anforderungs- und Bereitstellungsobjekte (vergleiche Anforderung A01) und die Capability List (vergleiche Anforderung A05). Da diese Hilfsobjekte unverschlüsselte identifizierende Merkmale enthalten, wird hier analysiert, inwieweit die Hilfsobjekte angepasst werden müssen, um der Datenschutzanforderung 4 aus dem Abschnitt 7.1 „Der Versorgungsdatenbank bzw. ihrem Systemverwalter dürfen die identifizierenden Daten des Patienten in der Patientenliste nicht zugänglich gemacht werden“ gerecht zu werden. Da so wenige Anpassungen wie möglich am ePA- und Forschungssystem erfolgen sollen, müssen diese Hilfsobjekte von den Komponenten der Forschungsschnittstelle angepasst werden.

8.2.1. Anforderungsobjekt und Bereitstellungsobjekt

Um der Datenschutzanforderung 4 des Versorgungsmoduls gerecht zu werden, dürfen die Metainformation und die Inhalte, die als Informationsobjekte von der ePA an die Versorgungsdatenbank gesendet werden, die Identität des Patienten nicht preisgeben. Auf die Inhalte, also die Nutzlast der Informationsobjekte, kann der ePA-Forschungsadapter keinen Einfluss nehmen, da zumindest die medizinischen Informationen nutzerzentriert verschlüsselt sind und somit vom ePA-Forschungsadapter nicht eingesehen werden können. Die Nutzlast muss also (wie in Voraussetzung VE03 und VF04 beschrieben) vor dem Versenden von jeglichen identifizierenden Merkmalen des Patienten befreit worden sein. Daher wird hier nur auf die Metainformationen der Informationsobjekte eingegangen.

Sowohl das Anforderungsobjekt als auch das Bereitstellungsobjekt, das von der ePA des Patienten an die Versorgungsdatenbank gesendet wird, enthält im Feld „Quelle“ identifizierende Merkmale des Bürgers (siehe Anhang A3.1 Tabelle 39 und Tabelle 38). Daher muss die Quelle durch den ePA-Forschungsadapter bei der Kommunikation ersetzt werden.

Hier wird die Quelle einfach durch den String „Patient“ ersetzt. Zudem wird die Identität des Quellsystems aufgeführt und auch diese Information muss durch einen String „ePA“ ersetzt werden. Ein weiteres identifizierendes Merkmal ist die Akten-ID (auch ePA-ID genannt). Diese Akten-ID wird, wie schon im Abschnitt 7.2 Architekturentscheidung 2 festgelegt, aus dem Informationsobjekt durch den ePA-Forschungsadapter durch eine TID ersetzt. Mit diesen Anpassungen durch den ePA-Forschungsadapter können die Informationsobjekte der LE-Schnittstelle für die Forschungsschnittstelle eingesetzt werden.

8.2.2. Capability List

Im nachfolgenden Abschnitt wird der Inhalt der Capability List daraufhin analysiert, ob ein Konflikt mit der Datenschutzanforderung 4 des Versorgungsmoduls entsteht. Des Weiteren wird beschrieben, wie die Capability List von den Forschungs-Client-IDAT und -MDAT abgerufen werden kann und wie dieser Vorgang sich vom Abrufen der Capability List durch den ePA-LE-Client unterscheidet.

Der Aufbau der Capability List ist im Anhang A3.1 in der Tabelle 40 beschrieben. Die Capability List enthält als identifizierende Daten den öffentlichen Aktenschlüssel der ePA, für die die Capability List erstellt wurde. Dieser öffentlichen Aktenschlüssel darf dem Forschungs-Client-MDAT nicht zugänglich gemacht werden und muss somit vor dem Übersenden an den Forschungs-Client-MDAT entfernt werden, da er als identifizierendes Merkmal eingestuft wird, durch das ein Bezug zum Patienten hergestellt werden kann. Außerdem ist noch die ePA-ID in den Adressinformationen der Capability List enthalten, die vor dem Übersenden an den Forschungs-Client-MDAT durch die PID des Patienten ausgetauscht werden muss.

Normalerweise wird die Capability List direkt durch den ePA-LE-Client von der ePA-Kommunikationskomponente abgerufen. Da sowohl der Forschungs-Client-IDAT als auch -MDAT nur indirekt über den ePA-Forschungsadapter mit der ePA-Kommunikationskomponente kommunizieren, muss die Capability List über den ePA-Forschungsadapter von der Kommunikationskomponente abgerufen werden. Der Forschungs-Client-IDAT muss immer, bevor Daten von der Patientenliste aus der ePA angefordert oder für die ePA bereitgestellt werden, die Capability List abrufen, um zu überprüfen ob die ePA die Kommunikationsmuster und die Semantic Signifier unterstützt. Das Gleiche gilt auch für den Forschungs-Client-MDAT.

Die Capability List enthält keine medizinischen Daten und ist auch dem Forschungs-Client-IDAT zugänglich. Somit kann die Capability List vom Forschungs-Client-MDAT über den Forschungs-Client-IDAT angefordert werden. Der Forschungs-Client-IDAT nimmt die oben beschriebene Entfernung des Schlüsselmaterials und der Adressinformationen vor. Dieses Verfahren hat den Vorteil, dass die Zuordnung von ePA-ID und PID für die Capability List bei der Anforderung und bei der Bereitstellung direkt über den Forschungs-Client-IDAT erfolgen kann und keine aufwendige De- bzw. Pseudonymisierung durch den ePA-Forschungsadapter erfolgen muss. Eine detaillierte Beschreibung des Abrufens der Capability List durch den Forschungs-Client-IDAT und -MDAT befindet sich im Anhang A4.1.

8.3. Schnittstellen und Operationen des Forschungs-Client-IDAT

Wie auf der Abbildung 25 zu sehen ist, stellt der Forschungs-Client-IDAT dem Forschungs-Client-MDAT die Schnittstelle S1 zur Verfügung und tritt somit als Dienstanbieter gegenüber dem Forschungs-Client-MDAT auf.

Nachfolgend wird auf Grundlage der Beschreibung der generischen Kommunikationsmuster UC-4-1 und UC-4-2 in Abschnitt 7.5 analysiert, welche Operationen die Schnittstelle S1 dem Forschungs-Client-MDAT zur Verfügung stellen muss, um diese Kommunikationsmuster implementieren zu können. UC-3-1, UC-3-2 müssen nicht berücksichtigt werden, da der Forschungs-Client-MDAT bei diesen Kommunikationsmustern nicht involviert ist und somit keine Kommunikation zwischen den beiden Clients stattfindet (siehe Abbildung 21 und Abbildung 22). Eine detaillierte Beschreibung des Verhaltens des Forschungs-Clients-IDAT beim Ausführen der Operationen der Schnittstelle S1 als auch beim Aufrufen der Schnittstelle S2 des ePA-Forschungsadapters befindet sich im Anhang A4.4.

Der Forschungs-Client-MDAT ruft den Forschungs-Client-IDAT im UC-4-1 „Daten aus einer ePA einer medizinischen Datenbank des Forschungsverbundes bereitstellen“ auf, um vom Forschungs-Client-IDAT zu einer TID die entsprechende PID des Patienten zu bekommen (vergleiche Tabelle 14, Schritte 15-20).Hierfür stellt der Forschungs-Client-IDAT die Operation „Anfordern einer PID durch den Forschungs-Client-MDAT“ zur Verfügung. Des Weiteren ruft der Forschungs-Client-MDAT den Forschungs-Client-IDAT im UC-4-2 „Daten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA bereitstellen“ auf, um zu einer PID eine TID zu bekommen (vergleiche Tabelle 15, Schritte 3-7). Hierfür wird die Operation „Anfordern einer TID durch den Forschungs-Client-MDAT“ der Schnittstelle S1 aufgerufen. Beide Anfragen werden in Form eines Anforderungsobjektes an den Forschungs-Client-IDAT übertragen und sollten sofort bearbeitet werden. Daher kommt hier eine synchrone Kommunikation zum Einsatz, die eine Anforderung mit sofortiger Bereitstellung vorsieht. Diese beiden Operationen werden durch eine RLUS-List Operation umgesetzt (siehe Abbildung 26). Für die beiden Operationsaufrufe müssen zwei Semantic Signifier definiert werden. Zum Anfordern der PID wird der Semantic Signifier **SemSigGetPID** verwendet und zum Anfordern der TID der Semantic Signifier **SemSigGetTID.**

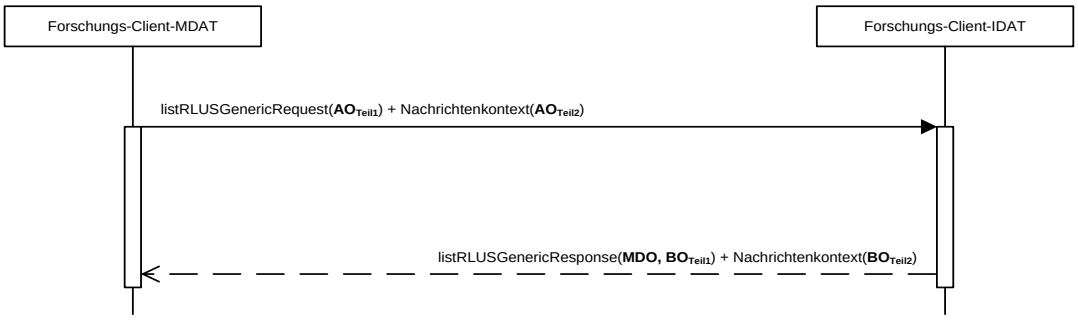

Abbildung 26: Kommunikation zwischen dem Forschungs-Client-IDAT und MDAT über die Schnittstelle

Bevor ein Forschungs-Client-MDAT Informationsobjekte an die ePA eines Patienten verschicken kann, muss der Forschungs-Client-MDAT eine Capability List über den Forschungs-Client-IDAT abrufen (siehe auch Tabelle 53: Abrufen der Capability List durch den Forschungs-Client-MDAT Schritt 2 und 15), um sicher zu stellen, dass die ePA die Kommunikationsmuster und die Semantic Signifier unterstützt. Das Abrufen der Capability List erfolgt über die Operation „Anfordern der Capability List durch den Forschungs-Client-

MDAT“ des Forschungs-Clients-IDAT. Der Aufruf sollte ohne große Zeitverzögerung erfolgen, daher kommt hier eine synchrone Kommunikation zum Einsatz, die eine Anforderung mit sofortiger Bereitstellung vorsieht. Die Operation wird durch eine RLUS-List Operation umgesetzt (siehe Abbildung 26). Für den Operationsaufruf wird der von der LE-Schnittstelle genutzte Semantic Signifier **Capability List** verwendet.

Die vom Forschungs-Client-IDAT bereitgestellte Schnittstelle S1 stellt dem Forschungs-Client-MDAT somit die folgenden RLUS-Operationen bereit:

- Anfordern einer PID durch den Forschungs-Client-MDAT:
  RLUS-List(Parameter):SemSigGetPID
- Anfordern einer TID durch den Forschungs-Client-MDAT:
  RLUS-List(Parameter):SemSigGetTID
- Anfordern der Capability List durch den Forschungs-Client-MDAT:
  RLUS-List(Parameter): Capability List

8.4. Schnittstellen und Operationen des Forschungs-Client-MDAT

Der Forschungs-Client-MDAT ist sowohl Dienstnutzer der Schnittstelle S1 des Forschungs-Client-IDAT als auch Dienstnutzer der Schnittstelle S3 des ePA-Forschungsadapters. Der Forschungs-Client-MDAT tritt selbst nicht als Dienstanbieter einer Schnittstelle auf (siehe auch Abbildung 25). Daher muss hier keine Analyse einer Schnittstelle durchgeführt werden. Eine detaillierte Beschreibung des Verhaltens des Forschungs-Clients-MDAT beim Aufrufen der Operationen S1 und S3 befindet sich im Anhang A4.5.

8.5. Schnittstellen und Operationen des ePA-Forschungsadapter

Der ePA-Forschungsadapter stellt als Dienstanbieter die Schnittstellen S2, S3 und S5 zur Verfügung. Die einzelnen Operationen der Schnittstellen S2, S3 und S5 werden im Folgenden hergeleitet. Das detaillierte Verhalten des ePA-Forschungsadapters wird beim Ausführen der Operationen der Schnittstellen als auch beim Aufrufen der Schnittstelle S4 wird im Anhang A4.6 beschrieben.

8.5.1. Kommunikation zwischen dem ePA-Forschungsadapter und dem Forschungs-Client-IDAT

In diesem Abschnitt wird auf Grundlage der Beschreibungen der generischen Kommunikationsmuster UC-3-1, UC-3-2, UC-4-1 und UC-4-2 analysiert, wie die Kommunikation zwischen dem Forschungs-Client-IDAT und dem ePA-Forschungsadapter über RLUS-Operationen umgesetzt werden kann.

Der Forschungs-Client-IDAT tritt gegenüber dem ePA-Forschungsadapter immer als Dienstnutzer auf. Er ruft die Schnittstelle S2 des ePA-Forschungsadapters auf (siehe Abbildung 25). Im UC-3-1 „Informationen aus einer Patientenliste einer ePA bereitstellen“ schickt der Verwalter der Patientenliste über den Forschungs-Client-IDAT ein Informationsobjekt an den ePA-Forschungsadapter (vergleiche Tabelle 12, Schritt 5). Dies erfolgt durch das Aufrufen der Operation „Zustellung eines Informationsobjektes durch den IDAT-Verwalter“ der Schnittstelle S2. Hier erfolgt also eine asynchrone Bereitstellung eines Informationsobjektes durch den Forschungs-Client-IDAT an den ePA-Forschungsadapter, die über die RLUS-Put Operation umgesetzt wird (siehe Abbildung 27).

Abbildung 27: Asynchrone Bereitstellung eines Informationsobjektes durch den Forschungs-Client-IDAT an den Forschungsadapter

Bevor dieses Informationsobjekt verschickt werden kann, muss der Forschungs-Client-IDAT eine Capability List über den ePA-Forschungsadapter abrufen, um sicher zu stellen, dass die ePA die Kommunikationsmuster und die Semantic Signifier unterstützt und um die öffentlichen Schlüssel der ePA für die Verschlüsselung der Nachricht zu erhalten (Siehe Anhang A4.1.1). Hierzu ruft der Forschungs-Client-IDAT die Operation „Anfordern der Capability List durch den Forschungs-Client-IDAT“ des ePA-Forschungsadapters auf (siehe auch Tabelle 52 Schritt 2 und 6 und Tabelle 53 Schritt 7 und 11). Das Abrufen der Capability List sollte ohne große Zeitverzögerung erfolgen, daher kommt hier eine synchrone Kommunikation zum Einsatz, die eine Anforderung mit sofortiger Bereitstellung über eine RLUS-List Operation vorsieht (siehe Abbildung 28). Für den Operationsaufruf wird der von der LE-Schnittstelle genutzte Semantic Signifier **Capability List** verwendet.

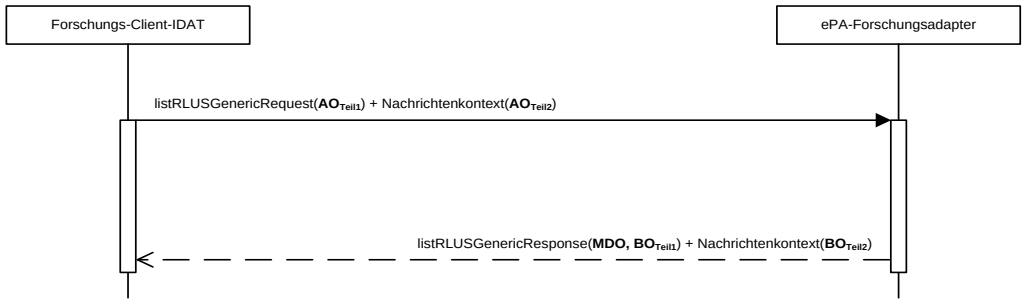

Abbildung 28: Synchrone Anforderung vom Forschungs-Client-IDAT mit direkter Bereitstellung durch den ePA-Forschungsadapter

Im UC-3-2 „Informationen aus einer ePA einer Patientenliste bereitstellen“ ruft der Verwalter der Patientenliste ein Informationsobjekt vom ePA-Forschungsadapter ab (vergleiche Tabelle 13, Schritt 5 und 6). Hierzu stellt der ePA-Forschungsadapter die Operation “Anfordern von Informationsobjekten durch den IDAT-Verwalter“ zur Verfügung. Diese Operation wird durch eine asynchrone Kommunikation umgesetzt, indem der Forschungs-Client-IDAT eine RLUS-List-Operation beim ePA-Forschungsadapter aufruft (siehe Abbildung 29).

Abbildung 29: Abrufen eines Informationsobjektes durch den Forschungs-Client-IDAT vom ePA-Forschungsadapter

Im UC-4-1 „Daten aus einer ePA einer medizinischen Datenbank des Forschungsverbundes bereitstellen“ ruft der Forschungs-Client-IDAT eine Pseudonymisierungs-Anfrage vom ePA-Forschungsadapter ab (vergleiche Tabelle 14, Schritt 5 und 6). Im UC-4-2 „Daten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA bereitstellen“ ruft der Forschungs-Client-IDAT eine Depseudonymisierungs-Anfrage vom ePA-Forschungsadapter ab (vergleiche Tabelle 15, Schritt 10 und 11). Für diese beiden Anfragen stellt die Schnittstelle S2 die Operationen „Anfordern von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT“ und „Anfordern von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT“ bereit. Beide Operationen werden durch einen RLUS-List umgesetzt (siehe Abbildung 29). Für das Anfordern einer TID wird der Semantic Signifier **SemSigGetTID** eingesetzt. Für das Anfordern einer ePA-ID wird der Semantic Signifier **SemSigGetePA-ID** eingesetzt.

Nachdem der Forschungs-Client-IDAT die Pseudonymisierungs- bzw. Depseudonymisierungs-Anfrage bearbeitet hat, stellt er die Ergebnisse der Anfrage dem ePA-Forschungsadapter bereit (vergleiche Tabelle 14, Schritt 10 und Tabelle 15, Schritt 16). Für das Zustellen dieser Informationen ruft der Forschungs-Client-IDAT die Operationen „Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT“ und „Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT“ auf. Beide Operationen werden durch eine RLUS-Put-Operation umgesetzt (siehe Abbildung 27).

Die vom ePA-Forschungsadapter bereitgestellte Schnittstelle S2 stellt dem Forschungs-Client-IDAT somit die folgenden RLUS-Operationen bereit:

- Zustellung eines Informationsobjektes durch den IDAT-Verwalter:
  RLUS-Put(IO)
- Anfordern der Capability List durch den Forschungs-Client-IDAT:
  RLUS-List(Parameter): Capability List
- Anfordern von Informationsobjekten durch den IDAT-Verwalter:
  RLUS-List(Parameter): IO
- Anfordern von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:
  RLUS-List(Parameter): SemSigGetTID
- Anfordern von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:
  RLUS-List(Parameter): SemSigGetePA-ID
- Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:
  RLUS-Put(SemSigGetTID)
- Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:
  RLUS-Put(SemSigGetePA-ID)

8.5.2. Kommunikation zwischen dem ePA-Forschungsadapter und dem Forschungs-Client-MDAT

In diesem Abschnitt wird auf Grundlage der Beschreibung der generischen Kommunikationsmuster UC-4-1 und UC-4-2 analysiert, wie die Kommunikation zwischen dem ePA-Forschungsadapter und dem Forschungs-Client-MDAT über RLUS-Operationen umgesetzt werden kann (die Kommunikation erfolgt über die Schnittstelle S3, siehe Abbildung 25). UC-3-1 und UC-3-2 müssen nicht berücksichtigt werden, da der Forschungs-Client-MDAT nicht involviert ist und somit keine Kommunikation zwischen ihm und dem ePA-Forschungs-

adapter stattfindet (siehe Abbildung 21 und Abbildung 22). Die Capability List wird nicht über den ePA-Forschungsadapter, sondern über den Forschungs-Client-IDAT abgerufen, so dass hier auch keine Kommunikation mit dem ePA-Forschungsadapter erfolgt.

Im UC-4-1 „Daten aus einer ePA einer medizinischen Datenbank des Forschungsverbundes bereitstellen“ wird von der ePA ein Informationsobjekt an die medizinische Datenbank des Forschungsverbundes übertragen. Auch hier kann der ePA-Forschungsadapter keine Verbindung zum Forschungs-Client-MDAT aufbauen. Daher ruft der Forschungs-Client-MDAT ein Informationsobjekt vom ePA-Forschungsadapter ab (vergleiche Tabelle 14, Schritt 13 und 14). Die Schnittstelle S3 stellt hierzu die Operation „Anfordern von Informationsobjekten durch den MDAT-Verwalter“ bereit. Diese Operation kann durch eine asynchrone Kommunikation erfolgen, indem der Forschungs-Client-MDAT ein RLUS-List beim ePA-Forschungsadapter aufruft (siehe Abbildung 30).

Abbildung 30: Abrufen eines Informationsobjektes durch den Forschungs-Client-MDAT vom ePA-Forschungsadapter

Im UC-4-2 „Daten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA bereitstellen“ schickt der Verwalter der medizinischen Datenbank des Forschungsverbundes über den Forschungs-Client-MDAT ein Informationsobjekt an den ePA-Forschungsadapter (vergleiche Tabelle 15, Schritt 9). Dafür ruft der Forschungs-Client-MDAT die Operation „Zustellung eines Informationsobjektes durch den MDAT-Verwalter“ der Schnittstelle S3 auf. Hier erfolgt also eine asynchrone Bereitstellung eines Informationsobjektes durch den Forschungs-Client-MDAT an den ePA-Forschungsadapter in Form eines RLUS-Put-Operationsaufrufes (siehe Abbildung 31).

Abbildung 31: Bereitstellen eines Informationsobjektes durch den Forschungs-Client-MDAT an den ePA-Forschungsadapter

Für die Verschlüsselung einer bereitzustellender Informationen durch den Forschungs-Client-MDAT an die ePA muss zuvor ein symmetrischer Schlüssel zur Verschlüsselung dieser Informationen angefordert werden, indem der Forschungs-Client-MDAT eine Anforderung an den ePA-Forschungsadapter schickt (siehe Abschnitt zum Verschlüsselungskonzept 9.5 bzw. UC-7-2 im Anhang A5.2.2). Hierzu wird dem Forschungs-Client-

MDAT die Operation „Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA“ durch den ePA-Forschungsadapter angeboten. Das Anfordern des symmetrischen Schlüssels durch den Forschungs-Client-MDAT sollte durch eine synchrone Kommunikation mittels RLUS-List erfolgen, da dieser Schlüssel sofort für die Verschlüsselung der Nutzlast benötigt wird (siehe Abbildung 32). Als Semantic Signifier wird **symkeyMDO** verwendet.

Abbildung 32: Synchrone Anforderung vom Forschungs-Client-MDAT mit direkter Bereitstellung durch den ePA-Forschungsadapter

Die vom ePA-Forschungsadapter bereitgestellte Schnittstelle S3 stellt dem Forschungs-Client-MDAT somit die folgenden RLUS-Operationen bereit:

- Anfordern von Informationsobjekten durch den MDAT-Verwalter:
  RLUS-List(Parameter): IO
- Zustellung eines Informationsobjektes durch den MDAT-Verwalter:
  RLUS-Put(IO)
- Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA:
  RLUS-List(Parameter): symkeyMDO

8.5.3. Kommunikation zwischen dem ePA-Forschungsadapter und der Kommunikationskomponente

In diesem Abschnitt wird auf Grundlage der Beschreibung der generischen Kommunikationsmuster UC-3-1, UC-3-2, UC-4-1 und UC-4-2 analysiert, wie die Kommunikation zwischen dem ePA-Forschungsadapter und der ePA-Kommunikationskomponente über RLUS-Operationen umgesetzt werden kann.

Der ePA-Forschungsadapter ist Dienstanbieter gegenüber der ePA-Kommunikationskomponente und stellt ihr die Schnittstelle S5 zur Verfügung (siehe Abbildung 25).

Im UC-3-2 „Informationen aus einer ePA einer Patientenliste bereitstellen“ und UC-4-1 „Daten aus einer ePA einer medizinischen Datenbank des Forschungsverbundes bereitstellen“ stellt die ePA-Kommunikationskomponente dem ePA-Forschungsadapter ein Informationsobjekt bereit (vergleiche Tabelle 13, Schritt 4 und Tabelle 14, Schritt 4). Hierzu wird von der ePA-Kommunikationskomponente die Operation „Zustellung eines Informationsobjektes durch die ePA-Kommunikationskomponente“ der Schnittstelle S5 aufgerufen. Diese Operation erfolgt über einen Aufruf der RLUS-Put-Operation seitens der ePA-Kommunikationskomponente beim ePA-Forschungsadapter (siehe Abbildung 33).

Abbildung 33: Bereitstellen eines Informationsobjektes durch die ePA-Kommunikationskomponente an den ePA-Forschungsadapter

Die vom ePA-Forschungsadapter bereitgestellte Schnittstelle S5 stellt der ePA-Kommunikationskomponente somit die folgende RLUS-Operation bereit:

- Zustellung eines Informationsobjektes durch die ePA-Kommunikationskomponente: **RLUS-Put(IO)**

8.6. Schnittstellen und Operationen des ePA-Kommunikationskomponente

In diesem Abschnitt werden nur die Schnittstellen der ePA-Kommunikationskomponente beschrieben, die für die Kommunikation mit der Forschungsschnittstelle notwendig sind. Alle anderen Schnittstellen sind in der Facharchitektur der LE-Schnittstelle beschrieben [144]. In Bezug auf die Forschungsschnittstelle ist nur eine Schnittstelle für die Kommunikation mit dem ePA Forschungsadapter relevant (siehe Schnittstelle S4, Abbildung 25), deren Operationen im Folgenden hergeleitet werden. Das detaillierte Verhalten beim Ausführen der Operationen der Schnittstelle S4 und beim Aufrufen der Schnittstelle S5 wird im Anhang A4.7 beschrieben.

Im UC-3-1 „Informationen aus einer Patientenliste einer ePA bereitstellen“ und im UC-4-2 „Daten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA bereitstellen“ stellt der ePA-Forschungsadapter der ePA-Kommunikationskomponente ein Informationsobjekt bereit (vergleiche Tabelle 12, Schritt 6 und Tabelle 15, Schritt 18). Hierzu nutzt der ePA-Forschungsadapter die Operation „Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter“ der Schnittstelle S4 der ePA-Kommunikationskomponente. Diese Operation erfolgt über einen Aufruf der RLUS-Put-Operation seitens des ePA-Forschungsadapter bei der ePA-Kommunikationskomponente (siehe Abbildung 34).

Abbildung 34: Bereitstellen eines Informationsobjektes durch den ePA-Forschungsadapter an die ePA-Kommunikationskomponente

Wie im Abschnitt 8.5.1 beschrieben muss der ePA-Forschungsadapter die Capability List einer ePA für die Forschungs-Client-IDAT abrufen (siehe auch Tabelle 52, Schritt 3 und 5 und Tabelle 53, Schritt 8 und 10). Da die Kommunikation zwischen dem Forschungs-Client-

IDAT und dem ePA-Forschungsadapter in diesem Fall synchron ist, muss die Kommunikation für das Abrufen der Capability List von der ePA-Kommunikationskomponente auch synchron durch das Aufrufen einer RLUS-List-Operation erfolgen (siehe Abbildung 35). Das Abrufen der erfolgt durch die Operation „Anfordern der Capability List durch den ePA-Forschungsadapter“ der ePA-Kommunikationskomponente. Als Semantic Signifier wird in diesem Fall wieder **Capability List** verwendet.

Zusätzlich muss der ePA-Forschungsadapter einen symmetrischen Schlüssel für den Forschungs-Client-MDAT abrufen (siehe Abschnitt 9.5 und UC-7-2 im Anhang A5.2.2). Da die Kommunikation zwischen dem Forschungs-Client-MDAT und dem ePA-Forschungsadapter in diesem Fall synchron ist, muss die Kommunikation für das Abrufen des symmetrischen Schlüssels von der ePA-Kommunikationskomponente auch synchron durch das Aufrufen einer RLUS-List-Operation erfolgen (siehe Abbildung 35). Hierzu ruft der ePA-Forschungsadapter die Operation “Anfordern eines symmetrischen Schlüssels von der ePA“ der Schnittstelle S4 auf und verwendet den Semantic Signifier symkeyMDO.

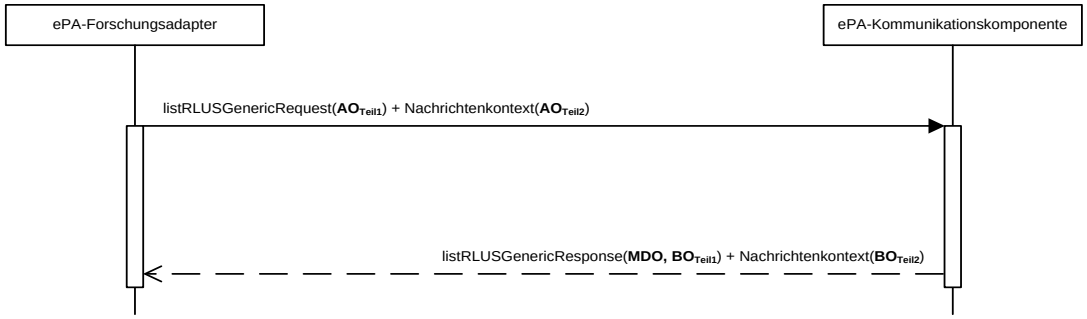

Abbildung 35: Synchrone Anforderung vom ePA-Forschungsadapter mit direkter Bereitstellung durch die ePA-Kommunikationskomponente

Die von der ePA-Kommunikationskomponente bereitgestellte Schnittstelle S4 stellt dem ePA-Forschungsadapter somit die folgenden RLUS-Operationen bereit:

- Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter:
  RLUS-Put(IO)
- Anfordern der Capability List durch den ePA-Forschungsadapter:
  RLUS-List(Parameter): Capability List
- Anfordern eines symmetrischen Schlüssels von der ePA:
  RLUS-List(Parameter): symkeyMDO

9. Sicherheitsarchitektur

In diesem Kapitel wird die Sicherheitsarchitektur der Forschungsschnittstelle als eine Erweiterung der Sicherheitsarchitektur der LE-Schnittstelle beschrieben. Hierzu wird die Sicherheitsarchitektur der LE-Schnittstelle betrachtet und untersucht, inwieweit die technischen Konzepte und Mechanismen der LE-Schnittstelle in Bezug auf die Sicherheit für die Forschungsschnittstelle übernommen werden können. Es gilt die Annahme, dass das ePA-System sicher ist und somit nur bei Konflikten mit den Datenschutzanforderungen des Versorgungsmoduls Anpassungen an der Sicherheitsarchitektur der LE-Schnittstelle vorgenommen werden müssen. D. h., in diesem Kapitel werden nur die Anpassungen der Sicherheitsarchitektur für die Forschungsschnittstelle beschrieben. Ansonsten gelten die Vorgaben der Sicherheitsarchitektur der LE-Schnittstelle (siehe auch Abschnitt 5.7 und Sicherheitsarchitektur der LE-Schnittstelle [155])

Nachdem im Abschnitt 5.7 die Sicherheitsarchitektur mit den Sicherheitsdiensten beschrieben wurde sowie auf die Vertrauens- und Kommunikationsbeziehungen der LE-Schnittstelle als auch die Autorisierung und Verschlüsslung eingegangen wurde, soll nun erläutert werden, wie diese Konzepte auf die Komponenten der Forschungsschnittstelle anzuwenden ist. Hierbei wird auf die Sicherung der Kommunikation zwischen den Diensten, die Authentifizierung der Nutzer, die Autorisierung der Nutzer und die Verschlüsselung der Daten eingegangen. Das Thema Signaturen medizinischer Datenobjekte für die Forschung muss noch gesondert betrachtet werden. Es wird in dieser Arbeit nicht vertieft und sollte in einer weiteren Arbeit auch im Hinblick auf die Schutzbedarfsanalyse aufgearbeitet werden. Auch die Sicherung der Nachrichten, Schlüssel und Hilfsobjekte durch Signaturen muss in einer weiteren Arbeit zusammen mit der Schutzbedarfsanalyse betrachtet werden. In diesem Kapitel werden nur Voraussetzungen genannt, die beim Umgang mit Signaturen im Zusammenhang mit der Forschungsschnittstelle beachtet werden müssen.

9.1. Architektur mit Sicherheitsdiensten

Im folgenden Abschnitt wird anhand einer Architekturübersicht beschrieben, welche Sicherheitsdienste der LE-Schnittstelle für die Forschungsschnittstelle eingesetzt werden und in welchen Sicherheitszonen sich die einzelnen Komponenten der Forschungsschnittstelle und die Sicherheitsdienste befinden.

Die Sicherheitsarchitektur der LE-Schnittstelle sieht einen Guarantor Token Service, einen Verzeichnisdienst, PKI-Dienste und einen Identity-Provider vor. Hinzukommt ein Access Token Service in der dezentralen Zone für die Ad-hoc-Autorisierung [155], der nicht zum Einsatz kommt, da die Ad-hoc-Autorisierung für die Forschungsschnittstelle nicht vorgesehen ist (vergleiche 5.7). In der nachfolgenden Abbildung wird die Forschungsschnittstelle mit den benötigten Sicherheitsdiensten dargestellt. Im FuE-ePA-Projekt werden drei verschiedene Sicherheitszonen definiert, die entsprechend auch für die Forschungsschnittstelle gelten (siehe Abbildung 36):

- In der **dezentralen Zone** befinden sich die Leistungserbringersysteme, im Fall der Forschungsschnittstelle befindet sich dort die IT-Infrastruktur des Versorgungsmoduls. Die IT-Infrastruktur des Versorgungsmoduls besteht aus der **Patientenliste** und **Versorgungsdatenbank,** die sich an zwei verschiedenen Standorten befinden (getrennt durch die gepunktete Linie). Die Patientenliste kommuniziert mit dem ePA-Forschungsadapter über den **Forschungs-Client-IDAT**. Die Versorgungsdatenbank kommuniziert über den **Forschungs-Client-MDAT** mit dem ePA-Forschungsadapter. An jedem Standort befindet sich ein Authentifizierungsdienst - der **Guarantor Token Service** -, über den ein Authentifizierungsnachweis (Guarantor Assertion) für den Forschungs-Client-IDAT und den Verwalter der Patientenliste bzw. dem Forschungs-Client-MDAT und den Verwalter der Versorgungsdatenbank erstellt werden kann. Die Guarantor Assertions werden zur Authentifizierung gegenüber dem sich in der zentralen Infrastruktur befindlichen Identity Provider benötigt.
- In der **zentralen Infrastruktur** befinden sich der **ePA-Forschungsadapter** sowie die ePA-Kommunikationskomponente, deren Funktionen in der Facharchitektur beschrieben wurden. Als Sicherheitsdienste sind der **Identity Provider**, der **Verzeichnisdienst** und die **PKI-Dienste** in der zentralen Infrastruktur angesiedelt. Der Identity Provider dient als zentraler Authentifizierungsdienst. Gegenüber diesem Dienst müssen sich der Verwalter der Patientenliste bzw. der Versorgungsdatenbank mit einer Guarantor Assertion authentisieren, bevor sie Daten an den ePA-Forschungsadapter schicken bzw. von dem ePA-Forschungsadapter abrufen. Das Gleiche gilt auch für den Forschungs-Client-IDAT, wenn er Pseudonymisierungs- bzw. Depseudonymisierungs-Anfragen vom ePA-Forschungsadapter anfragt bzw. Pseudonymisierungs- bzw. Depseudonymisierungs-Anfragen bereitstellt. Die PKI-Dienste sind für die Status-Prüfung der X.509-Zertifikate der einzelnen Dienste verantwortlich (z. B. die Zertifikate des ePA-Forschungsadapters oder der ePA-Kommunikationskomponente). Der Verzeichnisdienst dient zum Abrufen von weiteren Attributen der Leistungserbringer bzw. der Leistungserbringerinstitutionen [155] (z. B. der Institution, in der die Patientenliste oder die Versorgungsdatenbank betrieben werden bzw. der Verwalter der Patientenliste oder Versorgungsdatenbank angestellt sind).
- Die Aktensystemzone beinhaltet das ePA-Kernsystem, dessen Funktionen je nach Hersteller unterschiedlich sein können (siehe auch Abschnitt 5.1 und Abschnitt 5.3.3). Zusätzlich befindet sich der ePA-Bürger-Client in der Zone des Aktensystems. Der ePA-Bürger-Client ist optional und ermöglicht dem Bürger / Patienten direkt auf seine Akte zuzugreifen (siehe auch Abschnitt 5.3.3). Die Sicherheit in der Zone des Aktensystems und der Übergang zur Zone der zentralen Infrastruktur über die ePA-Kommunikationskomponente werden hier nicht betrachtet und liegen in der Verantwortung des Herstellers bzw. Betreibers. Hier gelten die Anforderungen, die im FuE-ePA-Projekt erarbeitet wurden (vergleiche Datenschutzkonzept [154] und Sicherheitsarchitektur [155] der LE-Schnittstelle).

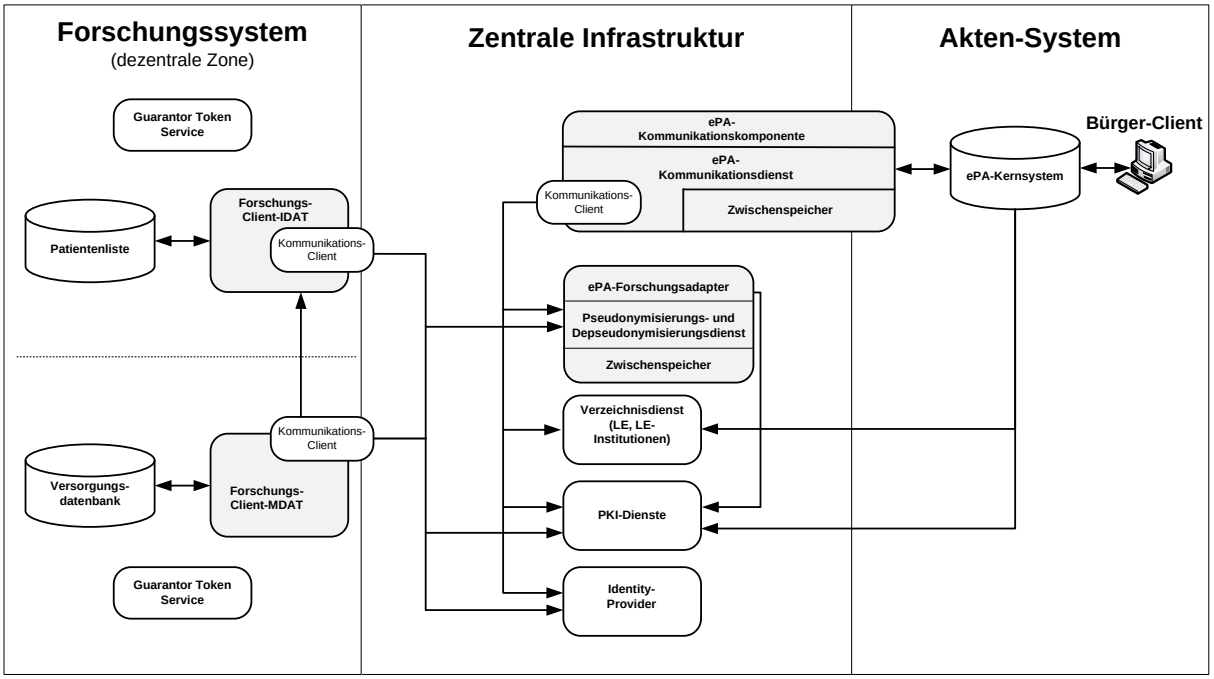

Abbildung 36: Gesamtübersicht der Forschungsschnittstelle mit den Sicherheitsdiensten (angelehnt an Abb. auf Seite 4 in [155])

9.2. Vertrauens- und Kommunikationsbeziehungen der Forschungsschnittstelle

Die nachfolgende Abbildung (Abbildung 37) zeigt die Vertrauensbeziehungen (durch Pfeile mit gestrichelter Linie dargestellt) zwischen den Komponenten der Forschungsschnittstelle untereinander als auch zwischen den Komponenten der Forschungsschnittstelle und den Komponenten der LE-Schnittstelle bzw. des Aktensystems in den einzelnen Sicherheitszonen. Da sich die Komponenten nicht alle in der gleichen Sicherheitszone befinden, müssen Vertrauensbeziehungen zwischen den Komponenten unterschiedlicher Sicherheitszonen hergestellt werden. Für die Komponenten der Forschungsschnittstelle bedeutet dies, dass eine Vertrauensbeziehung zwischen dem ePA-Kernsystem in der Sicherheitszone des Aktensystems und dem Forschungs-Client-IDAT bzw. -MDAT in der Sicherheitszone der IT-Infrastruktur des Forschungssystems über die ePA-Kommunikationskomponente, den Identity Provider und den Guarantor Token Service hergestellt werden muss. Eine Vertrauensbeziehung zwischen dem ePA-Forschungsadapter in der Sicherheitszone der zentralen Infrastruktur und dem Forschungs-Client-IDAT bzw. -MDAT in der Sicherheitszone der IT-Infrastruktur des Versorgungsmoduls muss über den Identity Provider und den Guarantor Token Service hergestellt werden. Der Identity Provider, der ePA-Forschungsadapter und der ePA-Kommunikationsdienst befinden sich in der gleichen Sicherheitszone und vertrauen sich somit gegenseitig. Das ePA-Kernsystem vertraut auch hier dem ePA-Kommunikationsdienst.

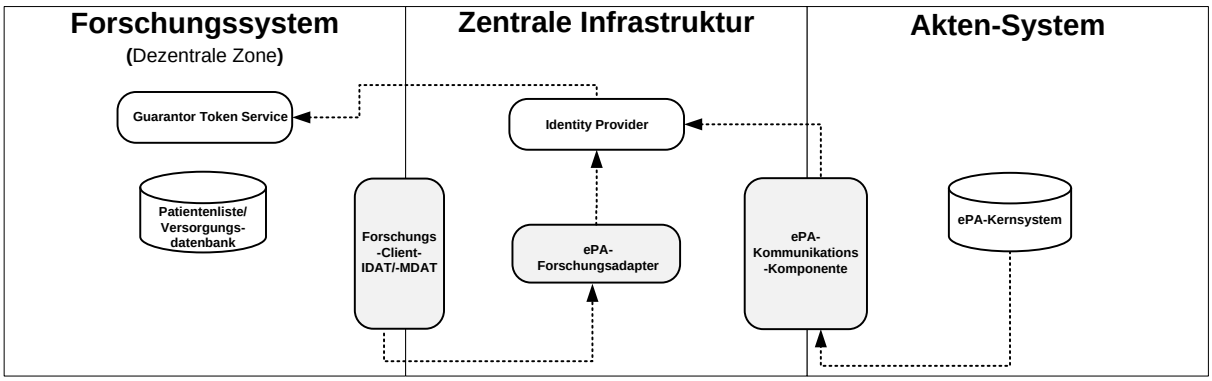

Abbildung 37: Vertrauensbeziehungen der Forschungsschnittstelle (angelehnt an Abb. auf Seite 10 in [155])

Auf Grundlage dieser Vertrauensbeziehungen wird in der nachfolgende Abbildung (Abbildung 38) die Kommunikation zwischen den einzelnen Komponenten der Forschungs- und der LE-Schnittstelle dargestellt. Die durchgezogenen Linien bedeuten Aufrufe durch einen Dedicated Service, die gestrichelten Linien sind Aufrufe durch einen Trusted Client. Die Details zum Dedicated Service und Trusted Client sind im Abschnitt 5.7.1 zu finden. Da sich der Forschungs-Client-IDAT und -MDAT in der gleichen Sicherheitszone befinden, können der Forschungs-Client-IDAT und -MDAT über Dedicated Services kommunizieren. Gleiches gilt für den ePA-Forschungsadapter und die ePA-Kommunikationskomponente. Die Kommunikation zwischen dem ePA-Forschungsadapter und den Forschungs-Client-IDAT und -MDAT wird über Trusted Clients umgesetzt, da sich die Forschungs-Client-IDAT und -MDAT in einer anderen Sicherheitszone als der ePA-Forschungsadapter befinden.

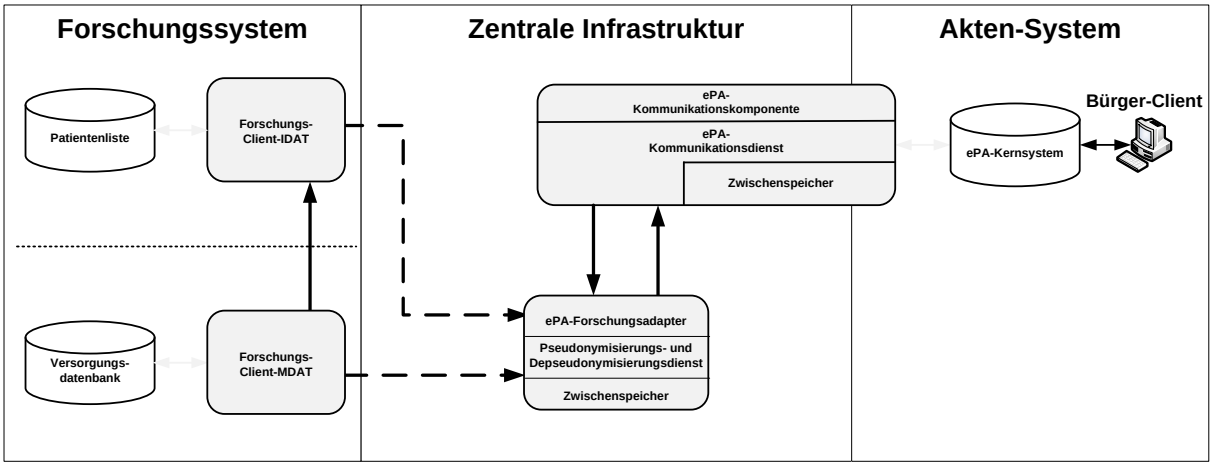

Abbildung 38: Kommunikationsbeziehungen zwischen den einzelnen Diensten (angelehnt an Abb. auf Seite 4 in [155])

9.3. Authentifizierung und Sicherung der Kommunikation

Im Folgenden Abschnitt wird untersucht, ob durch die Sicherung der Kommunikation zwischen den Komponenten und dem Authentifizierungskonzept der Sicherheitsarchitektur der LE-Schnittstelle Konflikte mit den Datenschutzanforderungen des Forschungssystems entstehen.

Die Sicherung der Kommunikation der Dienste erfolgt über X509 Zertifikate. Diese Sicherheitstoken enthalten identifizierende Merkmale des Absenders. Hier könnte also ein Konflikt mit der Datenschutzanforderung 4 „Der Versorgungsdatenbank bzw. ihrem System-verwalter dürfen die identifizierenden Daten des Patienten in der Patientenliste nicht

zugänglich gemacht werden“ entstehen. Identifizierenden Daten eines Patienten können nur bei einer vom ihn initiierten Kommunikation mit dem Sicherheitstoken ausgetauscht werden, d. h. bei einem Kommunikationsaufbau von der ePA-Kommunikationskomponente zum ePA-Forschungsadapter. Da die ePA-Kommunikationskomponenten hierfür nur ihr X509 Zertifikat verwenden [155], gibt es keine Konflikte, weil bei der Kommunikation keine Zertifikate ausgetauscht werden, die die Identität des Patienten bzw. seiner ePA enthalten.

Für die Authentifizierung der Nutzer werden IdentityAssertions verwendet, die identifizierende Merkmale des Absenders enthalten. Auch hier könnte wieder ein Konflikt mit der Datenschutzanforderung 4 entstehen. Da die Sicherheitsarchitektur von einer Authentifizierung des Patienten über eine IdentityAssertion absieht und bei einer von der ePA initiierten Kommunikation nur die ePA-Kommunikationskomponente authentifiziert werden muss [155], gibt es keine Konflikte im Hinblick auf die Datenschutzanforderung 4. Somit kann das Authentifizierungskonzept der LE-Schnittstelle von der Forschungsschnittstelle übernommen werden. Folgendes wird für die Forschungsschnittstelle in Bezug auf die Authentifizierung festgelegt:

- Werden Pseudonymisierungs- bzw. Depseudonymisierungs-Anfragen automatisch vom Forschungs-Client-IDAT abgefragt, reicht eine Authentifizierung des Clients aus. Dies gilt auch für das Abfragen von Pseudonymisierungs- bzw. Depseudonymisierungs-Anfragen durch den Forschungs-Client-MDAT beim Forschungs-Client-IDAT, da diese Pseudonymisierungs- bzw. Depseudonymisierungs-Anfragen automatisierte Anfragen sind, die keinen Personenbezug benötigen.
- Bei allen anderen Kommunikationsvorgängen müssen der IDAT- bzw. der MDAT-Verwalter authentifiziert werden. Eine Authentifizierung des Patienten erfolgt gegenüber seiner ePA. Beim Weiterleiten durch die ePA-Kommunikationskomponente wird keine Identity Assertion weitergeleitet. Hier wird der ePA-Kommunikationskomponente vertraut, dass der Patient richtig authentifiziert wurde.

Im Folgenden wird beschrieben wie das Authentifizierungskonzept im Einzelnen umgesetzt wird.

9.3.1. Kommunikation zwischen Forschungs-Client-IDAT und MDAT

Die Forschungs-Clients-IDAT und -MDAT befinden sich in der gleichen Sicherheitszone. Die Kommunikation zwischen dem Forschungs-Client-IDAT und MDAT erfolgt somit über einen Dedicated Service Aufruf. Die gegenseitige Authentifizierung der beiden Clients (Forschungs-Client-IDAT und -MDAT) erfolgt über die jeweiligen Zertifikate der SMC-B der Clients. Da keine identifizierenden Daten bzw. medizinischen Daten des Patienten ausgetauscht werden, muss sich der Verwalter der Versorgungsdatenbank nicht gesondert ausweisen.

9.3.2. Kommunikation zwischen Forschungs-Client-IDAT und dem ePA-Forschungsadapter

Der Forschungs-Client-IDAT und der ePA-Forschungsadapter befinden sich in unterschiedlichen Sicherheitszonen. Die Verbindung wird durch den Forschungs-Client-IDAT über einen Trusted-Client-Aufruf hergestellt. Der Forschungs-Client-IDAT authentisiert sich gegenüber dem ePA-Forschungsadapter über eine Identity Assertion. Die Identity Assertion muss für den Verwalter der Patientenliste ausgestellt worden sein, wenn die Capability List oder andere Informationsobjekte übertragen bzw. abgerufen werden sollen. Bei Pseudonymisie-

rung- oder Depseudonymisierungs-Anfragen muss die Identity Assertion für Forschungs-Client-IDAT ausgestellt worden sein.

9.3.3. Kommunikation zwischen Forschungs-Client-MDAT und dem ePA-Forschungsadapter

Der Forschungs-Client-MDAT und der ePA-Forschungsadapter befinden sich in unterschiedlichen Sicherheitszonen. Die Verbindung wird durch den Forschungs-Client-MDAT über einen Trusted-Client Aufruf hergestellt. Der Forschungs-Client-MDAT authentisiert sich gegenüber dem ePA-Forschungsadapter über eine Identity Assertion. Die Identity Assertion muss für den Verwalter der Versorgungsdatenbank ausgestellt worden sein.

9.3.4. Kommunikation zwischen dem ePA-Forschungsadapter und der ePA-Kommunikationskomponente

Der ePA-Forschungsadapter und die ePA-Kommunikationskomponente befinden sich in der gleichen Sicherheitszone. Die Kommunikation zwischen dem ePA-Forschungsadapter und ePA-Kommunikationskomponente erfolgt über einen Dedicated Service Aufruf. Die gegenseitige Authentifizierung der beiden Komponenten erfolgt über die jeweiligen Zertifikate. Der ePA-Forschungsadapter reicht mit dem Informationsobjekt auch die Identity Assertion des Verwalters der Patientenliste oder der Versorgungsdatenbank weiter(je nach dem, von wem die Anfrage oder Bereitstellung initiiert wurde). Bei Abrufen der Capability List durch den ePA-Forschungsadapter muss keine Identity Assertion mitgeschickt werden. Hier wird dem ePA-Forschungsadapter vertraut, dass er vorher eine Überprüfung der Identity Assertion des Verwalters der Patientenliste durchgeführt hat.

9.3.5. Kommunikation zwischen der ePA-Kommunikationskomponente und dem ePA-Forschungsadapter

Die ePA-Kommunikationskomponente und der ePA-Forschungsadapter befinden sich in der gleichen Sicherheitszone. Die Kommunikation zwischen der ePA-Kommunikationskomponente und dem ePA-Forschungsadapter erfolgt über einen Dedicated Service Aufruf. Die gegenseitige Authentifizierung der beiden Komponenten erfolgt über die jeweiligen Zertifikate. Es wird durch die ePA-Kommunikationskomponente keine Identity Assertion des Patienten weitergereicht, da die LE-Schnittstelle keine direkte Authentifizierung des Patienten vorsieht, sondern der ePA-Kommunikationskomponente vertraut, dass sie den Patienten richtig authentifiziert hat.

9.4. Autorisierung

Es kommt seitens der ePA nur die Vorabautorisierung bei der Kommunikation über die Forschungsschnittstelle zum Einsatz. Hierfür müssen der Verwalter der Versorgungsdatenbank und der Verwalter der Patientenliste authentifiziert werden. Dies erfolgt durch das Weiterleiten der Identity Assertion durch den ePA-Forschungsadapter. Eine Ad-hoc Autorisierung erfolgt nicht (siehe Abschnitt 5.8.4).

Seitens des Forschungssystems gibt es Anforderungen in Bezug auf die Autorisierung (siehe Architekturentscheidung 4 im Abschnitt 7.2), deren Umsetzung im Folgenden beschrieben wird.

9.4.1. Grundprinzipen der Autorisierung durch die Forschungsschnittstelle

Im Kapitel 7 in der vierten Architekturentscheidung „Autorisierung des Datenaustausches zwischen der ePA und dem Versorgungsmodul“ wurde festgelegt, dass vor jedem Kommunikationsvorgang von oder zur ePA durch den Forschungs-Client-IDAT überprüft werden muss, ob diese Informationen vom bzw. für den Patienten bereitstellt oder angefordert werden dürfen. Um diese Regel zu überprüfen, müssen dem Forschungs-Client-IDAT vier Informationen für die Autorisierungsentscheidung vorliegen:

1. Die Identität des Patienten (PID oder ePA-ID), da die Regeln pro Patienten definiert und für ihn im Forschungs-Client-IDAT abgelegt werden.
2. Ob es sich um eine Bereitstellung oder eine Anforderung handelt, da die Regeln unterscheiden, ob etwas bereitgestellt werden darf oder angefordert werden darf.
3. Ob Informationen an die ePA, die Patientenliste oder die Versorgungsdatenbank geschickt werden.
4. Der Semantic Signifier der Anforderung oder der Bereitstellung.

Diese vier Informationen werden im Forschungs-Client-IDAT in einer Autorisierungsliste (siehe Tabelle 16) geführt und mit den Informationen abgeglichen, die vom anfragenden bzw. bereitstellenden System bereitgestellt werden. Stimmen die Informationen überein, so wird eine positive Autorisierungsentscheidung getroffen. Gibt es keinen Eintrag mit diesen Informationen in der Autorisierungsliste, so wird eine negative Autorisierungsentscheidung getroffen.

Es wird nur die ePA-ID und nicht die PID gespeichert, da diese Liste sonst eine Zusammenführung der PIDs der Patienten mit dem identifizierenden Merkmal der ePA-ID außerhalb der Patientenliste wäre. Es wird eine Liste für die Kommunikation zwischen ePA und Patientenliste und eine Liste für die Kommunikation zwischen ePA und Versorgungsdatenbank geführt. Eine detaillierte Beschreibung der Umsetzung des Autorisierungskonzeptes für die vier generischen Kommunikationsmuster befindet sich im Anhang A5.1

ePA-ID	Semantic Signifier	Anforderung oder Bereitstellung	System
1234567890	„Kontaktdaten“	Anforderung	Patientenliste
1234567890	„Kontaktdaten“	Bereitstellung	ePA
1234567890	„Kontaktdaten“	Anforderung	ePA
1234567890	„Kontaktdaten“	Bereitstellung	Patientenliste
1234567890	„Basisdokumentation“	Bereitstellung	ePA
1234567890	„Basisdokumentation“	Anfordern	ePA
1234567890	„Basisdokumentation“	Bereitstellen	Versorgungsdatenbank
0987654321	„Kontaktdaten“	Anfordern	ePA
0987654321	„Kontaktdaten“	Bereitstellen	Versorgungsdatenbank

Tabelle 16: Beispiel einer Autorisierungsliste

9.4.2. Umsetzung der Anforderungen über das Autorisierungskonzept

Im Folgenden wird erläutert, wie die einzelnen Anforderungen 5-10 zur Autorisierung aus dem Abschnitt 7.1 über das Autorisierungskonzept der Forschungsschnittstelle umgesetzt werden können:

Datenschutzanforderung 5: Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Patientenliste nur die mit ihm vereinbarten Daten (z. B. Kontaktdaten bzw. identifizierenden Daten) bereitstellen kann.

Dies wird durch das Autorisierungskonzept abgedeckt, indem für jeden Patienten unter seiner ePA-ID in der Autorisierungsliste eingetragen wird, welche Semantic Signifier er der Patientenliste bereitstellen darf. Alle anderen Bereitstellungen des Patienten werden verworfen.

Datenschutzanforderung 6, 8 und 9: Die Forschungsschnittstelle muss vor der Kontaktierung eines Patienten überprüfen, ob eine entsprechende Einwilligung des Patienten vorliegt. Die Forschungsschnittstelle muss überprüfen, ob der Patient für neue Forschungsvorhaben rekrutiert werden möchte. Die Forschungsschnittstelle muss überprüfen, ob der Patient über neue Forschungsergebnisse informiert werden möchte.

Hier muss vorher zwischen dem Patienten und dem Forschungsverbund ausgehandelt worden sein, zu welchen Themen er kontaktiert werden darf und dies in Form einer Einwilligung festgehalten sein. Hier können je nach Forschungsverbund unterschiedliche Semantic Signifier in die Liste aufgenommen werden (z. B. Newsletters, Ergebnisse aus abgeschlossenen Studien, Terminerinnerung, neue Forschungsergebnisse, Rekrutierung etc.). Die Informationen werden dann von dem Forschungs-Client-IDAT nur weitergereicht, wenn ein entsprechender Eintrag in der Autorisierungsliste für den Patienten und den Semantic Signifier vorliegt.

Datenschutzanforderung 7: Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Versorgungsdatenbank nur Daten bereitstellt, die auch im Rahmen des Forschungsvorhabens benötigt werden und für die eine Einwilligung des Patienten vorliegt.

Hier müssen durch den Forschungsverbund entsprechende Semantic Signifier für die einzelnen Forschungsvorhaben definiert werden. Besteht die Notwendigkeit, dass im Rahmen eines Forschungsvorhabens bestimmte Informationen aus der ePA des Patienten an die Versorgungsdatenbank übertragen werden sollen, so wird für jeden Patienten ein Eintrag in der Autorisierungsliste mit den entsprechenden Semantic Signifier vorgenommen. Nur diese Informationen werden auch an die Versorgungsdatenbank weitergereicht. Alle anderen Bereitstellungen seitens der ePA werden verworfen.

Datenschutzanforderung 10: Es muss durch den Forschungsverbund festgelegt werden, welche Informationen einem Patienten direkt aus der Versorgungsdatenbank bereitgestellt werden können und welche über einen behandelnden Arzt zur Verfügung gestellt werden müssen. Diese Regeln müssen in der Forschungsschnittstelle abgebildet und überprüft werden.

Hierzu muss der Forschungsverbund festlegen, welche Informationen direkt an den Patienten übertragen werden dürfen. Entsprechende Semantic Signifier werden für jeden Patienten in der Autorisierungsliste hinterlegt. Hierbei wird ein Eintrag hinterlegt, dass der Patient die Informationen anfordern darf, und ein Eintrag angelegt, dass die Datenbank des Versorgungsmoduls die Informationen bereitstellen darf.

9.5. Verschlüsselung

In diesem Abschnitt wird untersucht, inwieweit das Verschlüsselungsmodell der LE-Schnittstelle (siehe Abschnitt 5.7.3) unter Berücksichtigung der Datenschutzanforderungen des Versorgungsmoduls umgesetzt werden kann. Bei entsprechenden Abweichungen wird gezeigt, wie die Verschlüsselung alternativ vorgenommen werden kann.

9.5.1. Analyse der Anforderungen des Versorgungsmoduls in Bezug auf die Verschlüsselung

Betrachtet man die erste Datenschutzanforderungen des Versorgungsmoduls (siehe Abschnitt 7.1), so widerspricht eine nutzerzentrierte Verschlüsslung nicht der Anforderung, dass nicht pseudonymisierte medizinische Daten des Patienten nur ihm oder den sich im Behandlungszusammenhang befindlichen Personen zugänglich gemacht werden dürfen. Im Gegenteil: erst nach einer Verschlüsselung ist es möglich, die Daten aus dem Versorgungsmodul zu depseudonymisieren und danach immer noch der Anforderung gerecht zu werden, dass die Daten nur den oben genannten Personen zugänglich sind.

Die zweite Datenschutzanforderung, dass der PIDv nur zwischen der Patientenliste und der Versorgungsdatenbank kommuniziert werden darf, bleibt von der nutzerzentrierten Verschlüsselung unberührt. Auch die Datenschutzanforderungen 5-10 in Bezug auf die Autorisierung werden durch eine nutzerzentrierte Verschlüsselung nicht betroffen, da die Autorisierungsentscheidungen auf Grundlage von Metadaten aus den Informationsobjekten getroffen werden (siehe Abschnitt 9.4) und die Verschlüsselung nur die Nutzlast der Bereitstellungsobjekte betrifft.

Bei der dritten Anforderung „Der Patientenliste bzw. ihrem Systemverwalter dürfen die medizinischen Daten der Patienten in der Versorgungsdatenbank nicht zugänglich gemacht werden“ ergeben sich durch die nutzerzentrierte Verschlüsselung keine Konflikte.

Betrachtet man die Anforderung 4 „Der Versorgungsdatenbank bzw. ihrem Systemverwalter dürfen die identifizierenden Daten des Patienten in der Patientenliste nicht zugänglich gemacht werden“, so gibt es einen Konflikt mit dem Verschlüsselungsmodell der LE-Schnittstelle beim Kommunikationsmuster „Daten aus einer Versorgungsdatenbank an eine ePA bereitstellen“. Dieser Konflikt entsteht dadurch, dass bei dem Verschlüsselungskonzept der LE-Schnittstelle für die Bereitstellung von Daten an die ePA der öffentliche Schlüssel der ePA für die Verschlüsselung seitens des Absenders (in diesem Fall wäre der Absender die Versorgungsdatenbank) genutzt wird. Der öffentliche Schlüssel der ePA wird als identifizierendes Merkmal eingestuft [16] und darf somit der Versorgungsdatenbank bzw. dem Verwalter der Versorgungsdatenbank nicht bekannt gemacht werden. Hier muss also ein alternatives Verfahren für die Bereitstellung von Daten aus der Versorgungsdatenbank an die ePA etabliert werden, welches eine Geheimhaltung der Identität der Patienten gegenüber der Versorgungsdatenbank bzw. dem Verwalter der Versorgungsdatenbank gewährleistet.

Wie im Abschnitt 5.7.3 beschrieben wird der private Aktenschlüssel (prkAS) beim „Abrufen von Informationsobjekten von einer ePA durch einen Leistungserbringer“ an den Leistungserbringer übertragen. Der prkAS unterliegt einem speziellen Schutz, indem er in einer

[16] Dies ist damit zu begründen, dass der öffentliche Aktenschlüssel der ePA von jedem Leistungserbringer mit der Capability List von der ePA-Zugangskomponente abgerufen werden kann.

speziell geschützten Ablaufumgebung (z. B. dem Konnektor) zwischengespeichert und verarbeitet wird, so dass er dem Leistungserbringer oder dem Leistungserbringersystem nicht offenbart wird. Auch in dem datenhaltenden System darf der private Aktenschlüssel nur verschlüsselt vorliegen [167]. Hier ist also erst mal davon auszugehen[17], dass der private Schlüssel der Versorgungsdatenbank bzw. dem Verwalter der Versorgungsdatenbank verborgen bleibt und somit keine alternative Entschlüsselung durch die Versorgungsdatenbank bzw. dem Forschungs-Client-MDAT vorgenommen werden muss.

9.5.2. Umsetzung des Verschlüsselungskonzepts der Forschungsschnittstelle

Es. wurde in Abschnitt 9.5.1 herausgestellt, dass für die Bereitstellung von Daten aus der Versorgungsdatenbank eine andere Verschlüsselung umgesetzt werden muss, als sie bisher durch die LE-Schnittstelle vorgesehen ist. Diese Verschlüsselung soll trotzdem mit der Verschlüsselungsmethode der LE-Schnittstelle kompatibel sein. D. h. am Ende des Vorgangs muss ein symmetrisch verschlüsseltes MDO mit einem durch den öffentlichen Aktenschlüssel (pubAS) gesicherten symmetrischen Schlüssel (symkeyMDO) vorliegen. Um dies zu erreichen, wird der symmetrische Schlüssel (symkeyMDO) in der ePA generiert und dort mit dem öffentlichen Aktenschlüssel (pubAS) sowie eine Kopie (symkeyMDO_Kopie) mit dem öffentlichen Schlüssel der Versorgungsdatenbank (pubVDB) gesichert (siehe Abbildung 39). Während der durch den öffentliche Aktenschlüssel gesicherte symkeyMDO im ePA-Kernsystem verbleibt und später mit den MDO abgelegt wird, wird die mit dem öffentlichen Schlüssel der Versorgungsdatenbank gesicherte Kopie (symkeyMDO_Kopie) an den Forschungs-Client-MDAT geschickt. Dort wird der symkeyMDO_Kopie mit dem privaten Schlüssel der Versorgungsdatenbank (prkVDB) entschlüsselt und das MDO mit dem symkeyMDO_Kopie verschlüsselt. Anschließend wird das verschlüsselte MDO an das ePA-Kernsystem geschickt. Dort wird es mit dem durch den öffentlichen Schlüssel der ePA gesicherten symkeyMDO zusammen abgelegt.

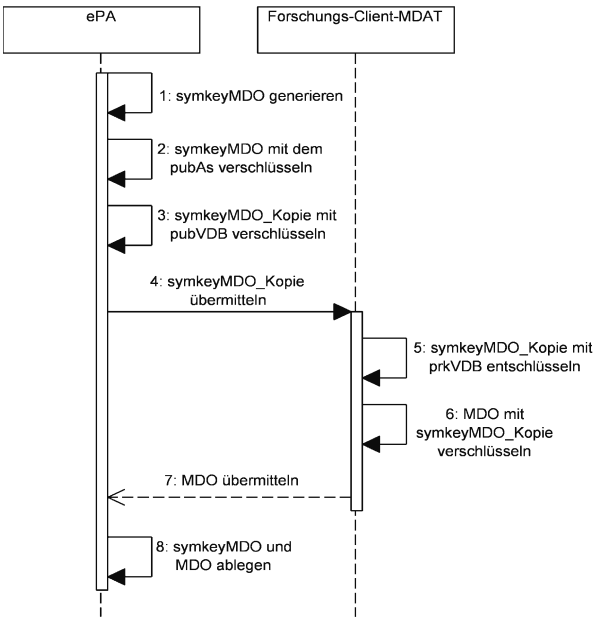

Abbildung 39: Verschlüsselungskonzept der Forschungsschnittstelle

[17] Mögliche Schwachstellen dieses Verfahrens beim Einsatz für die medizinische Forschung werden in der Diskussion aufgezeigt.

Der Forschungs-Client-MDAT muss sowohl eine Bereitstellung ohne Anforderung an die ePA des Patienten schicken können als auch Informationen bereitstellen, die zuvor vom Patienten über seine ePA angefordert wurden. Im Anhang A5.2 wird beschrieben, wie das oben aufgeführte Verschlüsselungskonzept für beide Fälle umgesetzt werden kann.

Anmerkung 1: Das Speichern eines Dummy-Objektes in der ePA ist nur beispielhaft. Die Umsetzung bleibt dem ePA-Hersteller überlassen. Er muss nur einen eindeutigen Bezug zwischen der Anforderung und der Bereitstellung herstellen und den Schlüssel der Bereitstellung später zuordnen.

Anmerkung 2: Wie der symkeyMDO und der symkeyMDO_Kopie erzeugt werden, ist den ePA-Herstellern überlassen. Es muss allerdings sichergestellt werden, dass die symkeyMDO nicht unverschlüsselt Unberechtigten (also auch dem ePA-Hersteller oder ePA-Betreiber) zugänglich gemacht werden. Eine Variante wäre die Erzeugung der Schlüssel im Bürger-Client. In der geschützten Umgebung des Bürger-Clients könnten mehrere symkeyMDO1-N erzeugt werden und jeweils mit dem öffentlichen Aktenschlüssel und dem öffentlichen Schlüssel der Versorgungsdatenbank gesichert werden. Anschließend könnten die gesicherten Schlüssel dann im ePA-Kernsystem gespeichert und bei Bedarf an die Versorgungsdatenbank geschickt werden (Details hierzu sind im Anhang A5.2.4 zu finden).

9.6. Signaturen

Wie schon in der Einleitung zu diesem Kapitel erwähnt wurde, werden die Signaturen medizinischer Datenobjekte für die Forschung in dieser Arbeit nicht betrachtet. Auch die Sicherung der Nachrichten, Schlüssel und Hilfsobjekte muss in einer weiteren Arbeit zusammen mit der Schutzbedarfsanalyse betrachtet werden. In diesem Abschnitt werden nur Voraussetzungen genannt, die beim Umgang mit Signaturen im Zusammenhang mit der Forschungsschnittstelle beachtet werden müssen.

Wird die Datenschutzanforderung des Versorgungsmoduls betrachtet, so besteht hier wie bei der Verschlüsselung der Konflikt mit der Anforderung 4 „Der Versorgungsdatenbank bzw. ihrem Systemverwalter dürfen die identifizierenden Daten des Patienten in der Patientenliste nicht zugänglich gemacht werden“. Auch bei der Prüfung einer von der ePA bzw. dem Patienten ausgestellten Signatur müsste dem Verwalter der Versorgungsdatenbank der öffentlichen Schlüssel der ePA oder des Patienten zugänglich gemacht werden und somit würde eine ungewollte Depseudonymisierung des Patienten stattfinden. Aus diesem Grund müssen alle Signaturen der ePA bzw. des Patienten vor dem Übertragen des Informationsobjektes entfernt und ggf. ersetzt werden (Abhängig vom Ergebnis der Schutzbedarfsanalyse).

Ein weiterer Punkt, der in einer anderen Arbeit betrachtet werden muss, ist das Ersetzen von Informationen aus den Informationsobjekten durch den ePA-Forschungsadapter (wie es in Abschnitt 8.2.1 beschrieben wird), da hierdurch bestehende Signaturen zur Sicherung der Informationsobjekte ungültig gemacht werden, so dass hier eine neue Signatur nötig ist. Wie die Integrität und Authentizität bei diesen Objekten weiterhin erhalten bleiben, muss in einer weiteren Arbeit im Zusammenhang mit einer Schutzbedarfsanalyse untersucht werden. Dies betriff die Kommunikation zwischen ePA und Versorgungsdatenbank in beide Richtungen (Austausch der ePA-ID bzw. der TID). Ein Beispiel wie Signaturen erfolgreich ausgetauscht werden können, wird im UC-7-2 im Anhang A5.2.2 beschrieben. Hier wird der von der ePA verschickte Schlüssel (symkeyMDO_Kopie) durch die Signatur der ePA gesichert. Da die

Versorgungsdatenbank die Signatur der ePA nicht überprüfen kann[18], wird diese von dem ePA-Forschungsadapter überprüft. Bei erfolgreicher Überprüfung signiert der ePA-Forschungsadapter den Schlüssel mit seiner Signatur. Da eine Vertrauensbeziehung zwischen dem ePA-Forschungsadapter und dem Forschungs-Client-MDAT besteht, ist für den Forschungs-Client-MDAT eine erfolgreiche Prüfung der Signatur des ePA-Forschungsadapters ausreichend, um den Schlüssel von der ePA als integer anzuerkennen.

Während bei der Kommunikation zwischen der ePA und der Versorgungsdatenbank Anpassungen in Bezug auf das Konzept der LE-Schnittstelle zum Schutz der Authentizität von Schlüsseln und Hilfsobjekten erforderlich sind, kann das Konzept für die Kommunikation zwischen der Patientenliste und der ePA übernommen werden.

Das Thema Signaturen medizinischer Datenobjekte für die Forschung muss noch gesondert betrachtet werden. Es wird hier zunächst festgelegt, dass die ePA die medizinischen Daten ohne Signatur an die Versorgungsdatenbank schicken soll, da auch Signaturen von Leistungserbringern des Patienten identifizierend sein können, sofern im Rahmen des Versorgungsmoduls nur ein oder sehr wenige Patienten von dem Leistungserbringer behandelt werden. Ob die Zertifikate von Leistungserbringer zum Einsatz kommen können, muss noch im Detail durch eine Schutzbedarfsanalyse, die nicht Teil dieser Arbeit ist, geklärt werden. Die Versorgungsdatenbank könnte die Daten soweit signieren. Allerdings können diese Daten nicht von den einzelnen Erfassern signiert werden, da deren Identitäten bzw. Zertifikate nicht unbedingt auch in der Telematikinfrastruktur bekannt sind bzw. gar keine Zertifikate existieren. Hier kann also nur von der Versorgungsdatenbank durch eine Signatur bestätigt werden. Auch diese Problematik sollte in einer weiteren Arbeit auch im Hinblick auf die Schutzbedarfsanalyse aufgearbeitet werden.

[18] Hier entsteht derselbe Konflikt wie bei der Verschlüsselung, dass der Versorgungsdatenbank der öffentlichen Schlüssel der ePA zur Überprüfung der Signatur nicht offenbart werden darf.

10. Diskussion

In diesem Kapitel werden die Ergebnisse dieser Arbeit in Bezug auf die Forschungsfragen diskutiert und die Ergebnisse mit den in der Literatur aufgeführten Ansätzen zur Nutzung von Versorgungsdaten für die Forschung verglichen.

10.1. Aufbau eines Forschungsverbundes und Auswahl der Anwendungsfälle

Durch die Untersuchung der ersten Forschungsfrage sollte das Forschungssystem genauer spezifiziert werden. Es wurde angenommen, dass nicht für alle Anwendungsfälle eines Forschungsverbundes die Kommunikation über die Forschungsschnittstelle mit Hilfe einer ePA verbessert werden kann. Daher wurde nicht nur der Aufbau eines Forschungsverbundes untersucht, sondern auch welche Anwendungsfälle eines medizinischen Forschungsverbundes für eine Kommunikation über eine ePA nach § 291a geeignet sind. Nur diese Anwendungsfälle sollten weiter betrachtet werden.

Das Forschungssystem wurde auf Grundlage der Anwendungsfälle und IT-Komponenten des Versorgungsmoduls, wie es in den Datenschutzkonzepten der TMF beschrieben wurde, definiert. Dies hat den Vorteil, dass die Anforderungen für ein definiertes System abgeleitet werden konnten. Es bedeutet aber auch, dass die in dieser Arbeit beschriebene Forschungsschnittstelle nicht alle im Kapitel 2 beschriebenen Anwendungsbereiche umsetzen kann. Auch wird im nachfolgenden kritisch hinterfragt, ob der in dieser Arbeit gewählte Ansatz, die Kommunikation der Anwendungsfälle über eine elektronische Patientenakte in der Datenhoheit des Patienten umzusetzen, immer Vorteil gegenüber den bestehenden Ansätzen hat.

Wird der in dieser Arbeit beschriebene Ansatz in Bezug auf die in der Literatur beschriebenen Anwendungsbereiche betrachtet (siehe Kapitel 2), so decken die beschriebenen Anwendungsfälle momentan die Anwendungsbereiche Selbstdokumentation, Nutzung von Versorgungsdaten für Register und Studien sowie Rekrutierung von Patienten ab. Somit können momentan drei der sieben herausgestellten Anwendungsbereiche durch die Forschungsschnittstelle abgedeckt werden. Obwohl damit nur knapp die Hälfe der Anwendungsbereiche abgedeckt werden, so ist dieser Ansatz im Vergleich mit den in der Literatur beschriebenen Ansätzen vorteilhafter, weil diese Ansätze häufig nur einen Anwendungsbereich abdecken. Dabei wurde die die Priorität der Anwendungsbereiche noch nicht berücksichtigt. Hier zeigt z. B. eine Umfrage im Bereich der Pharmaindustrie, dass die Rekrutierung an zweiter Stelle und der Anwendungsfall Data Collection an vierter Stelle der gewünschten Anwendungen steht. Von allen anderen Anwendungsbereichen wird nur die Meldung von unerwünschten Arzneimittelwirkungen von den Befragten mit Platz 1 als noch wichtiger eingestuft [17]. Eine Umfrage im Rahmen des EHR4CR Projektes hat ergeben, dass die Befragten dort eine Verbesserung der Rekrutierung von Patienten für klinische Studien als am wichtigsten ansehen [65]. D. h., dass die über die Forschungsschnittstelle umsetzbaren Anwendungsbereiche für die potentiellen Anwender eine höhere Priorität, in Vergleich zu den anderen Anwendungsbereichen haben. Eine Ausnahme ist die Meldung von unerwünschten Arzneimittelwirkungen.

Bei der Betrachtung der Umsetzung der Anwendungsbereiche sind besonders Stärken des in dieser Arbeit beschriebenen Ansatzes gegenüber den in Kapitel 2 beschriebenen Architekturansätzen im Bereich der Selbstdokumentation zu sehen, da der Patient mit der ePA eine Anwendung hat, die es ihm erlaubt, Daten selbst einzutragen. Bei anderen

Ansätzen gibt es zwar schon teilweise die Möglichkeit, dass der Patient Daten in der Versorgungseinrichtung ausfüllt und die Daten dann in das lokale KIS bzw. in die Studiensoftware übertragen werden, so dass hier auch keine Doppelerfassung der Daten erfolgt. Bei diesem Ansatz sind die Daten danach jedoch nicht mehr für den Patienten zugänglich. D. h. er kann diese Daten beispielweise nicht wie bei dem Eintragen in seiner ePA auch anderen Versorgern zur Verfügung stellen. Zu diesem Zweck müsste der Patient die Daten erneut ausfüllen. Der Ansatz über eine ePA ermöglicht dem Patienten zusätzlich eine kontinuierliche Dokumentation von zuhause und nicht nur zu bestimmten Visiten in der Versorgungseinrichtung. Dies hat den Vorteil, dass die Daten vom Patienten direkt während der Beobachtung erhoben werden können und nicht erst zwei Wochen danach, wenn der Patient einen Fragebogen ausfüllen soll. Hier kann es sogar vorkommen, dass der Patient die Daten erst zuhause notiert (z. B. in einem Schmerztagebuch) und diese Daten dann während der Visite übertragen werden müssen (Doppelerfassung).

Bei der Rekrutierung hat die Umsetzung über eine elektronische Patientenakte in der Datenhoheit des Patienten den Vorteil, dass der Patient direkt über seine ePA informiert werden kann. Voraussetzung für die Kommunikation über eine ePA ist, dass sich der Patient entscheidet, eine ePA zu führen. Das hat zur Folge, dass alle Patienten, die keine ePA führen, bei diesem Ansatz nicht erreicht werden können. Andere Ansätze, die eine Kommunikation ohne patientengeführte ePA vorsehen und die Daten aus den lokalen Versorgungssystemen nutzen, sind da im Vorteil, da sie auf alle Patienten zugreifen können, die in Behandlung waren und nicht nur auf die Daten der Patienten, die eine ePA führen. Ein Nachteil der Rekrutierung auf lokalem Versorgungssystem ist die Kontaktierung des Patienten, da sie komplizierter ist. Dies ist damit zu begründen, dass der Patient in der Regel nicht schon während des Versorgungsprozesses eingewilligt hat, dass seine im Rahmen der Versorgung erhobenen Daten für Forschungszwecke verwendet werden. Daher muss die Kontaktierung immer über den behandelnden Arzt erfolgen. Der behandelnde Arzt fragt den Patienten dann, ob er Interesse hat an einem Forschungsvorhaben teilzunehmen. Erst danach können die Verantwortlichen des Forschungsprojekts mit dem Patienten Kontakt aufnehmen [51,170]. Ein weiterer Vorteil der Rekrutierung über eine patientengeführte ePA ist, dass der Patient aus Eigeninitiative nach Studien suchen kann, die für ihn passen könnten (wie es im Abschnitt 2.4.2 beschrieben wurde). Voraussetzung ist hier natürlich, dass die Patienten dazu bereit sind, Daten aus ihrer ePA für die Forschung bereitzustellen. Hier hat eine Umfrage ergeben, dass 91% der Befragten die Daten aus ihrer ePA auch für die Forschung freigeben würden [171].

Bei der Nutzung von Versorgungsdaten für Register und Studien hat der in dieser Arbeit verfolgte Ansatz den größten Vorteil gegenüber den bereits bestehenden Ansätzen. Das gibt insbesondere wenn es sich um institutionsübergreifende bzw. nationale Forschungsprojekte handelt. Das ist dadurch zu begründen, dass die Systeme der Versorgung schon über eine standardisierte Schnittstelle an die ePA angeschlossen sind. Das Register oder die Studiendatenbank muss somit nur eine Verbindung zur Forschungsschnittstelle implementieren und kann Daten aus allen Versorgungssystemen erhalten. Sollen z. B. wie beim vierten Architekturansatz lokale Versorgungssysteme die Daten direkt an ein Register oder eine Studiendatenbank schicken, so muss für jedes lokales System eine Schnittstelle zu dem Register oder der Studiendatenbank implementiert werden. Während also über den in dieser Arbeit beschriebenen Ansatz eine eins zu eins Verbindung zwischen der Forschungsschnittstelle und dem Register bzw. der Studiendatenbank implementiert werden kann, muss bei dem vierten Architekturansatz eine eins zu n Verbindung zwischen den lokalen

Versorgungsystemen und dem Register bzw. der Studiendatenbank implementiert werden. Bereits bestehende Ansätze, die eine institutionsübergreifende ePA nutzen, um Daten für Register oder Studiendatenbanken zu gewinnen (Ansatz 5 im Abschnitt 2.2) müssten zwar auch nur eine Schnittstelle zwischen der ePA und dem Register bzw. der Studiendatenbank implementieren. Diesen Ansätzen fehlen allerdings bisher die einheitliche Schnittstelle und eine nationale Telematikinfrastruktur zur Kommunikation zwischen den Systemen der Versorgung und der ePA. D. h., dass bei dieser Lösung nur Schnittstellen zu bestimmten Institutionen implementiert wurden und somit nur die Daten einer Region oder eines Krankenhausverbundes für die ePA und damit auch für das Register bzw. die Studiendatenbank genutzt werden können.

Dass in dieser Arbeit nicht alle Anwendungsbereiche betrachtet wurden, liegt an der Einschränkung, nur die Anwendungsfälle des Versorgungsmoduls zu betrachten. Die Forschungsschnittstelle hat auch noch Potential in Bezug auf die noch nicht umgesetzten Anwendungsbereiche und könnte hier sogar gegenüber anderen Architekturansätzen Vorteile bieten. So wäre die Gewinnung von Phänotypdaten über eine patientengeführte lebenslange ePA sehr interessant, da in dieser ePA nicht nur die gesamte Krankheitsgeschichte des Patienten enthalten sein kann, sondern auch weitere gesundheitsrelevante Informationen, wie sein Ess- oder Fitnessverhalten. Der Anwendungsbereich des Qualitätsmanagements[19] wäre über diesen Ansatz ebenfalls umsetzbar. Besonders absetzen kann sich die Forschungsschnittstelle im Bereich des Qualitätsmanagements durch die Erfassung der Lebensqualität des Patienten über seine ePA. Keinen Vorteil scheint der in dieser Arbeit verfolgte Ansatz in Anwendungsbereichen der Behandlungsunterstützung oder der Meldung von unerwünschten Arzneimittelwirkungen gegenüber den anderen Ansätzen zu haben. Hier sind die lokalen Systeme der Leistungserbringer Hauptadressat der Anwendungen und beinhalten auch die Datenbasis für diese Anwendungsfälle.

Es kann zusammengefasst werden, dass die Forschungsschnittstelle einen Großteil der Anwendungsbereiche abdeckt bzw. durch eine Erweiterung abdecken kann. Sie ist besonders für Patienten interessant, die sich aktiv in die Versorgung bzw. Forschungsvorhaben einbringen wollen und auch ihre Daten in einer ePA in eigener Verantwortung pflegen möchten. Es ist allerdings nicht zu erwarten, dass alle Patienten die Lösung für sich als die Beste ansehen. Im Rahmen einer Studie der Barmer zu Nutzen und Akzeptanz von elektronischen Gesundheitsakten wurde herausgestellt, dass die Nutzer einer solchen Akte Patienten über 50 sind und meistens akute oder chronischen Krankheiten haben [172]. Die Forschungsschnittstelle ist also als eine Ergänzung zu anderen Architekturansätzen zu sehen. Sie hat nicht den Anspruch die komplette Kommunikation aller Anwendungsfälle in der medizinischen Forschung abzudecken und konzentriert sich auf Patienten, die aktiv an ihrer Versorgung bzw. der Forschung teilnehmen möchten. Ihren größten Vorteil gegenüber den anderen Architekturansätzen hat Forschungsschnittstelle durch die indirekte Integration aller Versorgungsysteme über die ePA. Dies wird besonders beim Anwendungsbereich „Nutzung von Versorgungsdaten für Register und Studien“ deutlich.

Wird das methodische Vorgehen zur Definition des Forschungssystems betrachtet, so wurde schon angemerkt, dass sich die Betrachtung eines Forschungsverbundes nur auf die Beschreibungen der Datenschutzkonzepte der TMF bezieht. Diese Einschränkung bedeutet, dass die Ergebnisse dieser Arbeit in Bezug auf das Forschungssystem sich nur auf

[19] Hier ist nicht die Qualität der erhobenen Daten gemeint, sondern die Behandlungsqualität.

medizinische Forschungsverbünde beziehen, die sich an den Datenschutzkonzepten der TMF orientieren. D. h. es kann keine Aussage gemacht werden, inwieweit die Kommunikation von Anwendungsfällen von Forschungsvorhaben über eine ePA umgesetzt werden kann, die sich nicht an den Datenschutzkonzepten der TMF orientieren. Die Einschränkung auf die Datenschutzkonzepte der TMF war dennoch notwendig, um überhaupt ein greifbares Forschungssystem zu definieren, entsprechende Anforderungen seitens des Forschungssystems zu erfassen und durch einen Experten-Review auf ihre Richtigkeit und Vollständigkeit überprüfen zu lassen.

Für das Forschungssystem wurden nur Anwendungsfälle des Versorgungsmoduls ausgewählt, die auch einen Patientenbezug haben, da nur für diese Anwendungsfälle die Kommunikation über die ePA umgesetzt werden sollte. Die Auswahl der Anwendungsfälle konnte nicht aufgrund von Aussagen aus der Literatur vorgenommen werden, sondern durch Annahmen des Autors. Somit konnte nicht formal nachgewiesen werden, dass alle Anwendungsfälle richtig ausgewählt wurden und die Forschungsschnittstelle alle relevanten Anwendungsfälle des Versorgungsmoduls umsetzen kann. Diese Auswahl ist jedoch eine wichtige Grundlage für das Kommunikationsmodell. Daher wurde die Auswahl durch einen Expertenreview für das Versorgungsmodul überprüft und bei Unstimmigkeiten mit den Experten diskutiert. Mit der Durchführung eines Experten-Reviews sind also keine Nachteile bei dem Nachweis der Richtigkeit der Auswahl der Anwendungsfälle im Vergleich zu einem Beleg durch die Fachliteratur entstanden.

10.2. Anbindung des Forschungssystems an das ePA-System

Um die zweite Forschungsfrage in Bezug auf die Anbindung des Forschungssystems an das ePA-System zu beantworten, wurden zunächst die IT-Komponenten einer elektronischen Patientenakte nach § 291a analysiert (siehe auch Kapitel 5). Für die Forschungsschnittstelle wurde festgelegt, dass sie nicht direkt mit dem ePA Kernsystem kommuniziert, sondern über die ePA-Kommunikationskomponente Daten von der ePA abruft bzw. der ePA bereitstellt. Diese Festlegung wurde getroffen, um möglichst wenige Anpassungen an den bestehen ePA-System vorzunehmen. Damit wurde auch festgelegt, dass die Forschungsschnittstelle die Schnittstelle der ePA-Kommunikationskomponente bedienen muss. Dieses Vorgehen hat zum einen den Vorteil, dass die Hersteller einer ePA nur gegen eine Schnittstelle implementieren müssen und so weniger Aufwand bei der Implementierung durch die Hersteller entsteht. Dies impliziert auch, dass durch die leichte Einbindung der Forschungsschnittstelle auch mehr Hersteller diese Forschungsschnittstelle unterstützen werden. Der Nachteil des Ansatzes ist, dass die Anforderungen aus der Forschung, z. B. die des Datenschutzes im Rahmen des ePA-Systems, umgesetzt werden müssen, was die Ansätze komplizierter machen kann (siehe z. B. das Konzept zur Verschlüsselung). Bei dieser Fragestellung wird kein Vergleich mit anderen Umsetzungen aus der Literaturrecherche angestrebt, da vergleichbare Löschungen bisher noch nicht publiziert wurden. Das liegt zum einen an den schon genannten gesetzlichen Hürden und zum anderen an der Komplexität und Spezialisierung dieses Themas (Telematikinfrastruktur und elektronische Patientenakte nach § 291a).

Es ist in Rahmen dieser Arbeit gelungen ein Konzept zu erstellen, das eine datenschutz-konforme Kommunikation zwischen der ePA und dem Forschungssystem ermöglicht und dabei so wenig Anpassung wie möglich an den bestehenden Systemen vornimmt. Es wurden aus Komplexitätsgründen Rahmenbedingungen definiert, unter denen eine Kommunikation zwischen dem Forschungs- und dem ePA-System möglich ist. Im Folgenden

werden die Auswirkungen dieser Rahmenbedingungen als auch die Entscheidung, dass die Forschungsschnittstelle über die ePA-Kommunikationskomponente mit dem ePA-Kernsystem kommuniziert, diskutiert:

- Für die Forschungsschnittstelle wurde festgelegt, dass die ePA dem Patienten für die Kommunikation mit dem medizinischen Forschungsverbund einen Bürger-Client zur Verfügung stellen muss. Damit werden Patienten von diesem Ansatz ausgeschlossen, die nur eine Basisakte bedienen können oder wollen. Der Ansatz sollte grundsätzlich auch mit Basisakten funktionieren. Es kann schon jetzt gesagt werden, dass es eine Anpassung an dem Verschlüsselungskonzept der Forschungsschnittstelle geben müsste. Diese Anpassung betrifft die Schlüsselgenerierung im Bürger-Client, die durch eine neue ebenso sichere Lösung ersetzt werden müsste. Durch das Wegfallen des Bürger-Clients wären weitere Funktionen anzupassen. Details hierzu müssen in einer weiteren Arbeit betrachtet werden. Erste Vorschläge hierzu werden im Ausblick (siehe Kapitel 11) aufgenommen. Die Entscheidung, die Forschungsschnittstelle über die ePA-Kommunikationskomponente anzubinden, hat für diesen Punkt weder Vor- noch Nachteile gegenüber einer eigenen Schnittstelle für das ePA-Kernsystem.
- Es wurde für die Forschungsschnittstelle festgelegt, dass sie sowohl Anforderungs- und Bereitstellungsobjekte, als auch Semantic Signifier unterstützen muss. Das bedeutet, dass das Forschungssystem die Nutzlast nach den inhaltlichen und strukturellen Vorgaben der Semantic Signifier aufbereiten bzw. die empfangenen Daten richtig in die Datenbanken des Forschungssystems schreiben muss. Es kommt hinzu, dass der ePA-Forschungsadapter entsprechende Anpassungen an den Bereitstellungs- und Anforderungsobjekten vornehmen muss (z. B. das Entfernen der Quelle oder des Quellsystems, siehe auch Abschnitt 8.2.1). Dies bedeutet auch, dass durch diese Anpassungen die Signaturen, die von dem Quellsystem für das Anforderungs- oder Bereitstellungsobjekt erstellt wurden, nicht mehr gültig sind und durch den ePA-Forschungsadapter ersetzt werden müssen. Hier wäre eine „eigene Lösung“ effizienter gewesen. Ob sie auch sicherer gewesen wäre, kann zum aktuellen Zeitpunkt nicht beurteilt werden, da keine Risikoanalyse durchgeführt worden ist (siehe 2.8), die Aussagen darüber enthält, ob diese Anpassungen das Sicherheitsrisiko erhöhen. Auch muss das Forschungssystem für jeden Semantic Signifier eine entsprechende Implementierung vorsehen. Da in der Forschung allerdings hauptsächlich mit strukturierten Daten gearbeitet wird, hätte hier sowieso ein Standard implementiert werden müssen, um strukturierte Daten zwischen der ePA und dem Versorgungsmodul auszutauschen, so dass hier kein höherer Aufwand betrieben werden muss. Es kommt hinzu, dass die gängigen Standards zum Austausch der Daten (HL7 [173], CDISC [174,175]) über die Semantic Signifier umgesetzt werden können. Der Einsatz von Semantic Signifiern für den Austausch von Daten zwischen dem Patienten, dem Leistungserbringer und dem Forschungsverbund ermöglicht einen effizienten Einsatz der ePA, da die Akteure ihren Informationsbedarf genau definieren können. Dies wirkt somit der befürchteten Informationsüberflutung durch patientengeführte ePAs [176] entgegen und bietet dadurch sogar einen Vorteil gegenüber einer proprietären eigenen Lösung. Zusammenfassend kann gesagt werden, dass der Einsatz von Semantic Signifiern eher Vorteile als Nachteile gegenüber einer eigenen Schnittstelle bringt. Der Einsatz der bestehenden Struktur der Anforderungs- und Bereitstellungsobjekte führt dazu, dass Anpassungen im ePA-Forschungsadapter an den Hilfsobjekten notwendig sind. Hier wäre eine eigene Lösung im Vergleich zur Verwendung der bestehenden Hilfsobjekte besser gewesen.

- Die Forschungsschnittstelle muss vor der Kommunikation mit einer ePA die Capability List der ePA abrufen und auswerten. Hier werden Anpassungen beim Abrufen der Capability-List durch den Forschungs-Client-IDAT vorgenommen. Während beim Abrufen der Capability List durch den Forschungs-Client-IDAT bzw. die Patientenliste keine Anpassungen vorgenommen werden müssen, müssen beim Abrufen der Capability List durch den Forschungs-Client-MDAT die ePA-ID und das Schlüsselmaterial aus der Capability-List entfernt werden. Somit wäre hier eine eigene Lösung aus den gleichen Gründen wie bei der Verwendung der Anforderungs- und Bereitstellungsobjekte effizierter gewesen.
- Im FuE-Projekt wurde festgelegt, dass es keinen zentralen Verzeichnisdienst für die Patientenakten geben soll. Vielmehr soll der Patient die Lokalisierungsinformationen direkt an den Leistungserbringer weitergeben. Als Lokalisierungsinformation dient die sogenannte ePA-ID oder auch die synonym verwendete Akten-ID [144]. Die Forschungsschnittstelle muss während der Kommunikation ein Mapping der Identitäten des Patienten im Forschungs- und ePA-System durchführen. Da das Pseudonym der ePA nicht bekannt sein darf und somit auch bei einer eigenen Schnittstelle nicht vorliegen würde, muss sowieso ein Mapping der Identität des Patienten in der ePA-Domäne auf die Identität des Patienten in der Forschungsdomäne stattfinden. Daher wäre ein eigener Ansatz nicht effizienter gewesen.
- Für die Forschungsschnittstelle wurde festgelegt, dass eine Vorab-Autorisierung aber keine Ad-Hoc-Autorisierung umgesetzt werden muss. Mit der Entscheidung die ePA-Kommunikationskomponente zur Anbindung des Forschungssystems an die ePA zu nutzen, wird auch das Autorisierungskonzept der LE-Schnittstelle verwendet. Da die Autorisierung allerdings nicht in der Schnittstelle, sondern im ePA-Kernsystem vorgenommen wird, müssen die vorgeschlagenen Funktionen in Bezug auf die Autorisierung immer durch die Systeme der Hersteller implementiert werden. Eine von diesen Funktionen ist z. B., dass bestimmte Datenobjekte von den Systemen der Leistungserbringer unmittelbar an die Versorgungsdatenbank weitergeleitet werden. Hier wäre eine Umsetzung durch eine eigene Lösung besser gewesen.
- Die LE-Schnittstelle sieht die Möglichkeit vor, dass die ePA als USB-Akte oder als Online-Akte umgesetzt wird (siehe auch Abbildung 10). In dieser Arbeit wurde festgelegt, dass die Forschungsschnittstelle nur mit einer Online-Akte genutzt werden kann. Auch hier wird eine Einschränkung vorgenommen, so dass durch den gewählten Ansatz alle Patienten mit einer USB-Akte nicht über die Forschungsschnittstelle kommunizieren können. Hier muss eine weitere Arbeit dieses Thema aufarbeiten, um eine Lösung für USB-Akten zu beschreiben. Erste Vorschläge hierzu werden im Ausblick aufgenommen. Erst wenn ein solcher Vorschlag vorliegt, kann auch analysiert werden, ob eine eigene Schnittstelle Vorteile gegenüber der Nutzung der bestehenden ePA-Kommunikationskomponente hat.
- Die Forschungsschnittstelle unterstützt nur asynchrone Kommunikationsmuster für den Austausch von Informationsobjekten zwischen der ePA und den IT-Systemen des Forschungsverbundes (nur Hilfsobjekte werden synchron kommuniziert), da bei keinem umzusetzenden Anwendungsfall eine direkte Antwort erwartet wird. Die Umsetzung der Kommunikation über synchrone und asynchrone Kommunikationsmuster hat keine negativen Auswirkungen auf die Forschungsschnittstelle im Vergleich zu einer eigenen Lösung. Dass die Forschungsschnittstelle nur asynchrone Kommunikationsmuster unterstützt, kann allerdings Auswirkungen auf eine mögliche Nutzung mit der Basisakte

und der USB-Akte haben, da diese beiden Akten nur synchrone Kommunikationsmuster unterstützen [162]. Auch hier muss zunächst ein konkreter Vorschlag erarbeitet werden, um beurteilen zu können, ob auch mit dem Einsatz einer Basis und einer USB-Akte eine eigene Schnittstelle Vorteile gegenüber der Nutzung der bestehenden ePA-Kommunikationskomponente hat.

Zusammenfassend hat die Architekturentscheidung, die ePA-Kommunikationskomponente als Schnittstelle zwischen der ePA und der Forschungsschnittstelle zu nutzen, den großen Vorteil, dass die Hersteller keine weitere Schnittstelle implementieren müssen. Als Nachteile sind zu nennen, dass die Autorisierung immer über die ePA laufen muss und die Anforderungs- und Bereitstellungsobjekte sowie die Capability List angepasst werden müssen. Die Einschränkungen, die für den Betrieb einer Forschungsschnittstelle vorgenommen wurden, führen dazu, dass Patienten mit einer Basisakte oder einer USB-Akte die Forschungsschnittstelle nicht nutzen können. Es scheint zum jetzigen Zeitpunkt grundsätzlich (eine notwendige Anpassung des Verschlüsselungskonzeptes wurde schon angesprochen) nichts gegen eine Erweiterung der Forschungsschnittstelle und somit eine Aufhebung der oben aufgeführten Einschränkungen zu sprechen. Erste Vorschläge werden im Ausblick skizziert.

Die Forschungsschnittstelle wurde unter der Annahme betrachtet, dass das ePA-System als vollständiges System funktioniert und verfügbar ist. Wird das ePA-System nun im Detail betrachtet, dann sind noch einige Baustellen zu finden.

Als erstes ist die Verfügbarkeit der Infrastruktur für Nutzung der ePA zu nennen. Auch wenn in Deutschland die Krankenkassen die ersten eGKs ausgeben und die Arztpraxen sowie die Krankenhäuser sich auf die Einführung der eGK einrichten, beinhaltet dieser sogenannte „Basis-Rollout“ nur das Auslesen der Versichertenstammdaten und die Europäische Krankenversicherungskarte für die Behandlung im europäischen Ausland [177]. In den nächsten Schritten Online-Rollout 1 und 2 wird die ePA als Anwendung noch nicht betrachtet [178], auch wenn mit der im 2. Schritt betrachteten elektronischen Fallakte [179] grundlegende Dienste (wie z. B. der Identity Provider) für die ePA eingeführt werden. Hier gibt es keinen Zeitplan, wann diese Dienste flächendeckend zur Verfügung gestellt werden können.

Werden die Aktenhersteller betrachtet, die momentan ein potentielles Produkt für eine ePA nach § 291a anbieten, so scheint hier der Markt in Deutschland eher kleiner zu werden [108,120,123]. Dies hängt mit dem oben genannten Punkt zusammen, dass die Infrastruktur für die Nutzung einer solchen Akte noch nicht aufgebaut ist. Es kommt hinzu, dass eine Integration in die bestehenden Arztinformationssysteme fehlt. Dies wird durch eine Studie der Barmer zur Nutzung und Akzeptanz von elektronischen Gesundheitsakten bestätigt. In der Studie wurde festgestellt, dass die Versicherten eine ePA nur akzeptieren, wenn die Daten vollständig, aktuell und zuverlässig sind (d. h. von allen Leistungserbringern die Daten automatisch in die ePA überführt werden)[172].

Im FuE ePA gibt es zwar eine Zusammenarbeit mit einem USB-Aktenhersteller [168], allerdings wird diese Zusammenarbeit nicht von der Forschungsschnittstelle unterstützt werden können (siehe oben) und auch hier kann keine flächendeckende Integration in alle Arztinformationssysteme vorgenommen werden.

Ein weiterer Punkt ist das Fehlen der Semantic Signifier für den Austausch zwischen dem Versorgungsmodul und der ePA bzw. den Leistungserbringersystemen. Auch hier müssten für einen flächendeckenden Einsatz alle ePA-Hersteller die Datenbanken des Versor-

gungsmoduls und alle Hersteller der Arztinformationssysteme diese Semantic Signifier unterstützen. Die Semantic Signifier für das Versorgungsmodul sollten allerdings überschaubar sein, so dass es vorstellbar ist, für eine Pilotregion mit einem Aktenhersteller und den dort verbreitetsten Herstellern von Arztinformationssystem diese Semantic Signifier umzusetzen (siehe auch Ausblick). Die Spezifikationen des FuE-ePA-Projektes sind noch nicht endgültig. Es wurde zwar ein Prototyp entwickelt, eine Referenzimplementierung durch einen Hersteller einer Onlineakte gibt es bisher noch nicht, so dass sich die Spezifikationen noch ändern können. Dies kann Auswirkungen auf die in dieser Arbeit vorgeschlagene Lösung haben, beispielsweise wenn sich das Verschlüsselungsmodell ändert.

Ein wichtiger Punkt ist die Einbeziehung der Ärzteschaft. Dies beutet sowohl eine flächendeckende Anbindung der Arztinformationssysteme als auch ein System zur Vergütung der Ärzte für die Unterstützung des Patienten bei der Nutzung und Pflege seiner ePA. Die Studie kommt hier zu dem Schluss: *„Dreh- und Angelpunkt für die Akzeptanz elektronischer Gesundheitsakten ist der automatische Datentransfer aus Arztpraxen. Solange in Deutschland keine flächendeckende Telematik-Infrastruktur vorhanden ist, werden moderne IT-Instrumente wie die elektronische Gesundheitsakte nicht zum Durchbruch gelangen.“* [172, Seite 29]

Zusammenfassend kann gesagt werden, dass solange die oben genannten Probleme noch nicht gelöst sind, die Vorteile, die sich aus der Nutzung einer nationalen Telematikinfrastruktur ergeben, gegenüber den bestehenden lokalen Ansätzen oder den Ansätzen mit regionalen institutionsübergreifenden ePAs nicht ausgenutzt werden können. Sobald eine funktionierende Telematikinfrastruktur inklusive funktionierendem ePA-System etabliert ist, kann die Forschungsschnittstelle ein enormes Potential entfalten und dabei durch die Verwendung einer bestehenden IT-Infrastruktur nicht nur relativ schnell umgesetzt werden, sondern auch extrem kostengünstig (im Vergleich zum Aufbau einer eigenen nationalen IT-Infrastruktur für die Forschung) etabliert werden.

10.3. Kommunikationsmodell für die Anbindung eines Versorgungsmoduls an eine ePA

Mit der Beantwortung der ersten und zweiten Forschungsfrage wurden das Forschungssystem und das ePA-System definiert und die Anforderungen seitens des ePA-Systems in Bezug auf die Kommunikation und den Zugriff auf die ePA durch das Forschungssystem herausgestellt. Anschließend wurde untersucht, wie ein generisches Kommunikationsmodell aussehen kann, über das die Kommunikationsvorgänge aller ausgewählten Anwendungsfälle mit Hilfe einer ePA nach § 291a umgesetzt werden können. Hier ist es gelungen, ein Kommunikationsmodell zu entwickeln und die Anforderungen herzuleiten, unter denen dieses Modell umgesetzt werden kann. Durch die Zusammenfassung der insgesamt 12 Kommunikationsmuster zu vier generischen Kommunikationsmustern wurde die Komplexität der umzusetzenden Kommunikation über die Schnittstelle erheblich vereinfacht. Dies hatte extreme Vorteile bei der Beschreibung sowohl der Facharchitektur als auch der Sicherheitsarchitektur, da die Facharchitektur als auch die Sicherheitsarchitektur nur noch für die vier Kommunikationsmuster beschrieben werden mussten.

Eine andere Möglichkeit die Fach- und Sicherheitsarchitektur herzuleiten, wäre den Schritt der Abstraktion in ein Modell wegzulassen und die Anwendungsfälle direkt als Grundlage für die Fach- und Sicherheitsarchitektur zu nutzen. Im Folgenden wird diskutiert, welche Vor-

und Nachteile sich aus der Nutzung eines Kommunikationsmodells im Vergleich zur direkten Verwendung von Anwendungsfällen für die Herleitung einer Fach- und Sicherheitsarchitektur der Forschungsschnittstelle ergeben.

Das Ziel, die Kommunikation zwischen der ePA und dem Versorgungsmodul medienbruchfrei zu gestalten, wurde durch das vorgeschlagene Kommunikationsmodell vollständig erreicht. Bei der Verbesserung der Kommunikation im Sinne einer direkteren Kommunikation zwischen dem Patienten und den Akteuren des Versorgungsmoduls konnten alle Kommunikationen, die nicht schon direkt erfolgten, durch eine direkte Kommunikation umgesetzt werden (siehe Tabelle 37 im Anhang A2.7). Um das Modell sinnvoll abbilden zu können, wurde die Komplexität reduziert. D. h., dass das Modell nur die Kommunikation zwischen dem Hauptakteur und dem Patienten berücksichtigt. Die restliche Kommunikation ist dem Forschungsverbund überlassen. Somit berücksichtigt das Modell nur die Kommunikation bis zur Patientenliste bzw. deren Verwalter und der Versorgungsdatenbank bzw. deren Verwalter. Bei den betrachteten Anwendungsfällen müssen der Verwalter der Patientenliste und der Verwalter der Versorgungsdatenbank teilweise noch mit anderen Akteuren kommunizieren. Beispielweise kommuniziert bei dem Anwendungsfall „Rekrutieren von Patienten“ der Forscher erst mit dem Verwalter der Versorgungsdatenbank und der Verwalter der Versorgungsdatenbank erst mit dem Patienten. Wie die Kommunikation zwischen den Akteuren innerhalb des Forschungsverbundes umgesetzt wird, liegt außerhalb der Betrachtung des Modells. Je nach Umsetzung kann es hier wieder zu Medienbrüchen kommen. Wäre der gesamte Anwendungsfall als einzelner betrachtet worden, so hätte hier eine gesamte Kommunikation medienbruchfrei konzipiert werden können. Weiterhin wurde bei der Beschreibung und Analyse der Kommunikation festgelegt, dass immer nur eine mögliche Umsetzung eines Anwendungsfalls betrachtet wird. Gab es mehrere Umsetzungsmöglichkeiten, so wurde immer die Umsetzung ausgewählt, die eine direkte Kommunikation zwischen dem Patienten und dem Forschungsverbund ermöglicht. Das bedeutet auch, dass das Kommunikationsmodell immer nur für diese eine Umsetzung funktioniert. Die Forschungsverbünde, die den Anwendungsfall anders umgesetzt haben, können den Anwendungsfall, wie in der Arbeit beschrieben, zusätzlich über die Forschungsschnittstelle umsetzen und / oder die bestehenden Prozesse ohne die Forschungsschnittstelle weiter umsetzen. Eine weitere Möglichkeit wäre die Anpassung der Kommunikation der Anwendungsfälle innerhalb des Forschungsverbundes [20]. Wären alle Umsetzungsmöglichkeiten der Anwendungsfälle betrachtet worden, so wären diese Anpassungen nicht notwendig.

Ein wesentlicher Nachteil der Betrachtung einzelner Anwendungsfälle als Grundlage für die Fach- und Sicherheitsarchitektur ist die Komplexität. So müsste bei der Herleitung der Fach- und Sicherheitsarchitektur gezeigt werden, dass die Anforderungen für jeden Anwendungsfall und seine unterschiedlichen Umsetzungsmöglichkeiten erfüllt wurden. Im Falle des Versorgungsmoduls wären dies 12 Anwendungsfälle und die entsprechenden unterschiedlichen Umsetzungsmöglichkeiten, während das Kommunikationsmodell nur 4 Kommunikationsmuster hat. Wenn die Forschungsschnittstelle auch noch für die anderen Module umgesetzt werden sollte, würde dies die Komplexität wegen einer Vielzahl an zusätzlichen Anwendungsfällen um einige erhöhen. Außerdem würden durch die Umsetzung der gesamten Kommunikation der einzelnen Anwendungsfalls auch erhebliche Eingriffe in

[20] Hierbei handelt es sich nicht um eine Anpassung der IT-System, sondern einzelner Prozesse innerhalb des Forschungsverbundes.

die bestehenden IT-Systeme eines Forschungsverbundes vorgenommen werden müssen. Genau dies sollte in dieser Arbeit vermieden werden. D. h., dass das hier gewählte Kommunikationsmodell die beste Lösung gewesen ist, da die Komplexität erheblich reduziert wird und den bestehenden IT-Systemen in der medizinischen Forschung genügend Spielraum für eine einfach Integration ohne viele Anpassungen an den IT-Systemen gegeben wird.

Wird nun die Methodik zur Herleitung des Kommunikationsmodells betrachtet, so wurde bei der Beschreibung der Kommunikation der einzelnen Anwendungsfälle immer herausgestellt, welche Informationen dem Patienten und welche Informationen dem Forschungsverbund nach Ablauf der Kommunikation vorliegen. Auf dieser Grundalge wurde dann abgeleitet, wie ein generischer Austausch von Informationen zwischen den Akteuren stattfinden kann. Bei diesem Vorgehen besteht die Möglichkeit, dass nicht alle Informationen identifiziert werden und somit eine wichtige Grundlage für die Herleitung des Kommunikationsmodells nicht vollständig ist. Daher wurde ein Review der Ergebnisse der Analyse durchgeführt und für jeden Anwendungsfall abgefragt, ob weitere Informationen zwischen dem Patienten und dem Forschungsverbund ausgetauscht werden. Dies bedeutet, dass diese Grundlage des Kommunikationsmodells in Bezug auf ihre Richtigkeit von Experten überprüft und bestätigt wurde.

Um die generischen Kommunikationsmuster umsetzen zu können wurden 14 (Datenschutz-) Anforderungen identifiziert. Zehn davon wurden durch die Forschungsschnittstelle, eine durch das Forschungssystem und drei durch das ePA-System umgesetzt. Hier wurde also das Ziel erreicht, möglichst wenig Anforderungen an das ePA- und das Forschungssystem zu stellen. Auch hier stellt sich die Frage, ob alle relevanten Datenschutzanforderungen erhoben wurden und somit die zweite Grundlage für das Kommunikationsmodell vollständig ist. Da es in der Literatur keine konkreten Angaben gibt (z. B. eine Auflistung aller relevanten Datenschutzanforderungen), konnte dies nur aus der Beschreibung der Anwendungsfälle abgeleitet werden. Diese Ableitung wurde ebenfalls durch einen Experten-Review überprüft, so dass auch die zweite Grundlage für das Kommunikationsmodell auf ihre Richtigkeit überprüft worden ist.

Zusammenfassend kann gesagt werden, dass die Auswahl eines Kommunikationsmodells für die Herleitung der Fach- und Sicherheitsarchitektur gegenüber einer direkten Herleitung aus den einzelnen Anwendungsfällen erheblich mehr Vorteile als Nachteile mit sich bringt. Außerdem konnte herausgestellt werden, dass die wichtigen Grundlagen für dieses Kommunikationsmodell durch Experten auf ihre Richtigkeit bzw. Vollständigkeit überprüft wurden und somit möglichen Schwachpunkten des Kommunikationsmodells aufgrund unvollständiger Grundlagen gegengewirkt werden konnte.

10.4. Spezifikation der Forschungsschnittstelle

Im Nachfolgenden werden die einzelnen Ergebnisse zur Umsetzung der Kommunikation zwischen einer ePA und dem Versorgungsmodul über eine Forschungsschnittstelle sowie der Fach- und der Sicherheitsarchitektur einzeln diskutiert.

Es wurde gezeigt, dass die generischen Kommunikationsmuster des Kommunikations-modells unter Berücksichtigung der herausgearbeiteten Datenschutzanforderungen über eine Erweiterung der Infrastruktur des ePA-Systems umgesetzt werden können. Im Folgenden wird der methodische Ansatz zur Umsetzung des Modells diskutiert, mögliche

Schwachpunkte in der Methodik herausgestellt und beschrieben, wie diesen Schwachpunkten entgegengewirkt wurde.

Bei der Beschreibung einer Umsetzung des Kommunikationsmodells durch eine Erweiterung des ePA-Systems wurden nicht nur die während der Analyse der Anwendungsfälle (siehe Abschnitt 6.2 und 6.3) herausgestellten Datenschutzanforderungen berücksichtigt, sondern auch die grundlegenden Datenschutzanforderungen, die an den Betrieb eines Versorgungsmoduls gestellt werden (siehe Abschnitt 7.1). Es ist hierbei wichtig, dass die Datenschutzanforderungen vollständig erfasst wurden. Während die speziellen Datenschutzanforderungen aus den Anwendungsfällen überprüft worden sind, stellt sich hier die Frage nach der Vollständigkeit der grundlegenden Datenschutzanforderungen an den Betrieb eines Versorgungsmoduls. Diese Anforderungen werden zwar indirekt in den Datenschutzkonzepten der TMF genannt, allerdings gibt es keine explizite Auflistung dieser Anforderungen, so dass die Vollständigkeit der grundlegenden Datenschutzanforderungen durch entsprechenden Literaturverweise schwer belegt werden kann. Um diesem Punkt entgegenzuwirken, wurde ein Review durchgeführt, durch den bestätigt wurde, dass alle relevanten Datenschutzanforderungen berücksichtigt wurden.

Anschließend wurden aus den Datenschutzanforderungen die Architekturentscheidungen abgeleitet und beschrieben, wie die generischen Kommunikationsmuster über diese Architektur umgesetzt werden können. Hierbei besteht der Anspruch, dass während jeder Kommunikation die herausgestellten Datenschutzanforderungen eingehalten werden. Dies wurde ebenfalls durch einen Experten-Review bestätigt, so dass nicht nur das Kommunikationsmodell durch Experten überprüft wurde, sondern auch die datenschutzkonforme Umsetzung des Kommunikationsmodells über die Komponenten der Forschungsschnittstelle. Die Datenschutzanforderungen an die Autorisierung wurden durch den Review nicht überprüft, da diese Anforderungen nicht im Kapitel 7 sondern erst im Kapitel 9 zur Sicherheitsarchitektur im Detail aufgenommen wurden. Im Rahmen des Reviews wurde beschrieben, an welcher Stelle eine Autorisierung stattfinden muss, so dass sich der Review nur auf die Umsetzung der ersten 4 Datenschutzanforderungen bezieht. Die Umsetzung der Sicherheitsarchitektur wurde nicht durch den Experten-Review bestätigt, da hierfür die Detailinformationen des FuE-ePA-Projektes notwendig sind und die Experten in Bezug auf das Thema Datenschutz in medizinischen Forschungsverbünden ausgewählt wurden. Hier wurden die Qualitätssicherungsmaßnahmen des FuE-ePA-Projektes (Kommentierung der Partner des FuE-ePA-Projektes und Diskussion der Kommentare) genutzt, um die Richtigkeit der Umsetzung der Sicherheitsarchitektur zu bestätigen.

Nachdem die Umsetzung des Kommunikationsmodells für die Komponenten der Forschungsschnittstelle beschrieben wurde, konnte auf dieser Grundlage eine Facharchitektur beschrieben werden, die das Verhalten der einzelnen Komponenten bei der Umsetzung der Kommunikation der einzelnen Kommunikationsmuster im Detail beschreibt. Alle Anforderungen an die Forschungsschnittstelle wurden berücksichtigt, so dass möglichst wenig Anpassungen bzw. Anforderungen an das ePA- und das Forschungssystem bestehen. Hier muss allerdings einschränkend gesagt werden, dass die Facharchitektur nur die Anforderungen des Versorgungsmoduls erfüllt. D. h. es gibt noch keine Aussagen dazu, ob und wie leicht sich die anderen Module eines Forschungsverbundes über diese Facharchitektur an das ePA-System anbinden lassen. Außerdem ist zu berücksichtigen, dass zwar die Einhaltung der Datenschutzanforderungen der Kommunikation durch die einzelnen Komponenten durch Experten überprüft wurde, aber das detaillierte Verhalten der

Komponenten der Forschungsschnittstelle (wie es in der Facharchitektur beschrieben wurde) nicht durch den Experten-Review abgedeckt war. Auch hier sind Detailinformationen aus dem FuE-ePA-Projekt notwendig, weshalb auch hier die Qualitätssicherungsmaßnahmen des FuE-ePA-Projektes genutzt wurden, um die Richtigkeit der Umsetzung der Facharchitektur zu bestätigen.

Es wurden Teile der Fach- und Sicherheitsarchitektur im Rahmen der Prototypentwicklung im FuE-ePA-Projekt entwickelt. Hier wurden die generischen Kommunikationsmuster UC-3-1 “Informationen aus einer Patientenliste einer ePA bereitstellen“ und UC-4-1 „Daten aus einer ePA einer Versorgungsdatenbank bereitstellen“ umgesetzt und gezeigt, dass die vorgeschlagene Facharchitektur implementierbar ist. Die anderen Kommunikationsmuster wurden aus Zeitgründen nicht mehr implementiert. Da die Mechanismen allerdings die gleichen sind und die Kommunikation zwischen den Komponenten umgesetzt wurde, ist davon auszugehen, dass auch die anderen beiden generischen Kommunikationsmuster umsetzbar sind. Das Abrufen der Capability List wurde ebenfalls nicht implementiert. Es handelt sich hier um eine Prototypimplementierung, in die ein Register eingebunden wurde. Allerdings können hier keine Aussagen über den Einsatz des Konzeptes in einer realen Umgebung getroffen werden und auch Aspekte wie die Performance, Usability etc. sind nicht untersucht worden. Da es sich in dieser Arbeit um eine Konzeption handelt und bis zu einer Umsetzung in einer realen Umgebung noch erhebliche Arbeiten geleistet werden müssen, wurden diese Themen von vornherein ausgeklammert und müssen in einer weiteren Arbeit betrachtet werden. Es konnte eine Sicherheitsarchitektur für die Forschungsschnittstelle auf Basis der Sicherheitsarchitektur der LE-Schnittstelle beschrieben werden, die alle Datenschutzanforderungen des Versorgungsmoduls erfüllt. Die Anforderungen an die Sicherheitsarchitektur wurden zwar im Rahmen des Experten-Reviews bestätigt, allerdings wurde die Richtigkeit der Umsetzung der Anforderungen im Rahmen der Sicherheitsarchitektur nicht überprüft. Hier wurde wie oben beschrieben eine Qualitätssicherung der Ergebnisse durch die FuE-ePA-Projektpartner durchgeführt, um die Richtigkeit der Sicherheitsarchitektur zu bestätigen.

Ein weiterer Punkt, den es zu beachten gilt, ist die getroffene Annahme, dass das ePA-System sicher ist. Es gibt allerdings keinen Nachweis dafür, dass die vorgeschlagene Sicherheitsarchitektur der LE-Schnittstelle wirklich sicher ist. Auch hier gibt es keinen formalen Nachweis der Richtigkeit, sondern nur eine Überprüfung der Sicherheitsarchitektur der LE-Schnittstelle durch die Projektpartner des FuE-ePA-Projektes und eine prototypische Implementierung. Eine Betrachtung der Sicherheit des Gesamtsystems ist zu diesem Zeitpunkt noch nicht möglich und kann erst durchgeführt werden, wenn die Spezifikationen der ePA und der Telematikinfrastruktur weiter fortgeschritten sind.

Auch wenn die Sicherheit des Gesamtsystems noch nicht bewertet werden kann, können einzelne mögliche Schwachpunkte jetzt schon identifiziert werden. Ein möglicher Schwachpunkt der Sicherheitsarchitektur ist das Verfahren der Entschlüsselung der medizinischen Daten aus der ePA beim Leistungserbringer durch den privaten Aktenschlüssel. Auch wenn dieses Verfahren für die Versorgung ausreichend sein kann, da ein Leistungserbringer immer nur Zugriff auf die privaten Schlüssel der Akten seiner Patienten hat, sollte dieses Verfahren nochmals in einer Schutzbedarfsanalyse (die nicht Bestandteil dieser Arbeit ist) für den Bereich der Forschung genauer betrachtet werden. Zum Beispiel kann der Verwalter der Versorgungsdatenbank bzw. der Patientenliste von allen ePAs, die für die Kommunikation des Versorgungsmoduls freigegeben wurden, Informationen abrufen (bei einem großen Register wie beispielweise dem Nationales Register für angeborene

Herzfehler nehmen ca. 40.000 Patienten teil [148]). Dies führt dazu, dass er alle privaten Aktenschlüssel dieser Patienten anfordern kann. Hier könnten Begehrlichkeiten geweckt werden, gerade in der Hinsicht, dass es gut vorstellbar ist, dass alle Patienten des Versorgungsmoduls bei einem Aktenbetreiber ihre Akte führen, wenn es z. B. ein kostenloser Service des Forschungsverbundes ist. Damit müssten sich nur ein verantwortlicher Administrator des Aktenbetreibers und der Verwalter der Patientenliste bzw. der Versorgungsdatenbank verbünden, um die Patientenakten der Patienten eines Forschungsverbundes zu entschlüsseln. In der Versorgung ist jedoch davon auszugehen, dass die Patienten eines Leistungserbringers bei diversen Aktenbetreibern sind, so dass hier die Gefahr nicht so hoch ist. Sollte sich während der Schutzbedarfsanalyse herausstellen, dass das Risiko für die Übertragung des privaten Aktenschlüssels zu hoch ist, so wird hier eine Umschlüsselung des symkeyMDO auf den öffentlichen Schlüssel der Versorgungsdatenbank durch den Patienten vorgeschlagen.

Ein weiterer offener Punkt ist der Umgang mit Signaturen. Hier wurden zwar Voraussetzungen genannt, wie in Bezug auf die Forschungsschnittstelle mit Signaturen umgegangen werden sollte. Es wurde aber keine genaue Analyse durchgeführt und auch kein Konzept für den Umgang mit Signaturen entwickelt. Aufgrund der Komplexität dieses Themas wurde es am Anfang der Arbeit extra abgegrenzt, so dass hier auch keine konkreten Ergebnisse erwartet wurden. Hier muss zu einem späteren Zeitpunkt eine Analyse durchgeführt und die Ergebnisse in die Konzeption der Forschungsschnittstelle bzw. ihrer Sicherheitsarchitektur eingearbeitet werden. Wie die Integrität von Objekten aus der ePA während der Übertragung zu der Versorgungsdatenbank aufrechterhalten werden kann, ohne dass die Identität des Patienten bzw. seiner ePA offenbart wird, wurde am Beispiel der Verschlüsselung im UC-7-2 im Anhang A5.2.2 beschrieben. Auf Grundlage dieses Beispiels kann in einer weiteren Arbeit das Signaturkonzept (weiter-)entwickelt werden.

Es wurde das Autorisierungskonzept und das Verschlüsselungskonzept prototypisch umgesetzt, so dass davon ausgegangen werden kann, dass die Sicherheitsarchitektur der Forschungsschnittstelle implementierbar ist. Bei der prototypischen Umsetzung wurde davon ausgegangen, dass die eGK und der HBA sowie ein Konnektor, Identity Provider als auch die PKI Services zur Verfügung stehen. Wie oben erwähnt ist die Telematikinfrastruktur gerade erst im Aufbau und die Ausgabe der eGKs noch nicht abgeschlossen, so dass momentan eine flächendeckende Umsetzung der Sicherheitsarchitektur der LE- und der Forschungsschnittstelle nicht möglich ist. Es ist auch eine Schutzbedarfsanalyse der Forschungsschnittstelle offen, die vielleicht noch Änderungen an der Sicherheitsarchitektur mit sich bringen kann. Auch wenn keine formale Schutzbedarfsanalyse durchgeführt wurde, kann davon ausgegangen werden, dass die Forschungsschnittstelle sicher ist, da die verwendeten Sicherheitsmechanismen aus Forschung und Versorgung, die sonst für den Schutz der Systeme und Daten eingesetzt werden, verwendet wurden. Zudem wurde analysiert, ob Konflikte zwischen den Schutzmechanismen auftreten und bei entsprechenden Konflikten das Sicherheitskonzept entsprechend angepasst. Eine Ausnahme bildet der Umgang mit Signaturen, der nicht genau analysiert wurde.

Im oberen Abschnitt (10.1) wurde schon herausgestellt, dass die Forschungsschnittstelle durch die gewählte Facharchitektur bei der Integration zwischen den Versorgungs- und Forschungssystemen gegenüber anderen in der Literatur beschriebenen Ansätzen Vorteile hat. Dies wurde dadurch begründet, dass nur das Forschungssystem über die Forschungsschnittstelle an die ePA angebunden werden muss und die Integration sämtlicher

Versorgungssysteme über die ePA erfolgt. Wird die Lösung nun in Bezug auf ihre Sicherheitsarchitektur mit anderen Lösungen zur Nutzung von Versorgungsdaten für die Forschung verglichen, so ist anzunehmen, dass die Forschungsschnittstelle dank der hohen Sicherheitsstandards innerhalb der Telematikinfrastruktur einen sehr hohes Sicherheitsniveau erfüllt, das andere Lösungen nur mit einem enormen Aufwand bieten können (z. B. Ausrollen von Smartcards, Konnektoren PKIs etc.). Somit ist die Forschungsschnittstelle auch für den Transport von sensiblen medizinischen Daten (z. B. genetischen Daten) gut geeignet. Die Nutzung der Telematikinfrastruktur bedeutet allerdings auch, dass sich der Nutzerkreis nur auf Deutschland bezieht und somit eine Nutzung der Forschungsschnittstelle innerhalb internationaler Forschungsvorhaben nicht möglich ist. Andere Ansätze wie z. B. das EHR4CR Projekt beinhalten eine EU-weite Kommunikation und sind der Forschungsschnittstelle in diesem Punkt überlegen.

Es ist auch noch nicht abzusehen, ob eine Nutzung der Telematikinfrastruktur für die Forschung in Zukunft möglich ist, oder ob die Telematikinfrastruktur in dem beschriebenen Umfang auch umgesetzt wird. Damit würde ein großer Vorteil der Forschungsschnittstelle gegenüber den anderen in Kapitel 2 aufgeführten Architekturansätzen verloren gehen, da die Infrastruktur für die Forschungsschnittstelle komplett aufgebaut werden müsste. Wird davon ausgegangen, dass dennoch eine Kommunikation mit der ePA eines Patienten über eine eigene Infrastruktur möglich wäre und die Anbindung der Systeme der Versorgung an die ePA etabliert wurde, so könnte die Forschungsschnittstelle mit einigen Anpassungen weiterhin umgesetzt werden. Während die Facharchitektur übernommen werden könnte, müsste die Sicherheitsarchitektur angepasst werden. Es könnten weiterhin die gleichen Sicherheitsmechanismen und Standards verwendet werden, allerdings sollte der Einsatz von Smartcards und Konnektoren durch Softwarezertifikate und einer entsprechenden PKI für die Forschung ersetzt werden. Es müsste auch ein eigener Identity Provider aufgebaut werden. Zudem müsste ein Forschungsadapter bei einer Trusted Third Party betrieben werden.

10.5. Resümee der Diskussion

Es ist gelungen eine Schnittstelle zu konzipieren, die eine sichere und datenschutzkonforme Kommunikation zwischen den Systemen der Versorgung und der medizinischen Forschung über eine patientengeführte ePA ermöglicht.

Über diese Schnittstelle können die meisten der in Kapitel 2.2 aufgeführten Anwendungsbereiche (Selbstdokumentation, Rekrutierung oder die Nutzung von Versorgungsdaten für Register und Studien) umgesetzt werden bzw. der Ansatz hat das Potential, um noch nicht umgesetzte Anwendungsbereiche erweitert zu werden (z. B. die Gewinnung von Phänotypdaten oder im Bereich des Qualitätsmanagements). Es wurde auch herausgestellt, dass der in dieser Arbeit verfolgte Ansatz nur Patienten einschließt, die auch eine eigene elektronische Patientenakte führen. Zusätzlich können nicht alle Anwendungsbereiche (z. B. Behandlungsunterstützung oder die Meldung von unerwünschten Arzneimittelwirkungen) sinnvoll über diesen Ansatz umgesetzt werden. Für diese beiden Anwendungsbereiche sind andere in der Literatur beschriebene Ansätze besser geeignet.

Bei der Konzeption konnte das Ziel erreicht werden, so wenige Anpassungen wie möglich an den bestehenden Systemen in der Versorgung und der medizinischen Forschung vorzunehmen und die meisten Anforderungen durch die Forschungsschnittstelle umzusetzen. Somit ist die Kommunikation zwischen der Versorgung und der medizinischen Forschung über eine patientengeführte ePA als eine sinnvolle Ergänzung zu bereits bestehenden

Ansätzen zu sehen. Bei der Konzeption wurde auf die bestehende Spezifikation des FuE-ePA-Projektes zur Anbindung einer ePA an die Systeme der Leistungserbringer aufgesetzt und es konnte gezeigt werden, dass die Anforderung seitens des Versorgungsmoduls erfolgreich umgesetzt werden konnten. Hier ist zu beachten, dass in dieser Arbeit einige Annahmen getroffen wurden, die erst in der Zukunft eintreten werden. Z. B. gibt es noch kein funktionierendes ePA-System, über das alle Leistungserbringer im deutschen Gesundheitswesen mit der ePA der Patienten kommunizieren können. Auch die Rechtslage lässt den hier entwickelten Ansatz momentan nicht zu. Diese sind zwei gravierende Punkte, die in Zukunft angegangen werden müssen, um das in dieser Arbeit vorgestellte Konzept erfolgreich umzusetzen.

Es ist gelungen die Kommunikation der Anwendungsfälle des Versorgungsmoduls auf ein Kommunikationsmodell abzubilden und die Anforderungen herzuleiten, unter denen dieses Modell umgesetzt werden kann. Über dieses Kommunikationsmodell kann die Kommunikation der ausgewählten Anwendungsfälle des Versorgungsmoduls ohne Medienbrüche und direkt zwischen dem Patienten und den Akteuren des Versorgungsmoduls erfolgen. Bei der Analyse der Kommunikation der Anwendungsfälle wurde immer nur eine mögliche Kommunikation betrachtet, so dass das Modell nicht für alle beliebigen Umsetzungen der Anwendungsfälle in Bezug auf die Kommunikation gilt. Für die wichtigen Grundlagen bzw. Herleitung und Umsetzung der Anforderungen für das Kommunikationsmodell wurde eine Überprüfung auf Richtigkeit durch einen Experten-Review durchgeführt. D. h. die Basis, auf der die Fach- und Sicherheitsarchitektur aufbauen, ist durch unabhängige Experten überprüft worden.

Es konnte eine Fach- und eine Sicherheitsarchitektur für das Kommunikationsmodell hergeleitet und beschrieben werden. Die in dieser Arbeit beschriebene Umsetzung der Forschungsschnittstelle, hängt jedoch stark von einer positiven Entwicklung der Telematikinfrastruktur ab. Dennoch konnte gezeigt werden, dass der Ansatz auch ohne Telematikinfrastruktur mit einigen Anpassungen umgesetzt werden kann. Es gibt noch einige zusätzliche Arbeiten im Bereich der Sicherheitsarchitektur zu leisten, im Besonderen bei dem Thema Signaturen. Abgesehen von diesen Punkten und davon, dass die Forschungsschnittstelle momentan keine internationalen Forschungsprojekte unterstützt, konnten die Vorteile der Fach- und Sicherheitsarchitektur gegenüber anderen in der Literatur beschriebenen Ansätze herausgestellt werden. Diese sind besonders in der Integration aller Versorgungssysteme und den hohen Sicherheitsstandards zu sehen.

11. Zusammenfassung und Ausblick

11.1. Zusammenfassung

In der medizinischen Forschung und in der Versorgung werden häufig dieselben Daten eines Patienten erfasst. Die Systeme der Forschung und Versorgung sind nicht integriert, so dass die Daten des Patienten in beide Systeme eingetragen werden müssen (Doppelerfassung). Um diesem Problem entgegen zu wirken, beschäftigen sich viele nationale und internationale Projekte mit dem Austausch von medizinischen Daten zwischen den Systemen der Forschung und der Versorgung. Eine Lösung für den Austausch von Daten zwischen den Systemen der Versorgung und der Forschung über eine patientengeführte elektronische Patientenakte in Verbindung mit der nationalen Telematikinfrastruktur wurde bisher noch nicht betrachtet. Der Vorteil dieses Ansatzes ist, dass über die Telematikinfrastruktur alle Systeme der Leistungserbringer integriert und eine einheitliche Schnittstelle für die ePA-Systeme etabliert werden soll. Wird nun eine Forschungsschnittstelle zwischen der ePA und den Systemen der Forschung definiert, so sind über die ePA alle Systeme der Leistungserbringer auch mit den Systemen der Forschung verbunden. Zum anderen werden die Patienten über ihre ePA aktiv in die Kommunikation eingebunden.

Der Fokus der Dissertation liegt auf der Konzeption bzw. Spezifikation eines sicheren Datenaustausches zwischen der medizinischen Versorgung und der medizinischen Forschung über eine patientengeführte ePA. Auf die rechtliche Problematik, den Einsatz von Biobanken und beispielweise die semantische Interoperabilität der Daten wurde nicht weiter eingegangen. Die Lösung sollte möglichst Anpassungen am ePA- und Forschungssystem vermeiden und neue Anforderungen durch die in dieser Arbeit zu spezifizierende Schnittstelle (in der Arbeit als Forschungsschnittstelle bezeichnet) zwischen der ePA und den IT-Systemen der Forschung umsetzen lassen. Eine wichtige Voraussetzung für diese Arbeit ist, dass sowohl das Forschungs- als auch das ePA-System wie in der Literatur beschrieben umgesetzt ist bzw. wird. Die Forschungsschnittstelle sollte als eine Erweiterung des ePA-Systems konzipiert werden und die Konzepte des ePA-Systems in Bezug auf die Kommunikation und die Sicherheit übernehmen. Es wurde also nicht nur ein „Secondary Use“ der medizinischen Daten für die Forschung sondern auch der Telematikinfrastruktur sowie der Schnittstelle und Konzepte des ePA-Systems angestrebt.

In dieser Arbeit wurde das ePA-System auf Grundlage der im Rahmen des FuE-ePA-Projektes entstandenen Spezifikationen definiert (siehe Kapitel 5). Das Forschungssystem wurde auf der Grundlage der Beschreibungen in den generischen Datenschutzkonzepten der TMF definiert. Hierbei wurde aus Komplexitätsgründen nur das Versorgungsmodul genauer betrachtet (siehe Kapitel 4). Aus dem Versorgungsmodul konnten Anwendungsfälle ausgewählt werden, bei denen die Kommunikation potentiell über eine ePA verbessert werden konnte. Eine Verbesserung der Kommunikation beinhaltet in diesem Fall eine direktere Kommunikation mit dem Patienten und den Akteuren eines Forschungsverbundes sowie die Vermeidung von Medienbrüchen.

Nachdem das ePA- sowie das Forschungssystem definiert wurden, konnte ein Kommunikationsmodell erstellt werden, das unter dem oben genannten Verbesserungspotential die Kommunikation der Anwendungsfälle des Versorgungsmoduls über eine ePA abbildet. Neben dem Modell wurden auch Anforderungen an den Datenschutz definiert, die bei der Umsetzung des Modells in Form einer Forschungsschnittstelle berücksichtigt werden

müssen (siehe Kapitel 6). Auf dieser Basis konnten die Komponenten der Forschungsschnittstelle definiert werden und die Forschungsschnittstelle als eine Erweiterung der IT-Infrastruktur des ePA-Systems beschrieben werden (siehe Kapitel 7). Unter Berücksichtigung der Datenschutzanforderungen des Versorgungsmoduls und der Spezifikationen des ePA-Systems aus dem FuE-ePA-Projekt wurde dann das detaillierte Verhalten der Komponenten der Forschungsschnittstelle untereinander und mit dem Forschungs- und ePA-System im Rahmen einer Fach- und Sicherheitsarchitektur beschrieben (siehe Kapitel 8 und 9). Anschließend wurden die Ergebnisse dieser Arbeit kritisch diskutiert und mit anderen Ansätzen aus der Literatur verglichen.

Zusammenfassend kann gesagt werden, dass die in dieser Arbeit verfolgten Ziele zur Konzeption eines Kommunikationsdienstes für die medizinische Forschung mittels elektronischer Patientenakten nach § 291a SGB V am Beispiel des Versorgungmoduls erfolgreich umgesetzt werden konnten und dieser Ansatz eine ideale Ergänzung neben anderen Ansätzen zur Nutzung von Versorgungsdaten für die medizinische Forschung ist. Besonders die Idee des „Secondary Use“ der Telematikinfrastruktur und bestehender bzw. im Aufbau befindlicher einheitlicher Schnittstellen sollte auch für andere Ansätze des Austausches von Versorgung und Forschung ohne ePA betrachtet werden. Voraussetzung hierfür bleibt natürlich die Anpassung der gesetzlichen Regelungen und der Ausbau der Telematikinfrastruktur bzw. des ePA-Systems.

11.2. Ausblick

Im Laufe der Arbeit wurden weitere Themen identifiziert, die nicht im Rahmen dieser Arbeit behandelt werden, aber in weiteren Arbeiten vertieft werden sollten. Im Folgenden wird auf diese Themen eingegangen und ein Vorschlag unterbreitet, wie mit diesen Punkten weiter verfahren werden sollte.

In dieser Arbeit wurde der Fokus auf das Versorgungsmodul gelegt und die Forschungsschnittstelle für die Anwendungsfälle des Versorgungsmoduls konzipiert. Während der Analyse eines medizinischen Forschungsverbundes stellte sich heraus, dass auch die Kommunikationsvorgänge einiger Anwendungsfälle des Studien- oder Forschungsmoduls über eine ePA umgesetzt werden könnten (siehe Tabelle 21 im Anhang A1.4). Unter diesen Anwendungsfällen sind sowohl die von anderen Projekten verfolgten Anwendungsfälle (z. B. das Managen von unerwünschten Ereignissen (EHR4CR)) als auch Anwendungsfälle, die im Rahmen dieser Arbeit umgesetzt wurden (z. B. das Auskunftsrecht des Patienten und der Rückzug der Einwilligung des Patienten). Daher wird hier empfohlen, die Forschungsschnittstelle um das Studien- sowie das Forschungsmodul zu erweitern. Hierzu müsste eine detaillierte Analyse der Kommunikation der Anwendungsfälle vorgenommen werden und überprüft werden, ob weitere Anforderungen an die Forschungsschnittstelle entstehen. Auf dieser Basis könnte dann eine Erweiterung der Forschungsschnittstelle erarbeitet werden.

Eine weitere Arbeit sollte sich mit den Anwendungsfällen einer Biobank beschäftigen und die interessanten Anwendungsfälle in Bezug auf die Kommunikation mit Hilfe einer ePA herausstellen. Es sollte untersucht werden, wie der Anwendungsbereich „Gewinnung von Phänotypdaten“ (siehe Abschnitt 2.3.4) über die ePA realisiert werden kann. Ein wichtiger Punkt könnte die Kommunikation mit dem Patienten sein, um neue Einwilligungserklärungen einzuholen (z. B. wenn die Probe für ein neues Forschungsvorhaben eingesetzt werden soll und keine Einwilligung dafür vorliegt). Weitere interessante Anwendungsfälle der Biobank für die Umsetzung über eine ePA während der Rückfluss von Forschungsergebnissen, die aus

den Proben des Patienten gewonnen wurden sowie eine Übersicht, welche Forschung gerade mit den Proben eines Patienten durchgeführt wird. Kaye J et.al geben hier in ihrem Artikel „From patients to partners: participant-centric initiatives in biomedical research“ einen Ausblick, wie Patienten besser über die Nutzung ihrer Daten für die Forschung entscheiden können [180].

Es wurde in der Diskussion herausgestellt, dass der in dieser Arbeit entwickelte Ansatz momentan nicht für die Basisakte und die USB-Akte ausgelegt ist und somit Patienten, die eine solche Akte benutzen wollen, nicht über die Forschungsschnittstelle kommunizieren können. Diese beiden Themen sollten jeweils in einer weiteren Arbeit verfolgt werden. Momentan sind zwei Ansätze vorstellbar, deren Vor- und Nachteile beleuchtet werden sollten. Zum einen könnten in der Basisakte Weiterleitungsregeln für bestimmte Dokumente hinterlegt werden. Nachdem von einem Leistungserbringer ein bestimmtes Dokument an die ePA geschickt wird, werden die Weiterleitungsregeln ausgelöst und das Dokument wird automatisch an die Versorgungsdatenbank weitergeleitet. Da die Daten, die aus der Versorgung für das Forschungsvorhaben genutzt werden sollen, vorher festgelegt werden, sind diese Regeln relativ statisch und müssten daher selten geändert werden. Ein zweiter Ansatz wäre eine Umleitung der Daten in der ePA-Kommunikationskomponente (siehe Abbildung 40). D. h. für die Patienten, die an einem Forschungsvorhaben teilnehmen, würden in der ePA-Kommunikationskomponente für die entsprechenden Dokumente Weiterleitungsregeln hinterlegt werden. Sobald ein Leistungserbringer ein Dokument an die ePA des Patienten schickt, das auch in das Versorgungsmodul übernommen werden soll, wird dieses Dokument nicht nur in die ePA des Patienten übernommen, sondern auch eine Kopie an das Versorgungsmodul weitergeleitet. Diese Variante hätte den Vorteil, dass nicht jeder Hersteller diese Weiterleitungsregeln implementieren müsste. Durch diese Variante wäre auch ein Einsatz von USB-Akten mit der Forschungsschnittstelle vorstellbar. Hier würde der Leistungserbringer nicht nur die Dokumente auf der USB-Akte speichern, sondern auch Dokumente, die für die Versorgungsdatenbank vorgesehen sind, an die ePA-Kommunikationskomponente schicken, wo sie dann nicht in eine ePA übernommen werden, sondern über den ePA-Forschungsadapter an das Versorgungsmodul geschickt werden würden. Hier müssten allerdings noch Varianten für die Kommunikation vom Forschungsverbund zum Patienten diskutiert werden, da dem Patienten die Daten nicht wie bei der Online-Akte zugesendet werden können bzw. Daten vom Patienten angefordert werden können. Es wäre z. B. ein Postfach für den Patienten vorstellbar, dass beim Leistungserbringer oder ggf. von Patienten zuhause abgerufen werden kann.

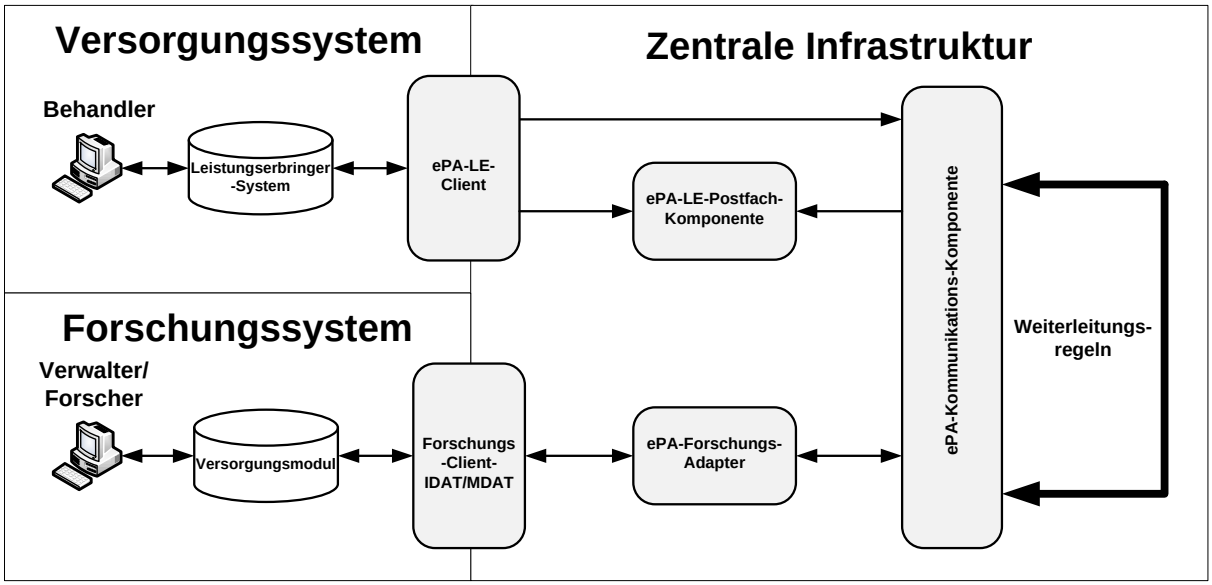

Abbildung 40: Mögliche Weiterentwicklung der Forschungsschnittstelle

Auch wenn durch die vorgestellte Arbeit dargelegt wurde, wie die Systeme aus der Versorgung über eine ePA mit den Systemen der Forschung kommunizieren können, so wurde darüber hinaus herausgestellt, dass dieses Konzept nicht alle Anwendungsfälle der Forschung abdecken kann und auch nicht alle Patienten eine ePA führen werden. Es sollte also in einer weiteren Arbeit untersucht werden, inwiefern die beschriebene Architektur auch für eine direkte Kommunikation zwischen den Systemen der Leistungserbringer und denen eines medizinischen Forschungsverbundes umgesetzt werden könnte. Auch hier könnte die in der Abbildung 40 vorgeschlagene Weiterleitungsregel eine mögliche Lösung sein, auch ohne ePA des Patienten eine Kommunikation zwischen den Systemen eines Forschungsverbundes und den Systemen der Leistungserbringer zu realisieren. Da der Patient ohne ePA auch keine ePA-ID hat, müsste hier anstatt der ePA-ID eine Forschungs-ID auf der eGK gespeichert werden, die auch in der ePA-Kommunikationskomponente und der Patientenliste zu dem Patienten hinterlegt wird. Diese ID könnte dann von den Leistungserbringern von der eGK ausgelesen und für die Kommunikation mit dem Forschungsverbund verwendet werden.

In dieser Arbeit wurden keine neuen Anwendungsfälle für die Kommunikation zwischen einem Patienten und einem Forschungsverbund über die ePA des Patienten betrachtet. Hier könnte besonders die Verwendung von Daten aus der ePA für retrospektive Studien von Interesse sein. Sollte die ePA einen Patienten von Geburt an begleiten und der Patient seine Krankheitsgeschichte sowie weitere selbsterfasste Daten in seiner ePA vorhalten, so könnte dieses für retrospektive Studien von großem Wert sein. Dieses Thema sollte in einer weiteren Arbeit ausgearbeitet werden, besonders wie Patienten für solche Studien identifiziert werden können ohne dass die ePAs der Patienten „durchsucht“ werden.

Viele Forschungsprojekte werden mittlerweile international durchgeführt. Die hier vorgeschlagene Lösung beschränkt sich nur auf den deutschen Raum, wie in der Diskussion schon angemerkt wurde. D. h. es sollte untersucht werden, ob und ggf. wie internationale Forschungsprojekte über die Forschungsschnittstelle umgesetzt werden können. Sollte es keine Lösung geben, die Forschungsschnittstelle für internationale Projekte zu nutzen, könnte die Forschungsschnittstelle in diesen Projekten für die deutschen Patienten genutzt werden und die anderen Patienten würden wie gehabt über das Versorgungsmodul erfasst werden.

Ein nächster wichtiger Schritt ist es, die vorgeschlagene Lösung im Rahmen einer Pilotinstallation zu testen. Hierzu müsste ein entsprechendes Forschungsprojekt, das den Aufbau eines Versorgungsmoduls plant, oder ein bestehendes Forschungsprojekt gefunden werden. Es sollte sich möglichst auf einen Aktenhersteller und die in einer Region verbreitetsten Arztinformationssysteme konzentriert werden. Hier wäre zu überlegen, ob ein solches Projekt nicht im Rahmen einer vom BMBF geförderten Gesundheitsregion [181] umgesetzt wird, in der die Aktenhersteller und Hersteller von Arztinformationssystemen schon kooperieren. Vorstellbar wäre auch eine Umsetzung im Rahmen des Aufbaus der Infrastrukturen eines der Deutschen Zentren wie beispielweise des Deutschen Zentrums für Herz-Kreislauf-Forschung [182]. Es müssten die Semantic Signifier für das Versorgungsmodul definiert werden und die Sicherheitsdienste für die LE- und die Forschungsschnittstelle implementiert werden.

Ein weiterer essentieller Punkt ist die Klärung des rechtlichen Rahmens. Nach momentaner Gesetzeslage „*sind die Nutzung der auf oder mittels der Gesundheitskarte gespeicherten Daten und die Speicherung zusätzlicher Daten zu Forschungszwecken unzulässig*“ [23, Seite 543]. D. h. bevor der Einsatz der Forschungsschnittstelle weiter geplant wird, sollten die Diskussionen über eine Änderung des § 291a SGB V in Richtung einer Nutzung der eGK bzw. der mit der eGK gesammelten Daten für die medizinische Forschung wieder aufgenommen werden. Hierfür können die Ergebnisse dieser Arbeit sowohl Anwendungsbeispiele als auch eine Lösung für eine sichere Anbindung der medizinischen Forschung an eine ePA nach § 291a liefern.

Aufgrund der Vielzahl der Akteure und Systeme sowie der Heterogenität der Daten, ist der Aufbau einer nationalen Telematikinfrastruktur zur Vernetzung der IT-Landschaft des Gesundheitssystems zum größten IT-Projekt Europas geworden. Aufgrund der Sensibilität der auszutauschenden Daten sind der Datenschutz und die Datensicherheit ein zentraler Punkt des Gesamtprojektes. Die obengenannten Punkte führen zu einer Komplexität, die sich auch in der über 5000 Seiten langen Spezifikation für die grundlegenden Dienste der Telematikinfrastruktur widerspiegelt. Diese Komplexität und Vielschichtigkeit wurde auch in der Abgrenzung und im Ausblick verdeutlicht. Es sind noch viele Punkte nicht komplett ausgearbeitet und müssen weiterverfolgt werden. Um das Thema in seiner Tiefe zu bearbeiten, müsste eine Organisation gebildet werden, die sich mit dem Aufbau und Ausbau sowie langfristigen Betrieb von IT-Infrastrukturen für die medizinische Forschung beschäftigt und u. a. auch den Austausch zwischen der medizinischen Versorgung und Forschung mit Hilfe der Telematikinfrastruktur berücksichtigt.

Die Ergebnisse dieser Arbeit zeigen, dass ein sicherer und datenschutzkonformer Datenaustausch zwischen einer ePA gemäß § 291a und den IT-Systemen der medizinischen Forschung möglich ist. Diese Ergebnisse sollten in die Diskussionen um eine Änderung der gesetzlichen Rahmenbedingungen aufgenommen werden[21]. Sollten die rechtlichen Rahmenbedingungen in der Zukunft die Nutzung der auf oder mittels der Gesundheitskarte gespeicherten Daten für die medizinische Forschung beinhalten, so könnten auf Grundlage dieser Arbeit sowohl die Nutzung der ePA nach § 291a als auch andere Anwendungen für die bessere Vernetzung der Versorgung und medizinischen Forschung etabliert werden. Damit kann das enorme Potential der Telematikinfrastruktur nicht nur für die Versorgung, sondern auch für die medizinische Forschung genutzt werden.

[21] Eine entsprechende Empfehlung wurde in den Abschlussbericht des Forschungs- und Entwicklungsprojektes zur Elektronischen Patientenakte gemäß § 291a SGB V aufgenommen und es wurde darüber hinaus ein Wortlaut für eine Gesetzesänderung vorgeschlagen.

Literaturverzeichnis

1. Dorda WG: WAREL; a system for retrieval of clinical data considering the course of diseases. Methods Inf Med 1989 Jul;28:133–141.

2. Safran C, Porter D, Lightfoot J, Rury CD, Underhill LH, Bleich HL, et al.: ClinQuery: a system for online searching of data in a teaching hospital. Ann Intern Med 1989 Nov 1;111:751–756.

3. Dorda WG: Data-screening and retrieval of medical data by the system WAREL. Methods Inf Med 1990 Jan;29:3–11.

4. Safran C: Using routinely collected data for clinical research. Stat Med 1991 Apr;10:559–564.

5. Papaconstantinou C, Theocharous G, Mahadevan S: An expert system for assigning patients into clinical trials based on Bayesian networks. J Med Syst 1998 Jun;22:189–202.

6. Murphy SN, Morgan MM, Barnett GO, Chueh HC: Optimizing healthcare research data warehouse design through past COSTAR query analysis. Proc AMIA Symp 1999;1999:892–896.

7. NIHR Health Technology Assessment programme [Internet] [cited 2012 Sep 6];Available from: http://www.hta.ac.uk/

8. The National Institute for Health Research [Internet] [cited 2012 Sep 6];Available from: http://www.nihr.ac.uk/Pages/default.aspx

9. Williams JG, Cheung WY, Cohen DR, Hutchings HA, Longo MF, Russell IT: Can randomised trials rely on existing electronic data? A feasibility study to explore the value of routine data in health technology assessment. Health Technol Assess 2003;7:iii, v–x, 1–117.

10. Powell J, Buchan I: Electronic Health Records Should Support Clinical Research. J Med Internet Res 2005 Mar 14;7. DOI: 10.2196/jmir.7.1.e4

11. De Lusignan S, Metsemakers JFM, Houwink P, Gunnarsdottir V, Van der Lei J: Routinely collected general practice data: goldmines for research? A report of the European Federation for Medical Informatics Primary Care Informatics Working Group (EFMI PCIWG) from MIE2006, Maastricht, The Netherlands. Informatics in Primary Care 2006;14:203–209.

12. The added value of electronic health records (EHRs): Linking patient care, clinical research and public health [Internet] 2008 Jul 14 [cited 2012 Jul 16];Available from: http://www.eurorec.org/files/filesPublic/High_Level_Statement_EHR%20in%20EU__FINAL%20_July%2014.pdf

13. Prokosch H-U, Ganslandt T: Perspectives for Medical Informatics Reusing the Electronic Medical Record for Clinical Research. Methods Inf Med 2009;48:38–44.

14. Embi PJ, Payne PRO, Kaufman SE, Logan JR, Barr CE: Identifying Challenges and Opportunities in Clinical Research Informatics: Analysis of a Facilitated Discussion at the 2006 AMIA Annual Symposium. AMIA Annu Symp Proc 2007;2007:221–225.

15. Safran C, Bloomrosen M, Hammond WE, Labkoff S, Markel-Fox S, Tang PC, et al.: Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. Journal of the American Medical Informatics Association : JAMIA 2007;14:1–9.

16. Halamka JD, Mandl KD, Tang PC: Early experiences with personal health records. J Am Med Inform Assoc 2008 Feb;15:1–7.

17. Kim D, Labkoff S, Holliday SH: Opportunities for Electronic Health Record Data to Support Business Functions in the Pharmaceutical Industry - A Case Study from Pfizer, Inc. J Am Med Inform Assoc 2008;15:581–584.

18. EHR4CR: Electronic Health Records for Clinical Research [Internet] [cited 2012 Jul 16];Available from: http://www.ehr4cr.eu/

19. Kompetenznetze in der Medizin [Internet] [cited 2012 Jan 16];Available from: http://www.kompetenznetze-medizin.de/Home.aspx

20. Kaiser RH: Einführung von elektronischer Gesundheitskarte, elektronischem Rezept, HPC (Health Professional Card) und anderen Telematikanwendungen im Gesundheitswesen. Der Onkologe 2004 Nov;10:1247–1250.

21. Blobel B, Pharow P: Wege zur elektronischen Patientenakte. Datenschutz und Datensicherheit - DuD 2006 Mar;30:164–169.

22. Caumanns J, Weber H, Fellien A, Kurrek H, Boehm O, Neuhaus J, et al.: Die eGK-Lösungsarchitektur Architektur zur Unterstützung der Anwendungen der elektronischen Gesundheitskarte. Informatik-Spektrum 2006 Aug 26;29:341–348.

23. Roßnagel A, Hornung G: Forschung à la Card? MedR Medizinrecht 2008;26:538–543.

24. Kush R, Alschuler L, Ruggeri R, Cassells S, Gupta N, Bain L, et al.: Implementing Single Source: The STARBRITE Proof-of-Concept Study. J Am Med Inform Assoc 2007;14:662–673.

25. Dugas M, Breil B, Thiemann V, Lechtenbörger J, Vossen G: Single source information systems to connect patient care and clinical research. Stud Health Technol Inform 2009;150:61–65.

26. Embi PJ, Jain A, Clark J, Harris CM: Development of an Electronic Health Record-based Clinical Trial Alert System to Enhance Recruitment at the Point of Care. AMIA Annu Symp Proc 2005;2005:231–235.

27. Dugas M, Lange M, Berdel WE, Müller-Tidow C: Workflow to improve patient recruitment for clinical trials within hospital information systems - a case-study. Trials 2008;9:2.

28. Dugas M, Lange M, Müller-Tidow C, Kirchhof P, Prokosch H-U: Routine data from hospital information systems can support patient recruitment for clinical studies. Clin Trials 2010 Apr;7:183–189.

29. Thompson DS, Oberteuffer R, Dorman T: Sepsis alert and diagnostic system: integrating clinical systems to enhance study coordinator efficiency. Comput Inform Nurs 2003 Feb;21:22–26; quiz 27–28.

30. Murphy EC, Ferris FL, O'Donnell WR: An Electronic Medical Records System for Clinical Research and the EMR–EDC Interface. IOVS 2007 Jan 10;48:4383–4389.

31. Ganslandt T, Mate S, Helbing K, Sax U, Prokosch HU: Unlocking Data for Clinical Research – The German i2b2 Experience. Applied Clinical Informatics 2011 Mar 30;2:116–127.

32. Zapletal E, Rodon N, Grabar N, Degoulet P: Methodology of integration of a clinical data warehouse with a clinical information system: the HEGP case. Stud Health Technol Inform 2010;160:193–197.

33. Reng C-M, Pommerening K, Specker C, Debold P: Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin. Berlin, MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006.

34. Pommerening K, Drepper J, Helbing K, Ganslandt T, Speer R, Müller T, et al.: Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - Version 0.11a 2011;

35. Pommerening K, Reng M: Secondary use of the EHR via pseudonymisation. Stud Health Technol Inform 2004;103:441–446.

36. Brüntrup R, Lablans M, Ückert F: Generische Softwarebibliothek zur Web-Umsetzung des TMF-Datenschutzkonzepts A [Internet] [cited 2012 Apr 12];Available from: http://campus.uni-muenster.de/fileadmin/einrichtung/imfl/projekte/DSLib/Generische_Softwarebibliothek_zur_Web-Umsetzung_des_TMF-Datenschutzkonzepts_A.pdf

37. Krüger-Brand HE: Elektronische Patientenakte: Der Bürger als „Souverän der Akte“. Dtsch Arztebl 2011;108:A–2295 / B–1936 / C–1916.

38. Bales S, Holland J, Müller J, Dierks C: Die elektronische Gesundheitskarte: Rechtskommentar, Standpunkte und Erläuterungen für die Praxis. ed 1 Heidelberg, Müller (C.F.Jur.), 2007.

39. Arbeitskreis EPA/EFA: Elektronische Akten im Gesundheitswesen [Internet] 2011 Sep 21 [cited 2012 Dec 1];Available from: http://www.ztg-nrw.de/ZTG/content/e129/e686/e12133/e12616/pressfile/object12618/21092011_AKEPA-eFA_ElektronischeAktenimGesundheitswesen_web_ger.pdf

40. Tagaris A, Chondrogiannis E, Andronikou V, Tsatsaronis G: Semantic Interoperability between Clinical Research and Healthcare: the PONTE approach [Internet]; in : Extended Semantic Web Conference Workshop on Semantic Interoperability in Medical Informatics (ESWC SIMI 2012). Griechenland, 2012, [cited 2012 Aug 26].Available from: http://grid.ece.ntua.gr/sites/simi2012/paper5.pdf

41. Ponte [Internet] [cited 2012 Jul 16];Available from: http://www.ponte-project.eu/

42. Lovis C, Colaert D, Stroetmann VN: DebugIT for patient safety - improving the treatment with antibiotics through multimedia data mining of heterogeneous clinical data. Stud Health Technol Inform 2008;136:641–646.

43. El Fadly A, Rance B, Lucas N, Mead C, Chatellier G, Lastic P-Y, et al.: Integrating clinical research with the Healthcare Enterprise: From the RE-USE project to the EHR4CR platform. Journal of Biomedical Informatics 2011 Dec;44, Supplement 1:S94–S102.

44. Lowe HJ, Ferris TA, Hernandez PM, Weber SC: STRIDE – An Integrated Standards-Based Translational Research Informatics Platform. AMIA Annu Symp Proc 2009;2009:391–395.

45. Stanford Translational Research Integrated Database Environment (STRIDE) [Internet] [cited 2012 Jul 31];Available from: https://clinicalinformatics.stanford.edu/research/stride.html

46. Weber S, Lowe HJ, Malunjkar S, Quinn J: Implementing a Real-time Complex Event Stream Processing System to Help Identify Potential Participants in Clinical and Translational Research Studies. AMIA Annu Symp Proc 2010;2010:472–476.

47. Perna G: Leveraging the EMR for clinical science. The electronic medical record is proving itself to be a valuable tool in medical research. Healthc Inform 2012 Apr;29:42–43.

48. Delaney BC, Peterson KA, Speedie S, Taweel A, Arvanitis TN, Hobbs FDR: Envisioning a Learning Health Care System: The Electronic Primary Care Research Network, A Case Study. Ann Fam Med 2012 Jan;10:54–59.

49. electronic Primary Care Research Network (ePCRN) [Internet] [cited 2012 Aug 23];Available from: http://www.epcrn.bham.ac.uk/Home/tabid/138/Default.aspx

50. Peterson KA, Fontaine P, Speedie S: The Electronic Primary Care Research Network (ePCRN): A New Era in Practice-based Research. J Am Board Fam Med 2006 Jan 1;19:93–97.

51. Ainsworth J, Buchan I: Preserving consent-for-consent with feasibility-assessment and recruitment in clinical studies: FARSITE architecture. Stud Health Technol Inform 2009;147:137–148.

52. Thew S, Leeming G, Ainsworth J, Gibson M, Buchan I: FARSITE: evaluation of an automated trial feasibility assessment and recruitment tool. Trials 2011 Dec 13;12:A113.

53. Förderung von Instrumenten- und Methodenentwicklung für die patientenorientierte medizinische Forschung [Internet]. Bundesministerium für Bildung und Forschung [cited 2012 Aug 8];Available from: http://www.gesundheitsforschung-bmbf.de/de/4316.php#kis

54. D023-01 KIS-Rekrutierung - KIS-basierte Unterstützung der Patientenrekrutierung in klinischen Studien [Internet]. TMF eV [cited 2012 Jul 31];Available from: http://www.tmf-ev.de/Themen/Projekte/D023_01_KIS_Patientenrekrutierung.aspx

55. Breil B, Semjonow A, Müller-Tidow C, Fritz F, Dugas M: HIS-based Kaplan-Meier plots - a single source approach for documenting and reusing routine survival information. BMC Med Inform Decis Mak 2011 Feb 16;11:11.

56. West SL, Blake C, Zhiwen Liu, McKoy JN, Oertel MD, Carey TS: Reflections on the use of electronic health record data for clinical research. Health Informatics J 2009 Jun;15:108–121.

57. Duftschmid G, Gall W, Eigenbauer E, Dorda W: Management of data from clinical trials using the ArchiMed system. Medical informatics and the Internet in medicine 2002 Jun;27:85–98.

58. Fritz F, Ständer S, Breil B, Riek M, Dugas M: CIS-based registration of quality of life in a single source approach. BMC Med Inform Decis Mak 2011;11:26.

59. Fontaine P, Mendenhall TJ, Peterson K, Speedie SM: The “Measuring Outcomes of Clinical Connectivity” (MOCC) Trial: Investigating Data Entry Errors in the Electronic Primary Care Research Network (ePCRN). J Am Board Fam Med 2007 Apr;20:151–159.

60. Prokosch H-U, Ries M, Beyer A, Schwenk M, Seggewies C, Köpcke F, et al.: IT infrastructure components to support clinical care and translational research projects in a comprehensive cancer center. Stud Health Technol Inform 2011;169:892–896.

61. Mate S, Köpcke F, Wullich B, Breil B, Dugas M, Bürkle T, et al.: Aufbau einer auf Routinedaten basierenden, standortübergreifenden Forschungsplattform für das Deutsche Prostatakarzinom-Konsortium e.V. Mainz//2011 56 Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (gmds), 6 Jahrestagung der Deutschen Gesellschaft für Epidemiologie (DGEpi) 2011 Sep;2011:375–376.

62. Mate S, Bürkle T, Köpcke F, Breil B, Wullich B, Dugas M, et al.: Populating the i2b2 database with heterogeneous EMR data: a semantic network approach. Stud Health Technol Inform 2011;169:502–506.

63. Weber GM, Murphy SN, McMurry AJ, MacFadden D, Nigrin DJ, Churchill S, et al.: The Shared Health Research Information Network (SHRINE): A Prototype Federated Query Tool for Clinical Data Repositories. J Am Med Inform Assoc 2009;16:624–630.

64. Natter MD, Quan J, Ortiz DM, Bousvaros A, Ilowite NT, Inman CJ, et al.: An i2b2-based, generalizable, open source, self-scaling chronic disease registry. J Am Med Inform Assoc 2012 Jun 25; DOI: 10.1136/amiajnl-2012-001042

65. Kalra D, Schmidt A, Potts HWW, Dupont D, Sundgren M, De Moor G: Case Report from the EHR4CR Project - A European Survey on Electronic Health Records Systems for Clinical Research. iHealth Connections 2011;1:108–113.

66. EB: Forschung: Sekundärnutzung von Behandlungsdaten. Dtsch Arztebl 2012 Feb 17;109:A–336 / B–291 / C–287.

67. Kullo IJ, Fan J, Pathak J, Savova GK, Ali Z, Chute CG: Leveraging informatics for genetic studies: use of the electronic medical record to enable a genome-wide association study of peripheral arterial disease. J Am Med Inform Assoc 2010 Sep;17:568–574.

68. El Fadly A, Daniel C, Bousquet C, Dart T, Lastic P-Y, Degoulet P: Electronic Healthcare Record and clinical research in cardiovascular radiology. HL7 CDA and CDISC ODM interoperability. AMIA Annu Symp Proc 2007 Oct 11;:216–220.

69. Breil B, Dugas M: Transferring HIS data to population-based cancer registries - concept and first implementations. Stud Health Technol Inform 2009;150:86–90.

70. Ford DV, Jones KH, Verplancke J-P, Lyons RA, John G, Brown G, et al.: The SAIL Databank: building a national architecture for e-health research and evaluation. BMC Health Serv Res 2009;9:157.

71. McGregor J, Brooks C, Chalasani P, Chukwuma J, Hutchings H, Lyons RA, et al.: The Health Informatics Trial Enhancement Project (HITE): Using routinely collected primary care data to identify potential participants for a depression trial. Trials 2010 Apr 15;11:39.

72. Boyd AD, Hosner C, Hunscher DA, Athey BD, Clauw DJ, Green LA: An “Honest Broker” mechanism to maintain privacy for patient care and academic medical research. Int J Med Inform 2007 Jun;76:407–411.

73. Boyd AD, Saxman PR, Hunscher DA, Smith KA, Morris TD, Kaston M, et al.: The University of Michigan Honest Broker: A Web-based Service for Clinical and Translational Research and Practice. J Am Med Inform Assoc 2009;16:784–791.

74. Zahlmann G, Harzendorf N, Shwarz-Boeger U, Paepke S, Schmidt M, Harbeck N, et al.: EHR and EDC Integration in Reality [Internet]. Applied Clinical Trials 2009 Nov 16 [cited 2012 Jul 17];Available from: http://www.appliedclinicaltrialsonline.com/appliedclinicaltrials/article/articleDetail.jsp?id=641682

75. Linder JA, Haas JS, Iyer A, Labuzetta MA, Ibara M, Celeste M, et al.: Secondary use of electronic health record data: spontaneous triggered adverse drug event reporting. Pharmacoepidemiology and Drug Safety 2010 Dec;19:1211–1215.

76. Stephens MB, Reamy BV: A Novel Approach Using an Electronic Medical Record to Identify Children and Adolescents at Risk for Dyslipidemia: A Study from the Primary Care Education and Research Learning (PEARL) Network. J Am Board Fam Med 2008 Jan 7;21:356–357.

77. Adams T, Budden M, Hoare C, Sanderson H: Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent. BMJ 2004 Apr 10;328:871–874.

78. Sanderson H, Adams T, Budden M, Hoare C: Lessons from the central Hampshire electronic health record pilot project: evaluation of the electronic health record for supporting patient care and secondary analysis. BMJ 2004 Apr 10;328:875–878.

79. Newsham AC, Johnston C, Hall G, Leahy MG, Smith AB, Vikram A, et al.: Development of an advanced database for clinical trials integrated with an electronic patient record system. Comput Biol Med 2011 Aug;41:575–586.

80. Stakic SB, Tasic S: Secondary use of EHR data for correlated comorbidity prevalence estimate. Conf Proc IEEE Eng Med Biol Soc 2010;2010:3907–3910.

81. Salford Integrated Record - SIR System [Internet] [cited 2012 Aug 21];Available from: http://www.salford.nhs.uk/SIRSystem.aspx?section=4

82. Ainsworth J, Baker P, New J, Gibson M, Pioli D, Buchan I: Public Health e-Labs: A federated model for e-Epidemiology [Internet]; in : Public Health Informatics 2007. Seattle, 2007, [cited 2012 Aug 21].Available from: https://www.escholar.manchester.ac.uk/uk-ac-man-scw:71433

83. Ainsworth J, Buchan IE: e-Labs and Work Objects: Towards Digital Health Economies [Internet]; in : Communications Infrastructure. Systems and Applications in Europe. First International ICST Conference, EuropeComm 2009, London, UK, August 11-13, 2009, Revised Selected Papers. London, Springer, 2009, [cited 2012 Jul 17], pp 205–216.

84. Adida B, Sanyal A, Zabak S, Kohane IS, Mandl KD: Indivo X: Developing a Fully Substitutable Personally Controlled Health Record Platform. AMIA Annu Symp Proc 2010;2010:6–10.

85. Atkinson NL, Massett HA, Mylks C, Hanna B, Deering MJ, Hesse BW: User-Centered Research on Breast Cancer Patient Needs and Preferences of an Internet-Based Clinical Trial Matching System. J Med Internet Res 2007 May 15;9. DOI: 10.2196/jmir.9.2.e13

86. Pakhomov S, Weston SA, Jacobsen SJ, Chute CG, Meverden R, Roger VL: Electronic medical records for clinical research: application to the identification of heart failure. Am J Manag Care 2007 Jun;13:281–288.

87. Mandl KD, Mandel JC, Murphy SN, Bernstam EV, Ramoni RL, Kreda DA, et al.: The SMART Platform: early experience enabling substitutable applications for electronic health records. J Am Med Inform Assoc 2012 Jul;19:597–603.

88. Breil B, Semjonow A, Dugas M: HIS-based electronic documentation can significantly reduce the time from biopsy to final report for prostate tumours and supports quality management as well as clinical research. BMC Medical Informatics and Decision Making 2009 Jan 20;9:5.

89. Kullo IJ, Ding K, Jouni H, Smith CY, Chute CG: A Genome-Wide Association Study of Red Blood Cell Traits Using the Electronic Medical Record. PLoS One 2010 Sep 28;5:e13011.

90. Pathak J, Pan H, Wang J, Kashyap S, Schad PA, Hamilton CM, et al.: Evaluating Phenotypic Data Elements for Genetics and Epidemiological Research: Experiences from the eMERGE and PhenX Network Projects. AMIA Summits Transl Sci Proc 2011 Mar 7;2011:41–45.

91. McCarty CA, Chisholm RL, Chute CG, Kullo IJ, Jarvik GP, Larson EB, et al.: The eMERGE Network: A consortium of biorepositories linked to electronic medical records data for conducting genomic studies. BMC Med Genomics 2011 Jan 26;4:13.

92. Kho AN, Hayes MG, Rasmussen-Torvik L, Pacheco JA, Thompson WK, Armstrong LL, et al.: Use of diverse electronic medical record systems to identify genetic risk for type 2 diabetes within a genome-wide association study. J Am Med Inform Assoc 2012 Apr;19:212–218.

93. Kohane IS, Altman RB: Health-information altruists - a potentially critical resource. N Engl J Med 2005 Nov 10;353:2074–2077.

94. Dorda W, Wrba T, Duftschmid G, Sachs P, Gall W, Rehnelt C, et al.: ArchiMed: a medical information and retrieval system. Methods Inf Med 1999 Mar;38:16–24.

95. Boyd AD, Hunscher DA, Kramer AJ, Hosner C, Saxman P, Athey BD, et al.: THE “HONEST BROKER” METHOD OF INTEGRATING INTERDISCIPLINARY RESEARCH DATA. AMIA Annu Symp Proc 2005;2005:902.

96. Schmidt A, Kalra D, Dupont D, Claerhout B, Dugas M, Sundgren M, et al.: The Electronic Health Records for Clinical Research Project [Internet]. 2012 May 25 [cited 2012 Aug 26];Available from: http://www.touchhealthsciences.com/articles/electronic-health-records-clinical-research-project

97. Fritz F, Balhorn S, Riek M, Breil B, Dugas M: Qualitative and quantitative evaluation of EHR-integrated mobile patient questionnaires regarding usability and cost-efficiency. Int J Med Inform 2012 May;81:303–313.

98. Weitzman ER, Adida B, Kelemen S, Mandl KD: Sharing Data for Public Health Research by Members of an International Online Diabetes Social Network. PLoS One 2011 Apr 27;6:e19256.

99. Mandl KD, Simons WW, Crawford WCR, Abbett JM: Indivo: a personally controlled health record for health information exchange and communication. BMC Med Inform Decis Mak 2007 Sep 12;7:25.

100. Gesundheitsakte.de [Internet] [cited 2012 Aug 9];Available from: http://www.gesundheitsakte.de/

101. Die Personal Health Platform von careon [Internet] [cited 2012 Sep 3];Available from: http://www.gesundheitsakte.de/?id=146

102. Prokosch H-U, Ückert F, Ataian M, Görz M: akteonline.de: Patientenorientierte Gesundheitsakte. Dtsch Arztebl 2002;99:[21].

103. Die elektronische Gesundheitsakte akteonline.de [Internet]. Gesakon GmbH [cited 2012 Aug 9];Available from: http://www.gesakon.net/13.html

104. Ückert F, Müller ML, Bürkle T, Prokosch H-U: An electronic health record to support patients and institutions of the health care system. Ger Med Sci 2004 Aug 24;2:Doc06.

105. vita-x [Internet] [cited 2012 Sep 3];Available from: http://www.vita-x.de/vita-x.1.htm

106. Elektronische Patientenakte vita-X [Internet]. Telemedizinführer Deutschland 2009 [cited 2012 Sep 3];Available from: http://www.telemedizinfuehrer.de/index.php?option=com_content&task=view&id=446&Itemid=62

107. Riebling, J: vita-X – Die persönliche Gesundheitsakte [Internet]. Telemedizinführer Deutschland [cited 2012 Sep 3];Available from: http://www.telemedizinfuehrer.de/index2.php?option=com_content&do_pdf=1&id=331

108. LifeSensor Gesundheitsakte [Internet]. InterComponentWare AG (ICW) [cited 2012 Jun 27];Available from: http://www.icw-global.com/de/intercomponentware-ag/lifesensor-gesundheitsakte.html

109. Universitätsklinikum Heidelberg: Reibungslose einrichtungsübergreifende Kommunikation [Internet]. InterComponentWare AG [cited 2012 Sep 3];Available from: http://www.icw-global.com/de/referenzen/kundenreferenzen/university-hospital-heidelberg.html

110. Einrichtungsübergreifende Kommunikation zum Vorteil des Patienten [Internet]. InterComponentWare AG 2011 Apr [cited 2012 Sep 3];Available from: http://www.icw-global.com/fileadmin/user_upload/pdfs/references/de/icw-referenz-universitaetsklinik-heidelberg.pdf

111. Metropolregion: Metropolregion Rhein-Neckar - Leben in Bewegung [Internet] [cited 2012 Jul 26];Available from: http://www.m-r-n.com/

112. Metropolregion Rhein-Neckar - Raum für Gesundheit: Antrag für die Realisierungsphase im Rahmen des BMBF-Wettbewerbs “Gesundheitsregionen der Zukunft” [Internet] [cited 2012 Jul 16];Available from: http://www.treffpunktgesundheit.eu/download/090318_BMBF-Antrag_RfG.pdf

113. Metropolregion Rhein-Neckar: PEPA – Persönliche, einrichtungsübergreifende Patientenakte – Patienten am Drücker. Krankenhaus-IT Testimonials:26–27.

114. Heinze O, Bergh B: Establishing a personal electronic health record in the Rhine-Neckar region. Stud Health Technol Inform 2009;150:119.

115. Heinze O, Birkle M, Köster L, Bergh B: Architecture of a consent management suite and integration into IHE-based regional health information networks. BMC Med Inform Decis Mak 2011 Oct 4;11:58.

116. Hachman M: Microsoft Launches “HealthVault” Records-Storage Site [Internet]. PCMAG 2007 Oct 4 [cited 2012 Sep 4];Available from: http://www.pcmag.com/article2/0,2817,2191920,00.asp

117. Liao L, Chen M, Rodrigues JJPC, Lai X, Vuong S: A novel web-enabled healthcare solution on health vault system. J Med Syst 2012 Jun;36:1095–1105.

118. Shah BR, Adams M, Peterson ED, Powers B, Oddone EZ, Royal K, et al.: Secondary Prevention Risk Interventions Via Telemedicine and Tailored Patient Education (SPRITE) A Randomized Trial to Improve Postmyocardial Infarction Management. Circ Cardiovasc Qual Outcomes 2011 Jan 3;4:235–242.

119. Gerlof H: Microsoft geht mit Gesundheitsplattform im Internet erneut an den Start [Internet]. Ärtze Zeitung [cited 2012 Sep 3];Available from: http://www.aerztezeitung.de/kongresse/kongresse2011/duesseldorf2011-medica/article/679246/microsoft-geht-gesundheitsplattform-internet-erneut-start.html

120. Assignio Endbenutzerportal [Internet] [cited 2012 Jun 27];Available from: https://www.assignio.de/de/Home.aspx

121. Borchers D, Briegleb V: Microsoft-Patientenakte HealthVault kommt nach Deutschland [Internet]. heise online 2010 Jan 28 [cited 2012 Sep 4];Available from: http://www.heise.de/newsticker/meldung/Microsoft-Patientenakte-HealthVault-kommt-nach-Deutschland-916302.html

122. Microsoft HealthVault [Internet]. Microsoft HealthVault [cited 2012 Aug 26];Available from: http://www.HealthVault.com

123. Google Health has been discontinued [Internet] [cited 2012 Jun 27];Available from: https://accounts.google.com/ServiceLogin?service=health&nui=1&continue=https://health.google.com/health/p/&followup=https://health.google.com/health/p/&rm=hide

124. Leemhuis T: Das Ende von Google PowerMeter und Google Health [Internet]. c’t 2011 Jun 25 [cited 2012 Sep 4];Available from: http://www.heise.de/ct/meldung/Das-Ende-von-Google-PowerMeter-und-Google-Health-1268001.html

125. Wilkens A: Google Health ist online [Internet]. heise online 2008 May 20 [cited 2012 Sep 4];Available from: http://www.heise.de/newsticker/meldung/Google-Health-ist-online-208779.html

126. Bourgeois FC, Taylor PL, Emans SJ, Nigrin DJ, Mandl KD: Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients. J Am Med Inform Assoc 2008;15:737–743.

127. Dossia Personal Health Platform [Internet]. Dossia [cited 2012 Aug 26];Available from: http://www.dossia.org/

128. Szolovits P: Guardian Angel: Personal Lifelong Active Medical Assistant [Internet]. The MIT CDM Guardian Angel Project 2001 Feb 1 [cited 2012 Aug 8];Available from: http://groups.csail.mit.edu/medg/projects/ga/

129. Szolovits P, Doyle J, Long WJ, Kohane I, Pauker SG: Guardian Angel: Patient-Centered Health Information Systems [Internet] 1994 May [cited 2012 Aug 8];Available from: http://groups.csail.mit.edu/medg/projects/ga/manifesto/GAtr.pdf

130. Simons WW, Mandl KD, Kohane IS: The PING personally controlled electronic medical record system: technical architecture. J Am Med Inform Assoc 2005 Feb;12:47–54.

131. Kohane IS, Mandl KD, Taylor PL, Holm IA, Nigrin DJ, Kunkel LM: MEDICINE: Reestablishing the Researcher-Patient Compact. Science 2007 May 11;316:836–837.

132. Bonander J, Gates S: Public Health in an Era of Personal Health Records: Opportunities for Innovation and New Partnerships. J Med Internet Res 2010 Aug 10;12. DOI: 10.2196/jmir.1346

133. Sequist TD, Zaslavsky AM, Colditz GA, Ayanian JZ: Electronic Patient Messages to Promote Colorectal Cancer Screening: A Randomized, Controlled Trial. Arch Intern Med 2011 Apr 11;171:636–641.

134. Bales S: Die Einführung der elektronischen Gesundheitskarte in Deutschland. Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz 2005 Jul;48:727–731.

135. Unternehmensorganisation - Historie [Internet]. gematik [cited 2012 Sep 16];Available from: http://www.gematik.de/cms/de/gematik/unternehmensorganisation/historie_1/historie_1.jsp

136. Unternehmensorganisation - Gesetzliche Grundlagen [Internet]. gematik [cited 2012 Sep 16];Available from: http://www.gematik.de/cms/de/gematik/unternehmensorganisation/gesetzlichegrundlagen/gesetzlichegrundlagen_1.jsp

137. Lücke S, Köhler F: Die elektronische Gesundheitskarte - Schlüssel für die elektronische Vernetzung im deutschen Gesundheitswesen. DMW - Deutsche Medizinische Wochenschrift 2007 Mar;132:448–452.

138. Goetz CF-J: Gesundheitstelematik zwischen konventioneller Wahrnehmung und neuen Herausforderungen. Datenschutz und Datensicherheit 2011 Nov 27;35:847–852.

139. Spezifikation - Abgekündigte Releases [Internet]. gematik [cited 2012 Jan 2];Available from: http://www.gematik.de/cms/de/spezifikation/abgekuendigte_releases/releases_abgekuendigt.jsp

140. Arbeitsgruppe Datenschutz (AG DS) [Internet]. TMF eV 2012 Apr 18 [cited 2012 Jun 15];Available from: http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS.aspx

141. Arbeitsgruppe Datenschutz [Internet]. TMF eV 2010 Sep [cited 2012 Jun 15];Available from: http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=9728&PortalId=0

142. AG Datenschutz der TMF: Beratungs- und Implementationsstand zu Datenschutzkonzepten in der medizinischen Verbundforschung (Stand: 24.06.2008) 2008 Jun 24;

143. Kecher C: UML 2.0 : das umfassende Handbuch [aktuell zum UML-Standard 2.0, alle Diagramme und Notationselemente, Praxisbeispiele in C♯ und Java inkl. CD mit UML-Tools und A2-Poster]. 2., aktualisierte und erw. Aufl. Bonn, Galileo Press, 2006.

144. Kunz T, Viebeg U, Eckstein L, Kuhlisch R, Rode O, Gessner C, et al.: FuE ePA - AP6.2 - Fachkonzept und Facharchitektur (Version 1.0 Stand: 10.11.2011) 2011;

145. PubMed NCBI [Internet]. PubMed.gov - US National Library of Medicine National Institutes of Health [cited 2012 Oct 11];Available from: http://www.ncbi.nlm.nih.gov/pubmed/

146. Google Scholar [Internet] [cited 2012 Oct 11];Available from: http://scholar.google.de/

147. SpringerLink - electronic journals, protocols and books. [Internet] [cited 2012 Oct 11];Available from: http://www.springerlink.com

148. Kompetenznetz AHF: Nationales Register für angeborene Herzfehler [Internet] [cited 2012 Sep 30];Available from: http://www.kompetenznetz-ahf.de/forschung/register-biobank/

149. Pommerening K: Das Datenschutzkonzept der TMF für Biomaterialbanken (The TMF Data Protection Scheme for Biobanks). it - Information Technology 2007 Nov;49:352–359.

150. Helbing K, Demiroglu SY, Rakebrandt F, Pommerening K, Rienhoff O, Sax U: A data protection scheme for medical research networks. Review after five years of operation. Methods Inf Med 2010;49:601–607.

151. Becker R, Ihle P, Pommerening K, Harnischmacher U: BMB-Projekt: Ein generisches Datenschutzkonzept für Biomaterialbanken (Version 1.0) 2006;

152. Müller D, Augustin M, Banik N, Baumann W, Bestehorn K, Hense HW, et al.: Memorandum Register für die Versorgungsforschung [Internet] 2010;Available from: https://www.thieme-connect.com/ejournals/abstract/10.1055/s-0030-1263132

153. Forschungs- und Entwicklungsprojekt Elektronische Patientenakte gemäß § 291a SGB V [Internet] [cited 2012 Apr 24];Available from: https://www.epa291a.de/doku.php?id=start

154. Helbing K, Quade M, Eckstein L, Rode O, Krause R: FuE ePA - AP5.3 - Anwendungsspezifisches Datenschutzkonzept - Anforderungen aus Versorgung und Forschung (Version 0.6 Stand: 27.10.2011) 2011;

155. Eckstein L, Kuhlisch R, Kunz T, Rode O, Viebeg U, Kraufmann B, et al.: FuE ePA - AP5.9 - Sicherheitsarchitektur - Spezifikation der Sicherheitsdienste (Version 0.4 Stand: 02.02.2011) 2011;

156. Kuhlisch R, Rode O: FuE ePA - AP3.2 - Ausgestaltung von Anforderungs- und Bereitstellungsobjekten - Datenstrukturen (Version 0.3 Stand: 25.11.2010) 2010;

157. Kuhlisch R, Rode O: FuE ePA - AP3.1 - Zugang zu Akten - Konzept einer Capability List (Version 0.2 Stand: 02.02.2011) 2011;

158. Object Management Group [Internet]. Object Management Group [cited 2012 May 21];Available from: http://www.omg.org/index.htm

159. Object Management Group: Retrieve, Locate, and Update Service (RLUS) Specification (Version 1.0.1) [Internet] 2011 Jul [cited 2012 May 21];Available from: http://www.omg.org/spec/RLUS/1.0.1/PDF/

160. Rode O, Kuhlisch R, Caumanns J: FuE ePA - AP3.2 - Semantic Signifier: Definition und Verwaltung (Version 0.2 Stand: 10.02.2011) 2011;

161. Kunz T, Viebeg U, Eckstein L, Rode O, Kuhlisch R: FuE ePA - AP3.4 - Autorisierung durch den Bürger - Anforderungen und Basiskonzept (Version 1.0 Stand: 04.10.2011) 2011;

162. Causmanns J, Eckstein L, Semler S: Elektronische Patientenakte gemäß §291a SGB V - Die Patientenakte in der Versorgung: Kernkonzepte und technische Umsetzung [Internet] [cited 2011 Dec 18];Available from: http://www.isst.fraunhofer.de/Images/Fraunhofer_ISST-ePatientenakte-DIE%20PATIENTENAKTE%20IN%20DER%20VERSORGUNG_tcm81-86619.pdf

163. Rode O, Kuhlisch R, Caumanns J: FuE ePA - AP3.1 - Zugang zu Akten - Analyse relevanter Kommunikationsmuster (Version 1.0 Stand: 17.10.2011) 2011;

164. Gudgin M, Hadley M, Mendelsohn N, Moreau J-J, Nielsen HF, Karmarkar A, et al.: SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) - W3C Recommendation 27 April 2007 [Internet]. W3C 2007 Apr 27 [cited 2012 Sep 30];Available from: http://www.w3.org/TR/soap/

165. Mihindukulasooriya N: Understanding WS – Security Policy Language [Internet]. WSO2 2008 Jan 28 [cited 2012 Apr 16];Available from: http://wso2.org/library/3132

166. Nadalin A, Goodner M, Gudgin M, Barbir A, Granqvist H: WS-SecurityPolicy 1.3 - OASIS Standard [Internet]. OASIS 2009 Feb 2 [cited 2012 Jul 22];Available from: http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.pdf

167. Rode O, Caumanns J: FuE ePA - AP5.9 - Verschlüsselungskonzept - Duale Hybridverschlüsselung (Version 0.3 Stand: 07.06.2011) 2011;

168. Pollanz G: MED-O-CARD EPA ab Jannuar 2012 [Internet]. MED-O-CARD AG [cited 2011 Dec 27];Available from: http://www.med-o-card.de/medocard_news/newsitem.php?ID=44

169. Anwendungen der eGK [Internet]. gematik [cited 2012 Jun 29];Available from: http://www.gematik.de/cms/de/egk_2/anwendungen/anwendungen_1.jsp

170. Hewison J, Haines A: Overcoming barriers to recruitment in health research. BMJ 2006 Aug 5;333:300–302.

171. Weitzman ER, Kaci L, Mandl KD: Sharing Medical Data for Health Research: The Early Personal Health Record Experience. Journal of Medical Internet Research 2010 May 25;12:e14.

172. Kirchner H: Nutzen und Akzeptanz von elektronischen Gesundheitsakten. Abschlussbericht zum Forschungsvorhaben der BARMER GEK 2010 - Kurzfassung - [Internet]. BARMER GEK 2011 [cited 2012 Aug 3];Available from: https://www.barmer-gek.de/barmer/web/Portale/Versicherte/Rundum-gutversichert/Infothek/Wissenschaft-Forschung/Forschungsergebnisse/Elektronische_20Gesundheitsakte/eGA.html?w-cm=LeftColumn_tdocid

173. HL7 Deutschland e.V. [Internet] [cited 2012 Jun 27];Available from: http://www.hl7.de/

174. Clinical Data Interchange Standards Consortium (CDISC) [Internet] [cited 2012 Jun 27];Available from: http://www.cdisc.org/

175. BRIDG [Internet] [cited 2012 Jun 27];Available from: http://www.cdisc.org/bridg

176. Steward DA, Hofler RA, Thaldorf C, Milov DE: A method for understanding some consequences of bringing patient-generated data into health care delivery. Med Decis Making 2010 Aug;30:E1–E13.

177. Anwendungen der eGK - Verfügbare Anwendungen [Internet]. gematik [cited 2012 Jun 27];Available from: http://www.gematik.de/cms/de/egk_2/anwendungen/verfuegbare_anwendungen/verfuegbare_anwendungen_1.jsp

178. Anwendungen der eGK - In Vorbereitung [Internet]. gematik [cited 2012 Jun 27];Available from: http://www.gematik.de/cms/de/egk_2/anwendungen/vorbereitung/vorbereitung_1.jsp

179. Die elektronische Fallakte [Internet]. Verein elektronische FallAkte 2010 [cited 2012 Jun 27];Available from: http://www.fallakte.de/

180. Kaye J, Curren L, Anderson N, Edwards K, Fullerton SM, Kanellopoulou N, et al.: From patients to partners: participant-centric initiatives in biomedical research. Nat Rev Genet 2012 May;13:371–376.

181. Gesundheitsregionen [Internet]. Bundesministerium für Bildung und Forschung 2011 May 17 [cited 2012 Aug 7];Available from: http://www.bmbf.de/de/12547.php

182. DZHK - Deutsches Zentrum für Herz-Kreislauf-Forschung e. V. [Internet] [cited 2012 Aug 7];Available from: http://dzhk.de/

183. Caumanns J, Rode O, Kunz T, Eckstein L: FuE ePA - AP5.5 - ePA Signaturkonzept - Umgang mit elektronischen Signaturen auf Dokumenten einer ePA nach § 291a SGB V (Version 0.5 Stand: 10.06.2011) 2011;

184. Helbing K: FuE ePA - AP1.1 und AP1.2 - Anwendungsfälle einer elektronischen Patientenakte - Anwendungsfälle und IT-Komponenten der medizinischen Forschung (Version 0.4 Stand: 01.11.2011) 2011;

185. Helbing K: FuE ePA - AP5.8 - Interaktion Forschung und Versorgung - Kommunikation zwischen der ePA und einem medizinischen Forschungsverbund (Version 0.7 Stand: 13.09.2010) 2010;

186. Helbing K: FuE ePA - AP6.2 - Fachkonzept und Facharchitektur der Forschungsschnittstelle (Version 03 Stand: 18.11.2012) 2012;

187. Helbing K: FuE ePA - AP5.9 - Sicherheitsarchitektur der Forschungsschnittstelle (Version 0.2 Stand: 18.11.2012) 2012;

188. Drepper J, Pommerening K: GLOSSAR für die Revisionsfassung des generischen Datenschutzkonzepts der TMF 2010 Feb 21;

189. Helbing K: Experten-Review eines Kommunikationsmodells für die Anbindung eines Versorgungsmoduls an eine ePA nach §291a SGB V (Version 2.0 Stand: 18.05.12) 2012;

Anhang

A1. Anhang zur Literaturrecherche

A1.1. Elektronische Akten im Gesundheitswesen

Bezeichnung national	Bezeichnung international	Merkmale
Institutionelle Elektronische Fallakte	Keine Entsprechung	Alle Daten und Dokumente eines Behandlungsfalles einer Patientin und eines Patienten in einer Gesundheitsversorgungseinrichtung, ärztlich geführt und moderiert.
Institutionelle Elektronische Patientenakte (iEPA)	Electronic Medical Record (EMR), Electronic Patient Record (EPR)	Alle Daten und Dokumente aller Behandlungen einer Patientin und eines Patienten in einer Gesundheitsversorgungseinrichtung, ärztlich geführt und moderiert.
Einrichtungsübergreifende medizinische Fallakte (EFA)	Keine Entsprechung	Die zur Kommunikation bei einer gemeinsamen Behandlung von den Behandelnden als relevant eingestuften Daten und Dokumente über alle Gesundheitsversorgungseinrichtungen hinweg, ärztlich geführt und moderiert.
Einrichtungsübergreifende Elektronische Patientenakte (eEPA)	Electronic Health Record (EHR), Electronic Patient Record (EPR)	Die wichtigsten Daten und Dokumente aller Behandlungen einer Patientin und eines Patienten über alle Gesundheitsversorgungseinrichtungen hinweg, ärztlich geführt und moderiert, ggf. mit behandlungsrelevanten eigenen Eintragungen der Patientin oder des Patienten auf Anweisung der Ärztin bzw. des Arztes ergänzt
Persönliche Elektronische Patientenakte (pEPA)	Personal Electronic Health Record (PHR), Personally Controlled Health Record (PCHR)	Fallübergreifende Akte unter der Datenhoheit der Patientin bzw. des Patienten. Die Entscheidung über die konkrete Nutzung (Zweckbestimmung) erfolgt im Einzelfall durch die Patientin bzw. den Patienten, indem diese die Informationen bei Bedarf einer behandelnden Ärztin oder einem behandelnden Arzt zur Verfügung stellen. Die Patientin bzw. der Patient kann Rechte auch an eine Ärztin bzw. einen Arzt ihres / seines Vertrauens delegieren. Sinn der pEPA ist, als Quelle für die Speisung der zweckbestimmten Patientenakten in der Verantwortung der Ärztinnen und Ärzte zu dienen
Elektronische Gesundheitsakte (EGA)	Personal Electronic Health Record (PHR), Personally Controlled Health Record (PCHR)	Von den Patientinnen bzw. den Patienten ausgewählte Daten und Dokumente aller ihrer Behandlungen über alle Gesundheitsversorgungseinrichtungen hinweg, ärztlich- oder patientengeführt oder hybrid und rein patientenmoderiert, ergänzt um beliebige eigene Eintragungen der Patientin und des Patienten.
Elektronische Basisdokumentationsakte	Minimum Basic Data Set (MBDS)	Nur wenige ausgewählte, lebenslange und im Notfall wichtige medizinische Daten wie Diagnosen, Maßnahmen, Risikofaktoren etc., keine Dokumente, ärztlich geführt und moderiert.
Registerakte	Keine Entsprechung	Ganz wenige vollständig strukturierte und formalisierte Inhalte zu einer definierten Krankheitsklasse.

Tabelle 17: Definitionen elektronischer Akten im Gesundheitswesen des bundesweiten Arbeitskreises EPA/EFA [39, Seite 16]

A1.2. Verwendete Suchbegriffe für die Literaturrecherche

Versorgungssystem und EPA	Forschungssystem	Secondary Use	Elektronische Gesundheitskarte und Telematikinfrastruktur
Clinical Information System	EDC	Single Source	Elektronische Gesundheitskarte
Hospital Information System	Electronic Data Capture	Secondary Use	eGK
Health Records, Personal (MeSH)	Clinical Study	Reusing	Heilberufsausweis
Electronic Health Records (MeSH)	Clinical Research	Single Data Source	HBA
Personally Controlled Electronic Health Record (PCEHR)	Medical Research	Data Reuse	Gesundheitstelematik
	Health Research	Secondary Data Use	E-Card
	Biomedical Research	Reuse	Telematikinfrastruktur
	Clinical Data Management System	Re-Use	ePA
	CDMS	Integrated	§291a
	Clinical Research Data Capture		Elektronische Gesundheitsakte
	Remote Data Entry		Elektronische Patientenakte
	CDW		
	Clinical Data Warehouse		
	CRFs		
	eCRFs		
	Clinical Trial		

Tabelle 18: Verwendete Suchbegriffe für die Literaturrecherche

A1.3. Datenschutzkonzepte der medizinischen Forschungsverbünde

Verbund	Konzept vorhanden	Befürwortet (durch)
CAPNETZ	Ja	LfD
KN Rheuma	Ja	LfD
KN CED	Nein	LfD
Hepnet	Ja	TMF

Tabelle 19: Datenschutzkonzepte von 2002-2004

Verbund	Erst-vorstellung	Konzept vorhanden	Befürwortet durch (Quelle)[22]
BrainNet	24.06.2004	Ja	TMF (PT vom 21.02.2005)
„TMI-Server“	24.06.2004	Ja (Das Konzept des HIT-Verbundes ist eine aktuellere Version. Daher wird nur das Konzept des HIT-Verbundes analysiert.)	TMF (PT vom 21.02.2005)
KN Maligne Lymphome	24.06.2004	Nein	TMF (PT vom 18.11.2004)
KN Herzinsuffizienz	24.06.2004	Ja	k. A.
Konzept der Genbank Parkinson Deutschland, GEPARD	18.11.2004	Nein	LfD (Web)
Datenschutzkonzept KN Vorhof-flimmern	21.04.2005	Ja	TMF (PT vom 30.11.2005)
Datenschutzkonzept KN AHF	21.04.2005	Ja	LfD (PT vom 21.06.2006)
DS-Konzept NGFN-Kardio-Netz	29.09.2005	Nein	k. A.
DS-Konzept Hämophilie-Register des Paul-Ehrlich-Instituts	29.09.2005	Ja	TMF (PT vom 04.04.2006)
Kompetenznetz HIV/AIDS	21.06.2006	Ja	LfD (Web)
Datenschutzkonzept iCHIP des NGFN	07.09.2006	Ja	k. A.
HIT-Forschungsnetzwerk der Deutschen Kinderkrebshilfe	28.11.2006	Ja	TMF (Email KP)
Datenschutzkonzept zur Patienten-datenbank der German Breast Group	21.06.2007	Ja	LfD (Web)
Datenschutzkonzept des Netzwerks GeNeMove	28.11.2007	Nein	k. A.
EurIPFnet	18.06.2008	Ja	LfD (PT, 10.09.2008)
SKELNET	18.06.2008	Ja	Kein Votum bis jetzt (Email KP)

[22] Abkürzungen für die Quellen: LfD= es gibt ein Votum vom Landesdatenschutzbeauftragten, TMF = es liegt ein Votum der AG Datenschutz der TMF vor, PT = Protokoll, Email KP = Angaben aus Email von Prof. Klaus Pommerening, k.A. = Keine Angaben, Web = Angaben stammen aus einer Internetrecherche, Publikation = Angaben stammen aus einer Publikation.

Verbund	Erst-vorstellung	Konzept vorhanden	Befürwortet durch (Quelle)[22]
Datenschutzkonzept der Stiftung Präventivmedizin zur Erforschung der chronischen Niereninsuffizienz	10.09.2008	Ja	LfD (Web)
Internetgestützte Dokumentation in der kooperativen, palliativ-medizinischen Versorgung in der Pädiatrischen Onkologie	10.09.2008	Ja	Keine Forschung
Entwicklung von Statistik-Tools bei der BioArtProducts GmbH für zusammen-geführte Daten aus Arztpraxen	28.05. 2009	Nein (nur Abstract)	k. A
Entwurf eines Datenschutzkonzeptes für das Kompetenznetz Multiple Sklerose	05.11.2009	Ja	TMF (Email von KP)
PneumoGrid	11.02.2010	Nein (erster Entwurf)	k. A.
Europäisches Register zur Primären Hyperoxalurie des European Hyperoxaluria Consortium (OXALEUROPE)	11.02.2010	Nein (Abstract)	k. A.
Register für Minimale intensivmed. Notfalldatensätze (MIND3)	11.02.2010	Nein (Abstract)	k. A.
Register für pädiatrische Nierentransplantationen	08.04.2010	Ja	LfD (Publikation)
Deutsches Register für primäre Immundefekte	08.04.2010	Nein	k. A.
Datenbank der Arbeitsgemeinschaft für komplementäre Therapieverfahren in der Onkologie	08.04.2010	Ja	k. A.
German Network for Diffuse Parenchymal Lung Diseases (GOLDnet)	08.06.2010	Ja	TMF (Email von KP)
Kinderlungenregister	08.06.2010	Ja (wird jetzt im GoldNet umgesetzt, Quelle Web)	Bis jetzt kein Votum (Email von KP)
Verbundprojekt „Managing Infections of the Skeletal System in Germany“	08.11.2010	Nein	k. A.
Pharmakovigilanz- und Beratungs-zentrum für Embryonaltoxikologie	07.02.2011 (vorgestellt)	Nein	k. A.
Nationales Lipidaphereseregister	24.03.2011	Ja	Bis jetzt kein Votum (Email KP)
Internationale Kooperationen und Ausbau der Infrastruktur des CURE-Net	24.05.2011	Nein (Abstract)	
Institut für Lungenforschung GmbH	13.09.2011 (vorgestellt)	Nein (Abstract)	k. A.
BeoNet (Beobachtungsnetz zur krankheits-übergreifenden Versor-gungsforschung in Niedersachsen)	09.11.2011	Nein (Vorhabens-beschreibung)	k. A.

Tabelle 20: Auflistung aller in der AG Datenschutz der TMF vorgestellten Datenschutzkonzepte seit 2004

A1.4. Vollständige Erfassung der Anwendungsfälle aus dem DSK Leitfaden und den generischen Datenschutzkonzepten der TMF sowie der Literaturanalyse

Modul	Anwendungsfall	Patientenbezug	Quelle
Identitäts-management	Anmeldung eines Patienten an einem Forschungsverbund (Variante A)	Ja, weil der Patient Daten für die Patientenliste bereitstellt und einwilligt am Forschungsverbund teilzunehmen.	1) Modell A 2) Leitfaden
Identitäts-management	Anmeldung eines Patienten an einem Forschungsverbund (Variante B)	Ja, weil der Patient Daten für die Patientenliste bereitstellt und einwilligt am Forschungsverbund teilzunehmen.	1) Modell B 2) Leitfaden
Identitäts-management	Recht des Patienten auf Auskunft	Ja, weil der Patient Informationen anfordert und dem Patienten Informationen bereitgestellt werden.	1) Modell A 2) Modell B 3) Leitfaden
Identitäts-management	Aktualisierung der Daten	Ja, weil der Patient Daten für die Patientenliste bereitstellt.	Analyse
Identitäts-management	Patienten kontaktieren	Ja, weil dem Patienten Informationen bereitgestellt werden.	1) Modell A 2) Modell B 3) Leitfaden
Identitäts-management	Rückzug der Einwilligung	Ja, weil der Patient Informationen zum Löschen seiner Daten bereitstellt.	1) Modell A 2) Modell B 3) Leitfaden
Identitäts-management	Übertragen von Daten an die Forschungsdatenbank aus dem Versorgungs-kontext oder aus dem Studienkontext	Nein, weil keine Daten vom und für den Patienten angefordert bzw. bereitgestellt werden.	Leitfaden
Identitäts-management	Depseudonymisierung zur Datenqualitätssicherung	Nein, weil keine Daten vom und für den Patienten angefordert bzw. bereitgestellt werden.	Leitfaden
Identitäts-management	Todesfall eines Patienten oder Probanden	Nein, da dem Patienten keine Informationen bereitgestellt werden und der Patient auch keine Informationen bereitstellt.	Leitfaden
Identitäts-management	Umpseudonymisierung (Ersetzen vorhandener Pseudonyme durch neue)	Nein, da dem Patienten keine Informationen bereitgestellt werden und der Patient auch keine Informationen bereitstellt.	Leitfaden
Versorgungs-modul	Aufnahme in die Behandlungsdatenbank / das Versorgungsmodul	Ja, weil der Patient Daten für die Behandlungsdatenbank bereitstellt.	1) Modell A 2) Leitfaden
Versorgungs-modul	Erfassung und Zugriff auf Daten im Behandlungsprozess / Zugriff auf Identitätsdaten zu Behandlungszwecken	Ja, weil der Patient Daten für die Behandlungsdatenbank bereitstellt.	1) Modell A 2) Leitfaden
Versorgungs-modul	Vergabe von Zugriffsrechten / Autorisierung von Mit- oder Weiterbehandlern	Ja, weil der Patient Informationen bereitstellt, wer Zugriffrechte bekommt bzw. wem Zugriffrechte entzogen werden	1) Modell A 2) Leitfaden

Modul	Anwendungsfall	Patientenbezug	Quelle
Versorgungs-modul	Zugriff auf Daten für Zwecke der Qualitäts-sicherung	Nein, da dem Patienten weder Informationen bereitgestellt werden noch vom Patienten Informationen angefor-dert werden.	Leitfaden
Versorgungs-modul	Tod des Patienten	Nein, da dem Patienten weder Informa-tionen bereitgestellt werden noch vom Patienten Informationen angefordert werden.	Leitfaden
Versorgungs-modul	Machbarkeit einer Auswer-tung oder Studie prüfen	Nein, da dem Patienten weder Informa-tionen bereitgestellt werden noch vom Patienten Informationen angefordert werden.	Leitfaden
Versorgungs-modul	Rekrutierung für neue Studien	Ja, da dem Patienten eine Rekrutie-rungsanfrage bereitgestellt wird.	Leitfaden
Versorgungs-modul	Export von Daten	Nein, weil keine Anforderung oder Bereitstellung durch oder für den Patienten erfolgt.	1) Modell A 2) Leitfaden
Versorgungs-modul	Expertenforum	Nein, weil keine Anforderung oder Bereitstellung durch oder für den Patienten erfolgt.	Leitfaden
Versorgungs-modul	Informieren eines Patien-ten über Forschungser-gebnisse	Ja, weil dem Patient Forschungsergeb-nisse bereitgestellt werden.	Modell A
Versorgungs-modul	Medizinische Qualitäts-sicherung und Bench-marking	Nein, da dem Patienten keine Informa-tionen bereitgestellt werden oder vom Patienten Informationen angefordert werden.	Leitfaden
Versorgungs-modul	Recht des Patienten auf Auskunft	Ja, weil der Patient Informationen anfor-dert und dem Patienten Informationen bereitgestellt werden.	Modell A
Versorgungs-modul	Rückzug der Einwilligung / Löschen, Sperren oder Anonymisieren medizi-nischer Daten	Ja, weil der Patient Informationen zum Löschen seiner Daten bereitstellt.	1) Modell A 2) Leitfaden
Studienmodul	Aufnahme in eine Studie	Ja, weil der Patient Daten für die Auf-nahme bereitstellt (z. B. identifizierende Daten oder Basisdaten) und weil der Patient Daten z. B. Aufklärungsbögen, Visitenpläne etc. bekommt.	Leitfaden
Studienmodul	Erheben von Studiendaten	Ja, weil der Patient Daten bereitstellt.	Leitfaden
Studienmodul	Informieren nach der Aus-wertung von Studiendaten	Ja, da dem Patienten ggf. Ergebnisse der Auswertung bereitgestellt werden.	Analyse
Studienmodul	Managen von unerwarteten Ereignissen	Ja, da der Patient Daten zum unerwar-teten Ereignis bereitstellt.	Leitfaden
Studienmodul	Qualitätssicherung der Daten und Rückfrage-management	Nein, da dem Patienten weder Daten bereitgestellt werden noch Daten vom Patienten bereitgestellt werden.	Leitfaden
Studienmodul	Archivieren von Studien	Nein, da dem Patienten weder Daten bereitgestellt werden noch Daten vom Patienten bereitgestellt werden.	Leitfaden

Modul	Anwendungsfall	Patientenbezug	Quelle
Studienmodul	Auskunftsrecht des Patienten	Ja, da der Patient Informationen anfordert und dem Patienten Informationen bereitgestellt werden.	Analyse
Studienmodul	Rückzug der Einwilligung / Versterben des Patienten	Ja, da der Patient Daten für den Rückzug der Einwilligung bereitstellt (z. B. seine identifizierenden Daten, oder sein Pseudonym zum Löschen der Daten).	Leitfaden
Qualitäts-sicherungs-service	Qualitätssicherung und Übertragen der Daten in die Forschungsdaten-bank / Nutzung der Daten einer Forschungsdaten-bank zum Zwecke der Qualitätssicherung	Nein, weil keine Daten vom und für den Patienten angefordert bzw. bereitgestellt werden.	1) Modell B 2) Leitfaden
Forschungs-modul	Zugriff durch Wissen-schaftler / Auswertung und Sekundärauswertung	Nein, weil keine Daten vom und für den Patienten angefordert bzw. bereitgestellt werden. Sollte ein Patient über Ergeb-nisse informiert werden, erfolgt dies wie im Anwendungsfall „Informieren eines Probanden über Forschungsergeb-nisse“.	1) Modell B 2) Leitfaden
Forschungs-modul	Machbarkeit einer Studie prüfen	Nein, da weder vom Patienten Daten angefordert, noch für ihn Daten bereitgestellt werden. Eine eventuelle Kontaktierung erfolgt dann im Rahmen der Rekrutierung (siehe Rekrutierung von Patienten).	Leitfaden
Forschungs-modul	Rekrutierung von Patienten	Ja, da dem Patienten eine Rekrutie-rungsanfrage bereitgestellt wird.	Leitfaden
Forschungs-modul	Export von Forschungs-daten	Nein, weil keine Daten vom und für den Patienten angefordert bzw. bereitgestellt werden.	1) Modell B 2) Leitfaden
Forschungs-modul	Informieren eines Probanden über Forschungsergebnisse	Ja, da dem Patienten Informationen bereitgestellt werden.	1) Modell B 2) Leitfaden
Forschungs-modul	Recht des Patienten auf Auskunft	Ja, da der Patient Informationen anfor-dert und dem Patienten Informationen bereitgestellt werden.	1) Modell B 2) Leitfaden
Forschungs-modul	Rückzug der Einwilligung / Anonymisieren bzw. Löschen medizinischer Daten in der Forschungs-datenbank	Ja, weil der Patient Informationen zum Löschen seiner Daten bereitstellt.	1) Modell B 2) Leitfaden
Forschungs-modul	Datenabgleich mit externen Datenquellen	Nein, da weder vom Patienten Daten angefordert, noch für ihn Daten bereit-gestellt werden.	Leitfaden

Tabelle 21: Vollständige Erfassung der Anwendungsfälle aus dem DSK Leitfaden und den generischen Datenschutzkonzepten der TMF sowie der Literaturanalyse. Anwendungsfälle ohne Patientenbezug sind grau hinterlegt

A1.5. Spezifikationen des FuE-ePA-Projektes

Name	Kurzbeschreibung	Verwendung
Verschlüsselte Datenhaltung - Beschreibung eines alternativen Verschlüsselungsmodells- [167]	Beschreibt das Verschlüsselungsmodell der LE-Schnittstelle.	Das Verschlüsselungskonzept dient als Grundlage der Verschlüsselung für die Forschungsschnittstelle und wird im Kapitel 5 und Kapitel 9 analysiert.
AP3.1 Zugang zu Akten - Konzept einer »Capability List«- [157]	Beschreibt den Aufbau und das Abrufen der Capability List.	Auf die Capability List wird im Kapitel 5 kurz eingegangen. Auf den Aufbau und das Abrufen der Capability List über die Forschungsschnittstelle wird im Kapitel 8 eingegangen.
Ausgestaltung von Anforderungs- und Bereitstellungsobjekten - Datenstrukturen - [156]	Beschreibt die Funktionen und den Aufbau der Anforderungs- und Bereitstellungsobjekte.	Auf die Anforderungs- und Bereitstellungsobjekte wird im Kapitel 5 kurz eingegangen. Auf den Aufbau und die Verwendung im Zusammenhang mit der Forschungsschnittstelle wird im Kapitel 8 eingegangen.
AP3.2 - Semantic Signifier - Definition und Verwaltung - [160]	Beschreibt die Funktionsweise der Semantic Signifier sowie den Aufbau der im FuE-ePA-Projekt verwendeten Semantic Signifier.	Auf das Thema Semantic Signifier wird im Kapitel 5 eingegangen.
AP3.4 - Autorisierung durch den Bürger -Anforderungen und Basiskonzept- [161]	Beschreibt das Autorisierungskonzept für die ePA.	Auf das Autorisierungskonzept wird im Kapitel 5 und Kapitel 9 eingegangen.
AP 6.2 - Fachkonzept und Facharchitektur - [144]	Beschreibt das Fachkonzept und die Facharchitektur der LE-Schnittstelle.	Auf das Fachkonzept und die Facharchitektur der LE-Schnittstelle wird im Kapitel 5 und Kapitel 8 eingegangen.
Sicherheitsarchitektur - Spezifikation der Sicherheitsdienste - [155]	Beschreibt die Sicherheitsarchitektur der LE-Schnittstelle.	Auf die Sicherheitsarchitektur wird im Kapitel 5 und Kapitel 9 eingegangen.
ePA Signaturkonzept -Umgang mit elektronischen Signaturen auf Dokumenten einer ePA nach § 291a SGB V-[183]	Beschreibt die Anforderungen in Bezug auf Signaturen für die medizinischen Dokumente einer ePA und beschreibt auf deren Grundlage das Signaturkonzept.	Auf das Signaturkonzept wird nicht weiter eingegangen, da das Thema Signaturen in dieser Arbeit nicht im Detail betrachtet wird (siehe auch 9.6).

Tabelle 22: Übersicht der Spezifikationen der LE-Schnittstelle und deren Verwendung in den einzelnen Kapiteln dieser Arbeit

A1.6. Im FuE-ePA-Projekt veröffentlichte Dokumente des Autors zum Thema Forschungsschnittstelle

Name	Ergebnis auf Kapitel
AP1.1 und AP1.2 - Anwendungsfälle einer elektronischen Patientenakte - Anwendungsfälle und IT-Komponenten der medizinischen Forschung (Version 04)[184]	Kapitel 4 und Anhang A2
AP 5.8 - Interaktion Forschung und Versorgung Kommunikation zwischen der ePA und einem medizinischen Forschungsverbund (Version 07)[185]	Ansätze aus Kapitel 7
AP6.2 - Fachkonzept und Facharchitektur der Forschungsschnittstelle (Version 03)[186]	Abschnitt 4.4.1, Kapitel 7, Kapitel 8 und Anhang A4
AP5.9 - Sicherheitsarchitektur der Forschungsschnittstelle (Version 0.2)[187]	Abschnitt 7.1, Kapitel 9 und Anhang A5

Tabelle 23: Im FuE-ePA-Projekt veröffentlichte Dokumente des Autors zum Thema Forschungsschnittstelle

A2. Module und Anwendungsfälle eines medizinischen Forschungsverbundes

A2.1. Studiendatenbank

A2.1.1. Aufnahme in eine Studie

Nachdem ein Patient entsprechend aufgeklärt worden ist, seine Einwilligungserklärung unterzeichnet hat und im Forschungsverbund für eine Studie oder ein Forschungsprojekt angemeldet worden ist, kann er nun in der Studiendatenbank vom Studienarzt oder ggf. einer Study Nurse (Studienassistent) angelegt und die Basisdaten zum Patienten eingetragen werden (siehe UC-2-1 Erheben von Studiendaten). Anschließend kann der Studienarzt dem Patienten dem Visitenplan und ggf. Informationen zu besonderer Behandlung und / oder Medikation etc. übergeben. In einigen Fällen wird noch eine Referenzbegutachtung oder eine Verifizierung des Krankheitsbildes durchgeführt. Sollten hierbei falschpositive Patienten entdeckt werden, so werden diese informiert und in der Studiendatenbank gelöscht bzw. anonymisiert [34].

A2.1.2. Erheben von Studiendaten

Ist ein Patient in eine Studie oder ein Forschungsvorhaben aufgenommen worden, so werden dem Visitenplan entsprechend die vorgesehenen Items zu einem Patienten erhoben und in pseudonymiserter Form in die Studiendatenbank eingetragen. Die Daten können von einem Studienarzt oder Mitarbeiter eines Forschungsverbundes bzw. dem Patienten selbst eingetragen werden. Es kann sich hierbei um neu erhobene Daten oder um Daten, die vom Patienten selbst (z. B. Daten zur Lebensqualität) oder im Rahmen der Versorgung des Patienten erhoben wurden (z. B. Laboruntersuchungen), handeln. In einigen Fällen werden die Daten erst vom Studienarzt auf Papierbögen erfasst und dann von Dokumentaren in die Studiendatenbank übertragen. Die Daten können auch erst elektronisch auf Laptops oder anderen mobilen Geräten erfasst werden und später in die Studiendatenbank geladen werden [34].

A2.1.3. Managen von unerwünschten Ereignissen

Treten unerwünschte Ereignisse bei der Durchführung einer Studie auf, so sind diese vom Studienarzt zu dokumentieren und ggf. zu melden. Neben einer Dokumentation in der Patientenakte ist auch häufig eine Dokumentation in der Studiendatenbank vorgesehen [34].

A2.1.4. Informieren eines Patienten über Forschungsergebnisse

In einigen Fällen können während der Auswertung Forschungsergebnisse gewonnen werden, die für bestimmte Patienten die Behandlung ihrer Krankheit verbessern können. Diese Ergebnisse sollten den entsprechenden Patienten mitgeteilt werden. Voraussetzung hierfür ist, dass die Auswertung auf einen pseudonymisierten Datenexport erfolgt ist und der Patient eingewilligt hat, dass er über neue Forschungsergebnisse informiert werden möchte[23].

[23] Der Anwendungsfall war in der Version des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - noch nicht aufgenommen und stammt aus der Analyse der Datenschutzkonzepte der medizinischen Forschungsverbünde. Daher gibt es an dieser Stelle keine Quelle aus den TMF Datenschutzkonzepten.

A2.1.5. Recht des Patienten auf Auskunft

Verlangt ein Patient Einsicht in die über ihn in der Studiendatenbank gespeicherten Daten, so kann er sich an den Ansprechpartner des Forschungsverbundes oder seinen Studienarzt wenden und Einblick in die über ihn in der Studiendatenbank und in der Patientenliste gespeicherten Daten verlangen. Der Ablauf ist in beiden Fällen der gleiche. Es kann allerdings ethische oder gesetzliche Vorschriften geben, die eine Erläuterung der angeforderten Informationen durch den behandelnden Arzt erfordern. In einigen Projekten kann der Patient auch einen direkten Zugriff auf die Studiendatenbank beantragen und dann die über ihn gespeicherten Daten in der Studiendatenbank einsehen[24].

A2.1.6. Rückzug der Einwilligung

Zieht ein Patient seine Einwilligung zurück, so müssen die Daten des Patienten in der Studiendatenbank gefunden und gelöscht bzw. anonymisiert werden. Anschließend werden die identifizierenden Daten des Patienten im Identitätsmanagement gelöscht. Neben den zentral gespeicherten Daten sind auch die in den Zentren verbliebenen Daten zu anonymisieren bzw. zu löschen. Der Rückzug der Einwilligung kann entweder über den Behandler erfolgen oder über den Ansprechpartner des Forschungsverbundes. Ob die Daten gelöscht oder anonymisiert werden, wird meistens in der Einwilligungserklärung bzw. im Aufklärungsbogen festgehalten. Der Patient hat immer das Recht auf eine Löschung seiner Daten, sofern es keine gesetzlichen Vorgaben gibt, die eine Aufbewahrung der Daten fordern (wie z. B. das Arzneimittelgesetz - AMG).[34]

[24] Der Anwendungsfall war in der Version des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF Version 2 - noch nicht aufgenommen und stammt aus der Analyse der Datenschutzkonzepte der medizinischen Forschungsverbünde. Daher gibt es an dieser Stelle keine Quelle aus den TMF Datenschutzkonzepten.

A2.2. Forschungsdatenbank

A2.2.1. Rekrutierung von Patienten

„Patienten, die bereits an einem früheren Forschungsprojekt teilgenommen haben, können mit Hilfe des Forschungsmoduls auch effektiv für weitere Studien rekrutiert werden. Dies kann insbesondere bei chronischen Erkrankungen von Interesse sein. Anders als bei der Überprüfung der Machbarkeit wird hierfür eine Depseudonymisierung der Datensätze ausgelöst werden müssen, die den gesuchten Ein- und Ausschlusskriterien entsprechen." [34, Seite 55]

A2.2.2. Informieren eines Patienten über Forschungsergebnisse

Werden bei der Auswertung von Forschungsdaten neue Erkenntnisse gewonnen, die für die Weiterbehandlung eines speziellen Patienten bzw. Patientenkollektivs essentiell sind, so sollten diese über die neuen Erkenntnisse informiert werden. Je nachdem welche Erkenntnisse gewonnen wurden, sollte eine Beratung durch einen behandelnden Arzt oder einen Humangenetiker vorgesehen werden. Bei der Depseudonymisierung ist auch zu beachten, dass ggf. eine Entbindung der Schweigepflicht notwendig ist, sofern der Untersuchungsbefund nicht dem behandelnden Arzt offenbart wird [33,34].

A2.2.3. Recht des Patienten auf Auskunft

Verlangt ein Patient Einsicht in die über ihn in der Forschungsdatenbank gespeicherten Daten, so kann er sich an den Ansprechpartner des Forschungsverbundes wenden oder seinen Behandler aufsuchen und Einblick in die über ihn in der Forschungsdatenbank gespeicherten Daten verlangen [33,34].

A2.2.4. Rückzug der Einwilligung

Zieht ein Patient seine Einwilligung zurück, so müssen die Daten des Patienten in der Forschungsdatenbank gefunden und gelöscht bzw. anonymisiert werden. Anschließend werden die identifizierenden Daten des Patienten im Identitätsmanagement gelöscht. Der Rückzug der Einwilligung kann entweder über den Behandler erfolgen oder über den Ansprechpartner des Forschungsverbundes. Ob die Daten gelöscht oder anonymisiert werden, wird meistens in der Einwilligungserklärung bzw. im Aufklärungsbogen festgehalten. Der Patient hat immer das Recht auf eine Löschung seiner Daten, sofern es keine gesetzlichen Vorgaben gibt, die eine Aufbewahrung der Daten fordern (wie z. B. das AMG). [33,34].

A2.3. Patientenliste

Im Folgenden wird die Kommunikation der ausgewählten Anwendungsfälle der Patientenliste in Tabellenform und Sequenzdiagrammen beschrieben.

A2.3.1. Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler

Bezeichner	UC-1-1
Name	Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler
Kurzbeschreibung	Bevor die Daten eines Patienten in eine Versorgungsdatenbank eingetragen werden können, muss der Patient in der Patientenliste registriert, ein Pseudonym (PIDv) für ihn erzeugt werden und von der Patientenliste an die Versorgungsdatenbank übergeben werden.
Primärer Akteur	Patient
Andere Akteure	Behandler
Systeme	Patientenliste, Versorgungsdatenbank
Vorbedingungen	Der Arzt hat mit dem Patienten ein Aufklärungsgespräch geführt, ihm die Patienteninformationen vorgelegt und der Patient hat eine Einwilligungserklärung unterschrieben.
Nachbedingungen	Der Patient wurde in der Patientenliste angelegt. Der Patient hat weitere Informationen über das Versorgungsmodul und den Forschungsverbund erhalten.
Hauptszenario	1. Der Patient teilt dem Behandler seine identifizierenden bzw. Kontaktdaten mit. 2. Der Behandler trägt die Daten des Patienten in die Patientenliste ein. 3. Die Patientenliste generiert ein Pseudonym. 4. Die Patientenliste übermittelt das Pseudonym der Versorgungsdatenbank. 5. Die Versorgungsdatenbank legt den Patienten an. 6. Die Versorgungsdatenbank bestätigt der Patientenliste die Anmeldung. 7. Die Patientenliste bestätigt dem Behandler die Anmeldung. 8. Der Behandler übergibt dem Patienten Informationen zum Versorgungsmodul und zum Forschungsverbund.
Beziehungen zu anderen Use Cases	Aufnahme in die Versorgungsdatenbank
Bereitstellen von Daten durch den Forschungsverbund	Informationen über den Forschungsverbund, Patienteninformationen, Bestätigung der Anmeldung
Bereitstellen von Daten durch den Patienten	Identifizierende bzw. Kontaktdaten des Patienten

Tabelle 24: Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler

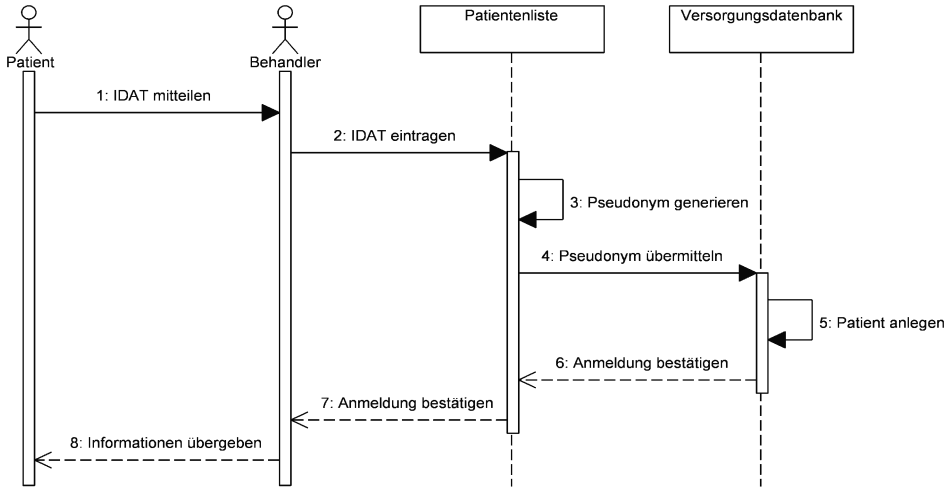

Abbildung 41: Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler

A2.3.2. Kontaktieren eines Patienten über den Verwalter der Patientenliste

Bezeichner	UC-1-2
Name	Kontaktieren eines Patienten über den Verwalter der Patientenliste
Kurzbeschreibung	Es liegen Informationen für den Patienten vor. Der Verwalter der Patientenliste kontaktiert den Patienten und übermittelt ihm die Nachricht.
Primärer Akteur	Verwalter Patientenliste
Andere Akteure	Patient
Systeme	Patientenliste
Vorbedingungen	Der Patient ist am Forschungsverbund angemeldet und hat eingewilligt, dass er kontaktiert werden darf. Es liegt eine Nachricht für den Patienten vor.
Nachbedingungen	Die Informationen für den Patienten liegen ihm vor.
Hauptszenario	1. Der Verwalter der Patientenliste ruft die Kontaktdaten des Patienten aus der Patientenliste ab. 2. Die Patientenliste zeigt dem Verwalter der Patientenliste die Kontaktdaten des Patienten an. 3. Der Verwalter der Patientenliste erstellt die Nachricht mit den Kontaktdaten. 4. Der Verwalter der Patientenliste übermittelt die Nachricht an den Patienten.
Beziehungen zu anderen Use Cases	Keine
Bereitstellen von Daten durch den Forschungsverbund	Allgemeine Ergebnisse aus Studien, Informationen über neue Forschungsprojekte, persönliche Nachrichten an den Patienten, Newsletter, eine aktualisierte Liste der Ärzte, die am Expertenforum teilnehmen etc.
Bereitstellen von Daten durch den Patienten	Keine

Tabelle 25: Kontaktieren eines Patienten über den Verwalter der Patientenliste

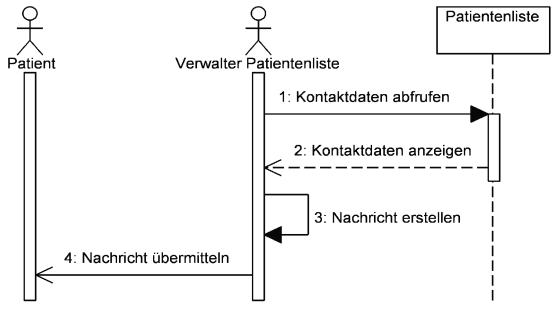

Abbildung 42: Kontaktieren eines Patienten über den Verwalter der Patientenliste

A2.3.3. Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten

Bezeichner	UC-1-3
Name	Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten
Kurzbeschreibung	Der Patient kontaktiert den Verwalter der Patientenliste, um diesem seine neuen Kontaktdaten mitzuteilen. Der Verwalter der Patientenliste aktualisiert die Daten entsprechend in der Patientenliste.
Primärer Akteur	Patient
Andere Akteure	Verwalter Patientenliste
Systeme	Patientenliste
Vorbedingungen	Der Patient ist am Forschungsverbund angemeldet.
Nachbedingungen	Die aktuellen Kontaktdaten des Patienten liegen in der Patientenliste vor.
Hauptszenario	1. Der Patient übermittelt dem Verwalter der Patientenliste die neuen Kontaktdaten. 2. Der Verwalter der Patientenliste aktualisiert die Kontaktdaten des Patienten in der Patientenliste.
Beziehungen zu anderen Use Cases	Keine
Bereitstellen von Daten durch den Forschungsverbund	Keine
Bereitstellen von Daten durch den Patienten	Identifizierende bzw. Kontaktdaten des Patienten

Tabelle 26: Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten

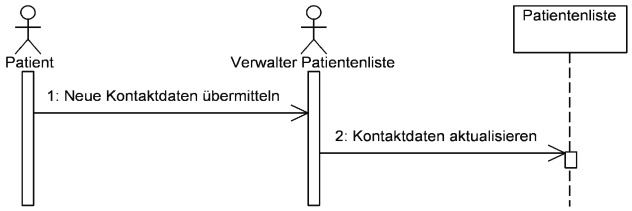

Abbildung 43: Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten

A2.3.4. Recht des Patienten auf Auskunft über die Daten in der Patientenliste

Bezeichner	UC-1-4
Name	Recht des Patienten auf Auskunft über die Daten in der Patientenliste
Kurzbeschreibung	Der Patient fordert sein Recht auf Auskunft ein. Der Ansprechpartner des Forschungsverbundes veranlasst die Erstellung eines Ausdrucks aller über den Patienten in der Patientenliste gespeicherten Daten und händigt diesen Ausdruck dem Patienten aus.
Primärer Akteur	Patient
Andere Akteure	Ansprechpartner des Forschungsverbundes, Verwalter Patientenliste
Systeme	Patientenliste
Vorbedingungen	Der Patient ist am Forschungsverbund angemeldet.
Nachbedingungen	Dem Patienten liegen die über ihn in der Patientenliste gespeicherten Daten vor.
Hauptszenario	1. Der Patient kontaktiert gemäß seinem Recht den Ansprechpartner des Forschungsverbundes und verlangt Auskunft. 2. Der Ansprechpartner des Forschungsverbundes fordert die Daten des Patienten beim Verwalter der Patientenliste an. 3. Der Verwalter der Patientenliste ruft die Daten aus der Patientenliste ab. 4. Die Patientenliste übermittelt die über den Patienten gespeicherten Daten an den Verwalter der Patientenliste. 5. Der Verwalter der Patientenliste leitet die Daten an den Ansprechpartner des Forschungsverbundes weiter. 6. Der Ansprechpartner des Forschungsverbundes händigt die Daten dem Patienten aus.
Beziehungen zu anderen Use Cases	Keine
Bereitstellen von Daten durch den Forschungsverbund	Identifizierende Daten des Patienten
Bereitstellen von Daten durch den Patienten	Anfrage nach Auskunft

Tabelle 27: Recht des Patienten auf Auskunft über die Daten in der Patientenliste

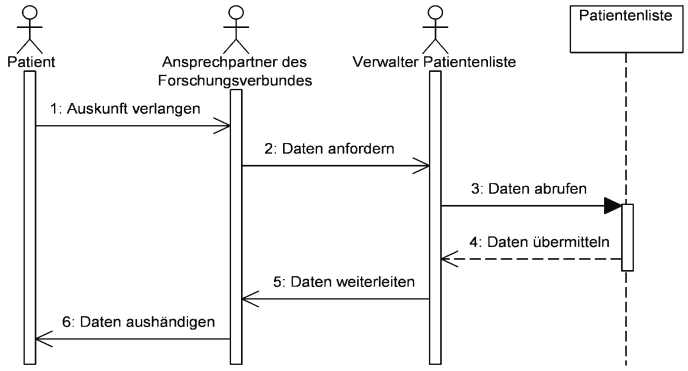

Abbildung 44: Recht des Patienten auf Auskunft über die Daten in der Patientenliste

A2.3.5. Rückzug der Einwilligung für die Teilnahme an einem Forschungsverbund

Bezeichner	UC-1-5
Name	Rückzug der Einwilligung für die Teilnahme an einem Forschungsverbund
Kurzbeschreibung	Der Patient zieht seine Einwilligung zurück. Der Ansprechpartner des Forschungsverbundes veranlasst die Löschung aller über den Patienten in der Patientenliste und der Versorgungsdatenbank gespeicherten Daten und händigt diesem die Bestätigung der Löschung aus.
Primärer Akteur	Patient
Andere Akteure	Ansprechpartner des Forschungsverbundes, Verwalter Patientenliste, Verwalter Versorgungsdatenbank
Systeme	Patientenliste, Versorgungsdatenbank
Vorbedingungen	Der Patient ist am Forschungsverbund angemeldet.
Nachbedingungen	Der Patient ist in der Patientenliste und der Versorgungsdatenbank gelöscht worden und dem Patienten liegt eine Bestätigung der Löschung vor.
Hauptszenario	1. Der Patient kontaktiert zum Rückzug seiner Einwilligung den Ansprechpartner des Forschungsverbundes. 2. Der Ansprechpartner des Forschungsverbundes beauftragt den Verwalter der Patientenliste mit dem Löschen der Daten des Patienten in der Patientenliste. 3. Der Verwalter der Patientenliste beauftragt den Löschvorgang der Daten des Patienten durch die Patientenliste. 4. Die Patientenliste übermittelt dem Verwalter der Versorgungsdatenbank einen Löschauftrag mit dem Pseudonym unter dem der Patient in der Versorgungsdatenbank geführt wird. 5. Die Patientenliste löscht die Daten des Patienten. 6. Die Patientenliste bestätigt dem Verwalter der Patientenliste die Löschung. 7. Der Verwalter der Patientenliste leitet die Bestätigung der Löschung an den Ansprechpartner des Forschungsverbundes weiter. 8. Der Verwalter der Versorgungsdatenbank löscht die Daten zu dem Pseudonym in der Versorgungsdatenbank. 9. Die Versorgungsdatenbank bestätigt die Löschung der Daten. 10. Der Verwalter der Versorgungsdatenbank leitet die Bestätigung an den Ansprechpartner des Forschungsverbundes weiter. 11. Der Ansprechpartner des Forschungsverbundes händigt die Bestätigung der Löschung dem Patienten aus.
Beziehungen zu anderen Use Cases	Keine
Bereitstellen von Daten durch den Forschungsverbund	Bestätigung der Löschung
Bereitstellen von Daten durch den Patienten	Auftrag zur Löschung

Tabelle 28: Rückzug der Einwilligung für die Teilnahme an einem Forschungsverbund

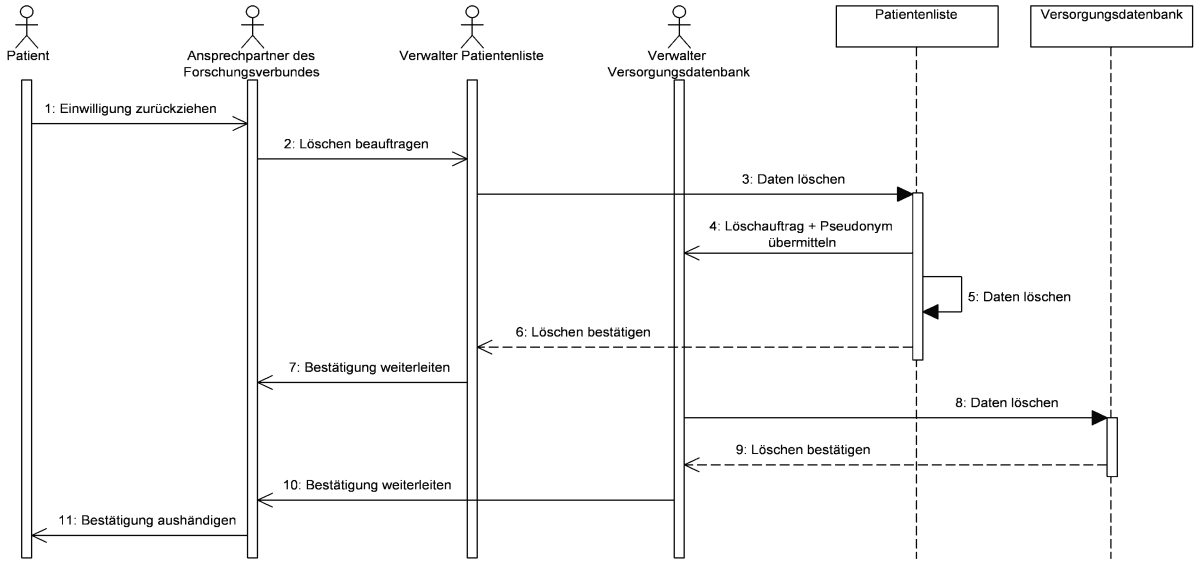

Abbildung 45: Rückzug der Einwilligung für die Teilnahme an einem Forschungsverbund

A2.4. Versorgungsdatenbank

A2.4.1. Erfassung und Zugriff auf Daten im Behandlungsprozess bzw. durch einen Patienten

Bezeichner	UC-2-1
Name	Erfassung und Zugriff auf Daten im Behandlungsprozess
Kurzbeschreibung	Der Behandler ruft Daten aus der Versorgungsdatenbank ab und ergänzt die Daten in der Versorgungsdatenbank durch neue Behandlungsdaten.
Primärer Akteur	Behandler
Andere Akteure	Patient
Systeme	Patientenliste, Versorgungsdatenbank
Vorbedingungen	Der Patient wurde in der Patientenliste angelegt und über die Versorgungsdatenbank aufgeklärt.
Nachbedingungen	In der Versorgungsdatenbank befindet sich ein aktueller Datensatz des Patienten.
Hauptszenario	1. Der Behandler übermittelt die identifizierenden Daten des Patienten an die Patientenliste. 2. Die Patientenliste generiert ein temporäres Pseudonym (TKT). 3. Die Patientenliste übermittelt dem Behandler das TKT. 4. Die Patientenliste übermittelt das TKT und das Pseudonym des Patienten an die Versorgungsdatenbank. 5. Die Versorgungsdatenbank ordnet das Pseudonym dem Datensatz des Patienten zu. 6. Der Behandler ruft mit dem TKT den Datensatz des Patienten aus der Versorgungsdatenbank ab. 7. Die Versorgungsdatenbank zeigt dem Behandler den Datensatz des Patienten an. 8. Der Behandler befragt bzw. untersucht den Patienten. 9. Der Patient beantwortet dem Behandler die Fragen. 10. Der Behandler trägt die neuen Daten des Patienten in der Versorgungsdatenbank ein. 11. Die Versorgungsdatenbank löscht das TKT zu dem Patienten wieder.
Beziehungen zu anderen Use Cases	UC-1-1
Bereitstellen von Daten durch den Forschungsverbund	Keine
Bereitstellen von Daten durch den Patienten	Medizinische Daten des Patienten z. B. Befunde, Bilder, Medikation, vom Patienten bereitgestellte Daten wie z. B. Blutzuckerwerte, Lebensqualität etc.

Tabelle 29: Erfassung und Zugriff auf Daten im Behandlungsprozess

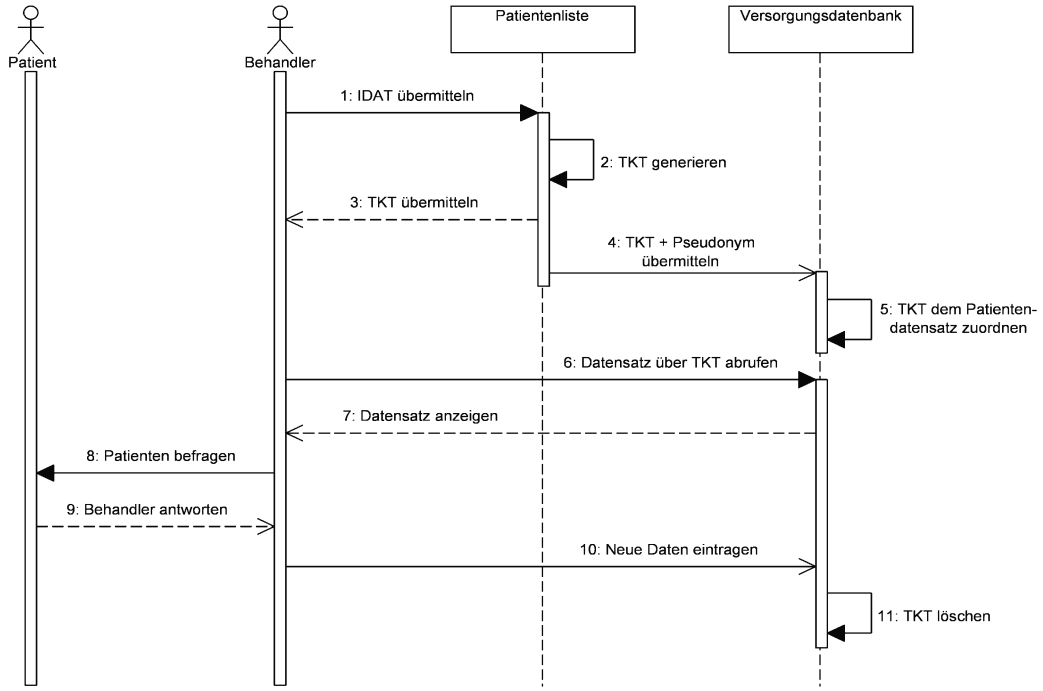

Abbildung 46: Erfassung und Zugriff auf Daten im Behandlungsprozess

Bezeichner	UC-2-2
Name	Erfassung und Zugriff auf Daten durch einen Patienten
Kurzbeschreibung	Der Patient ruft seine Daten aus der Versorgungsdatenbank ab und ergänzt die Daten in der Versorgungsdatenbank durch neue Daten.
Primärer Akteur	Patient
Andere Akteure	Keine
Systeme	Patientenliste, Versorgungsdatenbank
Vorbedingungen	Der Patient wurde in der Patientenliste angelegt und über die Versorgungsdatenbank aufgeklärt. Für den Patienten wurde ein Account zum Eintragen von Daten angelegt.
Nachbedingungen	In der Versorgungsdatenbank befindet sich ein aktueller Datensatz des Patienten.
Hauptszenario	1. Der Patient übermittelt seine identifizierenden Daten an die Patientenliste. 2. Die Patientenliste generiert ein temporäres Pseudonym (TKT). 3. Die Patientenliste übermittelt dem Patienten das TKT. 4. Die Patientenliste übermittelt das TKT und das Pseudonym des Patienten an die Versorgungsdatenbank. 5. Die Versorgungsdatenbank ordnet es anhand des Pseudonyms dem Datensatz des Patienten zu. 6. Der Patient ruft mit dem TKT den Datensatz des Patienten aus der Versorgungsdatenbank ab. 7. Die Versorgungsdatenbank zeigt dem Patienten seine Daten an. 8. Der Patient trägt die neuen Daten in der Versorgungsdatenbank ein. 9. Die Versorgungsdatenbank löscht das TKT zu dem Patienten wieder.
Beziehungen zu anderen Use Cases	UC-1-1
Bereitstellen von Daten durch den Forschungsverbund	Dem Patienten werden die bisher vom Patienten eingetragenen Daten im Versorgungsmodul angezeigt.
Bereitstellen von Daten durch den Patienten	Vom Patienten bereitgestellte Daten wie z. B. Blutzuckerwerte, Lebensqualität etc.

Tabelle 30: Erfassung und Zugriff auf Daten durch einen Patienten

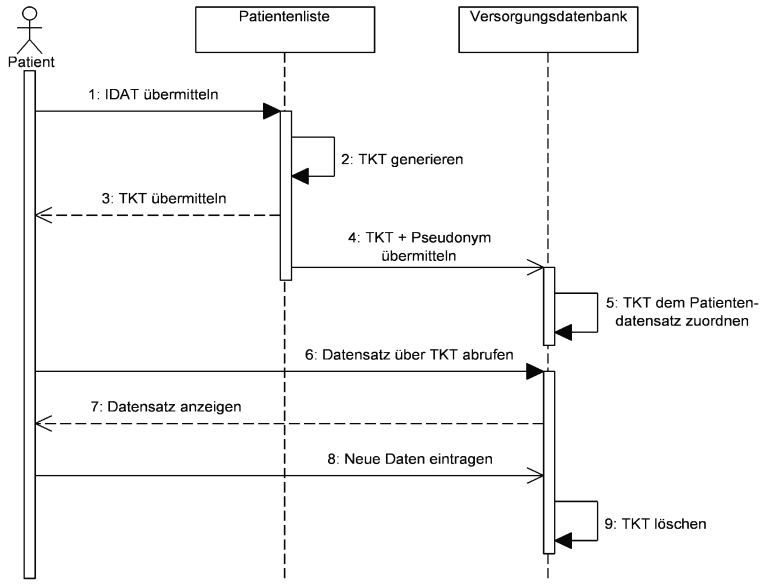

Abbildung 47: Erfassung und Zugriff auf Daten durch einen Patienten

A2.4.2. Rekrutierung von Patienten

Bezeichner	UC-2-3
Name	Rekrutierung von Patienten
Kurzbeschreibung	Ein Forscher hat für ein neues Forschungsvorhaben mit Hilfe der Versorgungsdatenbank potentielle Patienten identifiziert. Der Verwalter des Versorgungsmoduls leitet die Pseudonyme der identifizierten Patienten zwecks Kontaktierung an den Verwalter der Patientenliste weiter.
Primärer Akteur	Forscher
Andere Akteure	Verwalter Patientenliste, Verwalter Versorgungsdatenbank
Systeme	Patientenliste, Versorgungsdatenbank
Vorbedingungen	Der Patient wurde in der Patientenliste und in der Versorgungsdatenbank angelegt. Der Patient hat eingewilligt über neue Forschungsvorhaben zwecks Rekrutierung informiert werden zu dürfen.
Nachbedingungen	Die Rekrutierungsanfrage liegt dem Verwalter der Patientenliste vor.
Hauptszenario	1. Der Forscher identifiziert potentielle Patienten für ein neues Forschungsvorhaben in der Versorgungsdatenbank und formuliert für diese Patienten eine Rekrutierungsanfrage, die er dem Verwalter der Versorgungsdatenbank stellt. 2. Der Verwalter der Versorgungsdatenbank wird über die Rekrutierungsanfrage informiert. 3. Der Verwalter der Versorgungsdatenbank fordert die Liste mit den Pseudonymen aus der Versorgungsdatenbank an. 4. Die Versorgungsdatenbank übermittelt dem Verwalter der Versorgungsdatenbank die Liste mit den Pseudonymen. 5. Der Verwalter der Versorgungsdatenbank leitet die Liste mit den Pseudonymen der zu rekrutierenden Patienten an den Verwalter der Patientenliste weiter. 6. Der Verwalter der Patientenliste übermittelt die Pseudonyme der Patienten an die Patientenliste und leitet für diese Patienten die Kontaktierung ein (siehe UC-1-2).
Beziehungen zu anderen Use Cases	UC-1-2
Bereitstellen von Daten durch den Forschungsverbund	Informationen zum Forschungsvorhaben und Anfrage zur Teilnahme.
Bereitstellen von Daten durch den Patienten	Keine

Tabelle 31: Rekrutierung von Patienten

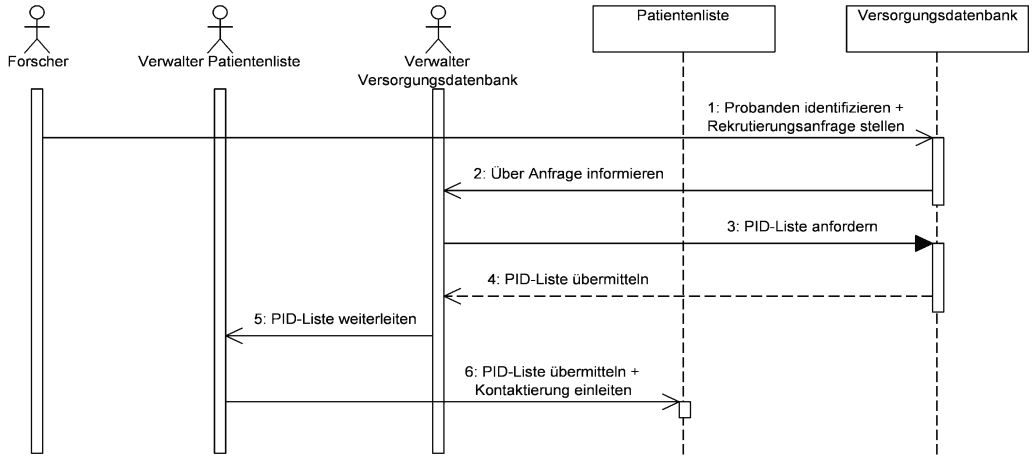

Abbildung 48: Rekrutierung von Patienten

A2.4.3. Informieren eines Patienten über Forschungsergebnisse

Bezeichner	UC-2-5
Name	Informieren eines Patienten über Forschungsergebnisse
Kurzbeschreibung	Ein Forscher hat neue Erkenntnisse gewonnen, die für die Behandlung eines oder mehrerer Patienten in der Versorgungsdatenbank wichtig sind. Nach einer Genehmigung des Ausschusses Datenschutz werden die Informationen an den behandelnden Arzt weitergeleitet, der diese dann seinem Patienten mitteilt.
Primärer Akteur	Forscher
Andere Akteure	Behandler, Patient, Ausschuss Datenschutz, Verwalter Versorgungsdatenbank, Verwalter Patientenliste
Systeme	Versorgungsdatenbank, Patientenliste
Vorbedingungen	Der Patient wurde in der Patientenliste und in der Versorgungsdatenbank angelegt. Der Patient hat eingewilligt über neue Forschungserkenntnisse informiert werden zu dürfen.
Nachbedingungen	Die neuen Erkenntnisse liegen dem Patienten vor.
Hauptszenario	1. Der Forscher übermittelt dem Ausschuss Datenschutz neue Forschungserkenntnisse und die Pseudonyme (EX-PIDs), unter denen die Patienten im Export des Forschers geführt werden. 2. Der Ausschuss Datenschutz gibt die Depseudonymisierung nach einer erfolgreichen Beratung frei. 3. Der Ausschuss Datenschutz übermittelt dem Verwalter der Versorgungsdatenbank die EX-PID und eine Vorgangsnummer. 4. Der Verwalter der Versorgungsdatenbank fordert unter Angabe der EX-PID die PID des Patienten von der Versorgungsdatenbank an. 5. Das Versorgungsmodul übermittelt die PID des Patienten. 6. Der Verwalter des Versorgungsmoduls leitet die PID und die Vorgangsnummer an den Verwalter der Patientenliste weiter. 7. Der Verwalter der Patientenliste fordert die identifizierenden Daten des Patienten und die Kontaktdaten des behandelnden Arztes zu der PID von der Patientenliste an. 8. Die Patientenliste übermittelt die Daten an den Verwalter der Patientenliste. 9. Der Verwalter der Patientenliste übermittelt die identifizierenden Daten des Patienten sowie die Vorgangsnummer an den behandelnden Arzt mit der Bitte den Ausschuss Datenschutz zu kontaktieren. 10. Der behandelnde Arzt fordert die neuen Forschungserkenntnisse anhand der Vorgangsnummer beim Ausschuss Datenschutz an. 11. Der Ausschuss Datenschutz übermittelt dem behandelnden Arzt die neuen Forschungserkenntnisse zu seinem Patienten. 12. Der behandelnde Arzt informiert den Patienten über die neuen Forschungserkenntnisse.
Beziehungen zu anderen Use Cases	Keine
Bereitstellen von Daten durch den Forschungsverbund	Neue Forschungserkenntnisse
Bereitstellen von Daten durch den Patienten	Keine

Tabelle 32: Informieren eines Patienten über Forschungsergebnisse

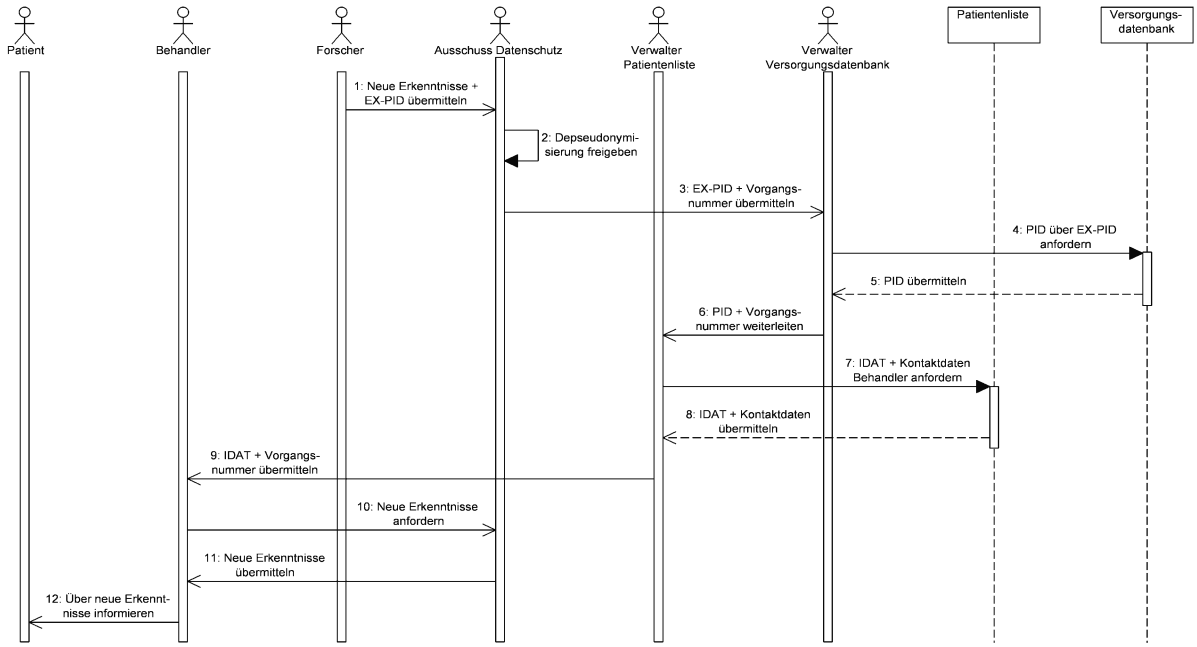

Abbildung 49: Informieren eines Patienten über Forschungsergebnisse

A2.4.4. Recht des Patienten auf Auskunft über die Daten in der Versorgungsdatenbank

Bezeichner	UC-2-6
Name	Recht des Patienten auf Auskunft über die Daten in der Versorgungsdatenbank
Kurzbeschreibung	Der Patient nimmt sein Recht auf Auskunft über den Ansprechpartner des Forschungsverbundes wahr. Dieser veranlasst einen Ausdruck der über den Patienten in der Versorgungsdatenbank und der Patientenliste gespeicherten Daten und händigt diesen dem Patienten aus.
Primärer Akteur	Patient
Andere Akteure	Ansprechpartner des Forschungsverbundes, Verwalter Patientenliste, Verwalter Versorgungsdatenbank
Systeme	Patientenliste, Versorgungsdatenbank
Vorbedingungen	Der Patient wurde in der Versorgungsdatenbank angelegt.
Nachbedingungen	Dem Patienten sind die über ihn in der Versorgungsdatenbank abgelegten Daten bekannt.
Hauptszenario	1. Der Patient verlangt Auskunft über seine im Versorgungsmodul gespeicherten Daten vom Ansprechpartner des Forschungsverbundes. 2. Der Ansprechpartner des Forschungsverbundes fordert die Daten des Patienten aus der Patientenliste vom Verwalter der Patientenliste an. 3. Der Verwalter der Patientenliste ruft die Daten des Patienten von der Patientenliste ab. 4. Die Patientenliste übermittelt die Daten des Patienten. 5. Der Verwalter der Patientenliste leitet die Daten an den Ansprechpartner des Forschungsverbundes weiter. 6. Der Ansprechpartner des Forschungsverbundes fordert die über den Patienten in der Versorgungsdatenbank gespeicherten Daten vom Verwalter der Versorgungsdatenbank an. 7. Der Verwalter der Versorgungsdatenbank ruft die über dem Patienten gespeicherten Daten aus der Versorgungsdatenbank ab. 8. Die Versorgungsdatenbank übermittelt dem Verwalter der Versorgungsdatenbank die über den Patienten gespeicherten Daten. 9. Der Verwalter der Versorgungsdatenbank leitet die Daten dem Ansprechpartner des Forschungsverbundes weiter. 10. Der Ansprechpartner des Forschungsverbundes händigt die Daten dem Patienten aus.
Beziehungen zu anderen Use Cases	Keine
Bereitstellen von Daten durch den Forschungsverbund	Alle Daten über den Patienten aus der Versorgungsdatenbank
Bereitstellen von Daten durch den Patienten	Anfrage zur Auskunft

Tabelle 33: Recht des Patienten auf Auskunft über die Daten in der Versorgungsdatenbank

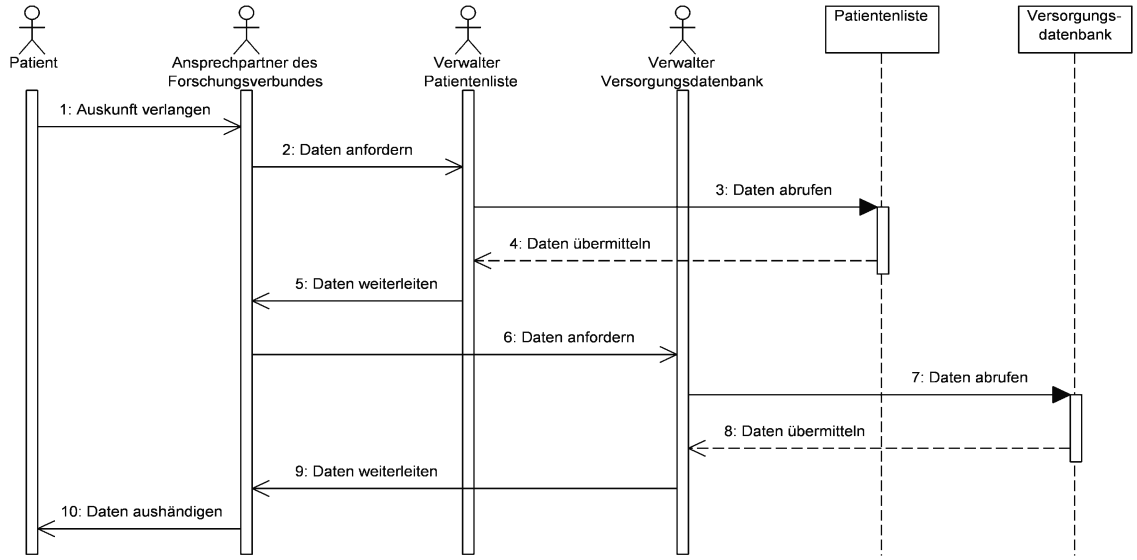

Abbildung 50: Recht des Patienten auf Auskunft über die Daten in der Versorgungsdatenbank

A2.5. Priorisierung der Module eines Forschungsverbundes

A2.5.1. Studiendatenbank

Im Folgenden wird die Studiendatenbank anhand der im Abschnitt 3.1.3 genannten Kriterien bewertet. Die Studiendatenbank wird von fünf Forschungsverbünden eingesetzt. Es wurden fünf Anwendungsfälle mit Patientenbezug identifiziert, von denen zwei einen Austausch mit der Versorgung vorsehen und einer eine Bereitstellung von selbst erhobenen Daten durch den Patienten vorsieht (siehe Tabelle 34). Somit erhält die Studiendatenbank eine Gesamtpunktzahl von dreizehn Punkten.

Anwendungsfall	**Bereitstellung von Daten durch den Forschungsverbund**	**Bereitstellung von Daten durch den Patienten**	**Austausch Versorgung**	**Bereitstellung selbst erhobener Daten**
Erheben von Studiendaten	Keine	Medizinische Daten des Patienten z. B. Befunde, Bilder, Medikation, vom Patienten bereitgestellte Daten wie z. B. Blutzuckerwerte, Lebensqualität etc.	Es können Daten aus der ePA (z. B. Laborbefunde, Diagnosen etc.) für die Studiendatenbank genutzt werden.	Der Patient kann selbst erhobene Daten (z. B. Daten zur Lebensqualität) bereitstellen.
Managen von unerwünschten Ereignissen	Informationen zu dem unerwünschten Ereignis	Keine	Die Informationen zum unerwünschten Ereignis können über die ePA anderen Behandlern bereitgestellt werden.	Keine
Informieren eines Patienten über Forschungsergebnisse	Neue Forschungserkenntnisse	Keine	Kein	Keine
Recht des Patienten auf Auskunft	Studiendaten des Patienten	Anfrage nach Auskunft	Kein	Keine
Rückzug der Einwilligung	Bestätigung der Löschung	Auftrag zur Löschung	Kein	Keine

Tabelle 34: Zusammenfassung der Bewertung der Studiendatenbank in Bezug auf die Auswahlkriterien

A2.5.2. Versorgungsmodul

Im Folgenden wird die Versorgungsdatenbank anhand der im Abschnitt 3.1.3 genannten Kriterien bewertet. Die Versorgungsdatenbank wird von acht Forschungsverbünden eingesetzt. Es wurden sechs Anwendungsfälle mit Patientenbezug identifiziert, von denen zwei einen Austausch mit der Versorgung vorsehen und einer eine Bereitstellung von selbst erhobenen Daten durch den Patienten (siehe Tabelle 35). Somit erhält die Versorgungsdatenbank eine Gesamtpunktzahl von siebzehn Punkten.

Anwendungsfall	**Bereitstellung von Daten durch den Forschungsverbund**	**Bereitstellung von Daten durch den Patienten**	**Austausch Versorgung**	**Bereitstellung selbst erhobener Daten**
Erfassung und Zugriff auf Daten im Behandlungsprozess	Keine	Medizinische Daten des Patienten z. B. Befunde, Bilder, Medikation, vom Patienten bereitgestellte Daten wie z. B. Blutzuckerwerte, Lebensqualität etc.	Die Daten werden für die Behandlung genutzt und wissenschaftlich ausgewertet.	Der Patient kann selbst erhobene Daten (z. B. Blutzuckerwerte, Lebensqualität etc.) in die Versorgungsdatenbank eintragen.
Vergabe von Zugriffrechten	Keine	Antrag zum Entzug von Zugriffsrechten.	Kein	Keine
Rekrutierung von Patienten	Anfrage zur Teilnahme und Informationen zum Forschungsvorhaben.	Keine	Kein	Keine
Informieren eines Patienten über Forschungsergebnisse	Neue Forschungserkenntnisse	Keine	Kein	Keine
Recht des Patienten auf Auskunft	Daten des Patienten aus der Versorgungsdatenbank	Anfrage nach Auskunft	Kein	Keine
Rückzug der Einwilligung	Bestätigung der Löschung	Auftrag zur Löschung	Kein	Keine

Tabelle 35: Zusammenfassung der Bewertung der Versorgungsdatenbank in Bezug auf die Auswahlkriterien

A2.5.3. Forschungsdatenbank

Im Folgenden wird die Forschungsdatenbank anhand der im Abschnitt 3.1.3 genannten Kriterien bewertet. Die Forschungsdatenbank wird von sechs Forschungsverbünden eingesetzt. Es wurden vier Anwendungsfälle mit Patientenbezug identifiziert, von denen keiner einen Austausch mit der Versorgung oder eine Bereitstellung von selbst erhobenen Daten des Patienten vorsieht (siehe Tabelle 36). Somit erhält die Forschungsdatenbank eine Gesamtpunktzahl von zehn Punkten.

Anwendungsfall	**Bereitstellung von Daten durch den Forschungsverbund**	**Bereitstellung von Daten durch den Patienten**	**Austausch Versorgung**	**Bereitstellung selbst erhobener Daten**
Rekrutierung von Patienten	Anfrage zur Teilnahme und Informationen zum Forschungsvorhaben.	Keine	Kein	Keine
Informieren eines Patienten über Forschungs-ergebnisse	Neue Forschungs-erkenntnisse	Keine	Kein	Keine
Recht des Patienten auf Auskunft	Über den Patienten in der Forschungs-datenbank und der Patientenliste gespeicherte Daten.	Anfrage nach Auskunft	Kein	Keine
Rückzug der Einwilligung	Bestätigung der Löschung	Auftrag zur Löschung	Kein	Keine

Tabelle 36: Zusammenfassung der Bewertung der Forschungsdatenbank in Bezug auf die Auswahlkriterien

A2.6. Akteure des Versorgungsmoduls

In die ausgewählten Anwendungsfälle des Versorgungsmoduls sind die folgenden acht Akteure involviert:

- „***Patient*** *und* ***Proband*** *sind die Personen, die dem Forschungsverbund Daten zu ihrer Gesundheit und Materialien ihres Körpers zu Zwecken der biomedizinischen Forschung zur Verfügung stellen. Erfolgt die Datengewinnung oder Probenentnahme im Behandlungszusammenhang, ist der Spender „Patient“. Erfolgt die Datengewinnung oder Probenentnahme im Forschungszusammenhang, ist der Spender „Proband“. Der Begriff „Proband“ wird auch als Oberbegriff für „Patient und / oder Proband“ verwendet, insbesondere, wenn eine Kontrollgruppe in die Studie involviert ist*“ [188, Seite 24].
- **Behandelnder Arzt** (auch Behandler genannt) … „*im Sinne des Forschungsnetzes kann nur werden, wer vertraglich an das Forschungsnetz gebunden ist. Der Arzt, der einen Patienten erstmals erfasst, d. h. der dessen Stammdaten erstmals anlegt, wird dadurch vom Forschungsnetz als dessen behandelnder Arzt geführt. Jeder weitere Arzt, der Daten zu diesem Patienten erfassen und auch die Vorbefunde dieses Patienten einsehen möchte, muss sich - nach eingeholter Zustimmung des Patienten - dem Forschungsnetz gegenüber in geeigneter Weise als behandelnder Arzt autorisieren. Erst dann wird er für den Zugang zu den Daten dieses Patienten als behandelnder Arzt in der klinischen Datenbank freigeschaltet*.“ [33, Seiten 36-37]
- „*Als* ***Systembetreuer*** *wird im generischen Modell für klinisch fokussierte Forschungsnetze die Person bezeichnet die über administrative Zugriffsrechte entweder zu den Daten der Patientenliste oder zu den Daten der Behandlungsdatenbank verfügt. Patientenliste und Behandlungsdatenbank haben je einen Systembetreuer. Es muss gewährleistet sein, dass die Systembetreuer voneinander unabhängig sind*.“ [33, Seite 31] Es gibt also einen **Systembetreuer der Patientenliste** (im Folgenden auch IDAT-Verwalter genannt) und einen **Systembetreuer der Versorgungsdatenbank** (im Folgenden auch MDAT-Verwalter genannt).
- Der **Ansprechpartner des Forschungsverbundes** ist eine vom Forschungsverbund ernannte Person, an die sich alle Teilnehmer des Forschungsverbundes wenden können, wenn sie Fragen zum Thema Datenschutz (Auskunftsrecht, Rücknahme der Einwilligung etc.) haben.
- Der **Datenschutzbeauftragte** ist für den regelkonformen Betrieb der Datenbanken des Forschungsverbundes mitverantwortlich und sollte auch Mitglied des Ausschusses Datenschutz sein.
- Als **Experten** werden ausgewählte Mitglieder des Expertenforums verstanden, die medizinische Aspekte von Erkrankungsfällen diskutieren. Das Forum kann sowohl nationale als auch internationale Experten enthalten [34].
- Ein **Forscher** ist: „*Jeder der die in einem medizinischen Forschungsverbund vorhandenen Daten oder Proben für ein Forschungsvorhaben nutzt.*“ … „*Da Daten und Proben des medizinischen Forschungsverbunds für Forschungszwecke genutzt werden sollen, sind die Nutzer stets Forscher. Sie können der Trägereinrichtung des Verbundes selbst angehören (= interne Forschung) oder aus anderen Einrichtungen kommen (= externe Forschung)*“ [188, Seite 21].

- „*Der **Ausschuss Datenschutz** ist ein Gremium eines Forschungsverbundes, das die Regelung aller mit dem Datenaustausch und dem Datenzugang zusammenhängenden Fragen verantwortet*.“ … „*Der Ausschuss Datenschutz kann auch durch ein Gremium verkörpert werden, das andere Aufgaben hat (und anders bezeichnet wird), z. B. einen Vorstand. Der Datenschutzbeauftragte des Forschungsverbunds soll diesem Gremium angehören; seine vom Datenschutzgesetz definierten Rechte und Pflichten sind dadurch unberührt. Die Aufgaben des Ausschusses Datenschutz gehen über die gesetzlich definierten Aufgaben des Datenschutzbeauftragten hinaus.*“ [188, Seiten 4-5]

A2.7. Bewertung der Kommunikationsmuster im Hinblick auf eine direktere und medienbruchfreie Kommunikation

Auszutauschende Informationen	Anwendungsfall	Medienbruchfrei	Direkte Kommunikation
Info01	Anmeldung eines Patienten an einem Forschungsverbund	Ja, da die Informationen direkt aus der Patientenliste an die ePA geschickt werden.	Nein, da die Informationen vorher schon dem Patienten direkt vom Behandler übergeben werden
Info02	Anmeldung eines Patienten an einem Forschungsverbund	Nein, da die Informationen nicht über die Forschungsschnittstelle übertragen werden.	Nein, da die Informationen nicht über die Forschungsschnittstelle übertragen werden.
Info03	Kontaktieren eines Patienten	Ja, da die Daten direkt zwischen der Patientenliste und der ePA kommuniziert werden.	Nein, da die Kommunikation vorher schon direkt zwischen dem Patienten und dem Verwalter der Patientenliste stattgefunden hat.
Info04	Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten	Ja, da die Daten direkt zwischen der Patientenliste und der ePA kommuniziert werden.	Nein, da die Kommunikation vorher schon direkt zwischen dem Patienten und dem Verwalter der Patientenliste stattgefunden hat.
Info05	Recht des Patienten auf Auskunft	Ja, da die Daten direkt zwischen der Patientenliste und der ePA kommuniziert werden.	Ja, da der Verwalter der Patientenliste und der Patient nun direkt miteinander kommunizieren können.
Info06	Recht des Patienten auf Auskunft	Ja, da die Daten direkt zwischen der Patientenliste und der ePA kommuniziert werden.	Ja, da der Verwalter der Patientenliste und der Patient nun direkt miteinander kommunizieren können.
Info07	Rückzug der Einwilligung	Ja, da die Daten direkt zwischen der Patientenliste und der ePA kommuniziert werden.	Ja, da der Verwalter der Patientenliste und der Patient nun direkt miteinander kommunizieren können.
Info08	Rückzug der Einwilligung	Ja, da die Daten direkt zwischen der Patientenliste und der ePA kommuniziert werden.	Ja, da der Verwalter der Patientenliste und der Patient nun direkt miteinander kommunizieren können.
Info09	Erfassung und Zugriff auf Daten im Behandlungsprozess bzw. durch einen Patienten	Ja. Allerdings kann durch die direkte Einbindung der Arztinformationssysteme eine zusätzliche Erfassung im Versorgungsmodul verhindert werden und somit eine medienbruchfreie Kommunikation zwischen den beiden Systemen erfolgen.	Nein. Eine Optimierung der Kommunikation erfolgt bei diesem Anwendungsfall nicht.

Auszutauschende Informationen	Anwendungsfall	Medienbruchfrei	Direkte Kommunikation
Info10	Erfassung und Zugriff auf Daten im Behandlungs-prozess bzw. durch einen Patienten	Ja. Allerdings kann durch die direkte Einbindung der Arztinformationssysteme eine zusätzliche Erfas-sung im Versorgungs-modul verhindert werden und somit eine medien-bruchfreie Kommunikation zwischen den beiden Systemen erfolgen.	Nein. Eine Optimierung der Kommunikation erfolgt bei diesem Anwendungsfall nicht.
Info11	Erfassung und Zugriff auf Daten im Behandlungs-prozess bzw. durch einen Patienten	Ja. Allerdings kann durch die direkte Einbindung der ePA eine zusätzliche Er-fassung im Versorgungs-modul verhindert werden und somit eine medien-bruchfreie Kommunikation zwischen den beiden Systemen erfolgen.	Nein. Eine Optimierung der Kommunikation erfolgt bei diesem Anwendungsfall nicht.
Info12	Rekrutierung von Patienten	Ja, da die Daten direkt zwischen der Versor-gungsdatenbank und der ePA kommuniziert werden.	Ja, da der Verwalter der Versorgungsdatenbank und der Patient nun direkt miteinander kommuni-zieren können.
Info13	Informieren eines Patienten über Forschungs-ergebnisse	Ja, da die Daten direkt zwischen der Versor-gungsdatenbank und der ePA kommuniziert werden	Ja, da der Verwalter der Versorgungsdatenbank und der Patient nun direkt miteinander kommuni-zieren können.
Info14	Recht des Patienten auf Auskunft	Ja, da die Daten direkt zwischen der Versor-gungsdatenbank und der ePA kommuniziert werden	Ja, da der Verwalter der Versorgungsdatenbank und der Patient nun direkt miteinander kommunizieren können.
Info15	Recht des Patienten auf Auskunft	Ja, da die Daten direkt zwischen der Versor-gungsdatenbank und der ePA kommuniziert werden	Ja, da der Verwalter der Versorgungsdatenbank und der Patient nun direkt miteinander kommuni-zieren können.

Tabelle 37: Bewertung der Kommunikationsmuster im Hinblick auf eine direktere und medienbruchfreie Kommunikation

A3. Die elektronische Patientenakte nach § 291a

A3.1. Aufbau der Hilfsobjekte der LE-Schnittstelle

Kernelement	Beschreibung
ID	Eindeutiger Identifizierer des Anforderungsobjektes *(Nutzung für spätere Referenzierbarkeit des AOs)*
Quelle	Urheber der Informationsanforderung Bürger *(z. B. repräsentiert durch KVNR, demografische Merkmale, Merkmale der eGK etc.)* Leistungserbringer *(z. B. repräsentiert durch Merkmale des HBA)* Leistungserbringerorganisationen *(z. B. repräsentiert durch Merkmale der SMC-B)*
Ziel	Adressat der Informationsanforderung Bürger *(z. B. repräsentiert durch KVNR, demografische Merkmale, Merkmale der eGK etc.)* Leistungserbringer *(z. B. repräsentiert durch Merkmale des HBA)* Leistungserbringerorganisationen *(z. B. repräsentiert durch Merkmale der SMC-B)*
Quellsystem	Systemidentität, welche das Anforderungsobjekt verschickt *(ePA-Kommunikationsdienst, Konnektor)*
Zielsystem	Systemidentität, welche die Informationen verfügbar macht *(ePA-Kommunikationsdienst, LE-Postfach)*
LE-Postfach-ID	Eindeutige ID des Leistungserbringerpostfachs
Akten-ID	Eindeutige ID der Patientenakte
Zeitstempel	Zeitpunkt der Anforderungserstellung
Ungültig Ab	Zeitpunkt, ab dem die gestellte Anforderung ungültig wird
Anforderung	Was wird angefordert? Metadaten beschreiben die u. U. verschlüsselte Nutzlast. Um dennoch eine automatisierte Verarbeitung zu gewährleisten, müssen fachliche Metadaten angegeben werden.
Wiederkehr	Einmalige Anforderung bzw. Anforderungsserie
Nutzlast	Anforderungsbegleitende Zusatzinformationen

Tabelle 38: Logischer Aufbau eines Anforderungsobjektes [156, Seite 3-4]

Kernelement	Beschreibung
ID	Eindeutiger Identifizierer des Bereitstellungobjektes
AO-Referenz	ID des referenzierten Anforderungsobjekts
Quelle	Urheber der Informationsbereitstellung Bürger *(z. B. repräsentiert durch KVNR, demografische Merkmale, Merkmale der eGK etc.)* Leistungserbringer *(z. B. repräsentiert durch Merkmale des HBA)* Leistungserbringerorganisationen *(z. B. repräsentiert durch Merkmale der SMC-B)*
Ziel	Adressat der Informationsbereitstellung Bürger *(z. B. repräsentiert durch KVNR, demografische Merkmale, Merkmale der eGK etc.)* Leistungserbringer *(z. B. repräsentiert durch Merkmale des HBA)* Leistungserbringerorganisationen *(z. B. repräsentiert durch Merkmale der SMC-B)*
Quellsystem	Systemidentität, welche das Bereitstellungsobjekt verschickt *(ePA-Kommunikationsdienst, Konnektor)*
Zielsystem	Systemidentität, welche das Bereitstellungsobjekt entgegen nimmt (ePA-Kommunikationsdienst, LE-Postfach, Konnektor)
Akten-ID	Eindeutige ID der Patientenakte
Zeitstempel	Zeitpunkt der Erstellung des Bereitstellungsobjektes
Beschreibung der Nutzlast	Bezeichnung / Beschreibung der zur Verfügung gestellten Information
Nutzlast	Bereitgestelltes Informationsobjekt

Tabelle 39: Logischer Aufbau eines Bereitstellungsobjektes [156, Seiten 12-13]

Unterstützte Kommunikations-muster	Nennung der durch die Akte unterstützten Kommunikationsmuster. Im FuE-Projekt werden insgesamt sechs verschiedene Kommunikationsmuster unterschieden. Diese können individuell in der Capability List referenziert werden.
Unterstützte Semantic Signifier	Beschreibung der durch die Akte unterstützten Semantic Signifier.
Zu verwendendes öffentliches Schlüsselmaterial	Öffentlicher Teil des Aktenschlüssels, der im Kontext der (hybriden) Verschlüsselung von Inhaltsobjekten der Akte genutzt werden muss.
Adressinforma-tionen	Adressinformationen der Akte, um eine korrekte Zuordnung auf Seite des Leistungserbringers vornehmen zu können.

Tabelle 40: Logischer Aufbau der Capability List [157, Seite 3]

A3.2. Kommunikationsmuster einer ePA

A3.2.1. Anfordern von Daten durch einen Leistungserbringer

Bezeichner	UC-0-1
Name	Anfordern von Daten durch einen Leistungserbringer
Kurzbeschreibung	Ein Leistungserbringer fordert über sein Arztinformationssystem (AIS) ein Bereitstellungsobjekt aus der ePA des Bürgers bzw. Patienten an.
Primärer Akteur	Leistungserbringer
Andere Akteure	Bürger bzw. Patient
Systeme	Arztinformationssystem, ePA-LE-Client, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Dem Leistungserbringer ist die Adresse der ePA des Bürgers bzw. Patienten bekannt.
Nachbedingungen	Die Anforderung für ein bestimmtes Bereitstellungsobjekt liegt dem Bürger bzw. Patienten vor und kann bearbeitet werden.
Hauptszenario	1. Die Anforderung wird vom Leistungserbringer in seinem AIS formuliert. 2. Das AIS übermittelt die Anforderung an den ePA-LE-Client. 3. Der ePA-LE-Client erstellt aus der Anforderung ein Anforderungsobjekt. 4. Der ePA-LE-Client übermittelt das Anforderungsobjekt an die ePA-Kommunikationskomponente. 5. Die ePA-Kommunikationskomponente leitet das Anforderungsobjekt an das ePA-Kernsystem weiter. 6. Der Bürger bzw. Patient ruft die Anforderung ab. 7. Die ePA zeigt dem Bürger bzw. Patienten die Anforderung an.
Beziehungen zu anderen Use Cases	UC-0-3

Tabelle 41: Anfordern von Daten durch einen Leistungserbringer

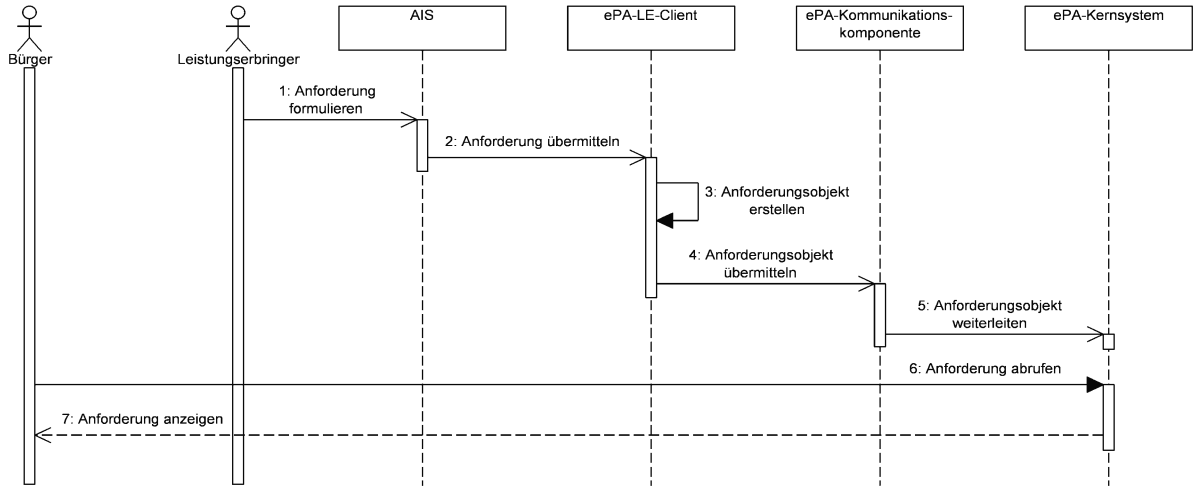

Abbildung 51: Anfordern von Daten durch einen Leistungserbringer

A3.2.2. Anfordern von Daten durch einen Bürger

Bezeichner	UC-0-2
Name	Anfordern von Daten durch einen Bürger
Kurzbeschreibung	Ein Bürger bzw. Patient fordert über seine ePA ein Bereitstellungsobjekt aus dem Arztinformationssystem (AIS) des Leistungserbringers an.
Primärer Akteur	Bürger bzw. Patient
Andere Akteure	Leistungserbringer
Systeme	Arztinformationssystem, ePA-LE-Client, LE-Postfach, ePA-Kommunikations-komponente, ePA-Kernsystem
Vorbedingungen	Dem Patienten ist der Name des Leistungserbringers und seiner Organisation bekannt.
Nachbedingungen	Die Anforderung für ein bestimmtes Bereitstellungsobjekt liegt dem Leistungserbringer vor und kann bearbeitet werden.
Hauptszenario	1. Die Anforderung wird vom Bürger bzw. Patienten in seinem ePA-Kernsystem formuliert. 2. Das ePA-Kernsystem erstellt aus der Anforderung ein Anforderungsobjekt. 3. Das ePA-Kernsystem übermittelt das Anforderungsobjekt an die ePA-Kommunikationskomponente. 4. Die ePA-Kommunikationskomponente leitet das Anforderungsobjekt an das LE-Postfach weiter. 5. Der ePA-LE-Client ruft das Anforderungsobjekt ab. 6. Das LE-Postfach übermittelt das Anforderungsobjekt an den ePA-LE-Client. 7. Der ePA-LE-Client leitet das Anforderungsobjekt an das AIS weiter. 8. Der Leistungserbringer ruft die Anforderung ab. 9. Das AIS zeigt dem Leistungserbringer die Anforderung an.
Beziehungen zu anderen Use Cases	UC-0-4

Tabelle 42: Anfordern von Daten durch einen Bürger

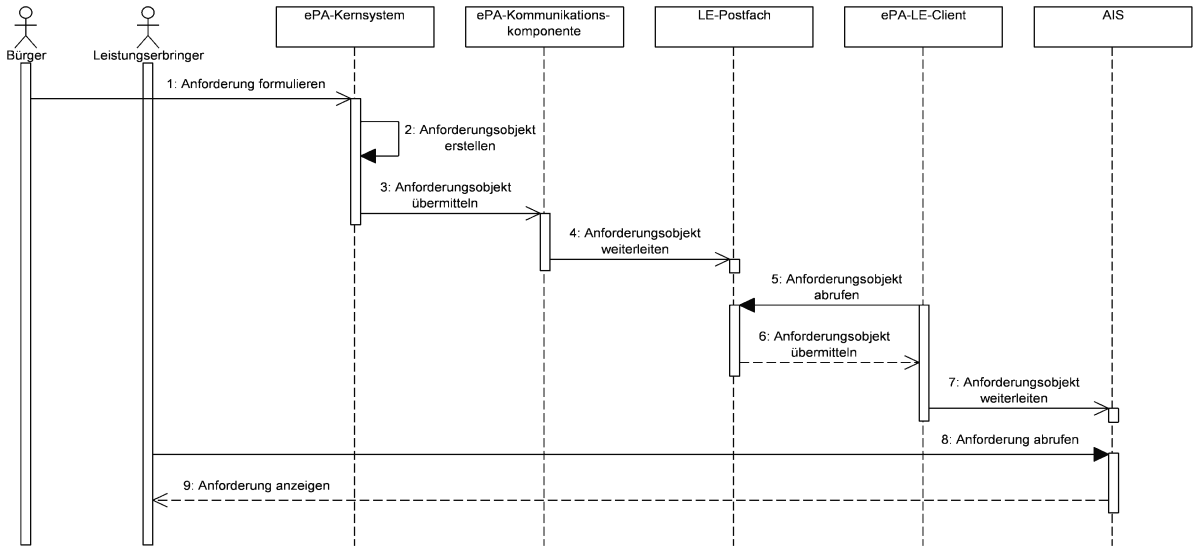

Abbildung 52: Anfordern von Daten durch einen Bürger

A3.2.3. Bereitstellen von Daten durch einen Bürger

Bezeichner	UC-0-3
Name	Bereitstellen von Daten durch einen Bürger
Kurzbeschreibung	Ein Bürger bzw. Patient stellt über seine ePA ein Bereitstellungsobjekt für das Arztinformationssystem (AIS) des Leistungserbringers bereit.
Primärer Akteur	Bürger bzw. Patient
Andere Akteure	Leistungserbringer
Systeme	Arztinformationssystem, ePA-LE-Client, LE-Postfach, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Dem Patienten ist der Name des Leistungserbringers und seiner Organisation bekannt.
Nachbedingungen	Die bereitgestellten Informationen liegen dem Leistungserbringer vor.
Hauptszenario	1. Die bereitzustellenden Informationen werden vom Bürger bzw. Patienten in seinem ePA-Kernsystem zusammengestellt. 2. Das ePA-Kernsystem erstellt aus den Informationen ein Bereitstellungsobjekt. 3. Das ePA-Kernsystem übermittelt das Bereitstellungsobjekt an die ePA-Kommunikationskomponente. 4. Die ePA-Kommunikationskomponente leitet das Bereitstellungsobjekt an das LE-Postfach weiter. 5. Der ePA-LE-Client ruft das Bereitstellungsobjekt ab. 6. Das LE-Postfach übermittelt das Bereitstellungsobjekt an den ePA-LE-Client. 7. Der ePA-LE-Client leitet das Bereitstellungsobjekt an das AIS weiter. 8. Der Leistungserbringer ruft die Informationen ab. 9. Das AIS zeigt dem Leistungserbringer die Informationen an. 10. Der Leistungserbringer überprüft die Informationen. 11. Der Leistungserbringer übernimmt die Informationen in sein AIS.
Beziehungen zu anderen Use Cases	UC-0-4

Tabelle 43: Bereitstellen von Daten durch einen Bürger

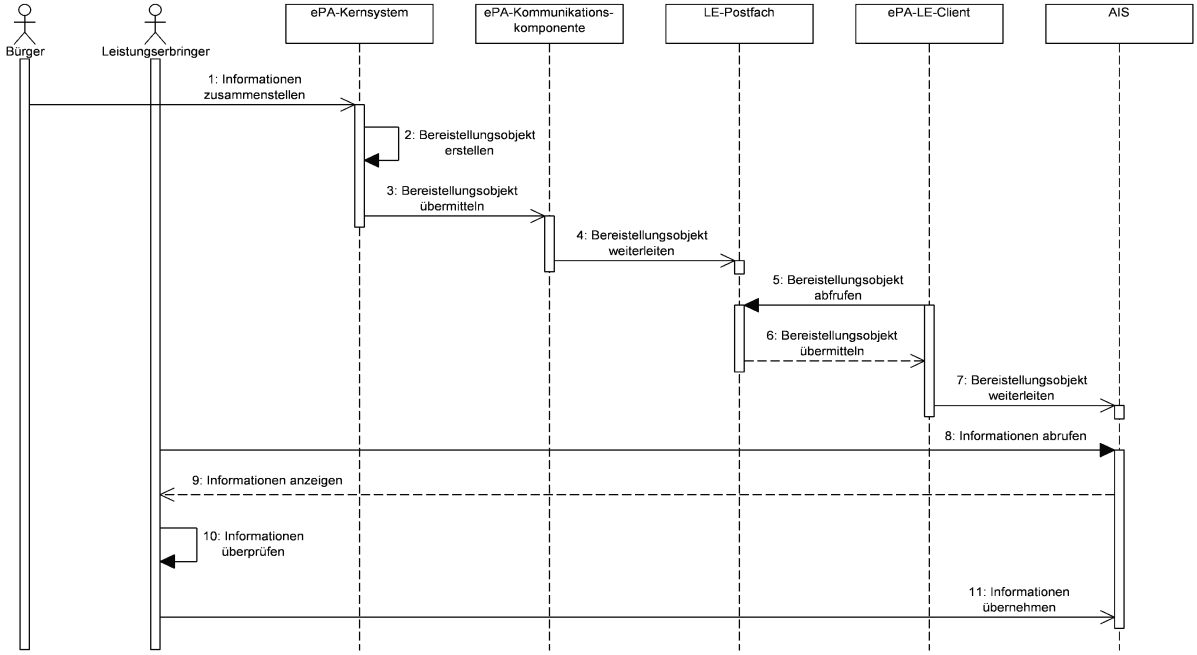

Abbildung 53: Bereitstellen von Daten durch einen Bürger

A3.2.4. Bereitstellen von Daten durch einen Leistungserbringer

Bezeichner	UC-0-4
Name	Bereitstellen von Daten durch einen Leistungserbringer
Kurzbeschreibung	Der Leistungserbringer stellt über sein Arztinformationssystem (AIS) ein Bereitstellungsobjekt für die ePA des Bürgers bzw. Patienten bereit.
Primärer Akteur	Leistungserbringer
Andere Akteure	Bürger bzw. Patient
Systeme	Arztinformationssystem, ePA-LE-Client, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Dem Leistungserbringer ist die Adresse der ePA des Bürgers bzw. Patienten bekannt.
Nachbedingungen	Die bereitgestellten Informationen liegen dem Bürger bzw. Patienten vor.
Hauptszenario	1. Die bereitzustellenden Informationen werden vom Leistungserbringer in seinem AIS zusammengestellt. 2. Das AIS übermittelt die Informationen an den ePA-LE-Client. 3. Der ePA-LE-Client erstellt aus den Informationen ein Bereitstellungsobjekt. 4. Der ePA-LE-Client übermittelt das Bereitstellungsobjekt an die ePA-Kommunikationskomponente. 5. Die ePA-Kommunikationskomponente leitet das Bereitstellungsobjekt an das ePA-Kernsystem weiter. 6. Der Bürger bzw. Patient ruft die Informationen ab. 7. Die ePA zeigt dem Bürger bzw. Patienten die Informationen an. 8. Der Bürger bzw. Patient überprüft die Informationen. 9. Der Bürger bzw. Patient übernimmt die Informationen in seine ePA.
Beziehungen zu anderen Use Cases	UC-0-2

Tabelle 44: Bereitstellen von Daten durch einen Leistungserbringer

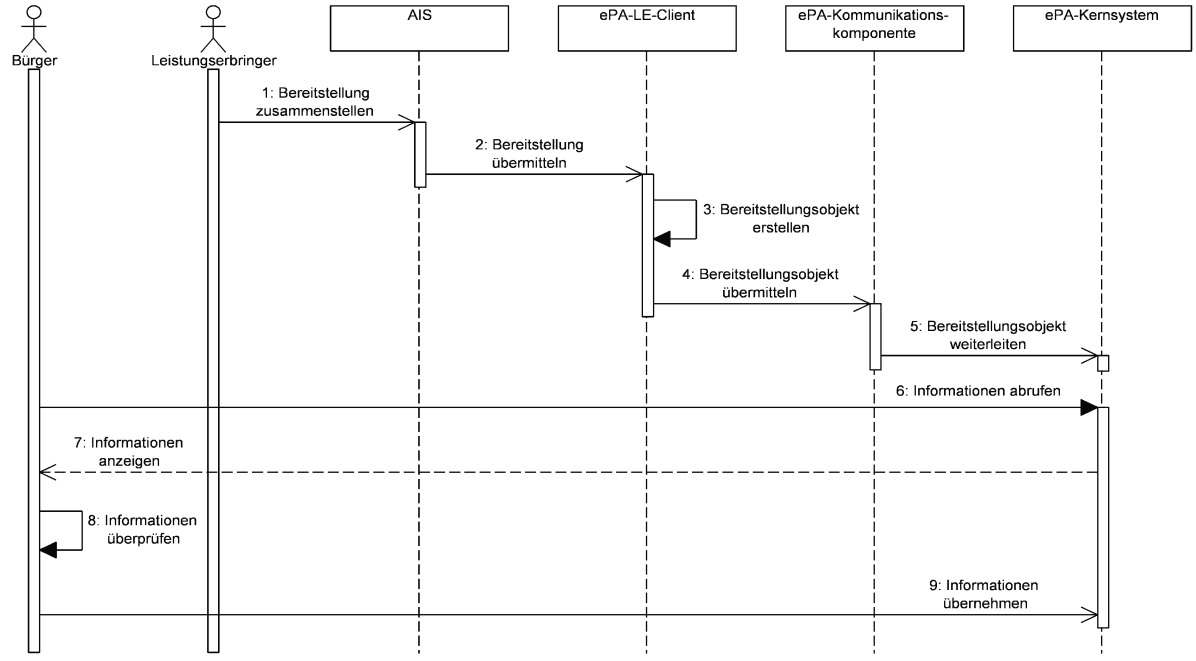

Abbildung 54: Bereitstellen von Daten durch einen Leistungserbringer

A3.2.5. Anfordern von Bereitstellungsobjekten durch einen Leistungserbringer mit unmittelbarer Zustellung

Dieses Kommunikationsmuster entspricht einer Kombination aus dem Kommunikationsmuster 1 und 3. Hier erfolgt allerdings nach der Anforderung durch den Leistungserbringer eine direkte Bereitstellung durch die Akte, ohne dass der Bürger hier noch eingreifen muss. Da der Ablauf des Kommunikationsmusters 5 nur einer Ausführung der Schritte des ersten und dritten Kommunikationsmusters hintereinander entspricht, wird dieser Kommunikationsmuster nicht nochmal beschrieben.

A3.2.6. Zustellen von Bereitstellungsobjekten durch einen Leistungserbringer mit unmittelbarer Verarbeitung

Da sich dieses Kommunikationsmuster nur bei der Übernahme der Bereitstellung in die ePA vom Kommunikationsmuster 4 unterscheidet, die Kommunikation zwischen den Komponenten aber die gleiche ist, wird es nicht nochmal getrennt beschrieben.

A3.3. Verwendete RLUS-Operationen

Operationsparameter /-element	Beschreibung
xs:any	XML-Dokument
RLUStypes:RLUSPutRequestSrcStruct	Informationen zum Aufrufkontext (Semantic Signifier, SourceIdentity, CBR-Context)
writeCommandEnum	Definiert die gewünschte Aktion im Zielsystem.

Tabelle 45: Beschreibung des PutRLUSGenericRequest [144, Seite 37]

Operationsparameter / -element	Beschreibung
RLUStypes:RLUSStatusCode	Status Code

Tabelle 46: Beschreibung der PutRLUSGenericResponse [144, Seite 37]

Operationsparameter /-element	Wert
RLUStypes:RLUSSearchStruct	Die High-Level Datenstruktur für eine „Suche anhand von Beispielen“ oder der Formulierung von Filterkriterien für eine RLUS-Suche
maxResultStreams	Angabe der maximalen Anzahl gleichzeitig zurückzugebender Informationsobjekte
previousResultID	ID der letzten Anfrage (für den Fall, dass die Ergebnismenge maxResultStreams übertrifft und ListRLUSGenericRequest mehrfach aufgerufen werden muss)

Tabelle 47: Beschreibung des ListRLUSGenericRequest [144, Seite 37]

Operationsparameter /-element	Beschreibung
Liste aus xs:any	XML-Dokumente
RLUStypes:RLUSStatusCode	Status Code
resultID	Beide Elemente erlauben eine iterative Abfrage einer Ergebnismenge.
finishedFlag	

Tabelle 48: Beschreibung der ListRLUSGenericResponse [144, Seite 38]

A3.4. Verschlüsselung der LE-Schnittstelle

A3.4.1. Bereitstellen von Informationsobjekten für eine ePA durch einen Leistungserbringer

1. In einem ersten Schritt muss der Leistungserbringer den öffentlichen Schlüssel des Aktensystems (pubAS) abrufen (siehe Abbildung 55). Dieser Schlüssel befindet sich in der Capability List der ePA und wird von jeder Kommunikation mit einer ePA von der ePA-Kommunikationskomponente abgerufen. Voraussetzung ist hierbei, dass der Anfragende sich als Leistungserbringer authentifiziert werden kann.
2. Als nächstes wird im LE-Client ein symmetrischer Schlüssel erstellt (KeyMDO).
3. Anschließend verschlüsselt der LE-Client die bereitzustellende Nutzlast mit dem symmetrischen Schlüssel (KeyMDO).
4. In einem nächsten Schritt wird der KeyMDO mit dem öffentlichen Schlüssel der ePA (pubAS) verschlüsselt.
5. Die Nutzlast und der Schlüssel werden in ein Bereitstellungsobjekt eingefügt und an das ePA-Kernsystem übermittelt.
6. Die ePA überprüft die Berechtigung des Leistungserbringers und übernimmt das Bereitstellungsobjekt [167].

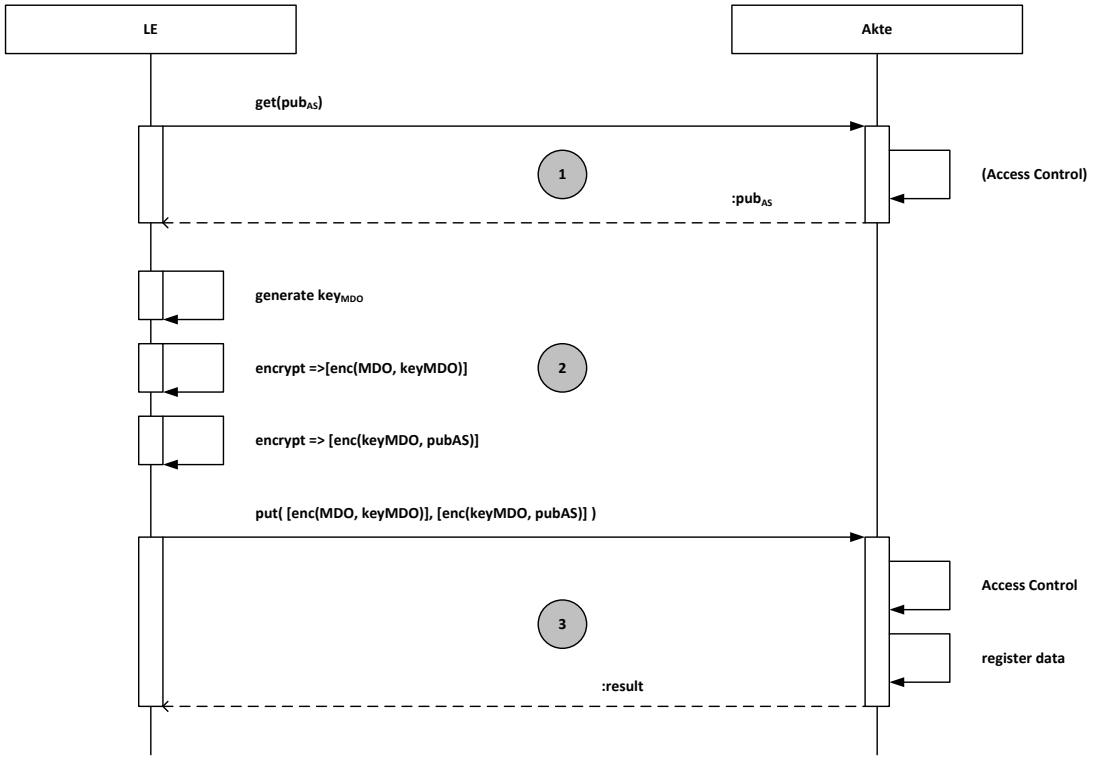

Abbildung 55: Abruf der Verschlüsslung bei der Bereitstellung von Informationsobjekten für eine ePA durch einen Leistungserbringer [167, Seite 9]

A3.4.2. Abrufen von Informationsobjekten von einer ePA durch einen Leistungserbringer

Im Verschlüsselungsmodell der LE-Schnittstelle wird eine Variante mit Vorab- und eine Variante mit Ad-hoc-Autorisierung beschrieben [167]. Hier wird nur auf die Variante mit Vorab-Autorisierung eingegangen, da keine Ad-hoc Autorisierung über die Forschungsschnittstelle stattfindet.

1. Der Leistungserbringer fordert ein Bereitstellungsobjekt an.
2. Im ePA-Kernsystem wird überprüft, ob eine entsprechende Vorab-Autorisierungsrichtlinie hinterlegt wurde.
3. Das ePA-Kernsystem sendet dem Leistungserbringer
   das angeforderte verschlüsselte medizinische Datenobjekt,
   - den durch den öffentlichen Aktenschlüssel (pubAS) gesicherten symmetrischen Schlüssel (symkeyMDO), mit dem das MDO verschlüsselt wurde,
   - den privaten Aktenschlüssel (prkAS), der mit einem symmetrischen Schlüssel (symkeyASN) gesichert wurde, und
   - den symkeyASN, der mit dem öffentlichen Schlüssel des HBAs (pubHBA) des Leistungserbringers gesichert wurde,

   in einem Bereitstellungsobjekt (siehe Abbildung 56).
4. Beim Leistungserbringer wird zunächst der symkeyASN mit dem privaten Schlüssel des HBAs entschlüsselt.
5. Anschließend wird der private Teil des Aktenschlüssels (prkAS) mit dem symkeyASN entschlüsselt.
6. Nun wird der symmetrische Schlüssel des MDOs (symkeyMDO) mit dem prkAS entschlüsselt.
7. Abschließend wird mit dem symkeyMDO das medizinische Datenobjekt entschlüsselt [167].

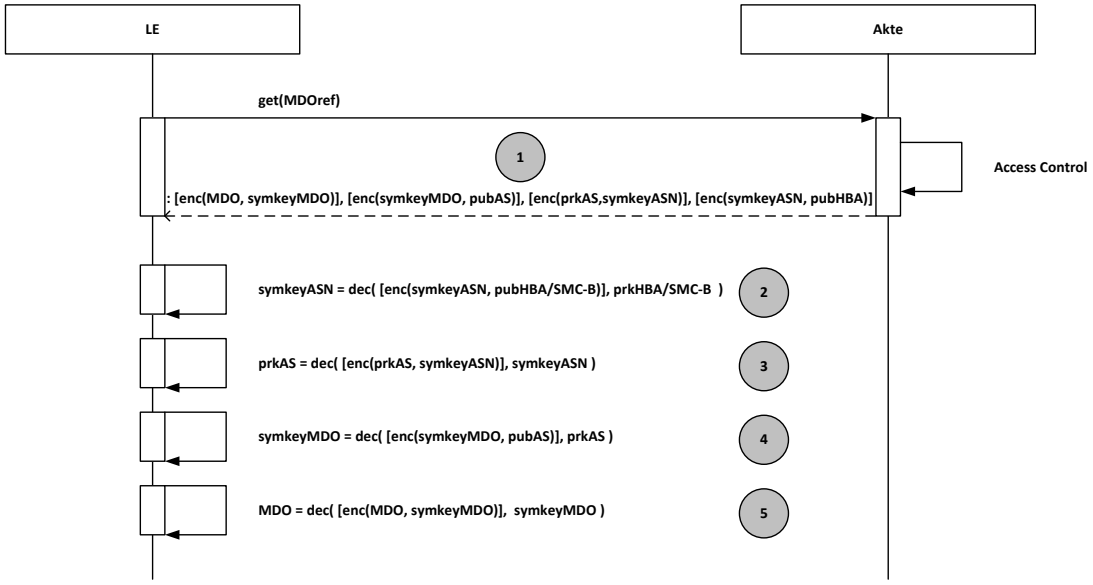

Abbildung 56: Ablauf der Entschlüsselung bei dem Abrufen von Informationsobjekten von einer ePA durch einen Leistungserbringer [167, Seite 11]

A3.5. Zusammenfassung der Anforderungen und Voraussetzungen an die Systeme

An.-Nr.	Anforderungsname	System	Kurzbeschreibung	Umgesetzt in Kapitel
A00	Kommunikation über die Operationen und Nachrichten der LE-Schnittstelle	Forschungs-schnittstelle	Da möglichst wenige Anpassungen an dem bestehenden ePA-System vorgenommen werden sollen, muss die Forschungsschnittstelle die Operationen und Nachrichten der Kommunikationskomponente unterstützen.	8
A01	Anforderungs- und Bereitstellungsobjekte unterstützen	Forschungs-schnittstelle	Die Forschungsschnittstelle muss Anforderungs- und Bereitstellungsobjekte unterstützen.	7
A02	Semantic Signifier unterstützen	Forschungs-schnittstelle	Die Forschungsschnittstelle muss Semantic Signifier unterstützen.	7
A03	Erstellung von Bereitstellungs- und Anforderungsobjekten	Forschungs-schnittstelle	Die Forschungsschnittstelle muss die Erstellung von Bereitstellungs- und Anforderungsobjekten übernehmen und die Nutzlast aus den Objekten extrahiert dem Forschungssystem bereitstellen.	7
A04	Zuordnung der Identitäten eines Patienten	Forschungs-schnittstelle	Die Forschungsschnittstelle muss während der Kommunikation ein Mapping der Identitäten des Patienten im Forschungs- und ePA-System durchführen.	7
A05	Abrufen der Capability List	Forschungs-schnittstelle	Die Forschungsschnittstelle muss vor der Kommunikation mit einer ePA die Capability List der ePA abrufen und auswerten.	8
A06	Austausch identifizierender Daten	Forschungs-schnittstelle	Über die ePA sollen nicht nur medizinische Daten an die Versorgungsdatenbank des Versorgungsmoduls übertragen werden. Sie soll auch eine Kommunikation zur Patientenliste ermöglichen und somit auch die Kommunikation von identifizierenden Daten und allgemeinen Informationen zwischen dem Patienten und dem Versorgungsmodul ermöglichen.	7.2
A07	Austausch medizinischer Daten	Forschungs-schnittstelle	Daten, die für Forschungsfragen interessant sind, sollen aus der ePA über die Forschungsschnittstelle an das Versorgungsmodul übertragen werden.	7.2
A08	Pseudonymisierung und Depseudonymisierung	Forschungs-schnittstelle	Da die Daten des Patienten in der Versorgungsdatenbank pseudonymisiert vorliegen und in der ePA mit identifizierenden Daten vorliegen, muss die Forschungsschnittstelle während der Kommunikation zwischen der ePA und dem Versorgungsmodul die Pseudonymisierung bzw. Depseudonymisierung vornehmen.	7.2

An.-Nr.	Anforderungsname	System	Kurzbeschreibung	Umgesetzt in Kapitel
A09	Überprüfung der Einwilligung zwecks Kontaktierung	Forschungs-schnittstelle	Es muss eine Überprüfung der Einwilligung erfolgen, bevor ein Patient kontaktiert wird.	7.2 / 9.4
A10	Überprüfung der Einwilligung zwecks Datenbereitstellung (identifizierende Daten)	Forschungs-schnittstelle	Dadurch, dass dem Patienten nun die Option ermöglicht wird, über seine ePA der Patientenliste Daten zu schicken, muss weiterhin sichergestellt werden, dass die Patientenliste nur Daten erhält, die auch für diesen Anwendungsfall notwendig sind. D. h. die Forschungsschnittstelle muss sicherstellen, dass der Patient der Patientenliste über seine ePA nur seine Kontaktdaten bzw. identifizierenden Daten bereitstellen kann.	7.2 / 9.4
A11	Überprüfung der Einwilligung zwecks Datenbereitstellung (medizinische Daten)	Forschungs-schnittstelle	Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Versorgungsdatenbank nur Daten bereitstellt, die auch im Rahmen des Forschungsvorhabens benötigt werden und für die eine Einwilligung des Patienten vorliegt.	7.2 / 9.4
A12	Überprüfung der Einwilligung zwecks Rekrutierung	Forschungs-schnittstelle	Eine Kontaktaufnahme bedarf der Einwilligung des Patienten, daher muss die Forschungsschnittstelle, wie im Anwendungsfall zur Kontaktierung, auch hier überprüfen, ob der Patient eingewilligt hat, dass er zwecks einer Rekrutierung kontaktiert werden darf.	7.2 / 9.4
A13	Überprüfung der Einwilligung zwecks informieren über neue Forschungsergebnisse	Forschungs-schnittstelle	Es muss sichergestellt werden, dass der Patient eingewilligt hat, dass er über die Forschungsergebnisse informiert werden darf. Diese Überprüfung wird durch die Forschungsschnittstelle übernommen.	7.2 / 9.4
A14	Überprüfung der Regelung zwecks Auskunftsrecht	Forschungs-schnittstelle	Hier muss durch den Forschungsverbund festgelegt werden, welche Informationen einem Patienten direkt aus der Versorgungsdatenbank bereitgestellt werden können und welche über einen behandelnden Arzt zur Verfügung gestellt werden müssen. Diese Regeln, die vorher vom Ansprechpartner des Forschungsverbundes berücksichtigt wurden, müssen nun in der Forschungsschnittstelle abgebildet und durchgeführt werden.	7.2 / 9.4

Tabelle 49: Anforderungen an die Forschungsschnittstelle

Vor.-Nr.	Voraussetzungs-name	Kurzbeschreibung	Festgelegt in Abschnitt
VE00	Speicherung der Adressen des Versorgungmoduls	Das ePA-System muss die Adressen der Datenbanken des Versorgungsmoduls speichern.	6.1.1
VE01	Differenzierter Rückzug der Einwilligung	Die ePA muss dem Patienten die Möglichkeit bieten, dass er seinen Rückzug der Einwilligung differenziert formulieren kann (z. B. Rückzug aus einem Forschungsvorhaben oder Rückzug aus dem ganzen Forschungsverbund).	6.2.5
VE02	Automatische Weiterleitung	Die ePA sollte es ermöglichen, Regeln zu hinterlegen, in denen eine automatische Weiterleitung der Daten aus der Versorgung an das Versorgungsmodul definiert werden können.	6.3.2
VE03	Entfernen von identifizierenden Merkmalen	Die verschlüsselten medizinischen Daten wiederum dürfen weder das Pseudonym des Patienten (PIDv) noch identifizierende Daten des Patienten enthalten. D. h. diese Informationen müssen vor der Verschlüsselung von der Versorgungsdatenbank bzw. dem ePA-Kernsystem entfernt werden.	7.2

Tabelle 50: Zusammenfassung der Voraussetzungen an das ePA-System für die Kommunikation mit dem Versorgungsmodul

Vor.-Nr.	Voraussetzungs-name	Kurzbeschreibung	Festgelegt in Abschnitt
VF00	Zentrale Patientenliste	Vorausgesetzt wird eine aus den teilnehmenden Zentren direkt zugreifbare Patientenliste, die in der Lage ist, die identifizierenden Daten und mehrere Pseudonyme eines Patienten aus unterschiedlichen Systemen bzw. Forschungsprojekten zu verwalten	4.2.1
VF01	Funktionen der Patientenliste	Die Patientenliste kann auch zusätzliche Funktionen haben wie z. B. das Erstellen von Serienbriefen zwecks Kontaktierung der Patienten oder das Verwalten von Einwilligungserklärungen. Bei der Betrachtung der Anwendungsfälle wird davon ausgegangen, dass diese Funktionen durch die Patientenliste für bestimmte Anwendungsfälle umgesetzt werden (z. B. beim Kontaktieren eines Patienten).	4.2.1
VF02	Semantic Signifier implementieren	Das Forschungssystem muss die Nutzlast nach den inhaltlichen und strukturellen Vorgaben der Semantic Signifier aufbereiten bzw. die empfangenen Daten richtig in die Datenbanken des Forschungssystems schreiben.	5.8.4
VF03	Speicherung der ePA-ID	Die Patientenliste muss die ePA-ID des Patienten als ein weiteres identifizierendes Merkmal zu dem Patienten speichern.	6.1.1
VF04	Entfernen von Pseudonymen	Die verschlüsselten medizinischen Daten dürfen weder das Pseudonym des Patienten (PIDv) noch identifizierende Daten des Patienten enthalten. D. h. diese Informationen müssen vor der Verschlüsselung von der Versorgungsdatenbank bzw. dem ePA-Kernsystem entfernt werden.	7.2

Tabelle 51: Zusammenfassung der Voraussetzungen an das Forschungssystem für die Kommunikation mit dem ePA-System

A4. Facharchitektur

In diesem Kapitel werden die Details der Facharchitektur beschrieben. Dies beinhaltet zum einen das Abrufen der Capability List. Zum anderen wird das Verhalten der einzelnen Komponenten beim Aufrufen der Operationen beschrieben und hergeleitet, welche Module die einzelnen Komponenten benötigen. Im Sinne eines generischen Ansatzes und zum Zwecke der Vereinheitlichung mit den Begrifflichkeiten im FuE-Projekt wird die Versorgungsdatenbank als medizinische Datenbank des Forschungsverbundes und das Versorgungsmodul als Forschungssystem bezeichnet.

A4.1. Abrufen der Capability

A4.1.1. Abrufen der Capability List durch den Forschungs-Client-IDAT

Das Abrufen der Capability List durch den Forschungs-Client-IDAT muss immer durchgeführt werden, bevor Daten von der Patientenliste aus der ePA angefordert oder für die ePA bereitgestellt werden, um zu überprüfen ob die ePA die Kommunikationsmuster und die Semantic Signifier unterstützt. Das Gleiche gilt auch für den Forschungs-Client-MDAT (siehe UC-5-2).

Bezeichner	UC-5-1
Name	Abrufen der Capability List durch den Forschungs-Client-IDAT
Kurzbeschreibung	Der Forschungs-Client-IDAT ruft vor einer Kommunikation die Capability List der ePA des Patienten ab, von der er Informationen anfordern bzw. der er Informationen bereitstellen möchte.
Primärer Akteur	Keine
Andere Akteure	Keine
Systeme	Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente
Vorbedingungen	Es liegen Informationen für den Patienten in der Patientenliste vor bzw. es sollen Informationen von der ePA des Patienten für die Patientenliste angefordert werden. Dem Forschungs-Client-IDAT liegt die ePA-ID des Patienten vor.
Nachbedingungen	Die Capability List liegt dem Forschungs-Client-IDAT vor.
Hauptszenario	1. Der Forschungs-Client-IDAT erstellt ein Anforderungsobjekt für eine Capability List einer ePA eines Patienten unter Angabe der ePA-ID des entsprechenden Patienten. 2. Der Forschungs-Client-IDAT übermittelt es an den ePA-Forschungsadapter. 3. Der ePA-Forschungsadapter leitet die Anforderung an die ePA-Kommunikationskomponente weiter. 4. Die ePA-Kommunikationskomponente ermittelt anhand der ePA-ID die entsprechende Capability List der ePA. 5. Die ePA-Kommunikationskomponente übermittelt die Capability List an den ePA-Forschungsadapter. 6. Der ePA-Forschungsadapter leitet die Capability List an den Forschungs-Client-IDAT weiter.
Beziehungen zu anderen Use Cases	UC-3-1 und UC-3-2

Tabelle 52: Abrufen der Capability List durch den Forschungs-Client-IDAT

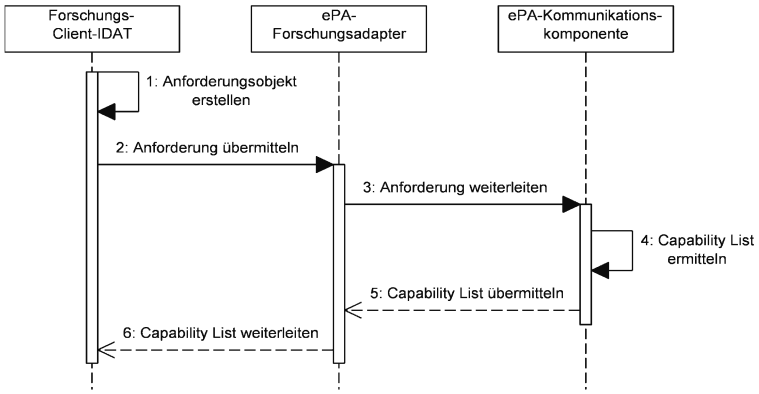

Abbildung 57: Abrufen der Capability List durch den Forschungs-Client-IDAT

A4.1.2. Abrufen der Capability List durch den Forschungs-Client-MDAT

Hier kann die Kommunikation zwischen dem Forschungs-Client-IDAT und -MDAT erfolgen und muss keine Pseudonymisierung durch die ePA-Forschungsadapter erfolgen, da die Capability List keine medizinischen Daten enthält und auch dem Forschungs-Client-IDAT zugänglich ist.

Bezeichner	UC-5-2
Name	Abrufen der Capability List durch den Forschungs-Client-MDAT
Kurzbeschreibung	Der Forschungs-Client-MDAT ruft vor einer Kommunikation die Capability List der ePA des Patienten ab, von der er Informationen anfordern bzw. der er Informationen bereitstellen möchte.
Primärer Akteur	Keine
Andere Akteure	Keine
Systeme	Patientenliste, Forschungs-Client-MDAT, Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente
Vorbedingungen	Es liegen Informationen für den Patienten in der medizinischen Datenbank des Forschungsverbundes vor bzw. es sollen Informationen aus der ePA des Patienten für die medizinische Datenbank des Forschungsverbundes angefordert werden. Dem Forschungs-Client-MDAT liegt die PID des Patienten vor.
Nachbedingungen	Die Capability List liegt dem Forschungs-Client-MDAT ohne identifizierende Merkmale des Patienten vor.
Hauptszenario	1. Der Forschungs-Client-MDAT erstellt ein Anforderungsobjekt für eine Capability List der ePA eines Patienten unter Angabe der PID des entsprechenden Patienten. 2. Der Forschungs-Client-MDAT übermittelt das Anforderungsobjekt an den Forschungs-Client-IDAT. 3. Der Forschungs-Client-IDAT erfragt die ePA-ID zu der PID des Patienten bei der Patientenliste an. 4. Die Patientenliste übermittelt die ePA-ID zu der PID. 5. Der Forschungs-Client-IDAT speichert die PID mit der ePA-ID zwischen. 6. Der Forschungs-Client-IDAT ersetzt die PID durch die ePA-ID im empfangenen Anforderungsobjekt. 7. Der Forschungs-Client-IDAT übermittelt die Anforderung an den ePA-Forschungsadapter. 8. Der ePA-Forschungsadapter leitet die Anforderung an die ePA-Kommunikationskomponente weiter. 9. Die ePA-Kommunikationskomponente ermittelt anhand der ePA-ID die entsprechende Capability List der ePA. 10. Die ePA-Kommunikationskomponente übermittelt die Capability List an den ePA-Forschungsadapter. 11. Der ePA-Forschungsadapter leitet die Capability List an den Forschungs-Client-IDAT weiter. 12. Der Forschungs-Client-IDAT liest die PID aus dem Zwischenspeicher aus. 13. Der Forschungs-Client ersetzt die ePA-ID in der Capability List durch die PID im Zwischenspeicher. 14. Der Forschungs-Client-IDAT entfernt das Schlüsselmaterial und die Signaturen aus der Capability List. 15. Der Forschungs-Client-IDAT übermittelt die Capability List an den Forschungs-Client-MDAT.
Beziehungen zu anderen Use Cases	UC-4-1 und UC-4-2

Tabelle 53: Abrufen der Capability List durch den Forschungs-Client-MDAT

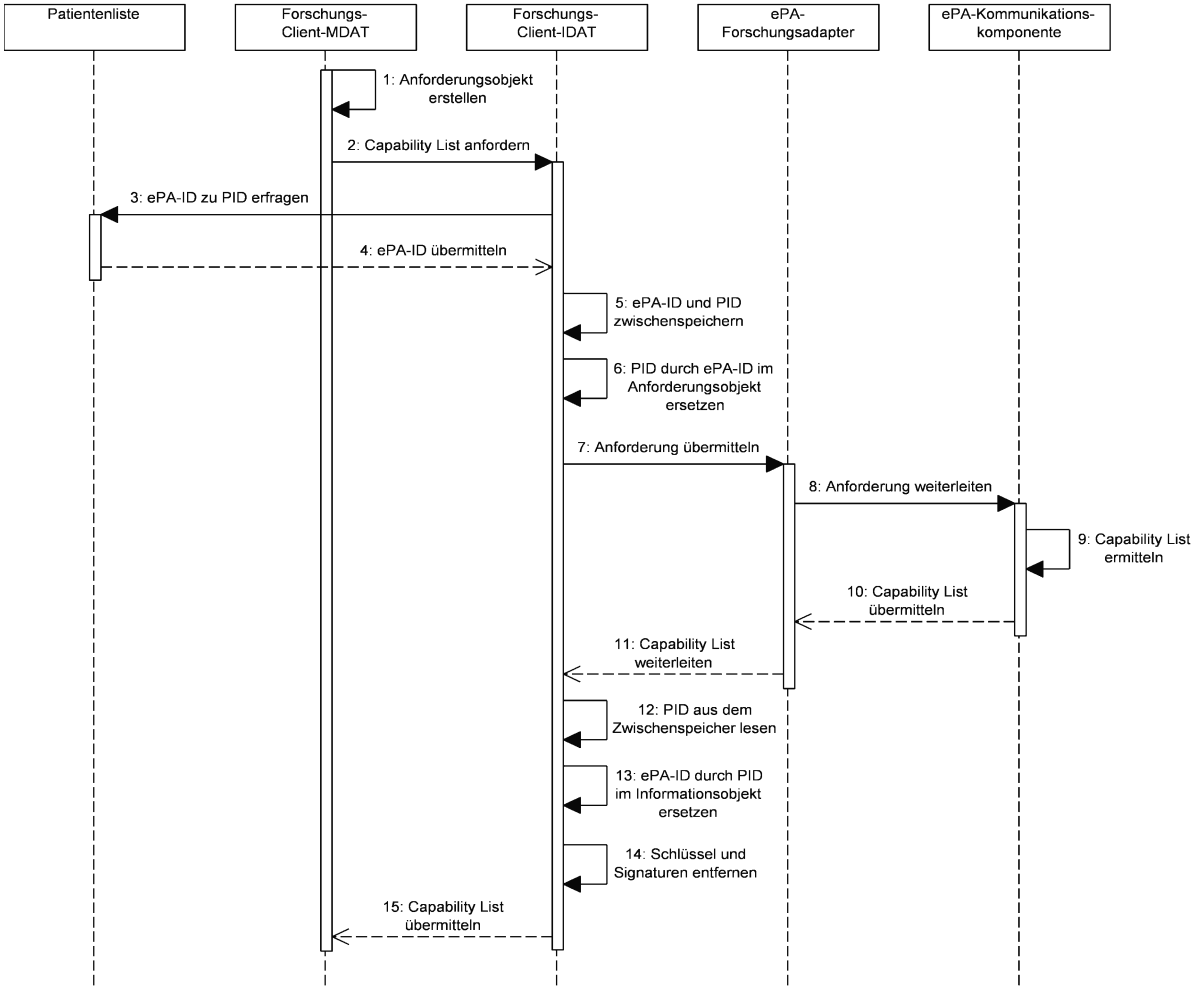

Abbildung 58: Abrufen der Capability List durch den Forschungs-Client-MDAT

A4.2. Erfolgs- und Fehlermeldungen

Da die Kommunikation zwischen dem ePA-System und den Systemen eines medizinischen Forschungsverbundes immer über mehrere Komponenten und Operationsaufrufe durchgeführt wird, können die Fehler- und Erfolgsmeldungen (im Sinne einer Zustellung beim Empfänger) nicht immer durch die aufgerufene Operation direkt an die bereitstellende Komponente zurückgegeben werden. Daher wird festgelegt, dass Fehler immer von der Operation, in der sie auftreten, an die aufrufende Komponente zurückgegeben werden. Die aufrufende Komponente sendet den Fehler an den Absender. Dies kann beispielsweise in Form eines Bereitstellungsobjektes mit einem entsprechenden Semantic Signifier und speziell definierten Fehlercodes erfolgen. Die Definition dieser Fehlercodes und Semantic Signifier ist nicht Bestandteil dieser Spezifikation. Erfolgsmeldungen werden nicht verschickt. Hier ist davon auszugehen, dass die Information zugestellt wurde, wenn keine Fehlermeldung zurückkommt. Im Folgenden wird im Sinne einer besseren Übersicht das Auswerten und Versenden von Fehlermeldungen durch die aufrufende Komponente einmal generell beschrieben und gilt dann für jeden Operationsaufruf.

Vorbedingung: Es wurde eine Operation aufgerufen.

Ablauf der Operation:

1. Zunächst wird der Rückgabewert der aufgerufenen Operation ausgewertet. Ist der Rückgabewert keine Fehlermeldung, so wird der Operationsaufruf beendet. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 59).
2. Die Komponente ermittelt den Absender der Nachricht, bei der ein Fehler aufgetreten ist.
3. Die Komponente erstellt ein Bereitstellungsobjekt mit einem entsprechenden Semantic Signifier und einem Fehlercode ggf. weitere Beschreibung des Fehlers.
4. Die Komponente übermittelt das Bereitstellungsobjekt an den Absender der Nachricht, bei der ein Fehler aufgetreten ist. Dies erfolgt durch den Aufruf der Operation, mit der sonst auch Informationsobjekte an den Absender bereitgestellt werden.
5. Die Komponente beendet den Operationsaufruf.

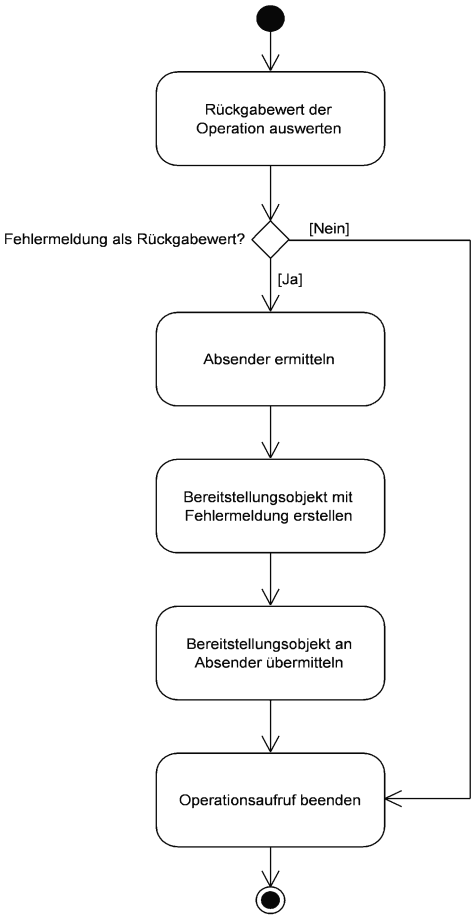

Abbildung 59: Auswerten von Erfolgs- und Fehlermeldungen

A4.3. Erstellen und Verifizieren von Nachrichten

Da jede Operation entweder eine empfangene Nachricht verifizieren und den Absender authentifizieren muss oder ein Nachricht erstellen und einen Authentifizierungsnachweis beim Identity-Provider anfordern muss, werden diese Vorgänge in diesem Abschnitt einmal im Detail beschrieben und im Folgenden bei jeder Beschreibung eines Operationsaufrufes bzw. der Durchführung einer Operation auf diese Abschnitte verwiesen.

A4.3.1. Erstellen von Nachrichten

Bevor eine Operation einer Schnittstelle aufgerufen werden kann, muss der Absender einen Authentifizierungsnachweis vom Identity-Provider anfordern und eine SOAP-Nachricht erstellen. Da dieser Prozess von jeder Komponente vor dem Absenden einer Nachricht durchgeführt werden muss, wird er hier einmal im Detail beschrieben und dann nur noch auf diesen Abschnitt verwiesen.

Vorbedingung: Es soll eine Operation einer anderen Komponente aufgerufen werden.

Ablauf der Operation:

1. In einem ersten Schritt muss der Absender einen Authentifizierungsnachweis beim Identity-Provider anfordern (Details siehe Sicherheitsarchitektur der LE-Schnittstelle [155]). Erhält er keinen Authentifizierungsnachweis so wird die Operation abgebrochen und eine Fehlermeldung an das aufrufende System zurückgeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 60).
2. Es wird ein Informationsobjekt erstellt[25].
3. Es wird eine SOAP-Nachricht erstellt, mit dem Authentifizierungsnachweis im SOAP-Header und dem Informationsobjekt im SOAP-Body.

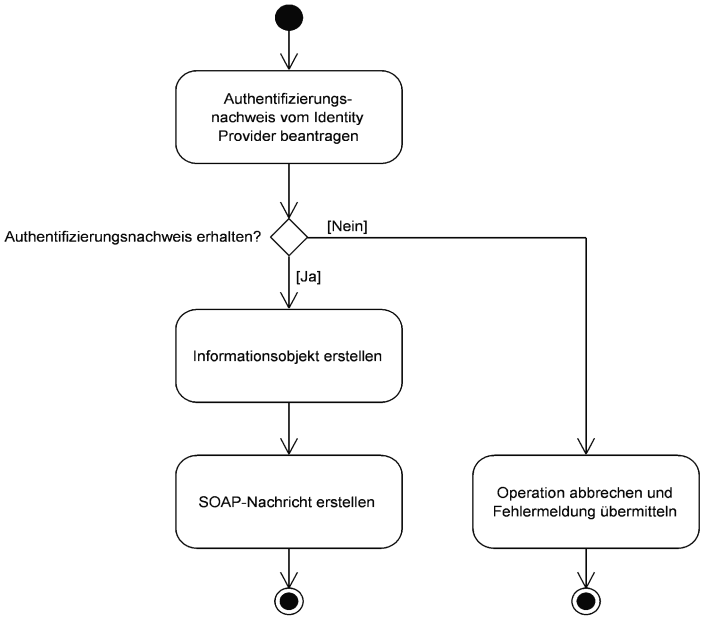

Abbildung 60: Erstellen von Nachrichten

[25] Wenn es sich um einen synchronen Aufruf handelt, wird kein Informationsobjekt generiert, sondern die Parameter des Informationsobjektes direkt in die SOAP-Nachricht eingebettet.

A4.3.2. Verifizierung von Nachrichten

Bevor eine Nachricht von einer Komponente verarbeitet werden kann, muss der Absender authentifiziert, die Transportnachricht verifiziert werden und eine syntaktische Prüfung der Nachricht erfolgen. Da dieser Prozess von jeder Komponente bei jeder empfangenen Nachricht durchgeführt werden muss, wird er hier einmal im Detail beschrieben und dann nur noch auf diesen Abschnitt verwiesen.

Vorbedingung: Eine andere Komponente hat eine Operation aufgerufen.

Ablauf der Operation:

1. In einem ersten Schritt wird überprüft, ob ein Authentifizierungsnachweis vorhanden ist. Sollte kein Authentifizierungsnachweis vorhanden sein, so wird die Operation abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 61).
2. Danach wird der Absender der Anforderung authentifiziert (Details siehe Sicherheitsarchitektur der LE-Schnittstelle [155]). Ist die Authentifizierung erfolgreich, so erfolgt eine weitere Verarbeitung, ansonsten wird eine Fehlermeldung an den Absender zurückgeben und die Operation abgebrochen.
3. Es erfolgt eine Verifizierung der Transportnachricht (s. a. Facharchitektur und Sicherheitsarchitektur der LE-Schnittstelle). Ist die Verifizierung erfolgreich, so erfolgt eine weitere Verarbeitung, ansonsten wird eine Fehlermeldung an den Absender zurückgeben und die Operation abgebrochen.
4. Im nächsten Schritt wird durch die Komponente eine syntaktische Validierung der Anforderung durchgeführt (Überprüfung der übermittelten RLUS-Parameter gemäß Spezifikation). Ist die Validierung erfolgreich, so wird der nächste Schritt eingeleitet, ansonsten wird eine Fehlermeldung an den Absender übermittelt und die Operation abgebrochen.

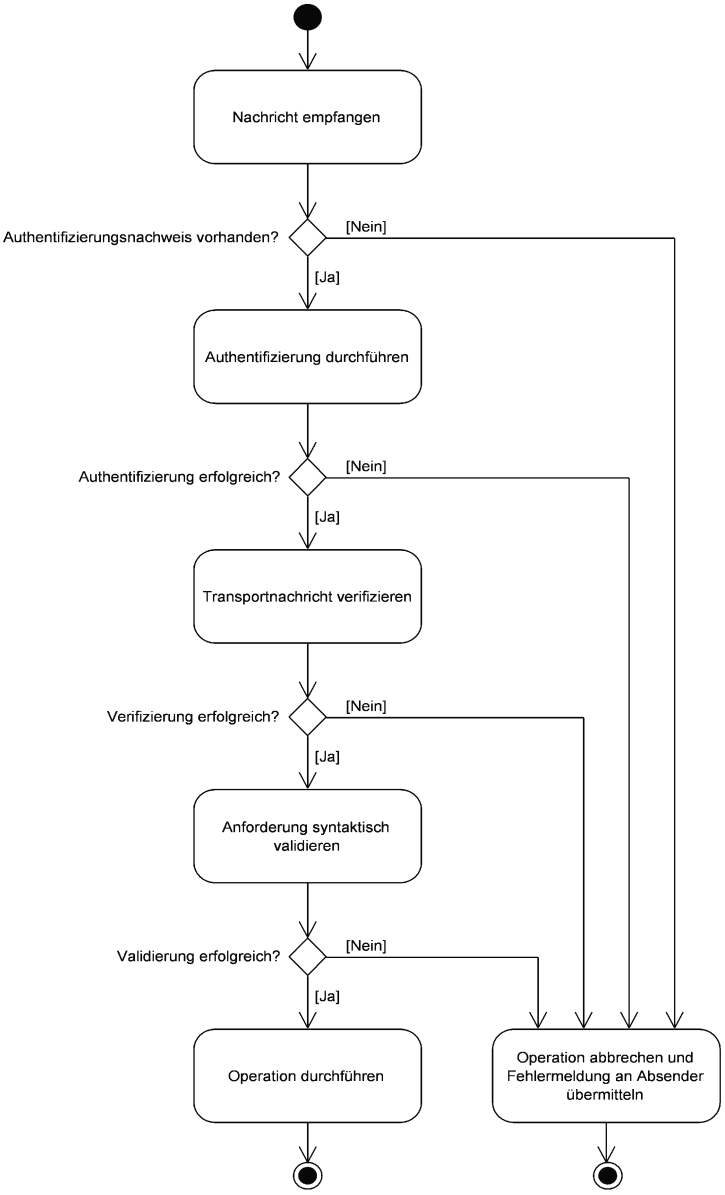

Abbildung 61: Verifizierung von Nachrichten

A4.4. Forschungs-Client-IDAT

In diesem Abschnitt wird das Verhalten des Forschungs-Client-IDAT beim Aufrufen und Durchführen von Operationen beschrieben. Der Forschungs-Client-IDAT ist sowohl Dienstnutzer gegenüber dem ePA-Forschungsadapter als auch Dienstanbieter gegenüber dem Forschungs-Client-MDAT. Zunächst wird auf die Kommunikation mit dem Forschungs-Client-MDAT eingegangen und anschließend auf die Kommunikation mit dem ePA-Forschungsadapter. Abschließend werden die Module des Forschungs-Clients-IDAT beschrieben.

A4.4.1. Kommunikation mit dem Forschungs-Client-MDAT

In diesem Abschnitt wird das Verhalten des Forschungs-Client-IDAT beim Aufrufen der einzelnen RLUS-Operationen der Schnittstelle S1 (siehe Abbildung 25) durch den Forschungs-Client-MDAT beschrieben.

Im Abschnitt 8.3 wurde herausgestellt, dass folgende Operationen durch die Schnittstelle S1 bereitgestellt werden müssen:

- **Anfordern einer PID durch den Forschungs-Client-MDAT:**
  RLUS-List(Parameter):SemSigGetPID
- **Anfordern einer TID durch den Forschungs-Client-MDAT:**
  RLUS-List(Parameter):SemSigGetTID
- **Anfordern der Capability List durch den Forschungs-Client-MDAT:**
  RLUS-List(Parameter): Capability List

Im Nachfolgenden werden die Aktionen beschrieben und in einem Ablaufdiagramm dargestellt, die der Forschungs-Client-IDAT bei den oben genannten Operation durchführen muss.

A4.4.1.1. Anfordern einer PID durch den Forschungs-Client-MDAT: RLUS-List(Parameter):SemSigGetPID

Vorbedingungen: Es wurde vorher eine Pseudonymisierungs-Anfrage vom ePA-Forschungsadapter bearbeitet.

Ablauf der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Bei Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 62).
2. Zur Auflösung der TID in eine PID wird zu der TID die entsprechende ePA-ID aus dem Zwischenspeicher des Forschungs-Clients-IDAT ausgelesen. Sollte sich kein Eintrag zu der TID im Zwischenspeicher befinden, so wird eine Fehlermeldung in Form eines Bereitstellungsobjektes an den Forschungs-Client-MDAT übermittelt und die Operation abgebrochen. Ansonsten wird zu der ePA-ID die entsprechende PID von der Patientenliste angefordert (Proprietäre Schnittstelle je nach Anbieter).
3. Im nächsten Schritt wird die Antwort der Patientenliste ausgewertet. Enthält die Antwort von der Patientenliste eine Fehlermeldung, so wird diese an den Forschungs-Client-MDAT in Form eines Bereitstellungsobjektes weitergeleitet und die Operation abgesprochen. Enthält die Antwort eine PID, so werden die PID und die TID in ein

Bereitstellungsobjekt verpackt und als Rückgabewert auf die Anfrage an den Forschungs-Client-MDAT übermittelt.

4. Anschließend werden die TID und die ePA-ID aus dem Zwischenspeicher gelöscht.

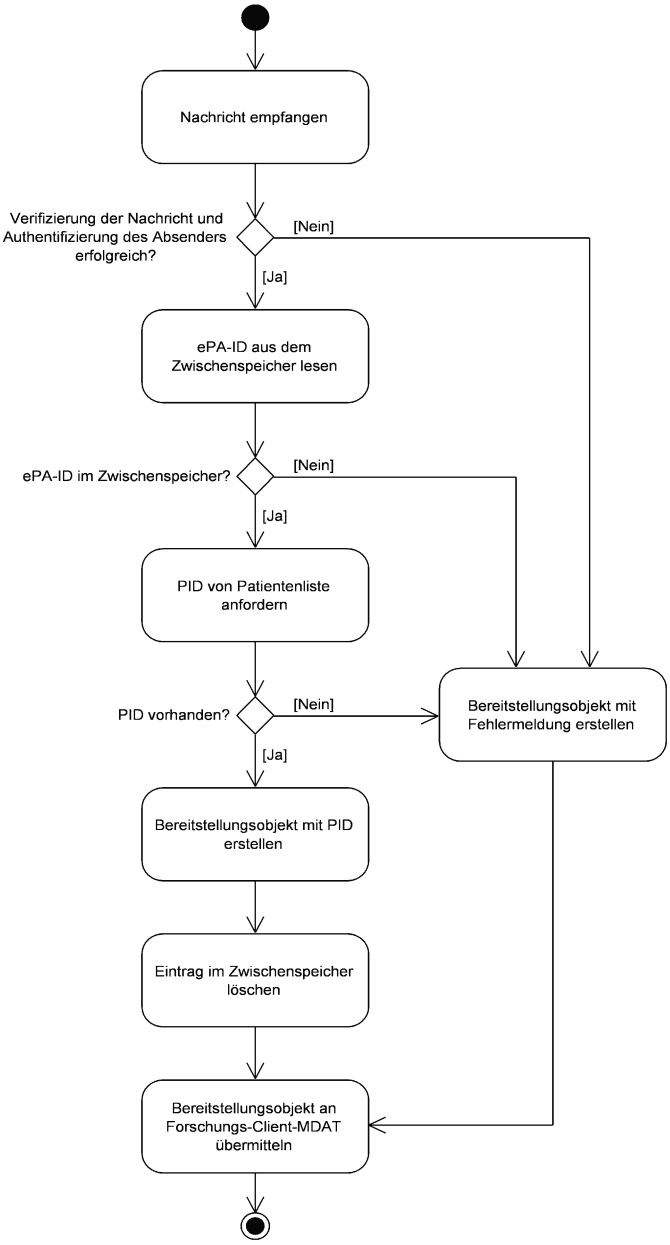

Abbildung 62: Anfordern einer PID durch den Forschungs-Client-MDAT

A4.4.1.2. Anfordern einer TID durch den Forschungs-Client-MDAT: RLUS-List(Parameter):SemSigGetTID

Vorbedingungen: Keine

Ablauf der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Bei Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 63).
2. Wird eine TID angefordert, so muss zunächst eine Autorisierung stattfinden, ob die geplante Anforderung bzw. Bereitstellung durch die Einwilligung des Patienten und die Regeln des Forschungsverbundes abgedeckt ist. Dies wird anhand der mitgelieferten Nutzlast (Angaben ob ein BO oder ein AO übermittelt werden soll und der Semantic Signifier des Objektes) aus den Anforderungsparametern überprüft (siehe Sicherheitsarchitektur der Forschungsschnittstelle). Ist die Autorisierung erfolgreich, so wird eine TID erstellt und mit der PID aus der Nutzlast der Anforderungsparameter im Forschungs-Client-IDAT zwischengespeichert. Ist die Autorisierung nicht erfolgreich, so wird eine Fehlermeldung an den Forschungs-Client-MDAT übermittelt und die Operation abgebrochen.
3. Im nächsten Schritt wird ein Bereitstellungsobjekt mit der TID und die PID als Nutzlast erstellt.
4. Abschließend wird das Bereitstellungsobjekt als Antwort an die Forschungs-Client-MDAT übermittelt.

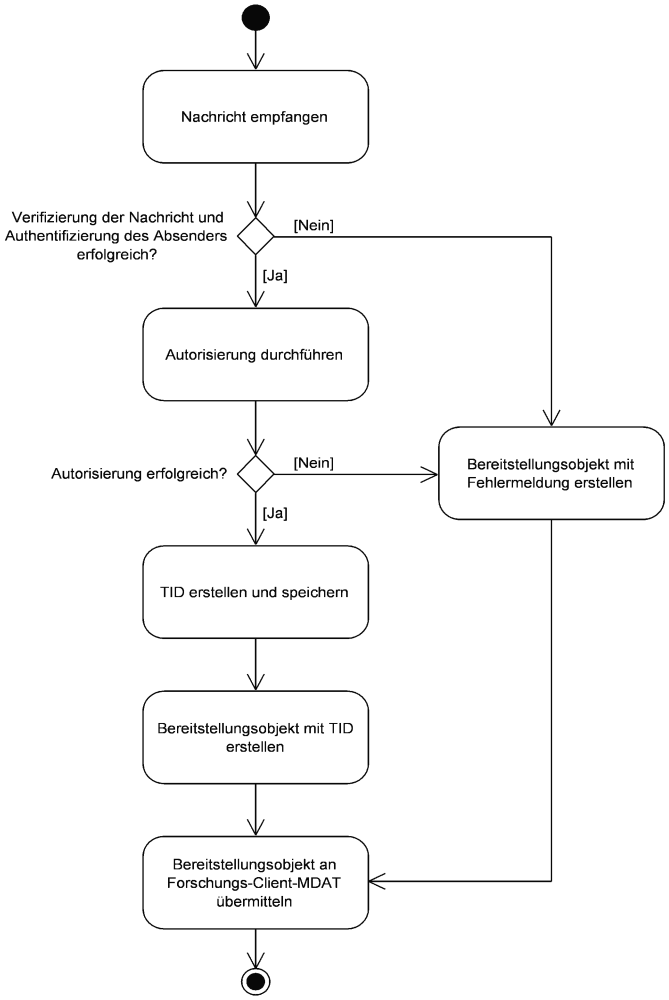

Abbildung 63: Anfordern einer TID durch den Forschungs-Client-MDAT

A4.4.1.3. Anfordern der Capability List durch den Forschungs-Client-MDAT: RLUS-List(Parameter): Capability List

Vorbedingungen: Keine

Ablauf der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Bei Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 64).
2. Anschließend wird die PID aus dem Anforderungsobjekt ausgelesen und von der Patientenliste die ePA-ID zu der PID angefordert. Ist der Rückgabewert der Patientenliste eine Fehlermeldung, so wird die Operation abgebrochen und die Fehlermeldung in Form eines Bereitstellungsobjektes an den Forschungs-Client-MDAT übermittelt. Andernfalls wird eine Capability List zu der ePA-ID vom ePA-Forschungsadapter angefordert (siehe Anfordern der Capability List durch den Forschungs-Client-IDAT: RLUS-List(Parameter): Capability List). Die ePA-ID und die PID werden zwischengespeichert.
3. Ist der Rückgabewert des ePA-Forschungsadapters eine Fehlermeldung, so wird diese in Form eines Bereitstellungsobjekts an den Forschungs-Client-MDAT weitergeleitet. Ist der Rückgabewert eine Capability List, so wird das Schlüsselmaterial entfernt, die ePA-ID durch die zu dieser ePA-ID zwischengespeicherte PID ersetzt und die Capability List als Rückgabewert an den Forschungs-Client-MDAT übermittelt.

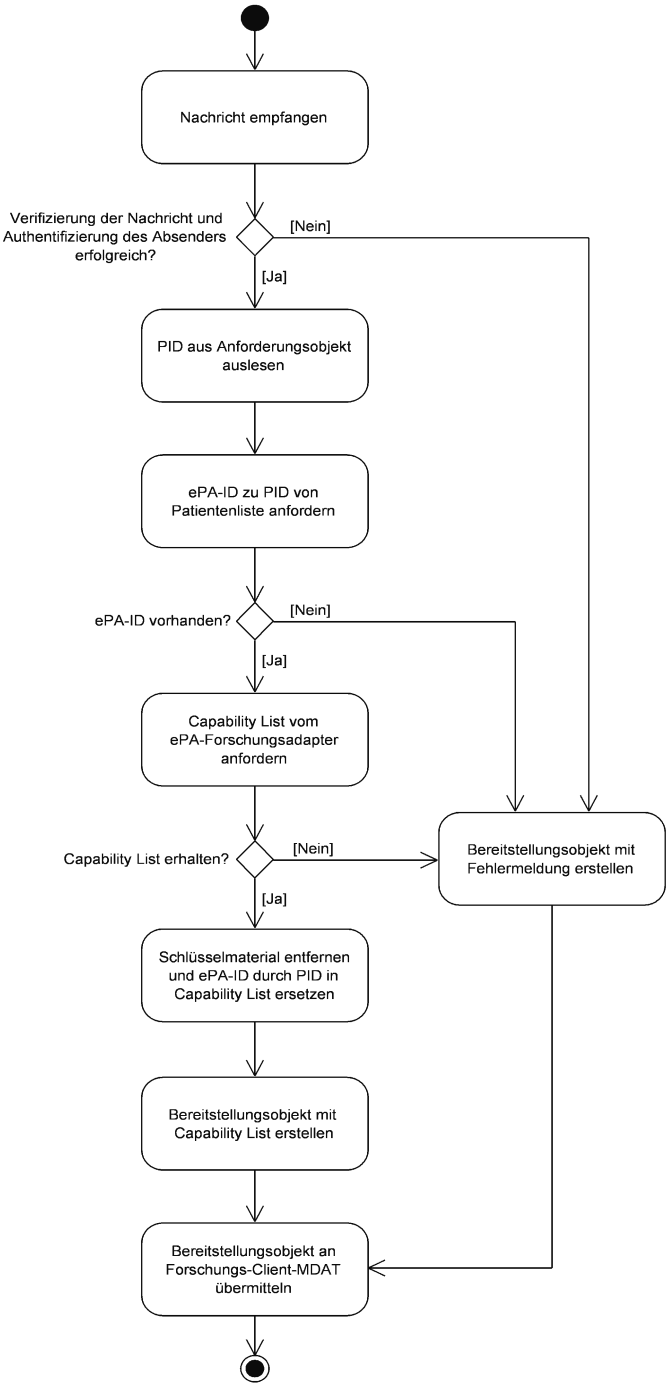

Abbildung 64: Anfordern der Capability List durch den Forschungs-Client-MDAT

A4.4.2. Kommunikation mit dem ePA-Forschungsadapter

Bei der Kommunikation mit dem ePA-Forschungsadapter tritt der Forschungs-Client-IDAT als Dienstnutzer auf, indem er die Operationen der Schnittstelle S2 aufruft. Im Abschnitt 8.5.1 wurden folgende Aufrufe der Operationen der Schnittstelle S2 durch den Forschungs-Clients-IDAT identifiziert:

- **Anfordern der Capability List durch den Forschungs-Client-IDAT:**
  RLUS-List(Parameter): Capability List
- **Zustellung eines Informationsobjektes durch den IDAT-Verwalter:**
  RLUS-Put(IO)
- **Anfordern von Informationsobjekten durch den IDAT-Verwalter:**
  RLUS-List(Parameter): IO
- **Anfordern von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-List(Parameter): SemSigGetTID
- **Anfordern von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-List(Parameter): SemSigGetePA-ID
- **Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-Put(SemSigGetTID):
- **Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-Put(SemSigGetePA-ID):

Im Folgenden werden die Aktionen beschrieben und in einem Ablaufdiagramm dargestellt, die der Forschungs-Client-IDAT bei den oben genannten Operationen-Aufrufen durchführen muss.

A4.4.2.1. Anfordern der Capability List durch den Forschungs-Client-IDAT: RLUS-List(Parameter): Capability List

Vorbedingungen:

1. Die ePA-Adresse des Patienten ist bekannt.
2. Es gibt einen internen Operationsaufruf („Anfordern der Capability List durch den Forschungs-Client-MDAT“) oder es soll eine Anforderung oder Bereitstellung von der Patientenliste erfolgen.

Aufrufen der Operation:

1. Es wird ein Anforderungsobjekt zum Abrufen der Capability List erstellt und eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und dem Anforderungsobjekt im Body erstellt (Details siehe Abschnitt A4.3.1).Tritt ein Fehler auf, so wird die Operation abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 65).
2. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-IDAT eine Capability-List oder im Fehlerfall eine Fehlernachricht, die an die aufrufende Operation weitergeleitet wird.

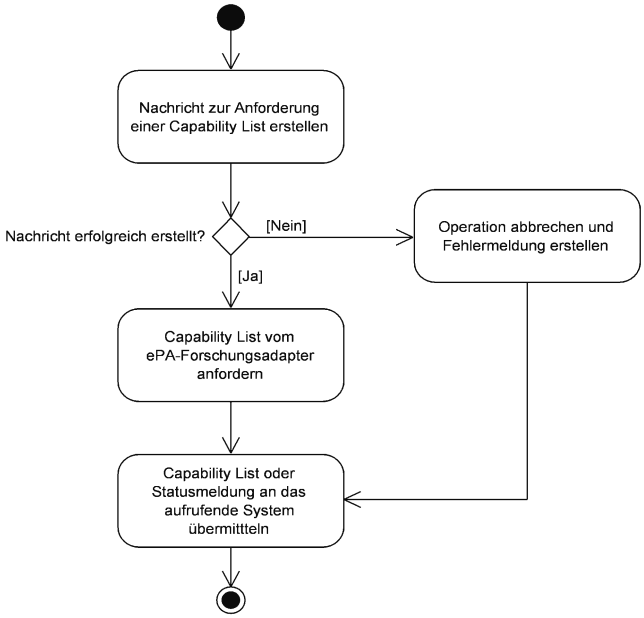

Abbildung 65: Anfordern der Capability List durch den Forschungs-Client-IDAT

A4.4.2.2. Zustellung eines Informationsobjektes durch den IDAT-Verwalter: RLUS-Put(IO)

Vorbedingungen:

1. Die Patientenliste hat eine Anforderung bzw. Bereitstellung für einen Patienten und seine PID an den Forschungs-Client-IDAT übergeben.
2. Es wurde eine Capability List angefordert und überprüft, ob die ePA das Kommunikationsmuster und den Semantic Signifier unterstützt.
3. Es wurde vom Forschungs-Client-IDAT überprüft, ob eine Einwilligung des Patienten für diese Kommunikation vorliegt und die Kommunikation den Regeln des Forschungsverbundes entspricht (Sicherheitsarchitektur der Forschungsschnittstelle).
4. Im Falle einer Bereitstellung wurde der öffentliche Schlüssel der ePA aus der Capability List extrahiert und die bereitzustellenden Informationen mit Hilfe des Schlüsselmaterials verschlüsselt.

Aufrufen der Operation:

1. Es wird ein Informationsobjekt erstellt und eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und dem Informationsobjekt im Body erstellt (Details siehe Abschnitt A4.3.1). Tritt bei diesem Schritt ein Fehler auf, so wird die Operation abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 66).
2. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-IDAT eine Erfolgs- oder eine Fehlermeldung.
3. Abschließend wird eine Statusmeldung an die Patientenliste weitergeleitet.

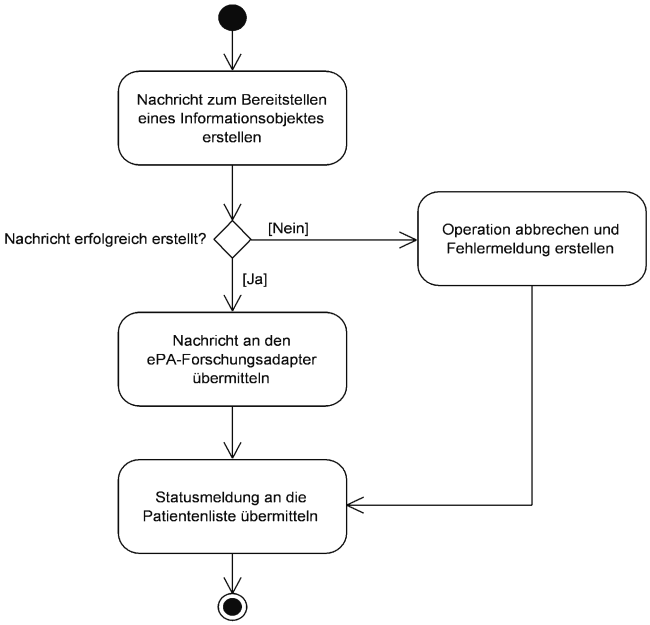

Abbildung 66: Zustellung eines Informationsobjektes durch den IDAT-Verwalter

A4.4.2.3. Anfordern von Informationsobjekten durch den IDAT-Verwalter: RLUS-List(Parameter): IO

Vorbedingungen: Die zum Entschlüsseln der durch den Patienten bereitgestellten Daten benötigten Schlüssel sind vorhanden (siehe Sicherheitsarchitektur der LE-Schnittstelle).

Aufrufen der Operation:

1. Es wird ein Anforderungsobjekt zum Abrufen der Informationsobjekte erstellt und eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und dem Anforderungsobjekt im Body erstellt (Details siehe Abschnitt A4.3.1). Sollte hierbei ein Fehler auftreten, so wird die Operation abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 67).
2. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-IDAT eine Fehlermeldung oder ein bzw. mehrere Informationsobjekte (diese werden dann zwischengespeichert und hintereinander abgearbeitet). Ist es eine Fehlermeldung, so wird mit Schritt 6 fortgefahren. Ansonsten wird mit Schritt 3 fortgefahren.
3. Es wird eine Autorisierung durch den Forschungs-Client-IDAT durchgeführt (siehe Sicherheitsarchitektur der Forschungsschnittstelle). Schlägt die Autorisierung fehl, so wird mit Schritt 5 fortgefahren, ansonsten mit Schritt 4.
4. Es wird überprüft, ob das Informationsobjekt ein Bereitstellungs- oder ein Anforderungsobjekt ist. Bei einem Bereitstellungsobjekt wird die verschlüsselte Nutzlast mit dem entsprechenden Schlüsselmaterial entschlüsselt und an die Patientenliste übergeben. Bei einem Anforderungsobjekt wird die enthaltene Anforderung an die Patientenliste übermittelt.
5. Es wird der Zwischenspeicher des Forschungs-Client-IDAT überprüft. Sind weitere Informationsobjekte vorhanden, so werden die Schritte 3-5 wiederholt. Ansonsten wird mit Schritt 6 fortgefahren.
6. Am Ende wird eine Statusmeldung an die Patientenliste übermittelt.

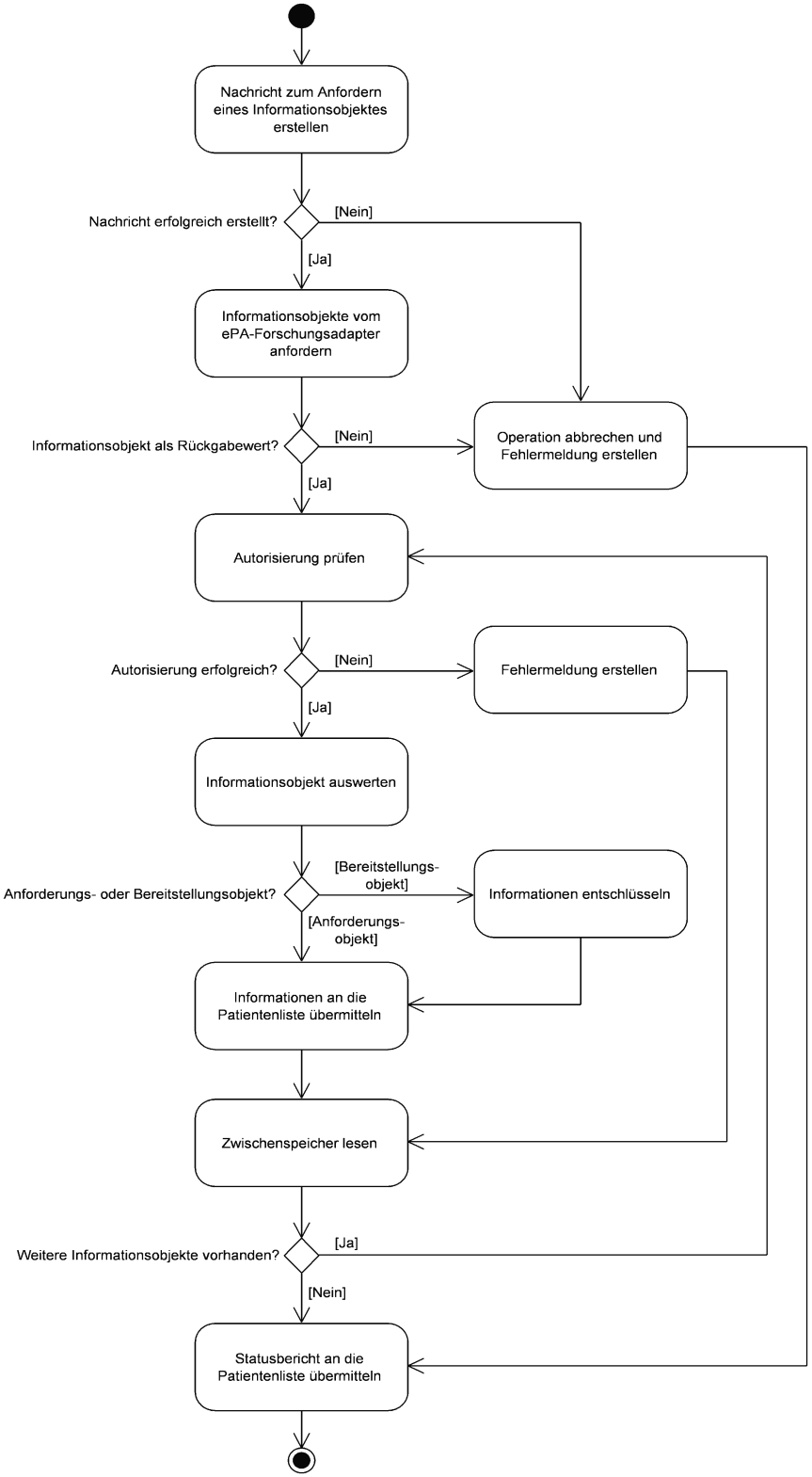

Abbildung 67: Anfordern von Informationsobjekten durch den IDAT-Verwalter

A4.4.2.4. Abrufen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-List(Parameter): SemSigGetTID

Voraussetzungen: Keine.

Aufrufen der Operation:

1. Es wird ein Anforderungsobjekt zum Abrufen von Pseudonymisierungs-Anfragen erstellt und eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und der RLUS-Nachricht im Body erstellt (Details siehe Abschnitt A4.3.1). Tritt ein Fehler auf, so wird die Operation mit einer Fehlermeldung abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 68).
2. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-IDAT eine Fehlermeldung oder kein, ein bzw. mehrere Anforderungsobjekte. Bekommt der Forschungs-Client-IDAT eine Fehlermeldung oder kein Anforderungsobjekt, so wird die Operation abgebrochen und eine Statusmeldung an die Patientenliste zurückgegeben. Andernfalls werden für jedes Objekt die Schritte 3 und 4 durchgeführt.
3. Wird eine TID angefordert, so muss zunächst eine Autorisierung stattfinden, ob die geplante Anforderung bzw. Bereitstellung durch die Einwilligung des Patienten und die Regeln des Forschungsverbundes abgedeckt ist (siehe Sicherheitsarchitektur der Forschungsschnittstelle). Ist die Autorisierung erfolgreich, so wird eine TID erzeugt, mit der ePA-ID aus der Nutzlast des Anforderungsobjektes im Forschungs-Client-IDAT zwischengespeichert und ein Bereitstellungobjekt mit der TID und der ePA-ID für den ePA-Forschungsadapter erstellt. Ist die Autorisierung nicht erfolgreich, so wird ein Bereitstellungsobjekt mit einer Fehlermeldung erstellt.
4. Im nächsten Schritt wird das Bereitstellungsobjekt an den ePA-Forschungsadapter übermittelt (siehe Operation Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-PUT(SemSigGetTID)).
5. Es wird überprüft, ob weitere Anforderungsobjekte vorhanden sind. Ist dies der Fall, so werden die Schritte 3 und 4 wiederholt. Ansonsten wird mit Schritt 6 fortgefahren.
6. Abschließend wird eine Statusmeldung an die Patientenliste zurückgegeben.

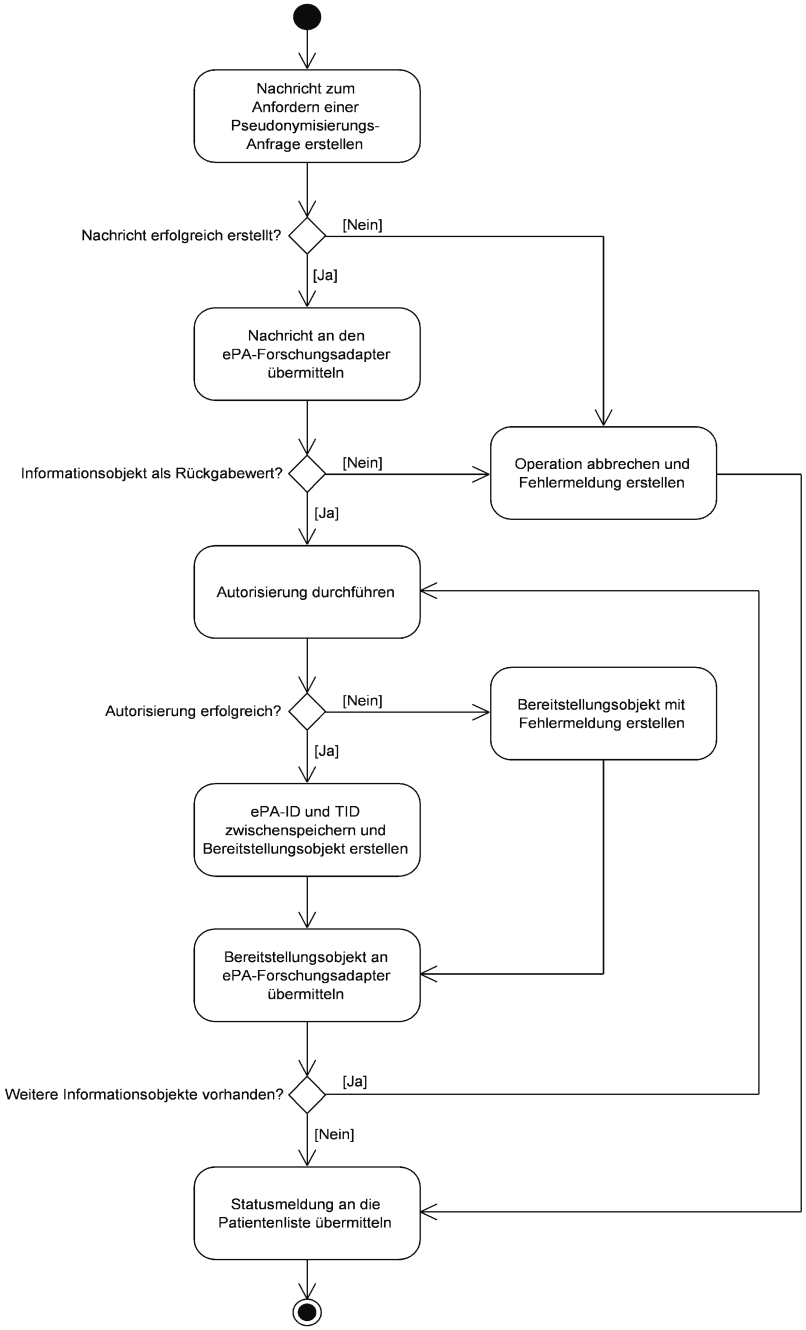

Abbildung 68: Abrufen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT

A4.4.2.5. Abrufen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-List(Parameter): SemSigGetePA-ID

Voraussetzungen: Es wurde eine TID vom Forschungs-Client-IDAT erstellt und an den Forschungs-Client-MDAT geschickt.

Aufrufen der Operation:

1. Es wird eine RLUS-List-Nachricht zum Abrufen von Depseudonymisierungs-Anfrage erstellt und eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und der RLUS-Nachricht im Body generiert (Details siehe Abschnitt A4.3.1). Tritt dabei ein Fehler auf, so wird die Operation mit einer Fehlermeldung abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 69).
2. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-IDAT eine Fehlermeldung oder kein, ein bzw. mehrere Anforderungsobjekte. Bekommt der Forschungs-Client-IDAT eine Fehlermeldung oder kein Anforderungsobjekt, so wird die Operation abgebrochen und eine Statusmeldung an die Patientenliste übermittelt. Andernfalls werden für jedes Objekt die Schritte 3 und 4 durchgeführt.
3. Zur Auflösung der TID in eine ePA-ID wird zu der TID die entsprechende PID aus dem Zwischenspeicher des Forschungs-Clients-IDAT ausgelesen. Sollte sich kein Eintrag zu der TID im Zwischenspeicher befinden, so wird ein Bereitstellungobjekt mit der Fehlermeldung erstellt und mit Schritt 5 fortgefahren. Ansonsten wird zu der PID die entsprechende ePA-ID von der Patientenliste angefordert (Proprietäre Schnittstelle je nach Anbieter).
4. Im nächsten Schritt wird die Antwort der Patientenliste ausgewertet. Enthält die Antwort von der Patientenliste eine Fehlermeldung, so wird ein Bereitstellungsobjekt mit der Fehlermeldung erstellt und mit Schritt 5 fortgefahren. Enthält die Antwort eine ePA-ID, so wird ein Bereitstellungsobjekt mit der ePA-ID erstellt.
5. Im nächsten Schritt wird das Bereitstellungsobjekt an den ePA-Forschungsadapter übermittelt (siehe Operation Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-Put(SemSigGetePA-ID) und überprüft, ob weitere Anforderungsobjekte abgearbeitet werden müssen. Ist dies der Fall, so werden die Schritte 3-5 wiederholt. Ansonsten wird mit Schritt 6 fortgefahren.
6. Abschließend wird eine Statusmeldung an die Patientenliste übermittelt.

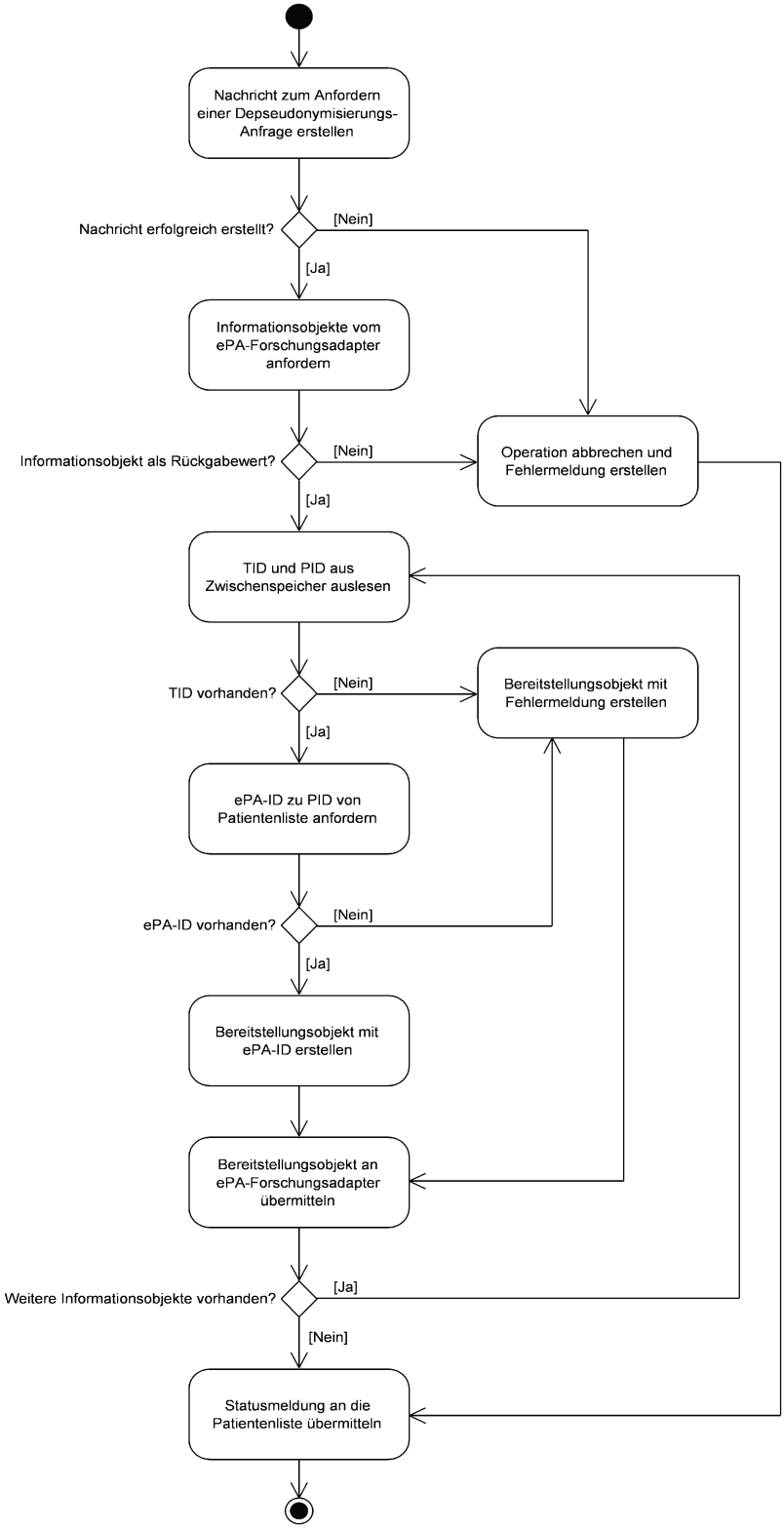

Abbildung 69: Abrufen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT

A4.4.2.6. Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-PUT(SemSigGetTID)

Vorbedingung:

Es liegt ein Bereitstellungsobjekt mit der Antwort oder einer Fehlermeldung auf eine Pseudonymisierungs-Anfrage des ePA-Forschungsadapters vor.

Aufrufen der Operation:

Der Ablauf entspricht dem des Operationsaufrufes „Zustellung eines Informationsobjektes durch den IDAT-Verwalter: RLUS-Put(IO)“. Das Informationsobjekt ist in diesem Fall ein Bereitstellungsobjekt mit einer TID.

A4.4.2.7. Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-Put(SemSigGetePA-ID)

Vorbedingung:

Es liegt ein Bereitstellungsobjekt mit der Antwort oder einer Fehlermeldung auf eine Depseudonymisierungs-Anfrage vor.

Aufrufen der Operation:

Der Ablauf entspricht dem des Operationsaufrufes „Zustellung eines Informationsobjektes durch den IDAT-Verwalter: RLUS-Put(IO)“. Das Informationsobjekt ist in diesem Fall ein Bereitstellungsobjekt mit einer ePA-ID.

A4.4.3. Module des Forschungs-Client-IDAT

Der Forschungs-Client-IDAT benötigt folgende Module um die oben beschriebenen Operationen durchführen zu können:

- Das **Authentifizierungsmodul** ermöglicht das Abrufen eines Authentifizierungsnachweises von einem externen Identity Provider.
- Der **Kommunikationsdienst** stellt dem Forschungs-Client-MDAT die folgenden Operationen zur Verfügung:
  - RLUS-List(Parameter):SemSigGetPID,
  - RLUS-List(Parameter):SemSigGetTID,
  - RLUS-List(Parameter): Capability List
- Das **Kommunikationsmodul** des Forschungs-Client-IDAT ermöglicht die Kommunikation mit der Patientenliste. Mit Hilfe dieses Moduls werden Informationen (z. B. die Kontaktdaten des Patienten) an die Patientenliste übergeben bzw. von der Patientenliste angenommen. Über dieses Modul werden auch die PIDs bzw. ePA-ID von der Patientenliste angefragt.
- Der **Kommunikations-Client** ermöglicht die Kommunikation mit dem ePA-Forschungsadapter. Er ruft die folgenden Operationen des ePA-Forschungsadapters auf:
  - RLUS-List(Parameter): Capability List,
  - RLUS-Put(IO), RLUS-List(Parameter): IO,
  - RLUS-List(Parameter): SemSigGetTID,
  - RLUS-List(Parameter): SemSigGetePA-ID,
  - RLUS-Put(SemSigGetTID),
  - RLUS-Put(SemSigGetePA-ID)
- Das **Nachrichtenmodul** und das **Verifikationsmodul** führen die Erstellung und Verifikation der Nachrichten durch. Diese Module haben die gleichen Funktionen wie die des ePA-LE-Clients [144].

A4.5. Forschungs-Client-MDAT

Der Forschungs-Client-MDAT ist sowohl Dienstnutzer gegenüber dem ePA-Forschungsadapter (Schnittstelle S3) als auch gegenüber dem Forschungs-Client-IDAT (Schnittstelle S1). Als Dienstanbieter tritt er nicht auf (siehe Abbildung 25). Im Folgenden wird das Verhalten des Forschungs-Client-MDAT beim Aufrufen der Operationen der oben genannten Schnittstellen beschrieben.

A4.5.1. Kommunikation mit dem Forschungs-Client-IDAT

Gegenüber dem Forschungs-Client-IDAT tritt der Forschungs-Client-MDAT als Dienstnutzer auf, indem er die Operationen der Schnittstelle S1 aufruft. Im Abschnitt 8.3 wurden folgende Aufrufe der Operationen der Schnittstelle S1 durch den Forschungs-Clients-MDAT identifiziert:

- **Anfordern einer PID durch den Forschungs-Client-MDAT:**
  RLUS-List(Parameter):SemSigGetPID
- **Anfordern einer TID durch den Forschungs-Client-MDAT:**
  RLUS-List(Parameter):SemSigGetTID
- **Anfordern der Capability List durch den Forschungs-Client-MDAT:**
  RLUS-List(Parameter): Capability List

Im Folgenden werden die einzelnen Aktionen des Forschungs-Client-MDAT beim Aufrufen der Operationen beschrieben.

A4.5.1.1. Anfordern einer PID durch den Forschungs-Client-MDAT: RLUS-List(Parameter):SemSigGetPID

Vorbedingungen:

1. Der Forschungs-Client-MDAT hat ein Informationsobjekt mit einer TID vom ePA-Forschungsadapter abgerufen.
2. Bei einem Bereitstellungsobjekt wurde das entsprechende Schlüsselmaterial zur Entschlüsselung der Nutzlast von der ePA abgerufen.

Aufruf der Operation:

1. Es wird eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und einem Anforderungsobjekt mit dem Semantic Signifier SemSigGetPID und der TID als Nutzlast im SOAP-Body erstellt (siehe Abschnitt A4.3.1). Tritt ein Fehler auf, so wird die Operation mit einer Fehlermeldung abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 70).
2. Die SOAP-Nachricht wird an den Forschungs-Client-IDAT übermittelt. Als Rückgabewert erhält der Forschungs-Client-MDAT ein Bereitstellungsobjekt mit einer PID zur angeforderten TID oder eine Fehlermeldung.
3. Ist der Rückgabewert eine Fehlermeldung, wird das Informationsobjekt verworfen und die Fehlermeldung an die medizinische Datenbank weitergeleitet. Ist die Antwort eine PID, so wird diese durch die TID im Informationsobjekt (was vom ePA-Forschungsadapter abgerufen wurde) ersetzt.
4. Ist das Informationsobjekt ein Anforderungsobjekt, so wird die Anforderung mit der PID an die medizinische Datenbank des Forschungsverbundes weitergeleitet. Ist das Infor-

mationsobjekt ein Bereitstellungsobjekt, so wird die Nutzlast des Informationsobjektes mit dem mitgeschickten Schlüsselmaterial entschlüsselt (siehe Sicherheitsarchitektur der Forschungsschnittstelle) und das Ergebnis der Entschlüsselung mit der PID an die medizinische Datenbank des Forschungsverbundes weitergeleitet.

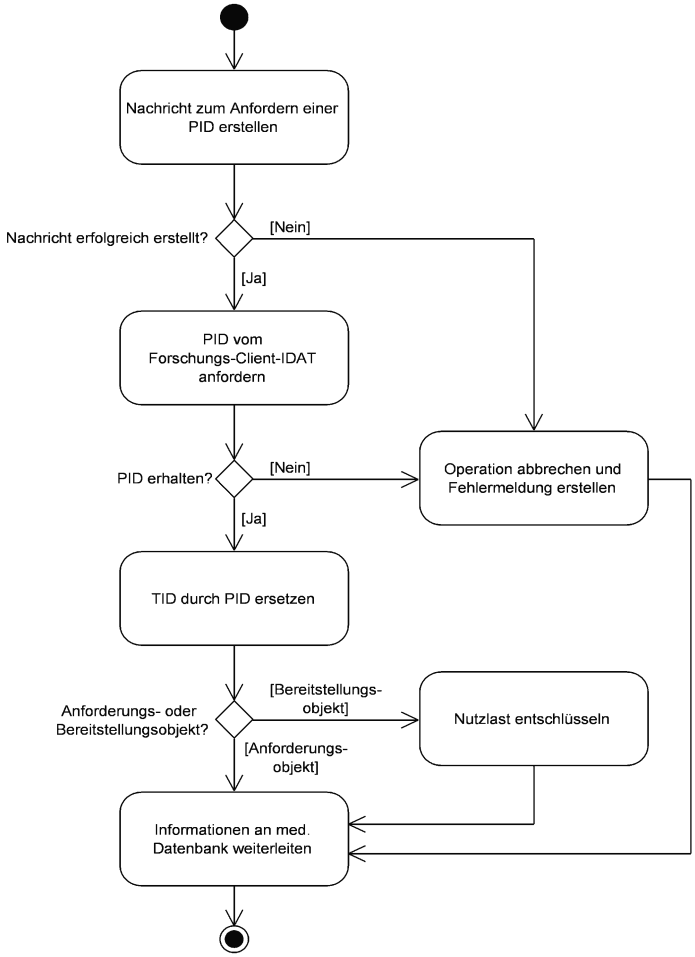

Abbildung 70: Anfordern einer PID durch den Forschungs-Client-MDAT

A4.5.1.2. Anfordern einer TID durch den Forschungs-Client-MDAT: RLUS-List(Parameter):SemSigGetPID

Vorbedingung: Die medizinische Datenbank hat Informationen an den Forschungs-Client-MDAT geschickt, die jetzt an die ePA eines Patienten (entsprechend der mitgelieferten PID) gesendet werden sollen.

Aufruf der Operation:

1. Es wird eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und Anforderungsobjekt mit dem Semantic Signifier SemSigGetTID und der PID als Nutzlast im SOAP-Body erstellt (siehe Abschnitt A4.3.1). Tritt ein Fehler auf, so wird die Operation mit einer Fehlermeldung abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 71).
2. Die SOAP-Nachricht wird an den Forschungs-Client-IDAT übermittelt. Als Rückgabewert erhält der Forschungs-Client-MDAT ein Bereitstellungsobjekt mit einer TID zur angeforderten PID oder eine Fehlermeldung.
3. Ist der Rückgabewert eine Fehlermeldung, wird die Operation abgebrochen und die Fehlermeldung an die medizinische Datenbank weitergeleitet. Ist die Antwort eine TID, so wird mit der TID und den durch die medizinische Datenbank bereitgestellten Informationen ein Informationsobjekt erstellt.
4. Anschließend wird das Informationsobjekt über den Operationsaufruf „Zustellung eines Informationsobjektes durch den MDAT-Verwalter: RLUS-Put(IO)“ an den ePA-Forschungsadapter übermittelt.
5. Abschließend wird eine Statusmeldung an die medizinische Datenbank des Forschungsverbundes übermittelt.

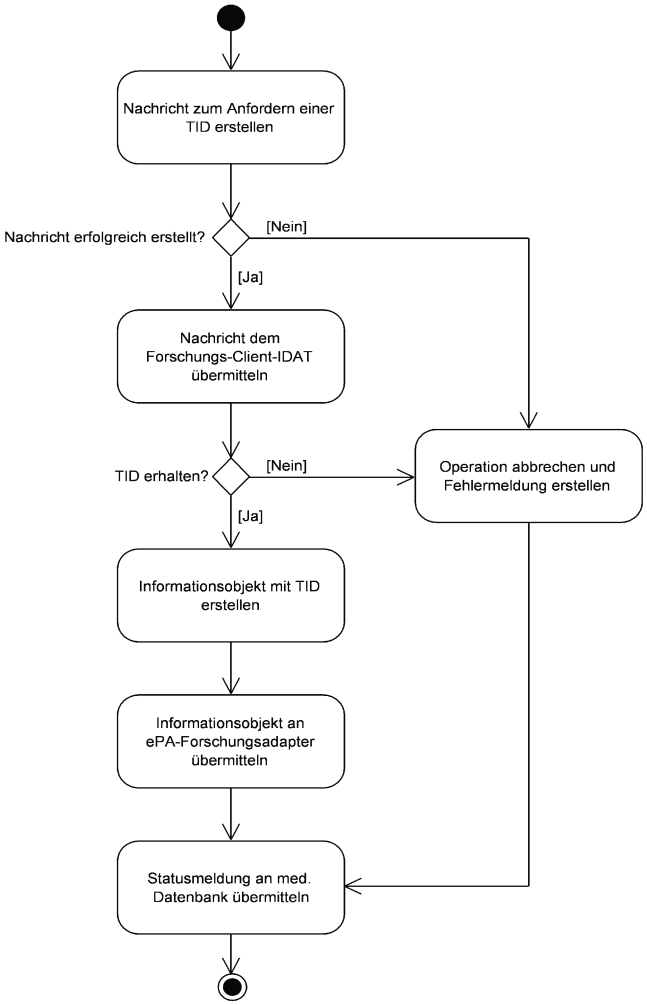

Abbildung 71: Anfordern einer TID durch den Forschungs-Client-MDAT

A4.5.1.3. Anfordern der Capability List durch den Forschungs-Client-MDAT: RLUS-List(Parameter): Capability List

Vorbedingung: Es liegt eine Information (Anforderung oder Bereitstellung) von der medizinischen Datenbank für einen Patienten und die PID des Patienten vor.

Aufruf der Operation:

1. Es wird eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und einem Anforderungsobjekt mit dem Semantic Signifier Capability List und der PID als Nutzlast SOAP-Body erstellt (siehe Abschnitt A4.3.1).Tritt ein Fehler auf, so wird die Operation abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 72).
2. Die SOAP-Nachricht wird an den Forschungs-Client-IDAT übermittelt. Als Rückgabewert erhält der Forschungs-Client-MDAT ein Bereitstellungsobjekt mit einer Capability List der ePA des Patienten zu der PID oder eine Fehlermeldung.
3. Die Capability List wird vom Forschungs-Client-MDAT ausgewertet.
4. Der aufrufenden Operation wird das Ergebnis der Auswertung oder eine Fehlermeldung zurückgegeben.

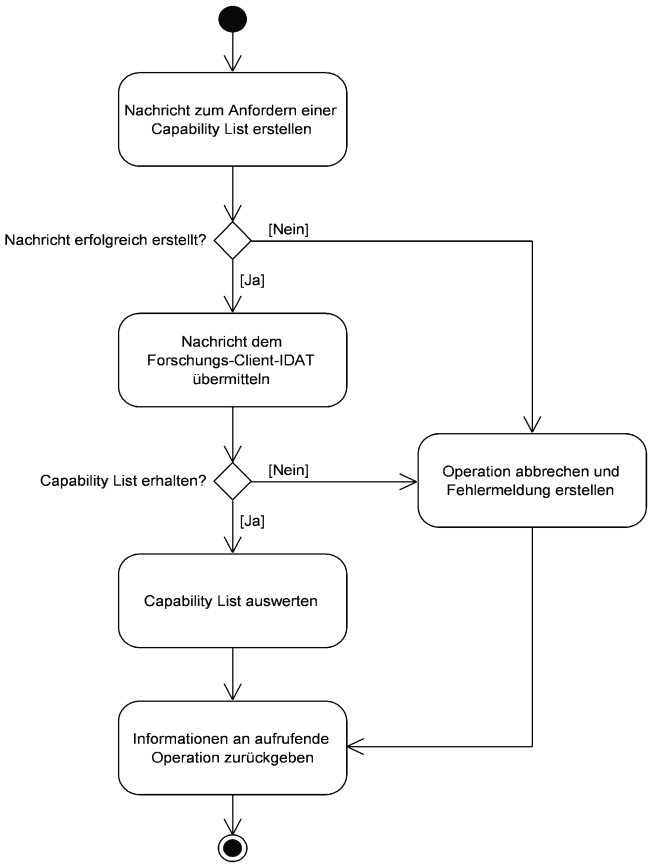

Abbildung 72: Anfordern der Capability List durch den Forschungs-Client-MDAT

A4.5.2. Kommunikation mit dem ePA-Forschungsadapter

Bei der Kommunikation mit dem ePA-Forschungsadapter tritt der Forschungs-Client-MDAT als Dienstnutzer auf, indem er die Operationen der Schnittstelle S3 aufruft. Im Abschnitt 8.5.2 wurden folgende Operationsaufrufe des Forschungs-Clients-MDAT identifiziert:

- **Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA:**
  RLUS-List(Parameter): symkeyMDO
- **Zustellung eines Informationsobjektes durch den MDAT-Verwalter:**
  RLUS-Put(IO)
- **Anfordern von Informationsobjekten durch den MDAT-Verwalter:**
  RLUS-List(Parameter): IO

Im Folgenden werden die einzelnen Aktionen des Forschungs-Client-MDAT beim Aufrufen der Operationen beschrieben.

A4.5.2.1. Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA: RLUS-List(Parameter): symkeyMDO

Vorbedingungen:

1. Es liegt eine Bereitstellung von der medizinischen Datenbank des Forschungsverbundes für die ePA eines Patienten vor.
2. Es wurde eine Capability List angefordert und überprüft, ob die ePA das Kommunikationsmuster und den Semantic Signifier unterstützt (Aufruf der Operation Anfordern der Capability List durch den Forschungs-Client-MDAT).
3. Es wurde eine TID vom Forschungs-Client-IDAT für die PID des Patienten angefordert (Aufruf der Operation „Anfordern einer TID durch den Forschungs-Client-MDAT“).
4. Das Zertifikat des ePA-Forschungsadapters zur Signaturprüfung liegt dem Forschungs-Client-MDAT vor.

Aufruf der Operation:

1. Es wird ein Anforderungsobjekt mit dem Semantic Signifier symkeyMDO und der von Forschungs-Client-IDAT angeforderten TID erstellt und eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und dem Anforderungsobjekt im Body erstellt (Details siehe A4.3.1). Tritt ein Fehler auf, so wird die Operation mit einer entsprechenden Fehlermeldung abgebrochen. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 73).
2. Der Forschungs-Client-MDAT speichert die PID des Patienten, die angeforderte TID und die Anforderungsobjekt-ID des Anforderungsobjektes, welches er gerade erstellt hat, zwischen.
3. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-MDAT eine Fehlermeldung oder ein Bereitstellungsobjekt mit einem symmetrischen Schlüssel. Erhält er eine Fehlermeldung, so wird mit Schritt 9 fortgefahren.
4. Der Forschungs-Client-MDAT liest die TID aus dem Bereitstellungsobjekt aus und ruft die Informationen zu der TID aus dem Zwischenspeicher auf. Befindet sich kein Eintrag

im Zwischenspeicher, so wird eine Fehlermeldung erstellt und mit Schritt 9 fortgefahren. Ansonsten wird mit Schritt 5 fortgefahren.

5. Der Forschungs-Client-MDAT überprüft die Signatur des Schlüssels mit dem öffentlichen Schlüssel des ePA-Forschungsadapters. Ist die Prüfung der Signatur erfolgreich, so wird mit Schritt 6 fortgefahren. Ansonsten wird eine Fehlermeldung erstellt und mit Schritt 9 fortgefahren.
6. Der Forschungs-Client-MDAT entschlüsselt mit seinem privaten Schlüssel den symmetrischen Schlüssel (symKeyMDO) und verschlüsselt die Informationen aus der medizinischen Datenbank des Forschungsverbundes mit dem Ergebnis dieser Entschlüsselung (symmetrischer Schlüssel aus der ePA).
7. Der Forschungs-Client-MDAT erstellt ein Bereitstellungsobjekt mit der verschlüsselten Nutzlast und Anforderungsobjekt-ID.
8. Danach werden das vorhandene Schlüsselmaterial (symKeyMDO und der mit dem öffentlichen Schlüssel der medizinischen Datenbank des Forschungsverbundes gesicherte symKeyMDO) und die genutzten Informationen aus dem Zwischenspeicher gelöscht.
9. Abschließend werden eine Statusmeldung oder die verschlüsselten Informationen an die aufrufende Operation zurückgegeben.

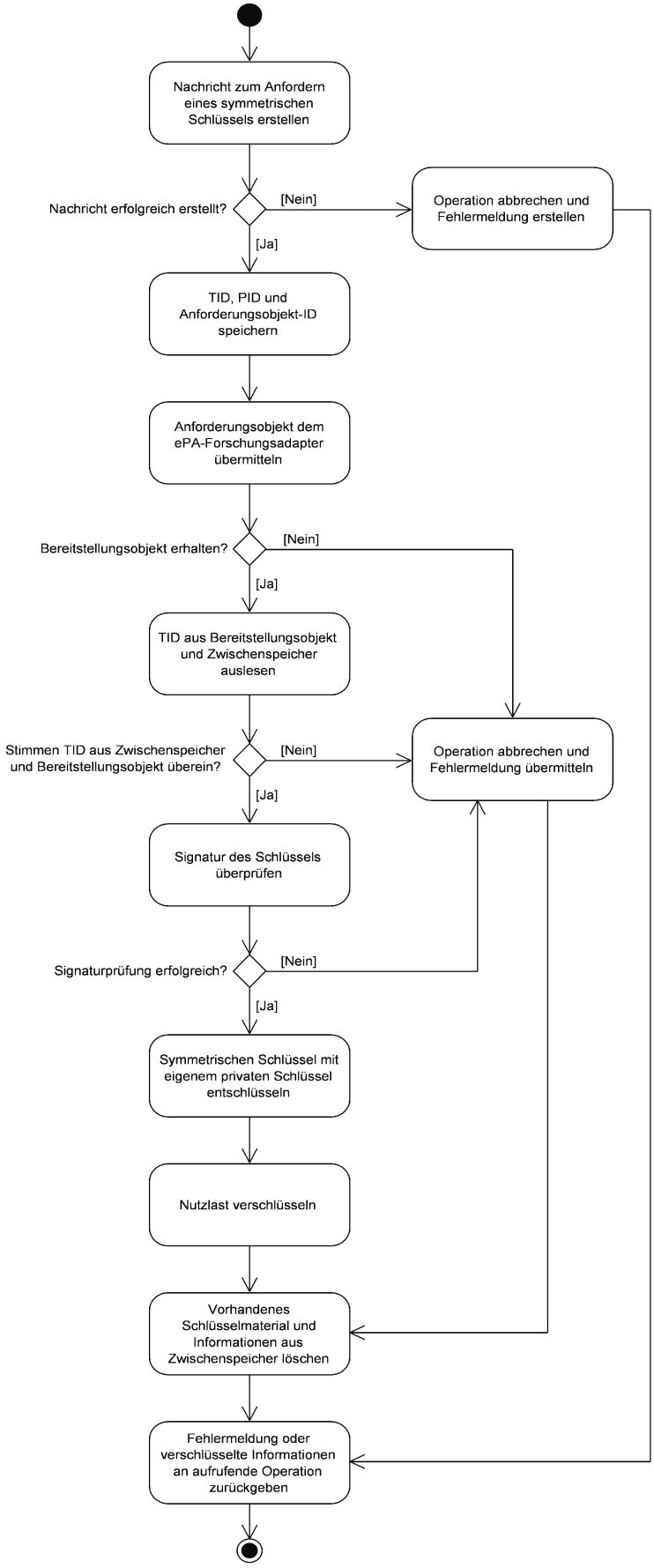

Abbildung 73: Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA

A4.5.2.2. Zustellung eines Informationsobjektes durch den MDAT-Verwalter: RLUS-Put(IO)

Vorbedingungen:

1. Es wurde eine Capability List angefordert und überprüft, ob die ePA das Kommunikationsmuster und den Semantic Signifier unterstützt (Aufruf der Operation „Anfordern der Capability List durch den Forschungs-Client-MDAT“).
2. Es wurde eine TID vom Forschungs-Client-IDAT für die PID des Patienten angefordert (Aufruf der Operation „Anfordern einer TID durch den Forschungs-Client-MDAT“).
3. Im Falle einer Bereitstellung wurde ein symmetrischer Schlüssel zum Verschlüsseln der Nutzlast angefordert (Aufruf der Operation „Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA“) bzw. mit einer Anforderung von der ePA mitgeschickt und die Nutzlast damit verschlüsselt (siehe Sicherheitsarchitektur der Forschungsschnittstelle).

Aufrufen der Operation:

Der Ablauf entspricht dem des Operationsaufrufes „Zustellung eines Informationsobjektes durch den IDAT-Verwalter: RLUS-Put(IO)“(siehe Abbildung 66) und wird daher nicht nochmal beschrieben.

A4.5.2.3. Anfordern von Informationsobjekten durch den MDAT-Verwalter: RLUS-List(Parameter): IO

Vorbedingung: Die zum Entschlüsseln der durch den Patienten bereitgestellten Daten benötigten Schlüssel sind vorhanden (siehe Sicherheitsarchitektur der LE-Schnittstelle).

Aufrufen der Operation:

1. Es wird eine SOAP-Nachricht mit dem Authentifizierungsnachweis im Header und einem Anforderungsobjekt im Body erstellt (Details siehe A4.3.1). Tritt ein Fehler auf, so wird die Operation mit einer Fehlermeldung abgebrochen. Ansonsten wird die Operation fortgeführt (siehe auch Abbildung 74).
2. Die SOAP-Nachricht wird an den ePA-Forschungsadapter übermittelt. Als Rückgabewert erhält der Forschungs-Client-MDAT eine Fehlermeldung oder ein oder mehrere Informationsobjekte. Ist der Rückgabewert eine Fehlermeldung, so wird diese an die medizinische Datenbank übermittelt und die Operation abgebrochen. Ist der Rückgabewert ein Informationsobjekt, so wird mit Schritt 3 und 4 fortgefahren. Werden mehrere Informationsobjekte zurückgegeben, so werden diese zwischengespeichert und Schritt 3 und 4 für jedes Informationsobjekt wiederholt.
3. Der Forschungs-Client-MDAT liest die TID aus dem Informationsobjekt aus und fordert eine PID beim Forschungs-Client-IDAT an (siehe Operationsaufruf: Anfordern einer PID durch den Forschungs-Client-MDAT: RLUS-List(Parameter):SemSigGetPID). Ist der Rückgabewert eine Fehlermeldung, so wird diese im Rahmen der Statusmeldung an die medizinische Datenbank übermittelt und mit Schritt 5 weitergemacht. Ist der Rückgabewert die PID, so wird die TID im Informationsobjekt durch die PID ersetzt und Schritt 4 ausgeführt.
4. Enthalten die Informationsobjekte verschlüsselte Nutzlast, so wird diese mit dem entsprechenden Schlüsselmaterial entschlüsselt (siehe Sicherheitsarchitektur der LE-

Schnittstelle) und der medizinischen Datenbank mit der entsprechenden PID übergeben. Enthalten die Informationsobjekte Anforderungen, so wird das im Anforderungsobjekt enthaltene Schlüsselmaterial zwischengespeichert (siehe Sicherheitsarchitektur der Forschungsschnittstelle) und die Anforderung an die medizinische Datenbank mit der entsprechenden PID weitergereicht.

5. Anschließend wird überprüft, ob weitere Informationsobjekte im Zwischenspeicher vorliegen. Ist dies der Fall, so wird Schritt 3 wiederholt. Ansonsten wird die Operation beendet und ein Status an die aufrufende Komponente zurückgegeben.

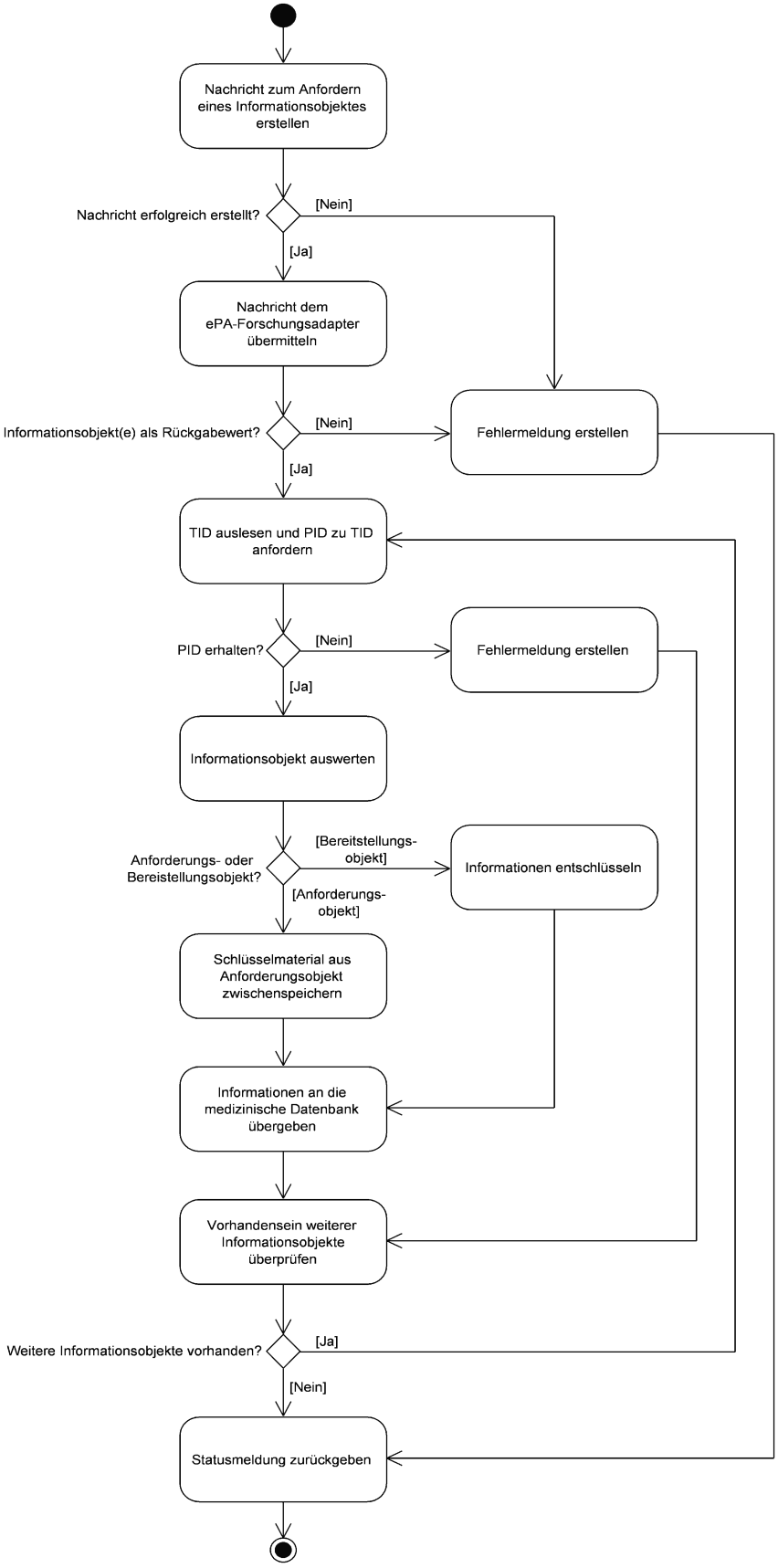

Abbildung 74: Anfordern von Informationsobjekten durch den MDAT-Verwalter

A4.5.3. Module des Forschungs-Client-MDAT

Der Forschungs-Client-MDAT benötigt folgende Module um die oben beschriebenen Operationen durchführen zu können:

- Das **Authentifizierungsmodul** ermöglicht das Abrufen eines Authentifizierungsnachweises von einem externen Identity Provider.
- Das **Kommunikationsmodul** für die medizinische Datenbank ermöglicht die Kommunikation mit der medizinischen Datenbank. Mit Hilfe dieses Moduls werden Informationen (z. B. medizinische Informationen) an die medizinische Datenbank übergeben bzw. von der medizinischen Datenbank angenommen.
- Der **Kommunikations-Client** ermöglicht die Kommunikation mit dem ePA-Forschungsadapter und dem Forschungs-Client-IDAT. Er ruft die folgenden Operationen des Forschungs-Clients-IDAT auf:
  - RLUS-List(Parameter):SemSigGetPID,
  - RLUS-List(Parameter):SemSigGetTID,
  - RLUS-List(Parameter): Capability List.

  Zusätzlich ruft er die folgenden Operationen des ePA-Forschungsadapters auf:
  - RLUS-List(Parameter): symkeyMDO,
  - RLUS-Put(IO),
  - RLUS-List(Parameter): IO
- Das **Nachrichtenmodul** und das **Verifikationsmodul** führen die Erstellung und Verifikation der Nachrichten durch. Diese Module haben die gleichen Funktionen wie die des ePA-LE-Clients [144].

A4.6. ePA-Forschungsadapter

Wie in Abbildung 25 dargestellt, ist der ePA-Forschungsadapter Dienstnutzer gegenüber der ePA-Kommunikationskomponente (Schnittstelle S4) als auch Dienstanbieter gegenüber der ePA-Kommunikationskomponente (Schnittstelle S5), dem Forschungs-Client-IDAT (Schnittstelle S2) und -MDAT(Schnittstelle S3).

A4.6.1. Kommunikation mit dem Forschungs-Client-IDAT

Bei der Kommunikation mit dem Forschungs-Client-IDAT tritt der ePA-Forschungsadapter als Dienstanbieter auf. Er stellt die folgenden Operationen über die Schnittstelle S2 bereit (siehe auch Abschnitt 8.5.1):

- **Anfordern der Capability List durch den Forschungs-Client-IDAT:**
  RLUS-List(Parameter): Capability List
- **Zustellung eines Informationsobjektes durch den IDAT-Verwalter:**
  RLUS-Put(IO)
- **Anfordern von Informationsobjekten durch den IDAT-Verwalter:**
  RLUS-List(Parameter): IO
- **Anfordern von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-List(Parameter): SemSigGetTID
- **Anfordern von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-List(Parameter): SemSigGetePA-ID
- **Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-PUT(SemSigGetTID)
- **Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT:**
  RLUS-Put(SemSigGetePA-ID)

Im Folgenden wird das Verhalten des ePA-Forschungsadapters beim Aufruf der oben genannten Operationen beschrieben.

A4.6.1.1. Anfordern der Capability List durch den Forschungs-Client-IDAT: RLUS-List(Parameter): Capability List

Vorbedingung: Keine

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Bei Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe Abbildung 75).
2. Als nächstes wird die Capability List von der entsprechenden ePA-Kommunikationskomponente angefordert (siehe Operation „Anfordern der Capability List durch den ePA-Forschungsadapter: RLUS-List(Parameter): Capability List“) und die Antwort der ePA-Kommunikationskomponente ausgewertet. Ist ein Fehler aufgetreten, so wird dieser an den Forschungs-Client-IDAT weitergeleitet. Im Erfolgsfall wird die Capability List an den Forschungs-Client-IDAT zurückgegeben.

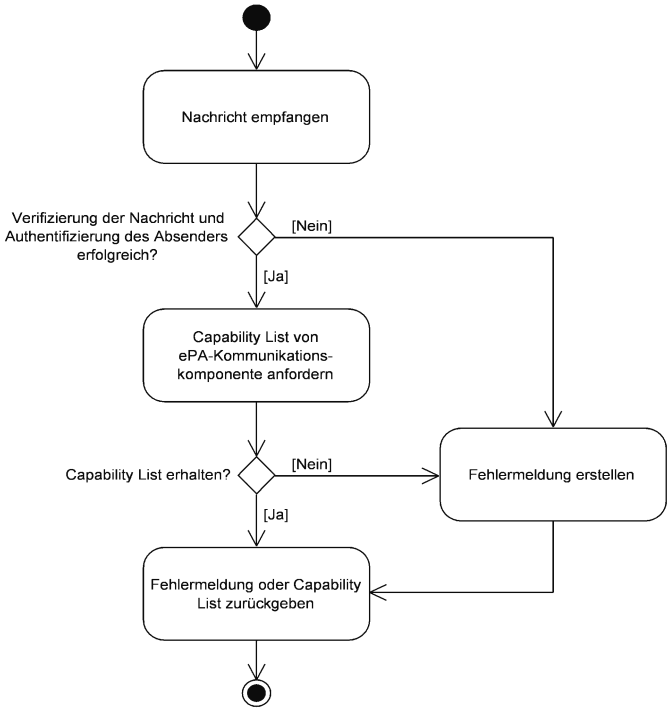

Abbildung 75: Anfordern der Capability List durch den Forschungs-Client-IDAT

A4.6.1.2. Zustellung eines Informationsobjektes durch den IDAT-Verwalter: RLUS-Put(IO)

Vorbedingung: Der ePA-Forschungsadapter hat ein Informationsobjekt vom Forschungs-Client-IDAT erfolgreich übertragen bekommen.

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Bei Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 76).
2. Der ePA-Forschungsadapter leitet das Informationsobjekt an die ePA-Kommunikationskomponente weiter (siehe Operationsaufruf „Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter: RLUS-Put(IO)“).
3. Im Erfolgsfall gibt der ePA-Forschungsadapter eine Meldung zurück, dass das Informationsobjekt weitergeleitet wurde. Im Fehlerfall gibt der ePA-Forschungsadapter eine entsprechende Fehlermeldung zurück.

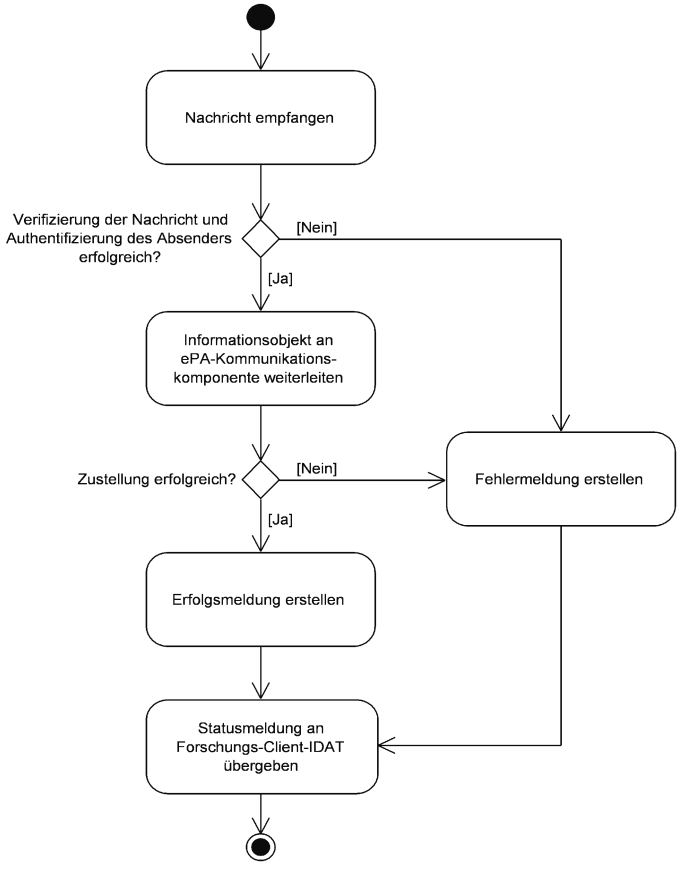

Abbildung 76: Zustellung eines Informationsobjektes durch den IDAT-Verwalter

A4.6.1.3. Anfordern von Informationsobjekten durch den IDAT-Verwalter: RLUS-List(Parameter): IO

Vorbedingung: Keine

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Beim Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 77).
2. Der ePA-Forschungsadapter liest die für den Forschungs-Client-IDAT gespeicherten Informationsobjekte aus dem entsprechenden Postfach aus.
3. Der ePA-Forschungsadapter gibt Forschungs-Client-IDAT als Rückgabewert eine Nachricht mit keinem, einem oder mehreren Informationsobjekten oder einer Fehlermeldung zurück.
4. Die an den Forschungs-Client-IDAT gesendeten Informationsobjekte werden aus dem Postfach des ePA-Forschungsadapters gelöscht.

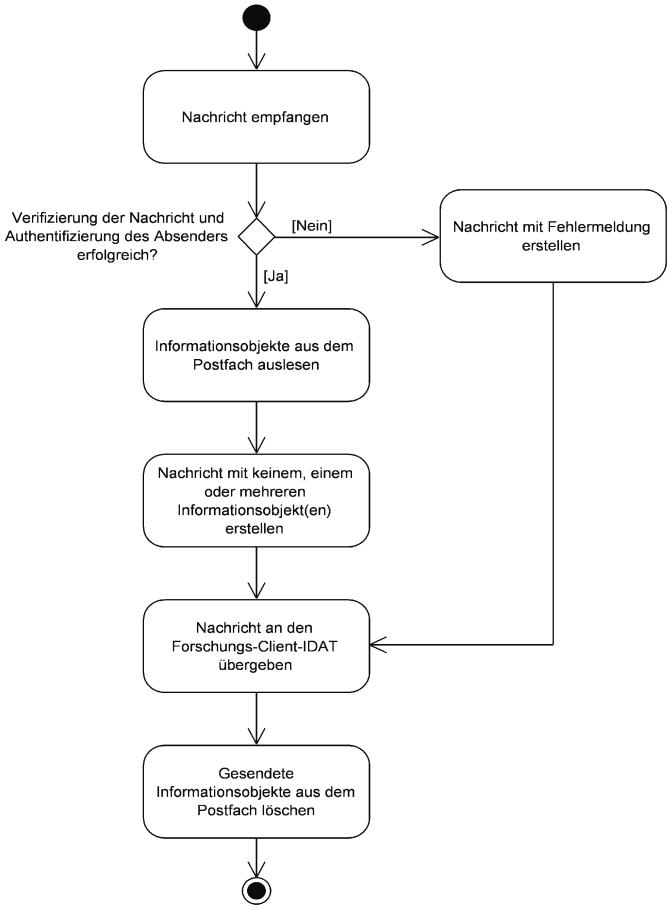

Abbildung 77: Anfordern von Informationsobjekten durch den IDAT-Verwalter

A4.6.1.4. Anfordern von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-List(Parameter): SemSigGetTID

Vorbedingung: Keine

Durchführen der Operation:

Der Ablauf entspricht dem des Operationsaufrufes „Anfordern von Informationsobjekten durch den IDAT-Verwalter: RLUS-List(Parameter): IO“. Bei diesem Aufruf wird allerdings der Semantic Signifier SemSigGetTID übergeben und es werden vom ePA-Forschungsadapter nur Bereitstellungsobjekte mit Pseudonymisierungs-Anfragen zurückgeben.

A4.6.1.5. Anfordern von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-List(Parameter): SemSigGetePA-ID

Vorbedingung: Keine

Durchführen der Operation:

Der Ablauf entspricht dem des Operationsaufrufes „Anfordern von Informationsobjekten durch den IDAT-Verwalter: RLUS-List(Parameter): IO“. Bei diesem Aufruf wird allerdings der Semantic Signifier SemSigGetePA-ID übergeben und es werden vom ePA-Forschungsadapter nur Bereitstellungsobjekte mit Depseudonymisierungs-Anfragen zurückgeben.

A4.6.1.6. Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-PUT(SemSigGetTID)

Vorbedingung: Es wurde eine Pseudonymisierungs-Anfrage an den Forschungs-Client-IDAT gestellt.

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Beim Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 78).
2. Der ePA-Forschungsadapter liest die ePA-ID und die TID aus dem Bereitstellungsobjekt aus. Anhand der AO-Referenz und der ePA-ID kann er das entsprechende Informationsobjekt, für das die Pseudonymisierungs-Anfrage vorgesehen ist, identifizieren und die ePA-ID durch die TID ersetzen.
3. Anschließend wird das Informationsobjekt in das Postfach für den Forschungs-Client-MDAT verschoben und kann nun vom Forschungs-Client-MDAT abgerufen werden (siehe Operationsaufruf „Anfordern von Informationsobjekten durch den MDAT-Verwalter: RLUS-List(Parameter): IO“).
4. Abschließend wird die Operation beendet und eine Statusmeldung an die Forschungs-Client-IDAT übergeben.

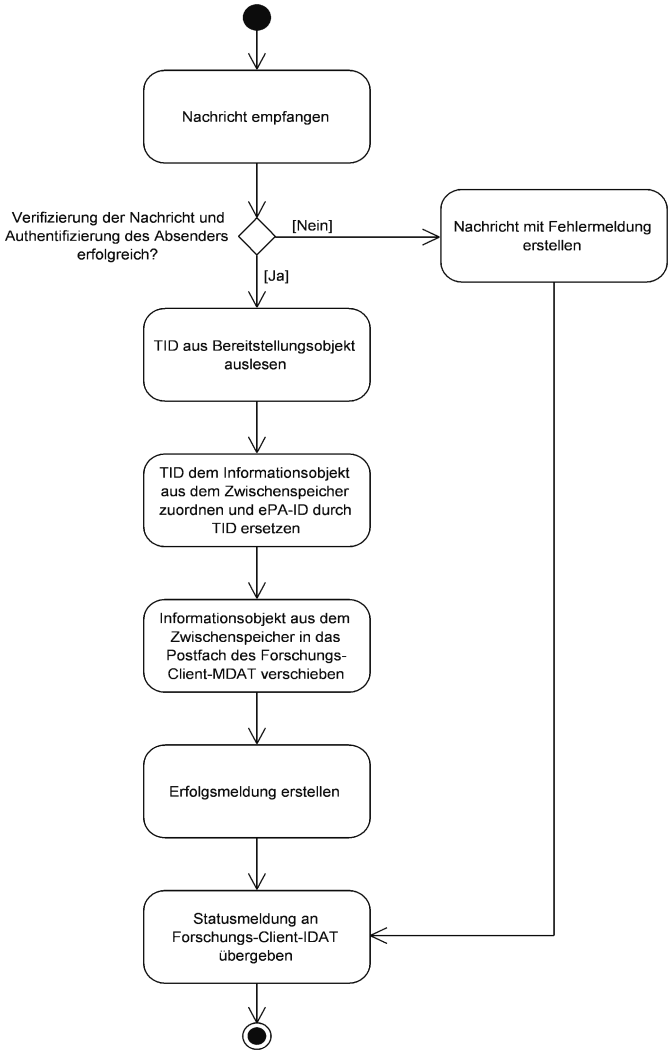

Abbildung 78: Bereitstellen von Pseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT

A4.6.1.7. Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT: RLUS-Put(SemSigGetePA-ID)

Vorbedingung: Es wurde eine Depseudonymisierungs-Anfrage an den Forschungs-Client-IDAT gestellt.

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Beim Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 79).
2. Der ePA-Forschungsadapter liest die ePA-ID und die TID aus dem Bereitstellungsobjekt aus. Anhand der AO-Referenz und der TID kann er das entsprechende Informationsobjekt, für das die Depseudonymisierungs-Anfrage vorgesehen ist, identifizieren und die TID durch die ePA-ID ersetzen.
3. Anschließend wird das Informationsobjekt an die ePA-Kommunikationskomponente weitergeleitet (siehe Operationsaufruf „Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter: RLUS-Put(IO)“) und eine Statusmeldung an den Forschungs-Client-IDAT übermittelt.

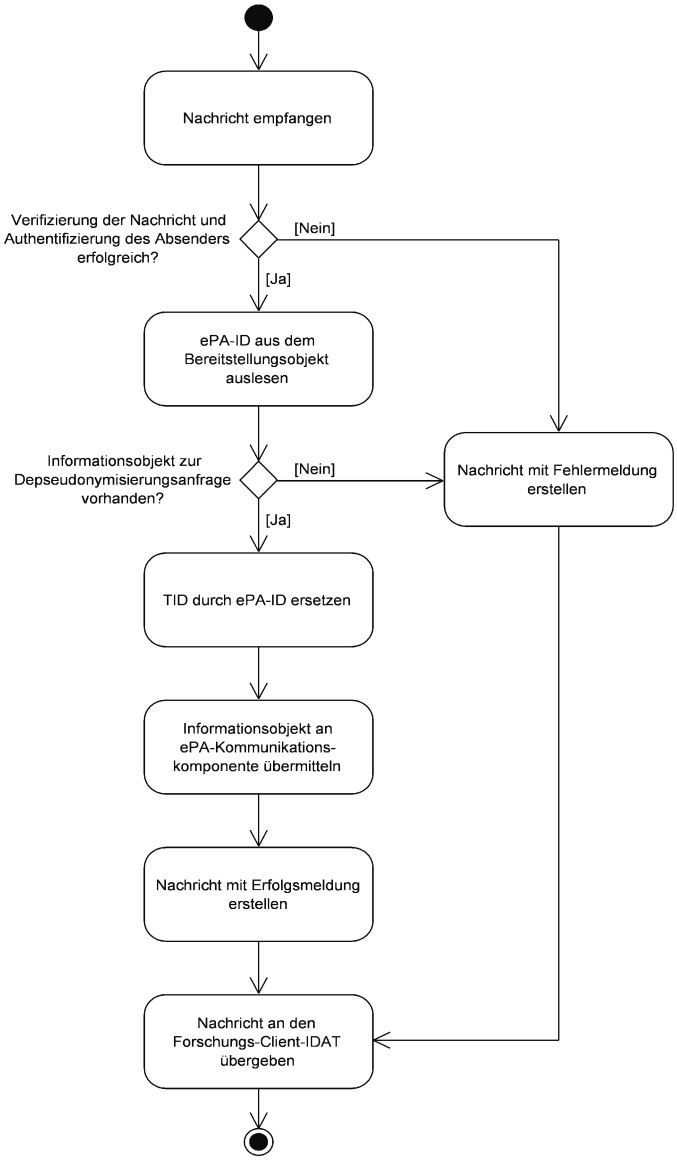

Abbildung 79: Bereitstellen von Depseudonymisierungs-Anfragen durch den Forschungs-Client-IDAT

A4.6.2. Kommunikation mit dem Forschungs-Client-MDAT

Bei der Kommunikation mit dem Forschungs-Client-MDAT tritt der ePA-Forschungsadapter als Dienstanbieter auf. Er stellt die folgenden Operationen über die Schnittstelle S3 bereit:

- **Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA:**
  RLUS-List(Parameter): symkeyMDO
- **Zustellung eines Informationsobjektes durch den MDAT-Verwalter:**
  RLUS-Put(IO)
- **Anfordern von Informationsobjekten durch den MDAT-Verwalter:**
  RLUS-List(Parameter): IO

Im Folgenden wird das Verhalten des ePA-Forschungsadapters beim Aufruf der oben genannten Operationen beschrieben:

A4.6.2.1. Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA: RLUS-List(Parameter): symkeyMDO

Vorbedingung: Keine

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Beim Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 80).
2. Der ePA-Forschungsadapter liest die TID aus dem Informationsobjekt aus, erstellt ein Anforderungsobjekt für eine Depseudonymisierungs-Anfrage, legt es in das Postfach des Forschungs-Clients-IDAT und wartet auf eine Antwort des Forschungs-Client-IDAT. Ist die Antwort eine Fehlermeldung, so gibt der ePA-Forschungsadapter diese als Rückgabewert an den Forschungs-Client-MDAT zurück und beendet die Operation. Ist die Antwort eine ePA-ID, so speichert er die ePA-ID, die TID und die Anforderungsobjekt-ID des Anforderungsobjektes für den symmetrischen Schlüssel zwischen.
3. Der ePA-Forschungsadapter ersetzt die TID im Anforderungsobjekt durch die ePA-ID.
4. Der ePA-Forschungsadapter leitet das Anforderungsobjekt an die ePA-Kommunikationskomponente weiter. Ist der Rückgabewert eine Fehlermeldung, so wird diese als Rückgabewert an den Forschungs-Client-MDAT zurückgegeben. Ist der Rückgabewert ein Bereitstellungsobjekt, so wird mit Schritt 5 fortgefahren.
5. Der ePA-Forschungsadapter fordert die Capability List der ePA von der ePA-Kommunikationskomponente an (siehe Anfordern der Capability List durch den ePA-Forschungsadapter: RLUS-List(Parameter): Capability List). Ist der Rückgabewert eine Fehlermeldung, so wird diese als Rückgabewert an den Forschungs-Client-MDAT zurückgegeben. Ist der Rückgabewert eine Capability List, so wird mit Schritt 6 fortgefahren.
6. Der ePA-Forschungsadapter überprüft mit Hilfe des öffentlichen Aktenschlüssels in der Capability List die Signatur des symkeyMDO

7. Der ePA-Forschungsadapter ersetzt die Signatur des symkeyMDO durch seine eigene Signatur.
8. Der ePA-Forschungsadapter liest die TID zu der ePA-ID und der Anforderungsobjekt-ID aus dem Zwischenspeicher und ersetzt die ePA-ID im Bereitstellungsobjekt durch die TID.
9. Der ePA-Forschungsadapter gibt das Bereitstellungsobjekt als Rückgabewert an den Forschungs-Client-MDAT zurück.

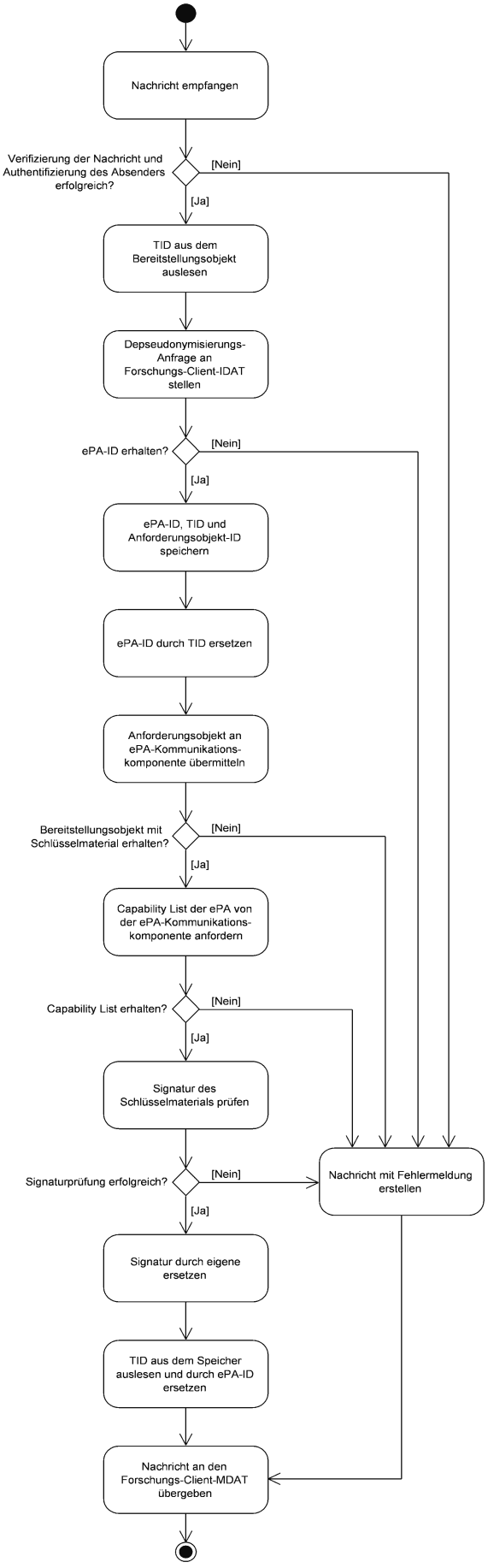

Abbildung 80: Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA

A4.6.2.2. Zustellung eines Informationsobjektes durch den MDAT-Verwalter: RLUS-Put(IO)

Vorbedingung: Keine

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Beim Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 81).
2. Der ePA-Forschungsadapter liest die TID aus dem Informationsobjekt aus, erstellt ein Anforderungsobjekt für eine Depseudonymisierungs-Anfrage und legt es in das Postfach des Forschungs-Clients-IDAT.
3. Das Informationsobjekt wird unter der AO-Referenz im Zwischenspeicher des ePA-Forschungsadapters abgelegt.
4. Der ePA-Forschungsadapter übermittelt dem Forschungs-Client-MDAT als Rückgabewert die Nachricht, dass das Informationsobjekt dem ePA-Forschungsadapter erfolgreich übermittelt wurde bzw. eine Fehlermeldung.

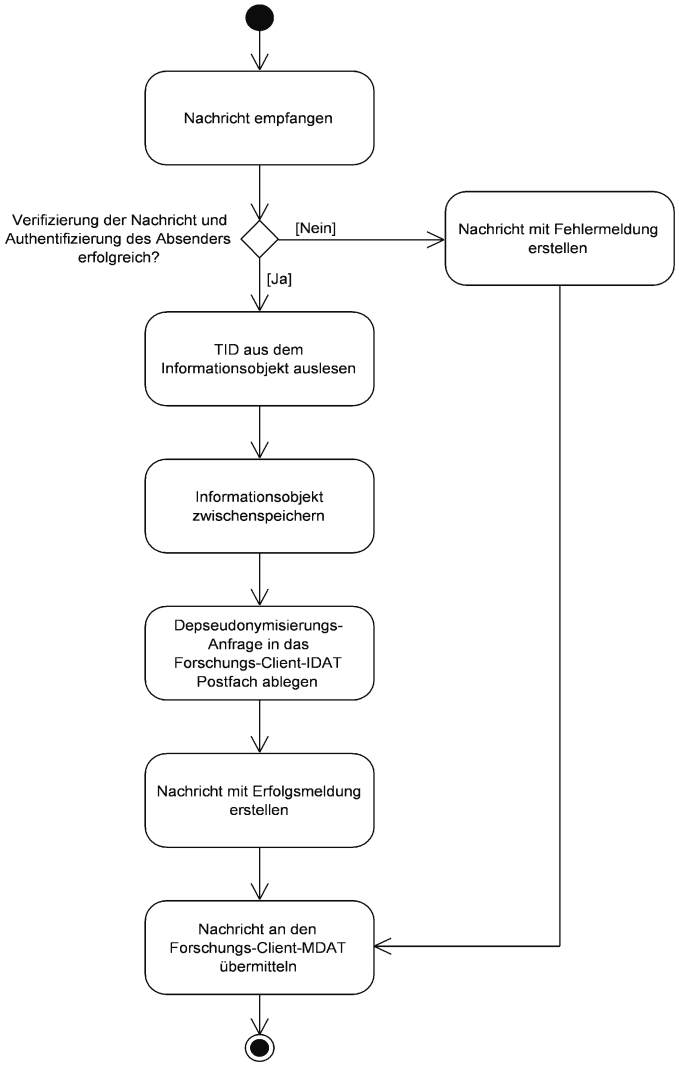

Abbildung 81: Zustellung eines Informationsobjektes durch den MDAT-Verwalter

A4.6.2.3. Anfordern von Informationsobjekten durch den MDAT-Verwalter: RLUS-List(Parameter): IO

Vorbedingung: Keine

Durchführen der Operation:

Der Ablauf entspricht dem der Operation „Anfordern von Informationsobjekten durch den IDAT-Verwalter: RLUS-List(Parameter): IO“ Der Unterschied besteht darin, dass die Informationsobjekte aus dem Postfach des Forschungs-Client-MDAT und nicht aus dem des Forschungs-Clients-IDAT geladen werden.

A4.6.3. Kommunikation mit der ePA-Kommunikationskomponente

Der ePA-Forschungsadapter ist sowohl Dienstnutzer gegenüber ePA-Kommunikations-komponente (siehe Schnittstelle S4, Abbildung 25) als auch Dienstanbieter gegenüber ePA-Kommunikationskomponente (siehe Schnittstelle S5, Abbildung 25). Als Dienstnutzer ruft der ePA-Forschungsadapter folgende Operationen der Schnittstelle S4 auf:

- **Anfordern der Capability List durch den ePA-Forschungsadapter:**
  RLUS-List(Parameter): Capability List
- **Anfordern eines symmetrischen Schlüssels von der ePA:**
  RLUS-List(Parameter): symkeyMDO
- **Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter:**
  RLUS-Put(IO)

Als Dienstanbieter stellt der ePA-Forschungsadapter der ePA-Kommunikationskomponente folgende Operationen über die Schnittstelle S5 bereit:

- **Zustellung eines Informationsobjektes durch die ePA-Kommunikations-komponente:**
  RLUS-Put(IO)

Im Folgenden wird das Verhalten des ePA-Forschungsadapters beim Aufruf der oben genannten Operationen beschrieben:

A4.6.3.1. Anfordern der Capability List durch den ePA-Forschungsadapter: RLUS-List(Parameter): Capability List

Vorbedingung:

Es wurde eine Anforderung für einen Capability List vom Forschungs-Client-IDAT gesendet („Anfordern der Capability List durch den Forschungs-Client-IDAT“). Oder es soll eine Überprüfung einer Signatur der ePA durch den ePA-Forschungsadapter erfolgen und es wurde von der Operation „Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA“ ein Anforderungsobjekt übergeben.

Durchführen der Operation:

1. Der ePA-Forschungsadapter nimmt das Anforderungsobjekt entgegen und übermittelt es an die ePA-Kommunikationskomponente (siehe auch Abbildung 82).
2. Als Rückgabewert bekommt der ePA-Forschungsadapter eine Capability List oder eine Fehlermeldung.
3. Der ePA-Forschungsadapter leitet die Antwort der ePA-Kommunikationskomponente an die aufrufende Komponente weiter.

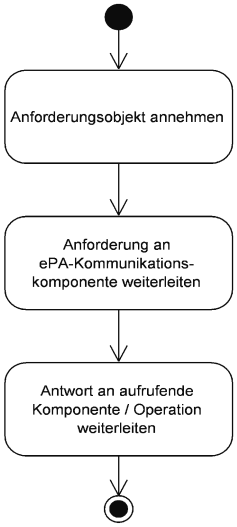

Abbildung 82: Anfordern der Capability List durch den ePA-Forschungsadapter

A4.6.3.2. Anfordern eines symmetrischen Schlüssels von der ePA: RLUS-List(Parameter): symkeyMDO

Vorbedingung:

Die Operation wurde von der internen Operation „Anfordern eines symmetrischen Schlüssels durch den Forschungs-Client-MDAT von der ePA“ aufgerufen und die Anforderung für einen symmetrischen Schlüssel vom Forschungs-Client-MDAT übergeben.

Durchführen der Operation:

1. Die Operation nimmt das Anforderungsobjekt an.
2. Der ePA-Forschungsadapter leitet das Anforderungsobjekt an die ePA-Kommunikationskomponente weiter.
3. Der Rückgabewert (Fehlermeldung oder Bereitstellungsobjekt mit symmetrischem Schlüssel) wird der aufrufenden Operation übergeben.

Das Ablaufdiagramm entspricht dem des Operationsaufrufes „Anfordern der Capability List durch den ePA-Forschungsadapter“(siehe Abbildung 82) und wird daher nicht nochmal abgebildet.

A4.6.3.3. Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter: RLUS-Put(IO)

Vorbedingung: Der Forschungs-Client-IDAT hat ein Informationsobjekt bereitgestellt, das an die ePA eines Patienten gesendet werden soll. Oder der Forschungs-Client-MDAT hat ein Informationsobjekt bereitgestellt, das an die ePA eines Patienten gesendet werden soll, und es ist bereits eine Depseudonymisierung des Informationsobjektes erfolgt.

Durchführen der Operation:

1. Der ePA-Forschungsadapter leitet das Informationsobjekt an die ePA-Kommunikationskomponente weiter (siehe auch Abbildung 83).
2. Der ePA-Forschungsadapter löscht das Informationsobjekt aus seinem Zwischenspeicher.

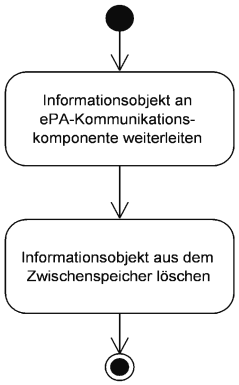

Abbildung 83: Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter

A4.6.3.4. Zustellung eines Informationsobjektes durch die ePA-Kommunikationskomponente: RLUS-Put(IO)

Vorbedingung: Keine.

Durchführen der Operation:

1. Es erfolgt eine Authentifizierung des Absenders und eine Verifizierung der Transportnachricht sowie eine syntaktische Überprüfung der Nachricht (siehe Abschnitt A4.3.2). Beim Auftreten eines Fehlers wird die Operation abgebrochen und der Fehler zurückgegeben. Ansonsten wird mit Schritt 2 fortgefahren (siehe auch Abbildung 84).
2. Ist das Informationsobjekt für die Patientenliste vorgesehen, so wird es in das Postfach des Forschungs-Clients-IDAT verschoben und mit Schritt 5 fortgefahren. Ist das Informationsobjekt für die medizinischen Datenbank des Forschungsverbundes vorgesehen, so wird ein Anforderungsobjekt für eine Pseudonymisierungs-Anfrage (mit dem Semantic Signifier „SemSigGetTID“ und der ePA-ID als Nutzlast) erstellt und in das Postfach des Forschungs-Clients-IDAT abgelegt.
3. Danach wird überprüft, ob das Informationsobjekt Schlüsselmaterial von der ePA enthält. Ist kein Schlüsselmaterial enthalten, so wird mit Schritt 4 fortgefahren. Ansonsten wird die Capability List von der ePA-Kommunikationskomponente angefordert (siehe Operationsaufruf „Anfordern der Capability List durch den ePA-Forschungsadapter“) und die Signatur mit dem in der Capability List erhaltenen öffentlichen Schlüssel der ePA überprüft. Danach wird das Schlüsselmaterial aus dem Informationsobjekt neu signiert (siehe auch Sicherheitsarchitektur der Forschungsschnittstelle).
4. Anschließend werden die identifizierenden Metadaten (siehe Abschnitt 8.2) entfernt und das Informationsobjekt unter der AO-Referenz im ePA-Forschungsadapter zwischengespeichert.
5. Der ePA-Kommunikationskomponente wird als Rückgabewert eine erfolgreiche Zwischenspeicherung im ePA-Forschungsadapter oder eine Fehlermeldung zurückgegeben.

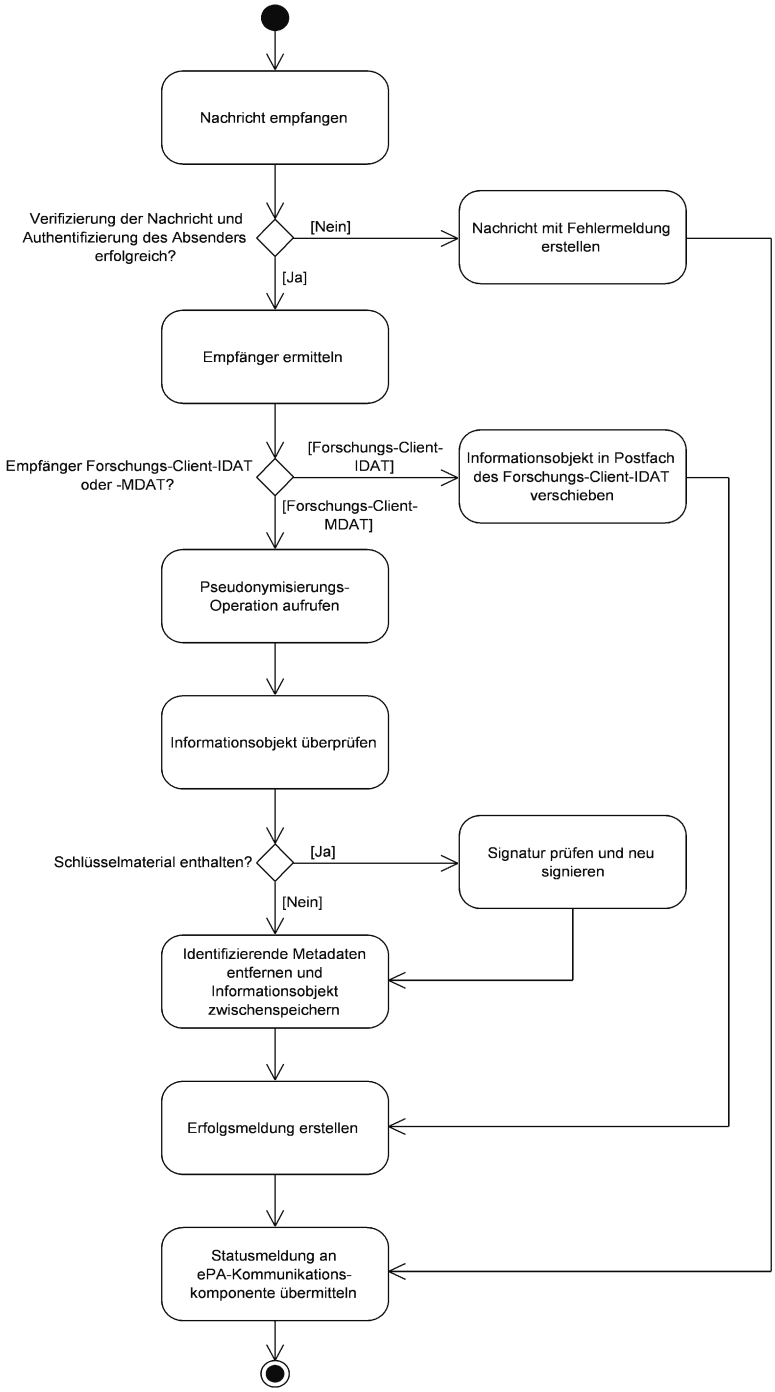

Abbildung 84: Zustellung eines Informationsobjektes durch die ePA-Kommunikationskomponente

A4.6.4. Module des ePA-Forschungsadapters

Der ePA-Forschungsadapter benötigt folgende Module um die oben beschriebenen Operationen durchführen zu können:

- Der **Kommunikationsdienst** stellt dem Forschungs-Client-IDAT die folgenden Operationen zur Verfügung:
  - RLUS-List(Parameter): Capability List,
  - RLUS-Put(IO),
  - RLUS-List(Parameter): IO.

  Dem Forschungs-Client-MDAT stellt der Kommunikationsdienst die folgenden Operationen zur Verfügung:
  - RLUS-List(Parameter): symkeyMDO,
  - RLUS-Put(IO) und
  - RLUS-List(Parameter): IO.

  Zusätzlich stellt er der ePA-Kommunikationskomponente die folgende Operation zur Verfügung:
  - RLUS-Put(IO).
- Einen **De-** und **Pseudonymisierungsdienst**, der dem Forschungs-Client-IDAT die folgenden Operationen bereitstellt:
  - RLUS-List(Parameter): SemSigGetTID,
  - RLUS-List(Parameter): SemSigGetePA-ID,
  - RLUS-PUT(SemSigGetTID) und
  - RLUS-Put(SemSigGetePA-ID).
- Der **Kommunikations-Client** ermöglicht die Kommunikation mit der ePA-Kommunikationskomponente und ruft folgende Operationen auf:
  - RLUS-List(Parameter): Capability List,
  - RLUS-List(Parameter): symkeyMDO und
  - RLUS-Put(IO)
- Das **Authentifizierungsmodul** und das **Verifikationsmodul** führen die Verifizierung der Nachrichten sowie die Authentifizierung der Absender durch. Diese Module haben die gleichen Funktionen wie die der LE-Postfach-Komponente [144].
- Das **Postfachmodul** dient als Speicher für Informationsobjekte, die für den Forschungs-Client-IDAT oder -MDAT bereitstellt werden sollen. Es gibt jeweils ein Postfach für den Forschungs-Client-IDAT und eines für den Forschungs-Client-MDAT.

A4.7. ePA-Kommunikationskomponente

Die ePA-Kommunikationskomponente kommuniziert nur mit dem ePA-Forschungsadapter der Forschungsschnittstelle. Die Kommunikation mit dem Forschungs-Client-IDAT und Forschungs-Client-MDAT wird immer über den ePA-Forschungsadapter vermittelt. Da die Forschungsschnittstelle die bestehenden Operationen der Schnittstelle der ePA-Kommunikationskomponente verwenden soll, wird hier nur darauf verwiesen durch welche Operationen der ePA-Kommunikationskomponente die hier benötigten Operationen umgesetzt werden können.

A4.7.1. Kommunikation mit dem ePA-Forschungsadapter

Die ePA-Kommunikationskomponente ist sowohl Dienstnutzer gegenüber dem ePA-Forschungsadapter (siehe Schnittstelle S5, Abbildung 25) als auch Dienstanbieter gegenüber dem ePA-Forschungsadapter (siehe Schnittstelle S4, Abbildung 25). Als Dienstnutzer ruft die ePA-Kommunikationskomponente folgende Operationen der Schnittstelle S5 auf:

- **Zustellung eines Informationsobjektes durch die ePA-Kommunikationskomponente:**
  RLUS-Put(IO)

Als Dienstanbieter stellt die ePA-Kommunikationskomponente dem ePA-Forschungsadapter folgende Operationen über die Schnittstelle S4 bereit:

- **Anfordern der Capability List durch den ePA-Forschungsadapter:**
  RLUS-List(Parameter): Capability List
- **Anfordern eines symmetrischen Schlüssels von der ePA:**
  RLUS-List(Parameter): symkeyMDO
- **Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter:**
  RLUS-Put(IO)

Im Folgenden wird das Verhalten der ePA-Kommunikationskomponente beim Aufruf der oben genannten Operationen beschrieben:

A4.7.1.1. Zustellung eines Informationsobjektes durch die ePA-Kommunikationskomponente: RLUS-Put(IO)

Das Verhalten der ePA-Kommunikationskomponente beim Aufrufen der Operation entspricht dem in der Facharchitektur der LE-Schnittstelle beschriebenen Verhalten **„Zustellen von Bereitstellungsobjekten durch den Bürger:** RLUS-Put(BO)“.

A4.7.1.2. Anfordern der Capability List durch den ePA-Forschungsadapter: RLUS-List(Parameter): Capability List

Diese Operation wird durch die in der Facharchitektur der LE-Schnittstelle beschriebenen Operation **„Anforderung der CapabilityList** (RLUS-List(Parameter):Capability List)“ abgedeckt.

A4.7.1.3. Anfordern eines symmetrischen Schlüssels von der ePA: RLUS-List(Parameter): symkeyMDO

Diese Operation wird durch die in der Facharchitektur der LE-Schnittstelle beschriebene Operation **„Anforderung von Bereitstellungsobjekten durch einen Leistungserbringer mit unmittelbarer Zustellung** (RLUS-List(Parameter):MDO)**“** abgedeckt.

A4.7.1.4. Zustellung eines Informationsobjektes durch den ePA-Forschungsadapter: RLUS-Put(IO)

Diese Operation wird durch die in der Facharchitektur der LE-Schnittstelle beschriebene Operation **„Zustellung von Bereitstellungsobjekten durch einen Leistungserbringer** (RLUS-Put(BO))**“** abgedeckt.

A4.7.2. Module der ePA-Kommunikationskomponente

Die Module der ePA-Kommunikationskomponente werden in der Facharchitektur der LE-Schnittstelle beschrieben [144], daher wird an dieser Stelle nicht weiter auf diese Module eingegangen.

A5. Sicherheitsarchitektur

In diesem Kapitel werden die detaillierten Abläufe bei der Umsetzung des Autorisierungs- und Verschlüsselungskonzeptes durch die Forschungsschnittstelle beschrieben. Im Sinne eines generischen Ansatzes und zum Zwecke der Vereinheitlichung mit den Begrifflichkeiten im FuE-Projekt wird die Versorgungsdatenbank als medizinische Datenbank des Forschungsverbundes und das Versorgungsmodul als Forschungssystem bezeichnet.

A5.1. Umsetzung der Autorisierung durch die Forschungsschnittstelle

Im Nachfolgenden wird beschrieben, wie die Autorisierung bei den vier generischen Kommunikationsmustern durch den Forschungs-Client-IDAT im Detail durchgeführt wird.

A5.1.1. Autorisierung des Bereitstellens von Informationsobjekten aus einer Patientenliste an eine ePA

Im generischen Kommunikationsmuster UC-3-1 „Informationen aus einer Patientenliste einer ePA bereitstellen“ findet die Autorisierung statt (vergleiche Abschnitt 7.4.1). Es muss durch den Forschungs-Client-IDAT anhand der im Abschnitt 9.4.1 aufgeführten Informationen entschieden werden, ob die Patientenliste das entsprechende Informationsobjekt an die ePA schicken darf.

Bezeichner	UC-6-1
Name	Autorisierung des Bereitstellens von Informationsobjekten aus einer Patientenliste an eine ePA
Kurzbeschreibung	Der Forschungs-Client-IDAT überprüft anhand seiner Autorisierungsliste, ob Informationen von der Patientenliste des Forschungssystems an eine ePA eines Patienten übertragen werden dürfen.
Primärer Akteur	Keine
Andere Akteure	Keine
Systeme	Patientenliste, Forschungs-Client-IDAT, ePA-Forschungsadapter
Vorbedingungen	Der Verwalter der Patientenliste hat ein Informationsobjekt für einen Patienten über die Patientenliste abgeschickt.
Nachbedingungen	Bei einer positiven Autorisierungsentscheidung wurde das Informationsobjekt an den ePA-Forschungsadapter weitergeleitet. Bei einer negativen Autorisierungsentscheidung wurde das Informationsobjekt verworfen und die Patientenliste über die Entscheidung informiert.
Hauptszenario	1. Die Patientenliste übermittelt dem Forschungs-Client-IDAT ein Informationsobjekt. 2. Der Forschungs-Client-IDAT liest die ePA-ID und den Semantic Signifier aus dem Informationsobjekt aus und überprüft, ob es ein Anforderungs- oder ein Bereitstellungsobjekt ist. 3. Der Forschungs-Client-IDAT überprüft in der Autorisierungsliste für die Kommunikation zwischen Patientenliste und ePA, ob es einen Eintrag mit der ePA-ID, dem Semantic Signifier, der Patientenliste als sendendem System und der Eigenschaft des Informationsobjektes (Anforderungs- oder Bereitstellungsobjekt) gibt. 4. Gibt es einen entsprechenden Eintrag, so wird eine positive Autorisierungsentscheidung gefällt. Gibt es keinen Eintrag, so wird eine negative Autorisierungsentscheidung gefällt. 5. Bei einer positiven Entscheidung wird das Informationsobjekt an den ePA-Forschungsadapter weitergeleitet.

Beziehungen zu anderen Use Cases	UC-3-1

Tabelle 54: Autorisierung des Bereitstellens von Informationsobjekten aus einer Patientenliste an eine ePA

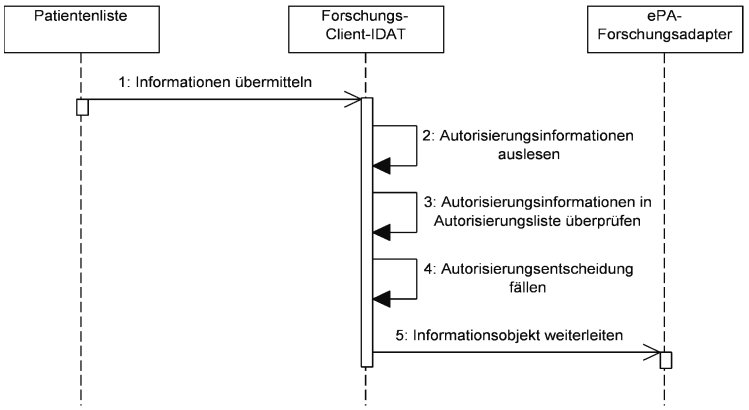

Abbildung 85: Autorisierung des Bereitstellens von Informationsobjekten aus einer Patientenliste an eine ePA

A5.1.2. Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine Patientenliste

Im generischen Kommunikationsmuster UC-3-2 „Informationen aus einer ePA einer Patientenliste bereitstellen“ findet die Autorisierung statt (vergleiche Abschnitt 7.4.2). Es muss durch den Forschungs-Client-IDAT anhand der im Abschnitt 9.4.1 aufgeführten Informationen entschieden werden, ob die ePA das entsprechende Informationsobjekt an die Patientenliste schicken darf. Im Folgenden wird die Autorisierungsentscheidung im Detail beschrieben.

Bezeichner	UC-6-2
Name	Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine Patientenliste
Kurzbeschreibung	Der Forschungs-Client-IDAT überprüft anhand seiner Autorisierungsliste, ob Informationen von einer ePA eines Patienten an die Patientenliste des Forschungsystems übertragen werden dürfen.
Primärer Akteur	Keine
Andere Akteure	Keine
Systeme	Patientenliste, Forschungs-Client-IDAT, ePA-Forschungsadapter
Vorbedingungen	Für die Patientenliste liegt ein Informationsobjekt im Postfach des ePA-Forschungsadapters zum Abrufen durch den Forschungs-Client-IDAT bereit.
Nachbedingungen	Bei einer positiven Autorisierungsentscheidung wurde das Informationsobjekt an die Patientenliste weitergeleitet. Bei einer negativen Autorisierungsentscheidung wurde das Informationsobjekt verworfen und der ePA-Forschungsadapter über die Entscheidung informiert.
Hauptszenario	1. Der Forschungs-Client-IDAT ruft ein Informationsobjekt vom ePA-Forschungsadapter für die Patientenliste ab. 2. Der ePA Forschungsadapter übermittelt ein Informationsobjekt. 3. Der Forschungs-Client-IDAT liest die ePA-ID aus dem Informationsobjekt und den Semantic Signifier aus und überprüft, ob es ein Anforderungs- oder eine Bereitstellungsobjekt ist. 4. Der Forschungs-Client-IDAT überprüft, ob es einen Eintrag in der Autorisierungsliste für die Kommunikation zwischen der ePA und der Patientenliste mit der ePA-ID, dem Semantic Signifier, der ePA des Patienten als sendendem System und der Eigenschaft des Informationsobjektes (Anforderungs- oder Bereitstellungsobjekt) gibt. 5. Gibt es einen entsprechenden Eintrag, so wird eine positive Autorisierungsentscheidung gefällt. Gibt es keinen Eintrag, so wird eine negative Autorisierungsentscheidung gefällt. 6. Das Informationsobjekt wird an die Patientenliste weitergeleitet.
Beziehungen zu anderen Use Cases	UC-3-2

Tabelle 55: Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine Patientenliste

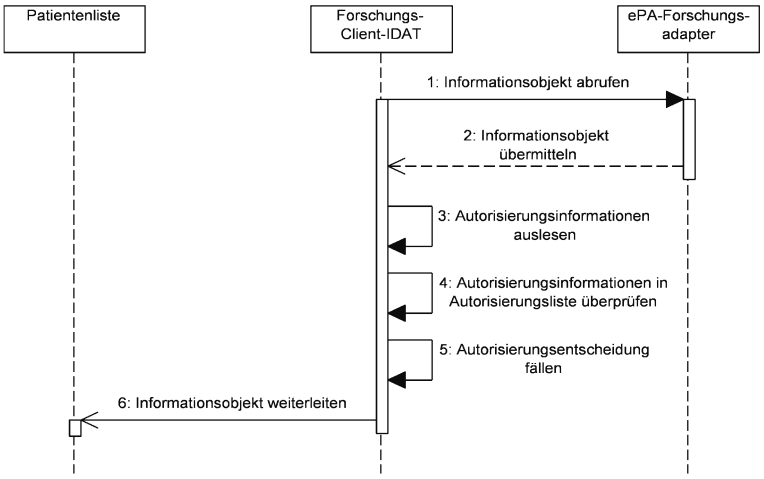

Abbildung 86: Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine Patientenliste

A5.1.3. Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine medizinische Datenbank eines Forschungsverbundes

Im generischen Kommunikationsmuster UC-4-1 „Daten aus einer ePA einer medizinischen Datenbank bereitstellen“ findet die Autorisierung statt (vergleiche Abschnitt 7.5.1). Es muss durch den Forschungs-Client-IDAT anhand der im Abschnitt 9.4.1 aufgeführten Informationen entschieden werden, ob die ePA das entsprechende Informationsobjekt an die medizinische Datenbank des Forschungsverbundes schicken darf. Im Folgenden wird die Autorisierungsentscheidung im Detail beschrieben.

Bezeichner	UC-6-3
Name	Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine medizinische Datenbank
Kurzbeschreibung	Der Forschungs-Client-IDAT überprüft anhand seiner Autorisierungsliste, ob Informationen von einer ePA eines Patienten an die medizinische Datenbank des Forschungsverbundes übertragen werden dürfen.
Primärer Akteur	Keine
Andere Akteure	Keine
Systeme	Forschungs-Client-IDAT, ePA-Forschungsadapter
Vorbedingungen	Es liegt eine Pseudonymisierungs-Anfrage für Forschungs-Client-IDAT beim ePA-Forschungsadapter vor.
Nachbedingungen	Bei einer positiven Autorisierungsentscheidung liegt dem ePA-Forschungsadapter eine TID vom Forschungs-Client-IDAT vor. Bei einer negativen Autorisierungsentscheidung liegt dem ePA-Forschungsadapter eine entsprechende Fehlermeldung vom Forschungs-Client-IDAT vor.
Hauptszenario	1. Der Forschungs-Client-IDAT ruft eine Pseudonymisierungs-Anfrage vom ePA-Forschungsadapter ab. 2. Der ePA Forschungsadapter übermittelt ein Anforderungsobjekt mit einer Pseudonymisierungs-Anfrage. 3. Der Forschungs-Client-IDAT liest die ePA-ID, den Semantic Signifier sowie die Eigenschaft des Informationsobjektes (Anforderungs- oder Bereitstellungsobjekt) aus der Pseudonymisierungs-Anfrage aus. 4. Der Forschungs-Client-IDAT überprüft, ob es einen Eintrag in der Autorisierungsliste für die Kommunikation zwischen der medizinischen Datenbank des Forschungsverbundes und der ePA mit der ePA-ID, dem Semantic Signifier, der ePA des Patienten als sendendem System und der Eigenschaft des Informationsobjektes (Anforderungs- oder Bereitstellungsobjekt) gibt. 5. Gibt es einen entsprechenden Eintrag, so wird eine positive Autorisierungsentscheidung gefällt. Gibt es keinen Eintrag, so wird eine negative Autorisierungsentscheidung gefällt. 6. Bei einer positiven Autorisierungsentscheidung generiert der Forschungs-Client-IDAT eine TID. 7. Bei einer positiven Autorisierungsentscheidung übermittelt der Forschungs-Client-IDAT dem ePA-Forschungsadapter eine TID.
Beziehungen zu anderen Use Cases	UC-4-1

Tabelle 56: Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine medizinische Datenbank des Forschungsverbundes

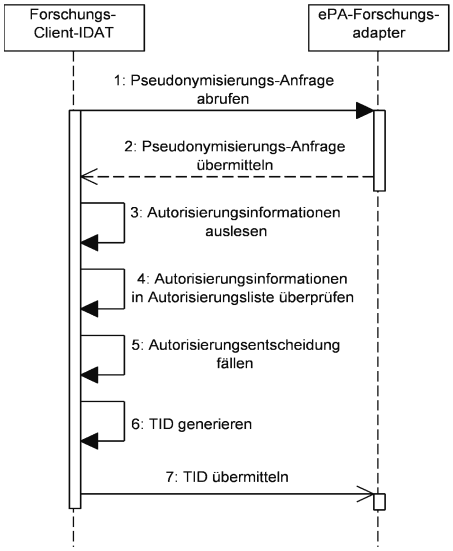

Abbildung 87: Autorisierung des Bereitstellens von Informationsobjekten aus einer ePA an eine medizinische Datenbank des Forschungsverbundes

A5.1.4. Autorisierung des Bereitstellens von Informationsobjekten aus einer medizinischen Datenbank eines Forschungsverbundes an eine ePA

Im generischen Kommunikationsmuster UC-4-2 „Daten aus einer medizinischen Datenbank an eine ePA bereitstellen“ findet die Autorisierung statt (vergleiche Abschnitt 7.5.2) Es muss durch den Forschungs-Client-IDAT anhand der im Abschnitt 9.4.1 aufgeführten Informationen entschieden werden, ob die medizinische Datenbank des Forschungsverbundes das entsprechende Informationsobjekt an die ePA schicken darf. Im Folgenden wird die Autorisierungsentscheidung im Detail beschrieben.

Bezeichner	UC-6-4
Name	Autorisierung des Bereitstellens von Informationsobjekten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA
Kurzbeschreibung	Der Forschungs-Client-IDAT überprüft anhand seiner Autorisierungsliste, ob Informationen von der medizinischen Datenbank des Forschungsverbundes an eine ePA eines Patienten übertragen werden dürfen.
Primärer Akteur	Keine
Andere Akteure	Keine
Systeme	Forschungs-Client-MDAT, Forschungs-Client-IDAT
Vorbedingungen	Dem Forschungs-Client-MDAT liegt ein Informationsobjekt vor, für das er eine TID beim Forschungs-Client-IDAT beantragen muss.
Nachbedingungen	Bei einer positiven Autorisierungsentscheidung liegt dem Forschungs-Client-MDAT eine TID vom Forschungs-Client-IDAT vor. Bei einer negativen Autorisierungsentscheidung liegt dem Forschungs-Client-MDAT eine entsprechende Fehlermeldung vom Forschungs-Client-IDAT vor.
Hauptszenario	1. Der Forschungs-Client-MDAT fordert vom Forschungs-Client-IDAT eine TID an. 2. Der Forschungs-Client-IDAT liest die PID, den Semantic Signifier sowie die Eigenschaft des Informationsobjektes (Anforderungs- oder Bereitstellungsobjekt) aus der Anfrage des Forschungs-Clients-MDAT aus. 3. Der Forschungs-Client-IDAT überprüft, ob es einen Eintrag in der Autorisierungsliste für die Kommunikation zwischen der medizinischen Datenbank des Forschungsverbundes und der ePA mit der ePA-ID, dem Semantic Signifier, der medizinischen Datenbank des Forschungsverbundes als sendendem System und der Eigenschaft des Informationsobjektes (Anforderungs- oder Bereitstellungsobjekt) gibt. 4. Gibt es einen entsprechenden Eintrag, so wird eine positive Autorisierungsentscheidung gefällt. Gibt es keinen Eintrag, so wird eine negative Autorisierungsentscheidung gefällt. 5. Bei einer positiven Autorisierungsentscheidung generiert der Forschungs-Client-IDAT eine TID. 6. Bei einer positiven Autorisierungsentscheidung übermittelt der Forschungs-Client-IDAT dem Forschungs-Client-MDAT eine TID.
Beziehungen zu anderen Use Cases	UC-4-2

Tabelle 57: Autorisierung des Bereitstellens von Informationsobjekten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA

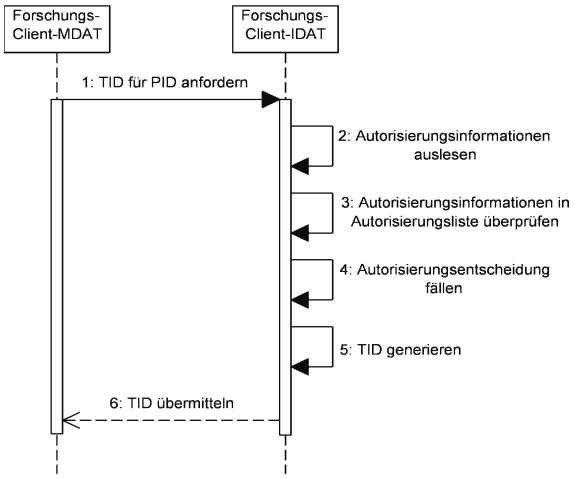

Abbildung 88: Autorisierung des Bereitstellens von Informationsobjekten aus einer medizinischen Datenbank des Forschungsverbundes an eine ePA

A5.2. Umsetzung des Verschlüsselungskonzeptes der Forschungsschnittstelle

Im Folgenden liegt der Fokus auf dem Austausch der Schlüssel zwischen den Komponenten. Daher werden die Vorgänge bei der Pseudonymisierung und Depseudonymisierung im Forschungs-Client-IDAT nicht im Detail beschrieben. Die Abläufe sind mit denen in der Tabelle 14 Schritte 5-10 sowie 13-21 für die Pseudonymisierung und der Tabelle 15 Schritte 3-7 sowie 10-16 für die Depseudonymisierung identisch.

A5.2.1. Anfordern eines Bereitstellungsobjektes von der ePA aus der medizinischen Datenbank eines Forschungsverbundes

Das Anfordern eines Bereitstellungsobjektes von der ePA aus einer medizinischen Datenbank eines Forschungsverbundes kommt z. B. beim Auskunftsrecht (UC-2-6) zum Einsatz. Hier fordert der Patient vom Verwalter der medizinischen Datenbank die über ihn in der medizinischen Datenbank gespeicherten Informationen an. Der Verwalter der medizinischen Datenbank stellt dem Patienten auf diese Anforderung die entsprechenden Informationen bereit. Im Nachfolgenden wird zunächst beschrieben, wie das „Anfordern eines Bereitstellungsobjektes von der ePA aus der medizinischen Datenbank“ im Hinblick auf das Verschlüsselungsmodell der Forschungsschnittstelle funktioniert. Die Bereitstellung wird dann im UC-7-3 beschrieben. Da auch die Signatur des Schlüssels mangels des öffentlichen Schlüssels der ePA nicht überprüft werden kann, wird die Signatur vom ePA-Forschungsadapter überprüft und bei erfolgreicher Überprüfung durch die Signatur des ePA-Forschungsadapters ersetzt. Die kann dann auch vom Forschungs-Client-MDAT verifiziert werden. Dies gilt sowohl für UC-7-1 als auch für UC-7-2.

Bezeichner	UC-7-1
Name	Anfordern eines Bereitstellungsobjektes von der ePA aus der medizinischen Datenbank eines Forschungsverbundes.
Kurzbeschreibung	Ein Patient fordert ein Bereitstellungsobjekt von der medizinischen Datenbank des Forschungsverbundes an. Da die medizinische Datenbank des Forschungsverbundes keinen Zugriff auf das Zertifikat der ePA haben sollte, wird der symmetrische Schlüssel für die Verschlüsselung der Nutzlast des Bereitstellungsobjektes von der ePA (bzw. dem Bürger-Client siehe UC-7-4) erstellt und in der Anforderung mitgeschickt.
Primärer Akteur	Patient
Andere Akteure	Verwalter der medizinischen Datenbank des Forschungsverbundes
Systeme	medizinische Datenbank des Forschungsverbundes, Forschungs-Client-MDAT Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Die Kommunikation mit dem Forschungssystem wurde eingerichtet. Der Patient darf diese Daten anfordern. Die Adresse und der öffentliche Schlüssel der medizinischen Datenbank des Forschungsverbundes sind bekannt. Im Bürger-Client wurde ein symmetrischer Schlüssel für die Verschlüsselung des medizinischen Datenobjekts generiert (siehe UC-7-4).
Nachbedingungen	Dem Forschungs-Client-MDAT liegen die für die ePA des Patienten bereitzustellenden Informationen aus der medizinischen Datenbank des Forschungsverbundes in verschlüsselter Form vor.
Hauptszenario	1. Der Patient stellt eine Anforderung für die medizinische Datenbank des Forschungsverbundes in seinem Bürger-Client zusammen und erstellt ein Schlüsselpaar (symkeyMDO und symkeyMDO_Kopie) zur Verschlüsselung der angeforderten Informationen (siehe UC-7-4). Beides übermittelt der Patient an das ePA-Kernsystem.

	2. Das ePA-Kernsystem erstellt ein Anforderungsobjekt 3. Das ePA-Kernsystem legt ein Dummy-Objekt (ohne Nutzlast) mit der ID des Anforderungsobjektes und dem symkeyMDO an. 4. Das ePA-Kernsystem fügt den symkeyMDO_Kopie der Nutzlast des Anforderungsobjektes hinzu. 5. Das ePA-Kernsystem übermittelt das Anforderungsobjekt an die ePA-Kommunikationskomponente. 6. Die ePA-Kommunikationskomponente leitet das Anforderungsobjekt an den ePA-Forschungsadapter weiter. 7. Der ePA-Forschungsadapter fordert die Capability List der ePA von der ePA-Kommunikationskomponente an. 8. Die ePA-Kommunikationskomponente übermittelt dem ePA-Forschungs-adapter die Capability List der ePA. 9. Der ePA-Forschungsadapter überprüft mit Hilfe des öffentlichen Akten-schlüssels in der Capability List die Signatur des symkeyMDO_Kopie. 10. Der ePA-Forschungsadapter ersetzt die überprüfte Signatur durch seine eigene Signatur. 11. Der Forschungs-Client-IDAT fragt regelmäßig Nachrichten für ihn ab. 12. Der ePA-Forschungsadapter fragt eine TID zu der ePA-ID des Anfor-derungsobjektes an. 13. Der Forschungs-Client-IDAT übermittelt die TID. 14. Der ePA-Forschungsadapter ersetzt die ePA-ID durch die TID. 15. Der Forschungs-Client-MDAT fragt das Anforderungsobjekt vom ePA-Forschungsadapter ab. 16. Der ePA-Forschungsadapter übermittelt dem Forschungs-Client-MDAT das Anforderungsobjekt. 17. Der Forschungs-Client-MDAT fordert eine PID zu der TID aus dem Anforderungsobjekt vom Forschungs-Client-IDAT an. 18. Der Forschungs-Client-IDAT übermittelt dem Forschungs-Client-MDAT die PID (Details zur Pseudonymisierung sind in UC-4-1 beschrieben). 19. Der Forschungs-Client-MDAT überprüft die Signatur des symkeyMDO_Kopie. 20. Der Forschungs-Client-MDAT speichert den symkeyMDO_Kopie mit der PID und der Anforderungsobjekt-ID zwischen. 21. Der Forschungs-Client-MDAT übermittelt die Anforderung und die Anfor-derungsobjekt-ID an die medizinische Datenbank des Forschungsver-bundes. 22. Der MDAT-Verwalter ruft die Anforderung ab. 23. Die medizinische Datenbank des Forschungsverbundes zeigt die Anfor-derung an. 24. Der MDAT-Verwalter überprüft die Anforderung. 25. Der MDAT-Verwalter bestätigt die Anforderung. 26. Die medizinische Datenbank des Forschungsverbundes stellt die Daten zusammen. 27. Die medizinische Datenbank des Forschungsverbundes leitet die Daten und die PID des Patienten und die Anforderungsobjekt-ID an den Forschungs-Client-MDAT weiter. 28. Der Forschungs-Client-MDAT entschlüsselt den symkeyMDO_Kopie mit seinem privaten Schlüssel. 29. Der Forschungs-Client-MDAT verschlüsselt die Informationen aus der medizinischen Datenbank des Forschungsverbundes mit dem Ergebnis der Entschlüsselung (Kopie symmetrischer Schlüssel aus der ePA). 30. Anschließend wird das Schlüsselmaterial gelöscht. 31. Der Forschungs-Client-MDAT erstellt ein Bereitstellungsobjekt mit der verschlüsselten Nutzlast und Anforderungsobjekt-ID. 32. Anschließend wird das Bereitstellungsobjekt übermittelt (siehe UC-7-3).
Beziehungen zu anderen Use Cases	UC-7-3, UC-7-4

Tabelle 58: Anfordern eines Bereitstellungsobjektes von der ePA aus der medizinischen Datenbank eines Forschungsverbundes.

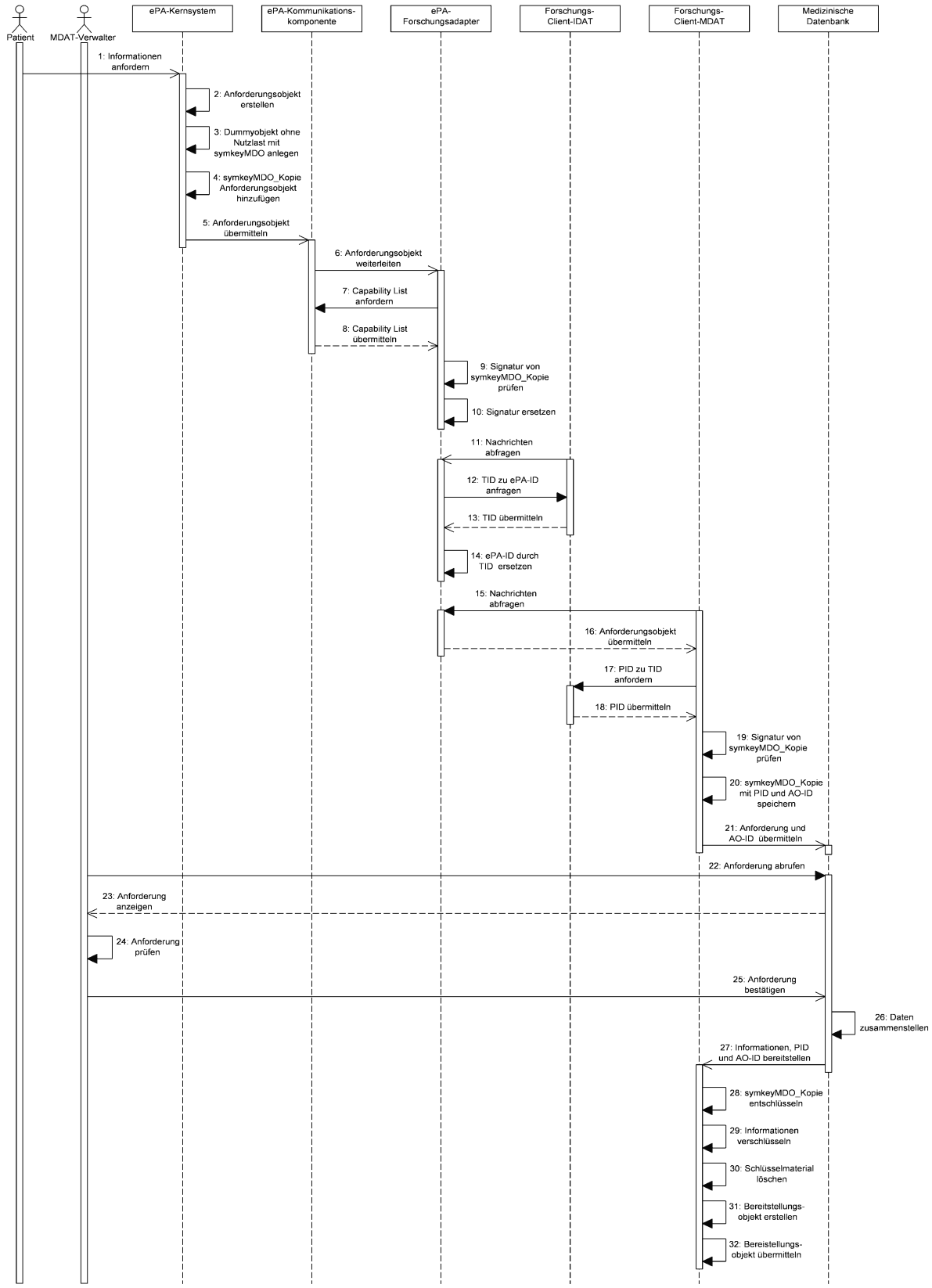

Abbildung 89: Anfordern eines Bereitstellungsobjektes von der ePA aus der medizinischen Datenbank eines Forschungsverbundes.

A5.2.2. Anfordern eines Schlüssels von der ePA durch die medizinische Datenbank eines Forschungsverbundes

Einige Anwendungsfälle der medizinischen Datenbank erfordern eine Bereitstellung von Daten durch die medizinische Datenbank an die ePA ohne vorherige Anforderung. Als Beispiel ist hier der Anwendungsfall UC-2-3 „Rekrutierung von Patienten“ genannt, bei dem der Verwalter der medizinischen Datenbank eine Rekrutierungsanfrage an die ePA des Patienten schickt. Nach dem Verschlüsselungsmodell der Forschungsschnittstelle muss der Forschungs-Client-MDAT hierzu zunächst einen symmetrischen Schlüssel für die Verschlüsselung des MDOs von der ePA anfordern. Diese Anforderung erfolgt durch ein Anforderungsobjekt mit dem Semantic Signifier „symkeyMDO“ und wird von der ePA durch ein entsprechendes Bereitstellungsobjekt mit einem symkeyMDO als Nutzlast beantwortet. Hierzu wird in der ePA des Patienten eine Vorab-Autorisierungsrichtlinie benötigt, die dem MDAT-Verwalter genehmigt, ein symkeyMDO abzurufen. Der symkeyMDO wurde vorher durch den Patienten im Bürger-Client erstellt und im ePA-Kernsystem zwischengespeichert (siehe UC-7-4). Der genauere Ablauf wird im Folgenden beschrieben. Die Bereitstellung wird dann im UC-7-3 beschrieben.

Bezeichner	UC-7-2
Name	Anfordern eines Schlüssels von der ePA durch die medizinische Datenbank
Kurzbeschreibung	Der MDAT-Verwalter möchte ein Bereitstellungsobjekt an die ePA des Patienten schicken. Da die medizinische Datenbank des Forschungsverbundes keinen Zugriff auf das Zertifikat der ePA haben sollte, muss der symmetrische Schlüssel für die Verschlüsselung der Nutzlast des Bereitstellungsobjektes von der ePA angefordert, dort erstellt und an die medizinische Datenbank des Forschungsverbundes zurückgeschickt werden.
Primärer Akteur	Verwalter der medizinischen Datenbank des Forschungsverbundes
Andere Akteure	Keine
Systeme	medizinische Datenbank des Forschungsverbundes, Forschungs-Client-MDAT, Forschungs-Client-IDAT, ePA-Forschungsadapter, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Die Kommunikation mit dem Forschungssystem wurde eingerichtet. Dem Patienten dürfen die Informationen bereitgestellt werden. Die ePA unterstützt eine synchrone Kommunikation. Es gibt eine Vorab-Autorisierungsrichtlinie, die die automatische Bereitstellung eines Bereitstellungsobjektes mit einem symmetrischen Schlüssel für den MDAT-Verwalter erlaubt. Es wurde ein entsprechender symkeyMDO vom Patienten im Bürger-Client erstellt und im ePA-Kernsystem zwischengespeichert.
Nachbedingungen	Dem Forschungs-Client-MDAT liegen die für die ePA des Patienten bereitzustellenden Informationen aus der medizinischen Datenbank des Forschungsverbundes in verschlüsselter Form vor.
Hauptszenario	1. Der MDAT-Verwalter stellt Informationen für die ePA eines Patienten zusammen. 2. Die medizinische Datenbank des Forschungsverbundes leitet die Informationen an den Forschungs-Client-MDAT weiter. 3. Der Forschungs-Client-MDAT fordert für die PID des Patienten eine TID vom Forschungs-Client-IDAT an. 4. Der Forschungs-Client-IDAT übermittelt dem Forschungs-Client-MDAT eine TID (Details zur Pseudonymisierung sind in UC-4-2 beschrieben). 5. Der Forschungs-Client-MDAT erstellt ein Anforderungsobjekt für einen symmetrischen Schlüssel.

	6. Der Forschungs-Client-MDAT speichert die PID, die TID und die Anforderungsobjekt-ID zwischen. 7. Der Forschungs-Client-MDAT übermittelt das Anforderungsobjekt an den ePA-Forschungsadapter. 8. Der Forschungs-Client-IDAT fragt regelmäßig Nachrichten für ihn vom ePA-Forschungsadapter ab. 9. Der ePA-Forschungsadapter übermittelt eine Anforderung für eine ePA-ID zu der TID des Anforderungsobjektes. 10. Der Forschungs-Client-IDAT übermittelt die ePA-ID (Details zur Pseudonymisierung sind in UC-4-2 beschrieben). 11. Der ePA-Forschungsadapter speichert die ePA-ID, die TID und die Anforderungsobjekt-ID zwischen. 12. Der ePA-Forschungsadapter ersetzt die TID im Anforderungsobjekt durch die ePA-ID. 13. Der ePA-Forschungsadapter übermittelt das Anforderungsobjekt an die ePA-Kommunikationskomponente. 14. Die ePA-Kommunikationskomponente leitet das Anforderungsobjekt an das ePA-Kernsystem weiter. 15. Das ePA-Kernsystem lädt das in UC-7-4 erstellte Schlüsselpaar (symkeyMDO und symkeyMDO_Kopie) aus dem Zwischenspeicher. 16. Das ePA-Kernsystem erzeugt ein Dummy-Objekt (ohne Nutzlast) mit der ID des Anforderungsobjektes und dem symkeyMDO. 17. Das ePA-Kernsystem erstellt ein Bereitstellungsobjekt mit dem symkeyMDO_Kopie als Nutzlast und der Anforderungsobjekt-ID. 18. Das ePA-Kernsystem übermittelt das Bereitstellungsobjekt an die ePA-Kommunikationskomponente. 19. Die ePA-Kommunikationskomponente leitet das Bereitstellungsobjekt an den ePA-Forschungsadapter weiter. 20. Der ePA-Forschungsadapter fordert die Capability List der ePA von der ePA-Kommunikationskomponente an. 21. Die ePA-Kommunikationskomponente übermittelt dem ePA-Forschungsadapter die Capability List der ePA. 22. Der ePA-Forschungsadapter überprüft mit Hilfe des öffentlichen Aktenschlüssels in der Capability List die Signatur des symkeyMDO_Kopie. 23. Der ePA-Forschungsadapter ersetzt die Signatur des symkeyMDO_Kopie durch seine eigene Signatur. 24. Der ePA-Forschungsadapter liest die TID zu der ePA-ID aus dem Zwischenspeicher und ersetzt die ePA-ID im Bereitstellungsobjekt durch die TID. 25. Der ePA-Forschungsadapter übermittelt dem Forschungs-Client-MDAT das Bereitstellungsobjekt zurück. 26. Der Forschungs-Client-MDAT ruft die Informationen zu der TID aus dem Bereitstellungsobjekt aus dem Zwischenspeicher auf. 27. Der Forschungs-Client-MDAT überprüft die Signatur des symkeyMDO_Kopie. 28. Der Forschungs-Client-MDAT entschlüsselt den symkeyMDO_Kopie mit seinem privaten Schlüssel 29. Der Forschungs-Client-MDAT verschlüsselt die Informationen aus der medizinischen Datenbank des Forschungsverbundes mit dem Ergebnis der Entschlüsselung (Kopie des symmetrischen Schlüssels aus der ePA). 30. Anschließend wird das Schlüsselmaterial gelöscht. 31. Der Forschungs-Client-MDAT erstellt ein Bereitstellungsobjekt mit der verschlüsselten Nutzlast und Anforderungsobjekt-ID. 32. Anschließend wird das Bereitstellungsobjekt übermittelt (siehe UC-7-3).
Beziehungen zu anderen Use Cases	UC-7-3, UC-7-4

Tabelle 59: Anfordern eines Schlüssels von der ePA durch die medizinische Datenbank

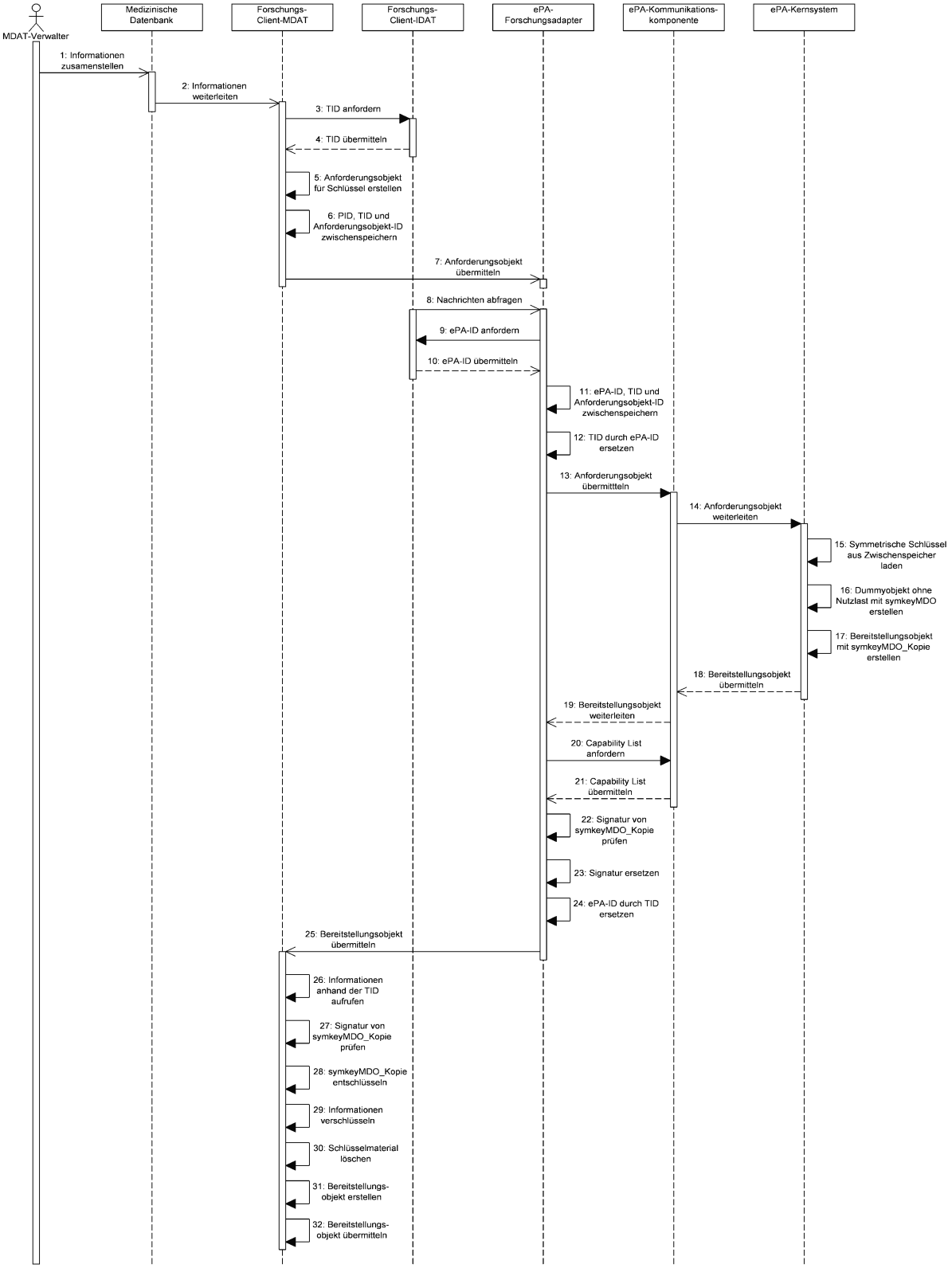

Abbildung 90: Anfordern eines Schlüssels von der ePA durch die medizinische Datenbank

A5.2.3. Bereitstellen von verschlüsselten Informationen aus der medizinischen Datenbank eines Forschungsverbundes an die ePA

Nachfolgend wird beschrieben, wie die Informationen in verschlüsselter Form aus der medizinischen Datenbank des Forschungsverbundes an die ePA geschickt werden und wie im ePA-Kernsystem die verschlüsselten Informationen dem richtigen Schlüssel (symkeyMDO) zugeordnet werden.

Bezeichner	UC-7-3
Name	Bereitstellen von verschlüsselten Informationen aus der medizinischen Datenbank des Forschungsverbundes an die ePA
Kurzbeschreibung	Der Forschungs-Client-MDAT schickt verschlüsselte Informationen aus der medizinischen Datenbank des Forschungsverbundes an die ePA.
Primärer Akteur	Patient
Andere Akteure	Keine
Systeme	Forschungs-Client-MDAT, Forschungs-Client-IDAT, ePA-Forschungs-adapter, ePA-Kommunikationskomponente, ePA-Kernsystem
Vorbedingungen	Dem Forschungs-Client-MDAT liegen die für die ePA des Patienten bereit-zustellenden Informationen aus der medizinischen Datenbank des Forschungsverbundes in verschlüsselter Form vor. D. h. zuvor wurden UC-7-1 oder UC-7-2 durchgeführt.
Nachbedingungen	Der ePA liegen die Informationen für den Patienten aus der medizinischen Datenbank des Forschungsverbundes in verschlüsselter Form sowie der Hybridschlüssel zur Entschlüsselung der Informationen vor.
Hauptszenario	1. Der Forschungs-Client-MDAT fordert eine TID zu der PID des Patienten an. 2. Der Forschungs-Client-IDAT übermittelt dem Forschungs-Client-MDAT die TID. 3. Der Forschungs-Client-MDAT setzt die TID in das Bereitstellungsobjekt ein. 4. Der Forschungs-Client-MDAT übermittelt das Bereitstellungsobjekt an den ePA-Forschungsadapter. 5. Der Forschungs-Client-IDAT fragt regelmäßig Nachrichten für ihn vom ePA-Forschungsadapter ab. 6. Der ePA-Forschungsadapter fordert eine ePA-ID zu der TID des Anfor-derungsobjektes an. 7. Der Forschungs-Client-IDAT übermittelt dem ePA-Forschungsadapter die ePA-ID. 8. Der ePA-Forschungsadapter ersetzt die TID im Bereitstellungsobjekt durch die ePA-ID. 9. Der ePA-Forschungsadapter übermittelt das Bereitstellungsobjekt an die ePA-Kommunikationskomponente. 10. Die ePA-Kommunikationskomponente leitet dem ePA-Kernsystem das Bereitstellungsobjekt weiter. 11. Das ePA-Kernsystem sucht anhand der Anforderungsobjekt-ID im Bereitstellungsobjekt das Dummy-Objekt und fügt diesem die verschlüsselte Nutzlast hinzu. 12. Der Patient ruft die Informationen aus dem ePA-Kernsystem ab. 13. Das ePA-Kernsystem zeigt die Informationen an. 14. Der Patient überprüft die Informationen. 15. Der Patient bestätigt bzw. übernimmt die Informationen.
Beziehungen zu anderen Use Cases	UC-7-1 und UC-7-2

Tabelle 60: Bereitstellen von verschlüsselten Informationen aus der medizinischen Datenbank des Forschungsverbundes an die ePA

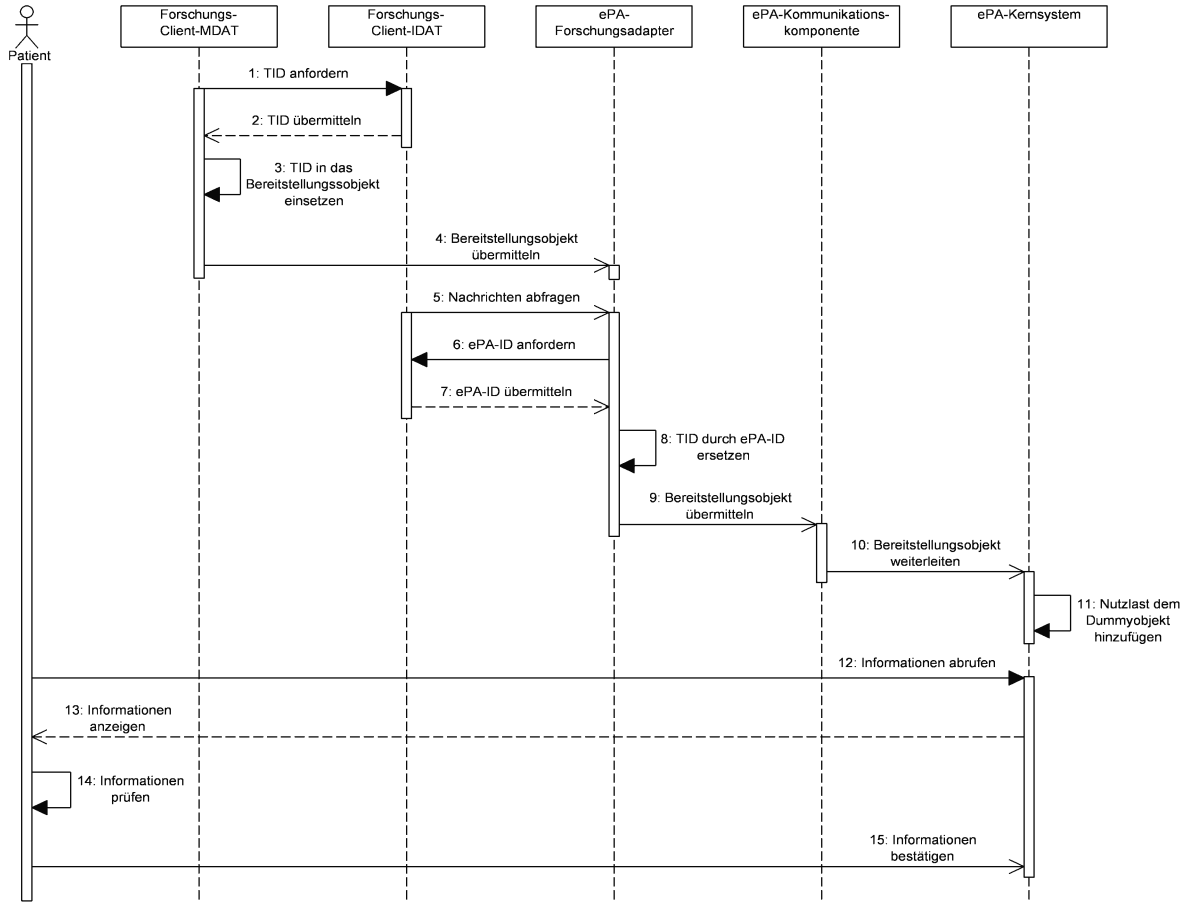

Abbildung 91: Bereitstellen von verschlüsselten Informationen aus der medizinischen Datenbank eines Forschungsverbundes an die ePA

A5.2.4. Symmetrischen Schlüssel im Bürger-Client erstellen

Bevor von der ePA Daten aus der medizinischen Datenbank eines Forschungsverbundes angefordert werden können bzw. Daten aus der medizinischen Datenbank der ePA bereitgestellt werden können, muss im Bürger-Client ein entsprechender symmetrischer Schlüssel zur Verschlüsselung der medizinischen Daten erstellt worden sein. Dieser Schlüssel kann zum einen während der „Anfordern eines Bereitstellungsobjektes von der ePA aus der medizinischen Datenbank eines Forschungsverbundes (UC-7-1)“ im Bürger-Client erstellt werden und mit der Anforderung an die medizinische Datenbank geschickt werden. Zum anderen kann der Schlüssel vor der „Anfordern eines Schlüssels von der ePA durch die medizinische Datenbank (UC-7-2)“ schon im Bürger-Client erstellt werden und im ePA-Kernsystem zwischengespeichert werden. Im Nachfolgenden wird der zweite Fall beschrieben. Der erste Fall unterscheidet sich nur dadurch, dass der Schlüssel mit der Anforderung an das ePA-Kernsystem weitergereicht wird und vom ePA-Kernsystem nicht zwischen gespeichert, sondern gleich verarbeitet wird. Sollten mehrere Schlüssel im ePA-Kernsystem zwischen gespeichert werden, so wird der unten beschriebene Ablauf entsprechend wiederholt.

Bezeichner	UC-7-4
Name	Symmetrischen Schlüssel im Bürger-Client erstellen
Kurzbeschreibung	Der Patient erstellt mit Hilfe seines Bürger-Clients einen oder mehrere symmetrische Schlüssel für die Verschlüsselung von medizinischen Daten in seiner ePA und stellt sie dem ePA-Kernsystem bereit.
Primärer Akteur	Patient
Andere Akteure	Keine
Systeme	Bürger-Client, ePA-Kernsystem
Vorbedingungen	Der Patient ist ordnungsgemäß am Bürger-Client angemeldet. Es besteht eine sichere Umgebung und das benötigte Schlüsselmaterial zur Sicherung des symmetrischen Schlüssels bzw. seiner Kopie ist vorhanden.
Nachbedingungen	Es liegt dem ePA-Kernsystem 1-n durch den öffentlichen Aktenschlüssel bzw. dem öffentlichen Schlüssel der medizinischen Datenbank des Forschungsverbundes gesicherte Paare des symkeyMDO mit entsprechendem symkeyMDO_Kopie vor.
Hauptszenario	1. Der Patient beauftragt in seinem Bürger-Client die Erstellung von symmetrischen Schlüsseln. 2. Der Bürger-Client generiert einen symmetrischen Schlüssel (symkeyMDO). 3. Der Bürger-Client kopiert den symkeyMDO und erhält den symkeyMDO_Kopie. 4. Der Bürger-Client verschlüsselt den symkeyMDO mit dem öffentlichen Schlüssel seiner Akte (pubAS). 5. Anschließend verschlüsselt der Bürger-Client den symkeyMDO_Kopie mit dem öffentlichen Schlüssel der medizinischen Datenbank (pubMD). 6. Der Bürger-Client signiert den symkeyMDO_Kopie. 7. Der Bürger-Client übermittelt die mit dem öffentlichen Schlüssel der Akte und der medizinischen Datenbank gesicherten Schlüssel (symkeyMDO und symkeyMDO_Kopie) dem ePA-Kernsystem. 8. Das ePA-Kernsystem speichert die Schlüssel zwischen. 9. Das ePA-Kernsystem bestätigt dem Bürger-Client die erfolgreiche Speicherung. 10. Der Bürger-Client bestätigt dem Patienten die erfolgreiche Speicherung der Schlüssel im ePA-Kernsystem.

	11. Der Bürger-Client löscht das erstellte Schlüsselmaterial in seiner gesicherten Umgebung.
Beziehungen zu anderen Use Cases	UC-7-1 und UC-7-2

Tabelle 61: Symmetrischen Schlüssel im Bürger-Client erstellen

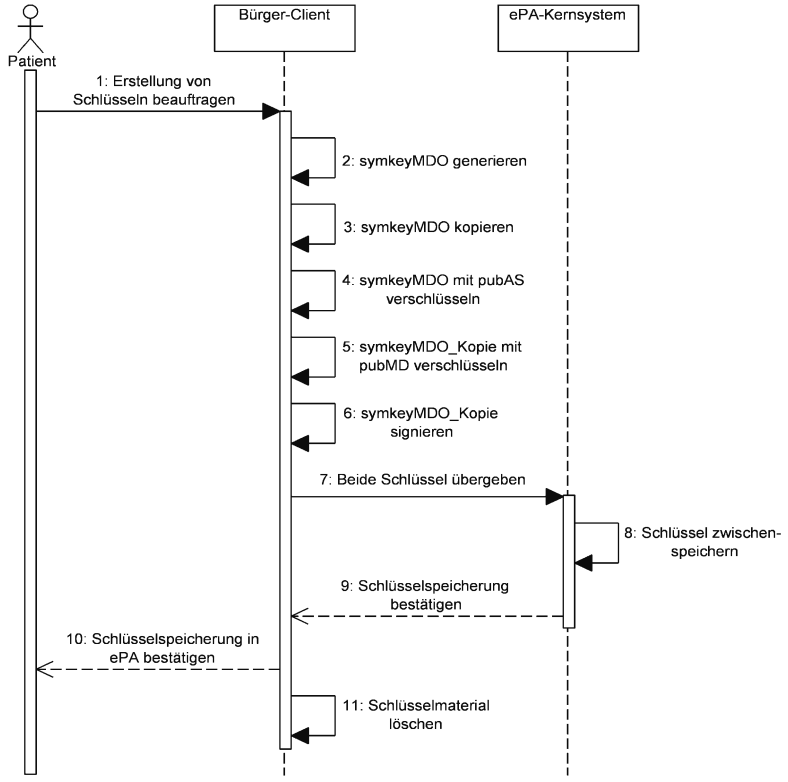

Abbildung 92: Symmetrischen Schlüssel im Bürger-Client erstellen

A6. Review der Ergebnisse

A6.1. Kommentierungsbögen zum Experten-Review

1. Auswahl der Anwendungsfälle des Versorgungsmoduls:

Durch den ersten Kommentierungsbogen soll die Frage geklärt werden, ob alle relevanten Anwendungsfälle des Versorgungsmoduls für die Anbindung einer ePA nach § 291a berücksichtigt worden sind. Anwendungsfälle werden als relevant angesehen, wenn es einen Patientenbezug gibt, d. h. der Patient bei diesem Anwendungsfall Informationen bekommt oder bereitstellt. In dem nachfolgenden Bogen kann von den Reviewern die Auswahl jedes Anwendungsfalls kommentiert werden. Die Reviewer haben die Möglichkeit für jeden Anwendungsfall zu entscheiden, ob er berücksichtigt (dann ist „Ja“ anzukreuzen), oder ob er nicht berücksichtigt werden sollte (dann ist „Nein“ anzukreuzen) (siehe Abschnitt 1.1 [26]und 1.2). Sollte die Empfehlung der Reviewer vom ursprünglichen Vorschlag abweichen, können sie ihre abweichende Empfehlung unter „Kommentar bei Abweichung vom Vorschlag“ begründen.

1.1. Patientenliste

Anwendungsfall - Anmeldung eines Patienten an einem Forschungsverbund (Variante A)

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Anmeldung eines Patienten an einem Forschungsverbund (Variante B)

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Recht des Patienten auf Auskunft

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Aktualisierung der Daten

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Patient kontaktieren

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Rückzug der Einwilligung

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

[26] Die Verweise in diesem Fragebogen beziehen sich nicht auf dieses Dokument, sondern auf das für den Review angefertigte Dokument „Experten-Review eines Kommunikationsmodells für die Anbindung eines Versorgungsmoduls an eine ePA nach §291a SGB V“ [189].

Anwendungsfall - Übertragen von Daten an die Forschungsdatenbank aus dem Versorgungskontext oder aus dem Studienkontext

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Depseudonymisierung zur Datenqualitätssicherung

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Todesfall eines Patienten oder Probanden

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Umpseudonymisierung (Ersetzen vorhandener Pseudonyme durch neue)

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

1.2. Versorgungsdatenbank

Anwendungsfall - Aufnahme in die Behandlungsdatenbank / das Versorgungsmodul

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Erfassung und Zugriff auf Daten im Behandlungsprozess / Zugriff auf Identitätsdaten zu Behandlungszwecken

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Vergabe von Zugriffsrechten / Autorisierung von Mit- oder Weiterbehandlern

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Zugriff auf Daten für Zwecke der Qualitätssicherung

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Tod des Patienten

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Machbarkeit einer Auswertung oder Studie prüfen

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Rekrutierung für neue Studien

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Export von Daten

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Expertenforum

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Informieren eines Patienten über Forschungsergebnisse

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Medizinische Qualitätssicherung und Benchmarking

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Recht des Patienten auf Auskunft

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

Anwendungsfall - Rückzug der Einwilligung / Löschen, sperren oder anonymisieren medizinischer Daten

Ja: ☐ Nein: ☐ Kommentar bei Abweichung vom Vorschlag:

2. Umsetzung der Kommunikation der Anwendungsfälle des Versorgungsmoduls

Durch diesen Kommentierungsbogen sollen die Reviewer zu den folgenden zwei Fragen Stellung nehmen:

1) Sind bei der Beschreibung der Kommunikation der ausgewählten Anwendungsfälle alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

2) Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Die Kommunikation der Anwendungsfälle des Versorgungsmoduls dient als Grundlage für die Herleitung des Kommunikationsmodells und die sich daraus an die einzelnen Systeme ergebenden Anforderungen. Daher ist die Richtigkeit der Kommunikation der Anwendungsfälle essentiell, um nicht aus einer falsch beschriebenen Kommunikation auch falsche Schlussfolgerungen zu ziehen.

Die Reviewer können mit Hilfe des Kommentierungsbogens das Ergebnis ihrer Prüfung in Bezug auf die Datenschutzkonformität für die Kommunikation jedes Anwendungsfalls dokumentieren. Dabei wird „Ja“ angekreuzt, wenn es keine Einwände bezüglich der Kommunikation gibt und „Nein“ angekreuzt, wenn es aus Sicht des Datenschutzes Einwände bezüglich der Kommunikation gibt. Sollte „Nein“ angekreuzt werden, so können die Reviewer die Entscheidung im Feld „Wenn nein, bitte kommentieren“ begründen. Dies bezieht sich immer auf die erste Frage in den nachfolgenden Abschnitten (also 2.x.1).

Es wird für jeden Anwendungsfall analysiert, welche Informationen während der Kommunikation dem Patienten und welche Informationen dem Forschungsverbund bereitgestellt werden. Dies dient als Grundlage für die Herleitung der über das Kommunikationsmodell umzusetzenden Kommunikationsmuster und sollte somit richtig und vollständig sein. Daher soll durch die Reviewer die Frage beantwortet werden, ob bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für den jeweiligen Anwendungsfall relevanten Informationen aufgeführt worden sind?

Um diese Frage zu beantworten, können die Reviewer in den Kommentierungsbögen für jeden Anwendungsfall anmerken, ob die für den Patienten bzw. Forschungsverbund im Rahmen dieses Anwendungsfalls relevanten Informationen bereitgestellt werden. Dabei wird „Ja“ angekreuzt, wenn im Rahmen dieses Anwendungsfalls alle relevanten Informationen für den Patienten bzw. für den Forschungsverbund aufgeführt worden sind. „Nein“ wird angekreuzt, wenn weitere Informationen ausgetauscht werden sollen oder die Kommunikation der aufgeführten Informationen nicht notwendig ist. Sollten die Reviewer „Nein“ ankreuzen, so können sie die Entscheidung im Feld „Wenn nein, bitte kommentieren“ begründen. Dies bezieht sich immer auf die zweite Frage (also 2.x.2) in den nachfolgenden Abschnitten.

2.1. Anwendungsfall 1-1 (Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler)

2.1.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.1.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.2. Anwendungsfall 1-2 (Kontaktieren eines Patienten über den Verwalter der Patientenliste)

2.2.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Kontaktieren eines Patienten über den Verwalter der Patientenliste“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn, nein bitte kommentieren:

2.2.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.3. Anwendungsfall 1-3 (Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten)

2.3.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn, nein bitte kommentieren:

2.3.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.4. Anwendungsfall 1-4 (Recht des Patienten auf Auskunft)

2.4.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Recht des Patienten auf Auskunft“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn, nein bitte kommentieren:

2.4.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.5. Anwendungsfall 1-5 (Rückzug der Einwilligung)

2.5.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Rückzug der Einwilligung“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn, nein bitte kommentieren:

2.5.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.6. Anwendungsfälle 2-1 (Erfassung und Zugriff auf Daten im Behandlungsprozess) und 2-2 (Erfassung und Zugriff auf Daten durch einen Patienten)

2.6.1. Sind bei der Beschreibung der Kommunikation der Anwendungsfälle UC-2-1 und UC-2-2 alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Anwendungsfall 2-1:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Anwendungsfall 2-2:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.6.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für die Anwendungsfälle UC-2-1 und UC-2-2 relevanten auszutauschenden Informationen aufgeführt?

Anwendungsfall 2-1:

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Anwendungsfall 2-2:

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.7. Anwendungsfall 2-3 (Rekrutierung von Patienten)

2.7.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Rekrutierung von Patienten“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.7.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.8. Anwendungsfall 2-4 (Expertenforum)

2.8.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Expertenforum“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.8.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.9. Anwendungsfall 2-5 (Informieren eines Patienten über Forschungsergebnisse)

2.9.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Informieren eines Patienten über Forschungsergebnisse“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.9.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.10. Anwendungsfall 2-6 (Recht des Patienten auf Auskunft)

2.10.1. Sind bei der Beschreibung der Kommunikation des Anwendungsfalls „Recht des Patienten auf Auskunft“ alle relevanten Anforderungen aus den TMF Datenschutzkonzepten in Bezug auf das Versorgungsmodul berücksichtigt worden?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

2.10.2. Werden bei der Analyse der zwischen dem Patienten und dem Forschungsverbund auszutauschenden Informationen alle für diesen Anwendungsfall relevanten auszutauschenden Informationen aufgeführt?

Bereitstellen von Daten durch den Forschungsverbund:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

Bereitstellen von Daten durch den Patienten:

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

3. Herleitung der Kommunikationsmuster und Ableitung der Anforderungen an die Systeme

Dieser Kommentierungsbogen dient den Reviewern zur Stellungnahme in Bezug auf die folgenden zwei Fragen:

1) Wurden alle Datenschutzanforderungen, die sich aus dem Kontext der Anwendungsfälle ergeben, identifiziert?

2) Werden die aus dem Kontext der Anwendungsfälle identifizierten Datenschutzanforderungen durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Die Reviewer können für jeden Anwendungsfall die Frage beantworten, ob die Datenschutzanforderungen, die sich aus dem Kontext der Anwendungsfälle ergeben, identifiziert wurden? Die Reviewer können „Ja“ ankreuzen, wenn alle Datenschutzanforderungen identifiziert wurden und „Nein“, falls weitere Datenschutzanforderungen berücksichtigt werden müssen. Sollten die Reviewer „Nein“ ankreuzen, so können sie unter „Wenn nein, bitte weitere Anforderungen nennen:“ entsprechende Anforderungen aufführen. Dies bezieht sich immer auf die erste Frage in den nachfolgenden Abschnitten, also 3.x.1.

Werden Datenschutzanforderungen identifiziert, so sollen diese durch Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt werden.

Jeder Reviewer kann hier für jeden Anwendungsfall „Ja“ ankreuzen, wenn die Anforderung richtig durch eine neue Anforderung an eines der Systeme abgedeckt wird. Er kann „Nein“ ankreuzen, wenn die Anforderung nicht richtig abgedeckt wird. Sollte der Reviewer „Nein“ ankreuzen, so kann er unter „Wenn nein, bitte kommentieren“ seine Entscheidung begründen. Dies bezieht sich immer auf die zweite Frage in den nachfolgenden Abschnitten, also 3.x.2. Diese Frage wird nur aufgeführt, wenn für den jeweiligen Anwendungsfall vorher eine entsprechende Datenschutzanforderung identifiziert wurde.

3.1. Anwendungsfall 1-1 (Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler)

3.1.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Anmeldung eines Patienten an einem Forschungsverbund durch einen Behandler“ ergeben, identifiziert?

Ergebnis der Analyse: Es wurden keine Anforderungen identifiziert.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.2. Anwendungsfall 1-2 (Kontaktieren eines Patienten über den Verwalter der Patientenliste)

3.2.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Kontaktieren eines Patienten über den Verwalter der Patientenliste“ ergeben, identifiziert?

Ergebnis der Analyse: Es muss eine Überprüfung der Einwilligung erfolgen, bevor ein Patient kontaktiert wird.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.2.2. Werden die identifizierten Datenschutzanforderungen aus dem Kontext des Anwendungsfalls „Kontaktieren eines Patienten über den Verwalter der Patientenliste“ durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Neue Anforderung an die Forschungsschnittstelle: Die Forschungsschnittstelle muss den Einwilligungsstatus überprüfen.

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

3.3. Anwendungsfall 1-3 (Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten)

3.3.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Aktualisieren der identifizierenden bzw. Kontaktdaten eines Patienten“ ergeben, identifiziert?

Ergebnis der Analyse: Es dürfen nur Kontaktdaten bzw. identifizierende Daten des Patienten an die Patientenliste übertragen werden.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.3.2. Werden die identifizierten Datenschutzanforderungen aus dem Kontext des Anwendungsfalls „Kontaktieren eines Patienten über den Verwalter der Patientenliste“ durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Neue Anforderung an die Forschungsschnittstelle: Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Patientenliste über seine ePA nur seine Kontaktdaten bzw. identifizierenden Daten bereitstellen kann.

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

3.4. Anwendungsfall 1-4 (Recht des Patienten auf Auskunft)

3.4.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Recht des Patienten auf Auskunft“ ergeben, identifiziert?

Ergebnis der Analyse: Es wurden keine Anforderungen identifiziert.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.5. Anwendungsfall 1-5 (Rückzug der Einwilligung)

3.5.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Rückzug der Einwilligung“ ergeben, identifiziert?

Ergebnis der Analyse: Es wurden keine Anforderungen identifiziert.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.6. Anwendungsfälle 2-1 (Erfassung und Zugriff auf Daten im Behandlungsprozess) und 2-2 (Erfassung und Zugriff auf Daten durch einen Patienten)

3.6.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext der Anwendungsfälle UC-2-1 und UC-2-2 ergeben, identifiziert?

Ergebnis der Analyse: Es dürfen dem Versorgungsmodul nur Daten bereitgestellt werden, für die der Patient im Rahmen eines Forschungsvorhabens eine Einwilligung abgegeben hat.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.6.2. Werden die identifizierten Datenschutzanforderungen aus dem Kontext der Anwendungsfälle UC-2-1 und UC-2-2 durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Neue Anforderung an die Forschungsschnittstelle: Die Forschungsschnittstelle muss sicherstellen, dass der Patient der Versorgungsdatenbank nur Daten bereitstellt, die auch im Rahmen des Forschungsvorhabens benötigt werden und für die eine Einwilligung des Patienten vorliegt.

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

3.7. Anwendungsfall 2-3 (Rekrutierung von Patienten)

3.7.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Rekrutierung von Patienten“ ergeben, identifiziert?

Ergebnis der Analyse: Es muss vor der Kontaktaufnahme überprüft werden, ob der Patient eingewilligt hat zwecks einer Rekrutierung kontaktiert zu werden.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.7.2. Werden die identifizierten Datenschutzanforderungen aus dem Kontext des Anwendungsfalls „Rekrutierung von Patienten“ durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Neue Anforderung an die Forschungsschnittstelle: Eine Kontaktaufnahme bedarf der Einwilligung des Patienten, daher muss die Forschungsschnittstelle, wie im Anwendungsfall zur Kontaktierung auch hier überprüfen, ob der Patient eingewilligt hat, dass er zwecks einer Rekrutierung kontaktiert werden darf.

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

3.8. Anwendungsfall 2-4 (Expertenforum)

3.8.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Expertenforum“ ergeben, identifiziert?

Ergebnis der Analyse: Es wurden keine Anforderungen identifiziert.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.9. Anwendungsfall 2-5 (Informieren eines Patienten über Forschungsergebnisse)

3.9.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Informieren eines Patienten über Forschungsergebnisse“ ergeben, identifiziert?

Ergebnis der Analyse: Es muss vor der Kontaktaufnahme überprüft werden, ob der Patient eingewilligt hat, zwecks neuer Forschungsergebnisse kontaktiert zu werden.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.9.2. Werden die identifizierten Datenschutzanforderungen aus dem Kontext des Anwendungsfalls „Informieren eines Patienten über Forschungsergebnisse“ durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Neue Anforderung an die Forschungsschnittstelle: Eine Kontaktaufnahme zwecks Übermittlung neuer Forschungsergebnisse bedarf der Einwilligung des Patienten, daher muss die Forschungsschnittstelle, wie im Anwendungsfall zur Kontaktierung auch hier überprüfen, ob der Patient eingewilligt hat, über neue Forschungsergebnisse informiert zu werden.

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

3.10. Anwendungsfall 2-6 (Recht des Patienten auf Auskunft)

3.10.1. Wurden alle Datenschutzanforderungen, die sich aus dem Kontext des Anwendungsfalls „Recht des Patienten auf Auskunft“ ergeben, identifiziert?

Ergebnis der Analyse: Es muss durch den Forschungsverbund festgelegt werden, welche Informationen einem Patienten direkt aus der Versorgungsdatenbank bereitgestellt werden können und welche über einen behandelnden Arzt zur Verfügung gestellt werden müssen.

Ja: ☐ Nein: ☐ Wenn nein, bitte weitere Anforderungen nennen:

3.10.2. Werden die identifizierten Datenschutzanforderungen aus dem Kontext des Anwendungsfalls „Recht des Patienten auf Auskunft“ durch die Anforderungen an das ePA-System, das Forschungssystem und die Forschungsschnittstelle abgedeckt?

Neue Anforderung an die Forschungsschnittstelle: Es muss durch den Forschungsverbund festgelegt werden, welche Informationen einem Patienten direkt aus der Versorgungsdatenbank bereitgestellt werden können und welche über einen behandelnden Arzt zur Verfügung gestellt werden müssen. Diese Regeln müssen in der Forschungsschnittstelle abgebildet und durchgeführt werden.

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4. Umsetzung der Datenschutzanforderung des Versorgungsmoduls durch das Kommunikationsmodell

Mit diesem Kommentierungsbogen sollen die Reviewer zu folgenden zwei Fragen Stellung nehmen:

1) Sind die Anforderungen an einen datenschutzkonformen Betrieb des Versorgungsmoduls vollständig aufgeführt?

2) Sind bei der Beschreibung der Umsetzung der generischen Kommunikationsmuster des Kommunikationsmodells über eine Erweiterung der Infrastruktur des ePA-Systems alle herausgearbeiteten Datenschutzanforderungen berücksichtigt worden?

Es wurden vier allgemeine Datenschutzanforderungen an das Versorgungsmodul identifiziert (siehe nachfolgende Auflistung). Diese Datenschutzanforderungen sollen durch das Kommunikationsmodell umgesetzt werden. Da der Anspruch besteht, möglichst alle Datenschutzanforderungen des Versorgungsmoduls zu erfüllen, sollten diese möglichst vollständig sein.

1) Die medizinischen Daten des Patienten aus dem Versorgungsmodul dürfen nur ihm und im Behandlungszusammenhang stehenden Personen zusammen mit den identifizierenden Daten des Patienten zugänglich gemacht werden.

2) Das Pseudonym des Patienten (PIDv) darf nur zwischen der Versorgungsdatenbank und der Patientenliste kommuniziert und auch nur dort (zwischen)gespeichert werden. Es darf nur den Systemverwaltern der Versorgungsdatenbank bzw. der Patientenliste zugänglich gemacht werden.

3) Der Patientenliste bzw. ihrem Systemverwalter dürfen die medizinischen Daten der Patienten in der Versorgungsdatenbank nicht zugänglich gemacht werden.

4) Der Versorgungsdatenbank bzw. ihrem Systemverwalter dürfen die identifizierenden Daten des Patienten in der Patientenliste nicht zugänglich gemacht werden.

Jeder Reviewer kann nachfolgend kommentieren, ob es weitere Datenschutzanforderungen aus Sicht des Versorgungsmoduls gibt. Sollten die Reviewer „Ja“ ankreuzen, so können sie im Feld „Weitere Anforderungen“ die Anforderungen ergänzen. Sollten alle Anforderungen berücksichtigt worden sein, so können sie „Nein“ ankreuzen:

Ja: ☐ Nein: ☐ Weitere Anforderungen:

Das Kommunikationsmodell besteht aus vier generischen Kommunikationsmustern. Diese werden in textueller Form und als Sequenzdiagramm beschrieben. Um die Frage zu beantworten, ob die herausgestellten Datenschutzanforderungen des Versorgungsmoduls durch das Kommunikationsmodell richtig umgesetzt worden sind, kann jeder Reviewer für jede beschriebene Kommunikation des Kommunikationsmodells jeweils die Datenschutzanforderung wie folgt kommentieren. Die Reviewer können „Ja“ ankreuzen, wenn die Datenschutzanforderung richtig umgesetzt wurde und „Nein“ wenn die Anforderung anders umgesetzt werden muss. Sollten sie „Nein“ ankreuzen, dann können die Reviewer diese Entscheidung unter „Wenn nein, bitte kommentieren“ entsprechend begründen. Dies

bezieht sich auf alle Fragen in den nachfolgenden Abschnitten. Diese Fragen beziehen nur die grundsätzlichen Datenschutzanforderungen, die für das Versorgungsmodul gelten, ein. Spezielle Datenschutzanforderungen, die sich aus den Anwendungsfällen ergeben, werden nicht berücksichtigt, da sie sich auf die Autorisierung beziehen und somit erst im Sicherheitskonzept Berücksichtigung finden (siehe auch Abschnitt 4.2). Bei der Überprüfung der Einhaltung der Datenschutzanforderungen bitte auch die Ableitung der Architekturentscheidungen berücksichtigen (siehe Abschnitt 4.2).

4.1. Informationen aus einer Patientenliste einer ePA bereitstellen

4.1.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.1.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.1.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.1.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.2. Informationen aus einer ePA einer Patientenliste bereitstellen

4.2.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.2.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.2.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.2.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.3. Informationen aus einer Versorgungsdatenbank einer ePA bereitstellen

4.3.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.3.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.3.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.3.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.4. Informationen aus einer ePA einer Versorgungsdatenbank bereitstellen

4.4.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.4.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.4.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

4.4.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?

Ja: ☐ Nein: ☐ Wenn nein, bitte kommentieren:

A6.2. Auswertung des Reviews

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
1. Auswahl der Anwendungsfälle des Versorgungsmoduls					
1.1. Patientenliste					
Anwendungsfall - Anmeldung eines Patienten an einem Forschungsverbund (Variante A)	Ja	Ja	Ja		
Anwendungsfall - Anmeldung eines Patienten an einem Forschungsverbund (Variante B)	Ja	Nein	Nein	Reviewer 1: Hängt von der Organisation des FV ab.	Muss nicht berücksichtigt werden, da nur das Versorgungsmodul ohne die Kombination weiterer Module berücksichtigt wird.
Anwendungsfall - Recht des Patienten auf Auskunft	Ja	Ja	Ja		
Anwendungsfall - Aktualisierung der Daten	Ja	Ja	Ja		
Anwendungsfall - Patient kontaktieren	Ja	Ja	Ja		
Anwendungsfall - Rückzug der Einwilligung	Ja	Ja	Ja		
Anwendungsfall - Übertragen von Daten an die Forschungsdatenbank aus dem Versorgungs-kontext oder aus dem Studienkontext	Nein	Nein	Nein		
Anwendungsfall - Depseudonymisierung zur Datenqualitätssicherung	Nein	Nein	Nein		
Anwendungsfall - Todesfall eines Patienten oder Probanden	Nein	Nein	Nein		
Anwendungsfall - Umpseudonymisierung (Ersetzen vorhandener Pseudonyme durch neue)	Nein	Nein	Nein		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
1.2. Versorgungsdatenbank					
Anwendungsfall - Aufnahme in die Behandlungsdatenbank / das Versorgungsmodul	Ja	-	Ja		
Anwendungsfall - Erfassung und Zugriff auf Daten im Behandlungsprozess / Zugriff auf Identitätsdaten zu Behandlungszwecken	Ja	Ja	Ja		
Anwendungsfall - Vergabe von Zugriffs-rechten / Autorisierung von Mit- oder Weiterbehandlern	Ja	Ja	Ja		
Anwendungsfall - Zugriff auf Daten für Zwecke der Qualitätssicherung	Nein	Nein	Nein	Reviewer 3: Grundsätzlich werden durch die Beschreibung des Anwendungsfalles Rückfragen an die Patienten nicht vollständig ausgeschlossen, z. B. wenn Inkonsistenzen im Datenbestand sich nicht durch einen Abgleich mit den Daten aus der Versorgung auflösen lassen o.ä. Diese Spezialfälle erscheinen allerdings im vorliegenden Kontext vernachlässigbar, so dass dieser Anwendungsfall aus der Betrachtung berechtigterweise ausgeschlossen wird.	Wird nicht aufgenommen, da nur Hinweis.
Anwendungsfall - Tod des Patienten	Nein	Nein	Nein		
Anwendungsfall - Machbarkeit einer Auswer-tung oder Studie prüfen	Nein	Nein	Nein		
Anwendungsfall - Rekrutierung für neue Studien	Ja	Ja	Ja		
Anwendungsfall - Export von Daten	Nein	Nein	Nein		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
Anwendungsfall - Expertenforum	Nein	Nein	Ja	Reviewer 1: Ergebnisse des Forums werden zunächst nur dem behandelnden Arzt bekannt gemacht. Reviewer 2: Fraglich - ich hatte das Expertenforum bisher eher als "Referenzpanel" z. B. zur Kontrolle wesentlicher Röntgenbefunde angesehen	Anwendungsfall wurde auf Grund der Kommentare aus dem Forschungssystem entfernt.
Anwendungsfall - Informieren eines Patienten über Forschungsergebnisse	Ja	Ja	ja		
Anwendungsfall - Informieren eines Patienten über Forschungsergebnisse	Nein	Nein	Nein		
Anwendungsfall - Recht des Patienten auf Auskunft	Ja	Ja	Ja		
Anwendungsfall - Rückzug der Einwilligung / Löschen, sperren oder anonymisieren medizinischer Daten	Ja	Ja	Ja		
2. Umsetzung der Kommunikation der Anwendungsfälle des Versorgungsmoduls					
2.1.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfall 1-1	Ja	Ja	Ja		
2.1.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 1-1: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Ja Ja	 Ja Ja	 Ja Ja		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
2.2.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfall 1-2	Ja	Ja	Ja		
2.2.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 1-2: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Ja Ja	 Ja Ja	 Ja Ja		
2.3.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfall 1-3	Ja	Ja	Ja		
2.3.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 1-3: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Ja Ja	 Ja Ja	 Ja Ja		
2.4.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfall 1-4	Nein	Ja	Ja	Reviewer 1: Die Rolle des Datenschutzbeauftragten ist fehlinterpretiert. Stattdessen ist der in der Aufklärung / Einwilligung genannte Ansprechpartner einzusetzen. Reviewer 2: Mir ist unklar, warum bei Informationen aus der Patientenliste (im Wesentlichen nur IDAT + Projektzugehörigkeit) überhaupt eine Entscheidung über eine Erläuterung durch einen Arzt nötig ist.	Zu 1. Datenschutzbeauftragter wurde durch „Ansprechpartner des Forschungsverbundes“ in der gesamten Arbeit ersetzt. Zu 2. Wurde im Abschnitt 6.2.4 zum Recht des Patienten auf Auskunft über die Daten in der Patientenliste entsprechend angepasst

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
2.4.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 1-4: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Ja Ja	 Ja Ja	 Ja Ja		
2.5.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfall 1-5	Nein	Nein	Nein	<u>Reviewer 1:</u> Wegen gesetzlicher o. ä. Aufbewahrungs- und Archivierungs-pflichten können u. U. nicht alle Daten gelöscht werden. Evtl. Anonymisierung. <u>Reviewer 2:</u> Sonderfälle anonymisierte Weiterführung der Daten bzw. keine Löschung aufgrund gesetzlicher Vorgaben (z. B. AMG) sollten ergänzt werden. <u>Reviewer 3:</u> Die Reihenfolge der Löschvorgänge in der Patientenliste und der Versor-gungsdatenbank sollte so abgeändert werden, dass die Löschbestätigung von der Versorgungsdatenbank anhand des mit übermittelten Pseudonyms noch einem eindeutigen Datensatz in der Patientenliste zugeordnet werden kann, der daher erst danach gelöscht werden sollte.	Zu 1. und 2. Kommentare wurden als Fußnote im Abschnitt 6.2.5 eingearbeitet. Zu 3. Beschreibung wurde im Abschnitt 6.2.5 unter „Ablauf“ angepasst.
2.5.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 1-5: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Nein Ja	 Ja Ja	 Ja Ja	<u>Reviewer 1:</u> Zu a. Angabe der nicht gelöschten Daten.	Auszutauschende Informationen wurden im Abschnitt 6.2.5 um den Kommentar ergänzt.

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
2.6.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation • des Anwendungsfalls 2-1 • des Anwendungsfalls 2-2	 Ja Ja	 Ja Ja	 Ja Ja		
2.6.2. Berücksichtigung aller relevanten auszutauschenden Informationen für • Anwendungsfall 2-1: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten • Anwendungsfall 2-2: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Nein Nein Ja Ja	 Ja Ja Ja Ja	 Nein Ja Ja Ja	<u>Reviewer 1:</u> Zu UC-2-1.a. Bereitstellen von Daten durch den Forschungsverbund Zu UC-2-1.b. Die Daten werden vom behandelnden Arzt bereitgestellt, der sie vom Patienten erhebt / gewinnt. <u>Reviewer 3:</u> Zu UC-2-1.a. Der Forschungsverbund muss zur Aktualisierung die alten Daten zur Verfügung stellen, sonst könnte der Behandler nicht feststellen, ob überhaupt etwas zu aktualisieren ist. Zu UC-2-1.b. Es bleibt etwas unklar, warum der Anwendungsfall berücksichtigt wird, da ja genau-genommen die Daten nicht vom Patienten sondern vom Behandler selbst bereit gestellt werden (im Beisein oder nach der Untersuchung des Patienten).	Zu1 und 2 Anzeigen / Bereitstellen der Daten in UC-2-1a wurde im Abschnitt 6.3.2 unter Auszutauschende Informationen ergänzt Anwendungsfall wurde aufgenommen, da es eine indirekte Bereitstellung durch den Patienten über den Arzt gibt.
2.7.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfall 2-3	Ja	Ja	Ja		
2.7.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 2-3: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Ja Ja	 Ja Ja	 Ja Ja		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
2.8.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfalls 2-4	Nein	Nein	Ja	Reviewer 1: Es geht im Expertenforum eher um Ideen zur Behandlung als um ein Votum. Daher ist der Patient auch nicht Adressat der Informationen. Reviewer 2: Es bleibt offen, ob der Patient im Expertenforum pseudonym oder identifiziert betrachtet wird. Bei den Vorbedingungen macht "...eingewilligt über neue Forschungsvorhaben informiert zu werden..." m.E. keinen Sinn. Das Ergebnis des Expertenforums wird m.E. nicht in jedem Fall an den Patienten zurückkommuniziert werden (s. 1.2) Reviewer 3: Bei den beteiligten Systemen sollte die Patientenliste mit aufgeführt werden, da diese mindestens initial bei der Freigabe eines Patienten durch den Behandler involviert sein muss.	Anwendungsfall wurde gelöscht.
2.8.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 2-4: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 entfällt entfällt	 Ja Ja	 Ja Ja		
2.9.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfalls 2-5	Nein	Ja	Ja	Reviewer 1: Evtl. muss bei gendiagnostischen Ergebnissen ein Humangenetiker eingeschaltet werden.	Kommentar wurde als Fußnote im Abschnitt 6.3.5 Informieren eines Patienten über Forschungsergebnisse eingearbeitet.

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
2.9.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 2-5: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Ja Ja	 Nein Ja	 Ja Ja	<u>Reviewer 2:</u> Zu a. EX-PID sollte ergänzt werden (oder ist sie implizit?); es ist die Frage, ob die EX-PID ggf. zusammen mit anderen Identifikatoren weiter vorne erläutert werden sollte (statt nur im Abkürzungsverzeichnis)	Erläuterung der EX-PID wurde im Abschnitt 4.2.3 aufgenommen.
2.10.1. Berücksichtigung aller relevanten Anforderungen bei der Beschreibung der Kommunikation des Anwendungsfalls 2-5	Nein	Ja	Ja	<u>Reviewer 1:</u> Der Datenschutzbeauftragte ist hier nicht primär zuständig (außer er hat eine Doppelfunktion). Das Recht auf Nichtwissen könnte relevant sein. <u>Reviewer 2:</u> Im Gegensatz zur Betrachtung bei der Patientenliste wird hier (Usecase-Beschreibung) nicht auf die ggf. notwendige Erläuterung der Daten durch einen Arzt eingegangen, obwohl hier auch MDAT beteiligt sind <u>Reviewer 3:</u> Eine noch bessere Variante zur Umsetzung dieses Anwendungsfalles wäre das Abrufen der Daten aus der Versorgungsdatenbank analog zum Abruf durch den Behandler (via TKT), so dass die PID auch dem Datenschützer gegenüber nicht offenbart werden müsste.	Zu 1: Datenschutzbeauftragter wurde durch Ansprechpartner des Forschungsverbundes ausgetauscht. Recht auf Nichtwissen wurde im Abschnitt 6.3.6 unter Analyse aufgenommen. Zu 2: Erläuterung der Informationen wurde im Abschnitt 6.3.6 unter Analyse aufgenommen. Zu 3: Kommentar ist richtig, wurde aber nicht aufgenommen, da bei der Umsetzung über die ePA die PID dem Ansprechpartner des Forschungsverbundes verborgen bleibt.

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
2.10.2. Berücksichtigung aller relevanten auszutauschenden Informationen für Anwendungsfall 2-5: a. Bereitstellen von Daten durch den Forschungsverbund b. Bereitstellen von Daten durch den Patienten	 Nein Ja	 Ja Ja	 Ja Ja	Reviewer 1: Zu a. Das Recht auf Nichtwissen könnte relevant sein.	Recht auf Nichtwissen wurde im Abschnitt 6.3.6 unter Analyse aufgenommen.
3. Herleitung der Kommunikationsmuster und Ableitung der Anforderungen an die Systeme					
3.1.1. Identifikation aller Datenschutz-anforderungen aus dem Kontext des Anwendungsfalls 1-1	Ja	Ja	Ja		
3.2.1. Identifikation aller Datenschutzan-forderungen aus dem Kontext des Anwendungsfalls 1-2	Ja	Ja	Ja		
3.2.2. Abdeckung der identifizierten Datenschutzanforderungen des Anwendungsfalls 1-3	Ja	Ja	Ja		
3.3.1. Identifikation aller Datenschutzan-forderungen aus dem Kontext des Anwendungsfalls 1-3	Ja	Ja	Ja		
3.3.2. Abdeckung der identifizierten Datenschutzanforderungen des Anwendungsfalls 1-3	Ja	Ja	Ja		
3.4.1. Identifikation aller Datenschutzan-forderungen aus dem Kontext des Anwendungsfalls 1-4	Ja	Ja	Ja	Reviewer 3: Eine, wenn auch nicht zwingende, Anforderung könnte sein, dass auch der Datenschützer die PID des Patienten nicht kennen sollte. Meiner Einschätz-ung nach wird diese Anforderung aber durch den Einsatz der hier konzipierten Forschungsschnittstelle automatisch eingehalten.	Wird nicht aufgenommen, da nur Hinweis.

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
3.5.1. Identifikation aller Datenschutzan-forderungen aus dem Kontext des Anwendungsfalls 1-5	Nein	Ja	Ja	Reviewer 1: Eventuelle Anonymisierungspflicht von Daten, die aufbewahrt oder archiviert werden müssen. Reviewer 2: Es sollten auch die Sonderfälle anonymisierte Weiterführung der Daten sowie Ausschluss des Löschens durch gesetzliche Vorgaben berücksichtigt werden.	Zu 1. und 2.: Kommentare wurden als Fußnote im Abschnitt 6.2.5 eingearbeitet.
3.6.1. Identifikation aller Datenschutz-anforderungen aus dem Kontext der Anwendungsfälle 2-1 und 2-2	Ja	Ja	Ja		
3.6.2. Abdeckung der identifizierten Datenschutzanforderungen der Anwendungsfälle 2-1 und 2-2	Ja	Ja	Ja		
3.7.1. Identifikation aller Datenschutz-anforderungen aus dem Kontext des Anwendungsfalls 2-3	Ja	Ja	Ja		
3.7.2. Abdeckung der identifizierten Datenschutzanforderungen des Anwendungsfalls 2-3	Ja	Ja	Ja		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
3.8.1. Identifikation aller Datenschutz-anforderungen aus dem Kontext des Anwendungsfalls 2-4	Nein	Ja	Ja	Reviewer 1: Pseudonymisierung Reviewer 3: Etwas unklar bleibt, leider auch im Leitfaden, ob es einer speziellen Einwilligung bedarf, dass die Daten des Patienten in pseudonymer Form im Expertenforum freigegeben werden. Im Review-Leitfaden heißt es auf S. 47 hierzu irreführend: "Der Patient hat eingewilligt über neue Forschungs-vorhaben informiert zu werden." Im allgemeinen Leitfaden zum Datenschutz wird lediglich darauf hingewiesen, dass das Expertenforum in der Patienten-aufklärung beschrieben sein muss (so dass sich dann die Einwilligung auch darauf mit beziehen kann).	Anwendungsfall „Expertenforum“ wurde gelöscht (siehe oben).
3.9.1. Identifikation aller Datenschutz-anforderungen aus dem Kontext des Anwendungsfalls 2-5	Ja	Ja	Ja		
3.9.2. Abdeckung der identifizierten Datenschutzanforderungen des Anwendungsfalls 2-5	Ja	Ja	Ja		
3.10.1. Identifikation aller Datenschutz-anforderungen aus dem Kontext des Anwendungsfalls 2-6	Ja	Ja	Ja		
3.10.2. Abdeckung der identifizierten Datenschutzanforderungen des Anwendungsfalls 2-6	Ja	Ja	Ja		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
4. Umsetzung der Datenschutzanforderung des Versorgungsmoduls durch das Kommunikationsmodell					
4.1.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?	Ja	Ja	Ja	Reviewer 2: Das Konzept lässt die Authentifizierung der Komponenten untereinander offen - wie wird verhindert, dass sich eine "illegale" Komponente als Patientenliste oder ePA ausgibt?	Die Authentifizierung der Komponenten wird in der Sicherheitsarchitektur beschrieben (siehe Abschnitt 9.3) und war somit nicht im Review enthalten.
4.1.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?	Ja	Ja	Ja		
4.1.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?	Ja	Ja	Ja		
4.1.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?	Ja	Ja	Ja		
4.2.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?	Ja	Ja	Ja		
4.2.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?	Ja	Ja	Ja		
4.2.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?	Ja	Ja	Ja		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
4.2.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?	Ja	Ja	Ja		
4.3.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?	Ja	Ja	Ja	Reviewer 2: Abschnitte 4.3 und 4.4 vertauscht?	Die Abschnitte 4.3 und 4.4 wurden im Kommentierungs-bogen vertauscht. Das hat aber keine Auswirkung auf die Ergebnisse des Reviews oder die Arbeit.
4.3.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?	Ja	Ja	Ja		
4.3.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?	Ja	Ja	Ja		
4.3.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?	Ja	Ja	Ja		
4.4.1. Besteht weiterhin nur für die berechtigten Personen Zugang zu den personenbezogenen, medizinischen Daten?	Ja	Ja	Ja		
4.4.2. Wird das Patientenpseudonym bei dieser Kommunikation ausschließlich dem IDAT-Verwalter bzw. dem MDAT-Verwalter offenbart?	Ja	Ja	Ja		

Frage	Reviewer 1	Reviewer 2	Reviewer 3	Kommentare	Einarbeitung der Kommentare
4.4.3. Bleiben bei dieser Kommunikation dem IDAT-Verwalter bzw. der Patientenliste die medizinischen Daten verborgen?	Ja	Nein	Ja	Reviewer 2: Warum erfolgt die Prüfung der Autorisierung (Schritt 7) beim IDAT-Client und nicht beim MDAT-Client? Es sollte zumindest klargestellt werden, dass in diesem Schritt nur Metadaten zum Informationsobjekt übertragen werden, und nicht der medizinische Inhalt selbst.	Dass nur Metadaten an den Forschungs-Client-IDAT übertragen werden und keine medizinischen Daten des Patienten, wird in der Sicherheitsarchitektur erläutert (9.4), die nicht Bestandteil des Review war.
4.4.4. Bleibt dem MDAT-Verwalter bzw. der Versorgungsdatenbank bei dieser Kommunikation die Identität des Patienten verborgen?	Ja	Ja	Ja		

Tabelle 62: Auswertung des Reviews

A7. Verzeichnisse Arbeit und Anhang

A7.1. Abkürzungsverzeichnis

AAL	Ambient Assisted Living
AG DS	Arbeitsgruppe Datenschutz
AHLTA	Armed Forces Health Longitudinal Technology Application
AIS	Arztinformationssystem
AMG	Arzneimittelgesetz
AMIA	American Medical Informatics Association
AO	Anforderungsobjekt
BildDAT	Bilddaten
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesministerium für Gesundheit
BO	Bereitstellungsobjekt
BRIDG	Biomedical Research Integrated Domain Group
CARRA	Childhood Arthritis & Rheumatism Research Alliance
CBR	Call By Reference
CDISC	Clinical Data Interchange Standards Consortium
CDMS	Clinical Data Management System
CDW	Clinical Data Warehouse
CRF	Case Report Form
DebugIT	Detecting and Eliminating Bacteria Using Information Technology
DSK	Datenschutzkonzept
DW	Data Warehouse
eCRF	Electronic Case Report Form
eEPA	Einrichtungsübergreifende Elektronische Patientenakte
eFA	Einrichtungsübergreifende elektronische / medizinische Fallakte
eGA	elektronische Gesundheitsakte
eGK	elektronische Gesundheitskarte (auch E-Card genannt)
EDC	Electronic Data Capture
EHR	Electronic Health Record
EHR4CR	Electronic Health Records for Clinical Research
EMR	Electronic Medical Record
ePA	elektronische Patientenakte
ePA-ID	Lokalisierungs-informationen der ePA (auch Akten-ID genannt)
ePCRN	electronic Primary Care Research Network
EPR	Electronic Patient Record
EX-PID	Pseudonym für den Export an Forscher

FARSITE	Feasibility Assessment and Recruitment System for Improving Trial Efficiency
FDA	Food and Drug Administration
FuE	Forschung und Entwicklung
GCP	Good Clinical Practice
GMG	GKV-Modernisierungsgesetz bzw. Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
HBA	Elektronischer Heilberufsausweis
HL7	Health Level 7
ICW	InterComponentWare AG
IDAT	Identifizierende Daten
IDAT-Verwalter	Verwalter der Patientenliste
iEPA	institutionelle Elektronische Patientenakte
IO	Informationsobjekt
KeyMDO	Im LE-Client erstellter symmetrischer Schlüssel
KIS	Krankenhausinformationssystem
KVNR	Krankenversicherungsnummer
LabID	ID zur Identifizierung von Proben
LE	Leistungserbringer
LE-Client	Leistungserbringer-Client
LE-Postfach	Leistungserbringer-Postfach
LE-Schnittstelle	Leistungserbringer-Schnittstelle
LE-System	Leistungserbringer-System
LfD	Landesbeauftragter für den Datenschutz
MBDS	Minimum Basic Data Set
MDAT	Medizinische Daten
MDATw	Entspricht dem Begriff MDAT in dieser Arbeit.
MDAT-Verwalter	Verwalter der medizinischen Datenbank eines Forschungsverbundes (z.B. Versorgungsdatenbank).
MDO	Medizinisches Datenobjekt
Mesh	Medical Subject Headings
MIE2006	Medical Informatics Europe 2006
OMG	Object Management Group
OrgDAT	Organisatorische Daten (Begleitdaten einer Probe)
pEPA	persönliche Elektronische Patientenakte
PCHR	Personally Controlled Health Record
PHR	Personal (Electronic) Health Record

PID	Patientenidentifikator bzw. Patientenpseudonym allgemein
PIDs	Patientenidentifikator bzw. Patientenpseudonym des Studienmoduls
PIDv	Patientenidentifikator bzw. Patientenpseudonym des Versorgungsmoduls
PKI	Public-Key-Infrastruktur
PONTE	Efficient Patient Recruitment for Innovative Clinical Trials of Existing Drugs to other Indications
prkAS	Privater Schlüssel der ePA
prkMD	Privater Schlüssel der medizinischen Datenbank eines Forschungsverbundes
prkVDB	Privater Schlüssel der Versorgungsdatenbank
ProbDAT	Probenanalysedaten (auch AnaDAT genannt)
PSN	Pseudonym (zweiter Stufe)
pubAS	Öffentliche Schlüssel der ePA
pubeGK	Öffentlicher Schlüssel der eGK
pubHBA	Öffentlicher Schlüssel des HBAs
pubMD	Öffentlicher Schlüssel der medizinischen Datenbank eines Forschungsverbundes
pubSMC	Öffentlicher Schlüssel der SMC
pubVDB	Öffentlicher Schlüssel der Versorgungsdatenbank
RE-USE	Retrieve from EHR Useful clinical data for Secondary Exploitation
RLUS	Retrieve, Locate, and Update Service
SemSigGetePA-ID	Semantic Signifier zum Anfordern einer ePA-ID
SemSigGetPID	Semantic Signifier zum Anfordern einer PID
SemSigGetTID	Semantic Signifier zum Anfordern einer TID
SGB V	Sozialgesetzbuch V
SIC	Subject Identification Code (Pseudonym eines Patienten für eine Studie)
SMC	Secure Module Card
SOAP	Simple Object Access Protocol
STRIDE	Stanford Translational Research Integrated Database Environment
symkeyAS1/n	Symmetrische Schlüssel zur Sicherung des prkAS.
symkeyMDO	Symmetrische Schlüssel zum Sichern eines medizinischen Datenobjektes in der ePA
symkeyMDO_Kopie	Kopie des symmetrischen Schlüssels zum Sichern eines medizinischen Datenobjektes in der ePA
TI	Telematikinfrastruktur

TID	Transaktions-ID
TKT	Ticket
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
TRANSFoRm	Translational Research and Patient Safety in Europe
UC	Use Case
UML	Unified Modeling Language
VE	Voraussetzung an das ePA-System
VF	Voraussetzung an das Forschungssystem
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations

A7.2. Abbildungsverzeichnis

A7.3. Tabellenverzeichnis

Lebenslauf

Persönliche Daten

Name: Krister Helbing
Geboren am 12.10.1980 in Hamburg
Staatsangehörigkeit: deutsch

Wissenschaftlicher Werdegang

2007-2012	Promotion an der Georg-August-Universität in Göttingen, Dissertationsthema: „Erweiterung des Konzeptes einer Patientenakte nach § 291a SGB V um eine Schnittstelle für die medizinische Forschung“
2005 - 2007	Master of Science in Medical Informatics (1,6) Masterthesis: „Forschungsorientierte medizinische Langzeitdokumentation auf Basis der gematik-Infrastruktur“ (1,3)
2001 - 2005	Bachelor of Science in Medical Informatics (2,0) Bachelorthesis: „Sichere Kommunikation und Authentifizierung in medizinischen Netzwerken mit Hilfe von Mikroprozessorkarten“(1,7)
2000	Allgemeine Hochschulreife, Hamburg

Veröffentlichungen, Vorträge

2011	Prototypische Umsetzung einer elektronischen Patientenakte nach § 291a SGB V für die medizinische Forschung, Vortrag: 56. GMDS-Jahrestagung (2011) in Mainz.
2010	Helbing K, Demiroglu SY, Rakebrandt F, Pommerening K, Rienhoff O, Sax U (2010) A data protection scheme for medical research networks Review after 5 years of operation. METHOD INFORM MED, 49 (6): 601-607.
2008	Datenschutzkonforme Umsetzung einer ePA für die Nutzung patientenbezogener Studiendaten in der Versorgung. Vortrag: 53. GMDS-Jahrestagung (2008) in Stuttgart.

Weiterbildung

2010-2011	Grundkurs zur Vermittlung von Basiswissen im Qualitätsmanagement
2009	Basistraining für Führungskräfte der Universitätsmedizin Göttingen

Praktika

2006	Siemens Medical Solutions, Malvern, USA,: Softwareentwicklung
2003	Information Technology Department, Metalex Manufacturing Inc, Cincinnati, USA: Softwareentwicklung, IT-Netzwerkausbau

Berufstätigkeit

Seit 2012	TMF - Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., Wissenschaftlicher Mitarbeiter
2007- 2012	Abt. Medizinische Informatik, Universitätsmedizin Göttingen, Wissenschaftlicher Mitarbeiter
2006	Abt. Medizinische Informatik, Universitätsmedizin Göttingen, Wissenschaftliche Hilfskraft
2003- 2004	Geschäftsbereich Informationstechnologie, Universitätsmedizin Göttingen, Wissenschaftliche Hilfskraft

Berlin, Dezember 2012