



U N I V E R S I T Ä T
K O B L E N Z · L A N D A U

Fachbereich 4: Informatik

Entwicklung eines Telemedizinregister- Anforderungskatalog

Diplomarbeit
im Studiengang Informatik

vorgelegt von
Dirk Steffes-Enn

Universität Koblenz-Landau
Campus Koblenz

Institut für Wirtschafts- und Verwaltungsinformatik
Professur Wimmer

Betreuer und Gutachter:

Prof. Dr. Maria A. Wimmer

Sebastian Alsbach

Koblenz, 13.06.2014

Eidesstattliche Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat und von dieser als Teil einer Prüfungsleistung angenommen wurde. Alle Ausführungen, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet.

Die Richtlinien der Forschungsgruppe für Qualifikationsarbeiten habe ich gelesen und anerkannt, insbesondere die Regelung des Nutzungsrechts.

Mit der Einstellung dieser Arbeit in die Bibliothek bin ich einverstanden. Ja Nein

Der Veröffentlichung dieser Arbeit im Internet stimme ich zu. Ja Nein

Koblenz, den 13.06.2014

Dirk Steffes-Enn

Danksagung

Hiermit möchte ich mich bei Frau Prof. Dr. Maria Wimmer und Herrn Sebastian Alsbach für die stets freundliche und sehr hilfreiche Betreuung der Diplomarbeit bedanken.

Einen besonderen Dank richte ich an meine Freundin und meine Familie, die bewundernswert viel Geduld und Unterstützung während der Arbeitsphase aufgebracht haben.

Des Weiteren richte ich meinen Dank an den Kooperationspartner dieser Arbeit, die medizinische Videobeobachtung GmbH in Koblenz und zusätzlich an Herrn Ansgar Mondorf, der als Mitarbeiter der Professur Wimmer mir konstruktive Hinweise zur Erstellung dieser Arbeit lieferte.

Zusammenfassung

Die Diplomarbeit „Entwicklung eines Telemedizinregister-Anforderungskatalog“ behandelt die Erstellung eines Anforderungskatalogs für die Entwicklung eines im telemedizinischen Bereich anwendbaren Registers zur Unterstützung von Abrechnungsvorgängen. Diese werden im deutschen Gesundheitswesen zwischen telemedizinischen Dienstleistern und Kostenträgern in Zusammenhang mit der integrierten Versorgungsform durchgeführt, um die Finanzierung durchgeführter telemedizinischer Behandlungen abzurechnen. Dabei dient das Telemedizinregister als eine datenvorhaltende Speicherstelle, die Kopien von Behandlungsdaten telemedizinischer Dienstleister aufnimmt und deren Verarbeitungsprozesse im Register protokolliert. Den beteiligten Kostenträgern wird Zugriff auf dieses Telemedizinregister gewährt, um die Validität der Therapiedaten überprüfen zu können, die ihnen durch telemedizinische Dienstleister zur Analyse vorgelegt werden. Die Arbeit beschreibt die theoretischen Grundlagen der Bereiche Datenschutz und Telemedizin, mit denen Anforderungslisten und ein SOLL-Modell eines Telemedizinregisters erstellt werden. Dieses Modell setzt sich aus Datenmodellen und Prozessbeschreibungen zusammen und wird mit Hilfe eines praktischen Beispiels einer telemedizinischen Behandlung überprüft. Die Integration verschiedener Standards, welche bei Datenaustausch-Prozessen eingesetzt werden können, ist ein weiterer Teil zur Konzeptionierung des Telemedizinregisters, zu dem mögliche Anwendungsfelder zur Erweiterung der Funktionalität beschrieben werden.

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Problemstellung.....	2
1.2	Ziele der Diplomarbeit	3
1.3	Struktureller Aufbau der Diplomarbeit	3
2	Grundlagen Telemedizin.....	5
2.1	Definitionen zur Telemedizin.....	5
2.2	Beteiligte Partner und Rollenverteilung	7
2.3	Entwicklung und Verbreitung in Deutschland	10
2.4	Internationale Entwicklung und Verbreitung	12
3	Rechtliche Grundlagen – Datenschutz.....	14
3.1	Definitionen des Datenschutzes	14
3.1.1	Grundsätze des Datenschutzes	15
3.1.2	Die „10 Gebote“ des Datenschutzes	16
3.2	Rechtliche Entwicklung	18
3.3	Verfahrensweisen im Datenschutz	19
3.3.1	Pseudonymisierung	19
3.3.2	Anonymisierung.....	21
3.3.3	Treuhänder	22
3.4	Datenschutzrechtliche Faktoren in der Medizin.....	23
4	Auflistung datenschutzrelevanter Modelle	27
4.1	Datenschutzmodelle des TMF.....	28
4.1.1	TMF – Modell A	30
4.1.2	TMF – Modell B	32
4.1.3	TMF – Modell Biodatenbanken.....	34
4.1.4	TMF Maximalmodell.....	35
4.2	Anwendbarkeit im Bereich der Telemedizin.....	37
4.3	Problemfälle	38
5	Grundlagen – Register	40
5.1	Begriffsdefinitionen Register	40
5.2	Verfahren der Datenübermittlung.....	43
5.3	Register-Speicherverwaltung	46
5.4	Projektbeispiele	50

6	Wissenschaftliche Methodik.....	54
6.1	Grundlegende Methodik.....	54
6.2	Desk-Research.....	57
6.3	Interview.....	58
6.3.1	Stakeholder.....	58
6.3.2	Thematische Struktur.....	60
6.4	Rich-Pictures.....	61
7	Anwendungsszenarien für ein Telemedizinregister.....	62
7.1	Detaillierte Beschreibung des Telemedizin – Registers.....	63
7.1.1	IST-Zustand.....	64
7.1.2	SOLL-Zustand.....	65
7.2	Module für Anwendungsszenarien.....	67
7.3	IHE – Standards.....	71
7.4	Profil XDS.b - Cross-Enterprise Document Sharing.....	75
7.4.1	Akteure bei der Verwendung des XDS.b-Profiles.....	78
7.4.2	Transaktionen bei der Verwendung des XDS.b-Profiles.....	80
7.5	Anwendungsszenarien aus sektorenfernen Projekten.....	88
8	Anforderungen an ein Telemedizin – Register.....	90
8.1	Rich-Pictures des IST- und SOLL-Zustands.....	90
8.2	Datenkategorien.....	94
8.2.1	Auswahl und Aufbereitung der Daten beim Dienstleister.....	98
8.2.2	Speicherung und Verarbeitung der Daten im Register.....	100
8.3	Anwendungsfälle.....	102
8.4	Anforderungsliste.....	107
8.4.1	Funktionale Anforderungen.....	109
8.4.2	Nichtfunktionale Anforderungen.....	111
9	SOLL – Modell eines Telemedizin – Registers.....	113
9.1	Struktur der Funktionsbereiche.....	113
9.2	Prozess – Modelle.....	115
9.2.1	I Auswahl der Daten beim Dienstleister.....	116
9.2.2	II Aufbereitung der Daten für das Register.....	116
9.2.3	III Übermittlung der Daten an das Register.....	122
9.2.4	IV Speicherung der Daten im Register.....	126
9.2.5	V Änderungen von Daten im Register.....	129

9.2.6	VI Verarbeitung von Anfragen der Kostenträger.....	132
9.2.7	VII Übermittlung der angefragten Daten	133
9.3	Praxisbezogene Überprüfung des SOLL – Modells am Beispiel der MVB GmbH.....	135
9.3.1	Bestandsanalyse der MVB GmbH	136
9.3.2	Überprüfung der einzelnen Prozessabschnitte	139
10	Diskussion und Empfehlungen	148
10.1	Reflektion	148
10.2	Offene Fragen und Problemfälle	150
10.3	Empfehlungen für weitere Anwendungsbereiche	151
11	Fazit und Ausblick.....	153
	Literaturverzeichnis.....	VI
	Anhang	XIV

Abbildungsverzeichnis

Abbildung 1, Anzahl IV-Verträge [12], [13], [14].....	11
Abbildung 2, Zuordnung mittels Hash-Funktion	20
Abbildung 3, Zuordnung mittels fester Werte	20
Abbildung 4, TMF Grundmodell [28]	29
Abbildung 5, TMF – Modell A [27]	30
Abbildung 6, Funktionsweise IDAT zu PID [33]	31
Abbildung 7, TMF – Modell B [32].....	33
Abbildung 8, TMF – Modell Biodatenbank [34]	34
Abbildung 9, Maximalmodell TMF [32]	35
Abbildung 10, Schema Register-Aufbau	42
Abbildung 11, Register – einzelne Datenübertragung	43
Abbildung 12, Register – blockweise Datenübertragung	44
Abbildung 13, zentrales Register	46
Abbildung 14, dezentrales Register	47
Abbildung 15, Cloud-Register	48
Abbildung 16, Nationales Waffenregister [41]	50
Abbildung 17, Meldeverfahren Krebsregister Bayern [43]	52
Abbildung 18, Wasserfallmodell [46].....	54
Abbildung 19, Funktionsweise Telemedizinregister.....	63
Abbildung 20, Gliederung Anwendungsszenario	67
Abbildung 21, Funktionsweise IHE [53]	72
Abbildung 22, Funktionsweise XDS [54].....	76
Abbildung 23, IHE-D XDS.b Actors and Transactions [54]	77
Abbildung 24, Transaktion Patient Identity Feed [54].....	80
Abbildung 25, Transaktion Provide and Register Document Set-b [54]	80
Abbildung 26, Transaktion Register Document Set-b [54]	81
Abbildung 27, Transaktion Registry Stored Query [54]	81
Abbildung 28, Transaktion Retrieve Document Set [54].....	82
Abbildung 29, Transaktion Provide and Register Imaging Document Set [54]	82
Abbildung 30, Transaktionen Image Document [54]	83
Abbildung 31, Transaktionen Update und Delete Document Set [54]	84

Abbildung 32, Transaktionen ID-Management [54].....	85
Abbildung 33, Transaktionen Demographics Query [54].....	86
Abbildung 34, Transaktionen Provider Informations [54].....	87
Abbildung 35, Rich-Picture IST-Zustand	91
Abbildung 36, Rich – Picture SOLL–Zustand.....	93
Abbildung 37, Anwendungsszenario C	95
Abbildung 38, Datenaufbereitung beim Dienstleister.....	98
Abbildung 39, Datentypen im Register.....	101
Abbildung 40, Anwendungsfall Datenaufbereitung	102
Abbildung 41, Anwendungsfall Telemedizinregister	104
Abbildung 42, Prozess Therapiedaten aufteilen.....	117
Abbildung 43, Prozess IDAT pseudonymisieren.....	118
Abbildung 44, Prozess MDAT+ erzeugen	119
Abbildung 45, Prozess Metadaten generieren.....	121
Abbildung 46, Prozess Userkonten erstellen	122
Abbildung 47, Prozess Sichere Verbindung herstellen.....	124
Abbildung 48, Prozess Übermittlung der Daten	125
Abbildung 49, Prozess Speicherung der Daten.....	126
Abbildung 50, Prozess Datensätze ergänzen	129
Abbildung 51, Prozess Datensätze ändern	130
Abbildung 52, Prozess Datensätze löschen.....	131
Abbildung 53, Prozess Anfrage verarbeiten	132
Abbildung 54, Prozess Export von Daten	133
Abbildung 55, Systemmodell MVB GmbH.....	136
Abbildung 56, Datenbankschema MVB GmbH	138
Abbildung 57, Beispiel Pseudonym Datenbank.....	140
Abbildung 58, Struktur Telemedizinregister für MVB GmbH.....	144

1 Einleitung

Die Telemedizin in Deutschland besitzt trotz langjährig etablierten Projektumsetzungen und verstärkter Förderung durch öffentliche Stellen eine noch vergleichsweise geringe Akzeptanz und Verbreitung durch Kostenträger im Gesundheitswesen im Vergleich mit traditionellen Behandlungsformen (ambulante / stationäre Versorgung). Den Status einer Regelleistung durch die Krankenkassen zu erhalten dient der langfristigen Sicherung von telemedizinischen Dienstleistungen.

Seit nunmehr fast 2 Jahrzehnten sind in Deutschland verschiedene Ideen und Ansätze zur telemedizinischen Versorgung realisiert worden. Diese sind aber meist nicht über einen Projektstatus hinweg gekommen. Basierend auf der demografischen Entwicklung und der Vielfalt von funktionalen Kommunikationstechnologien bietet der Sektor Telemedizin ein großes Potential an Qualitätsverbesserungen für die Bevölkerung und Kostensparnissen im Gesundheitswesen. Besonders Regionen mit strukturschwächeren Gebieten profitieren von telemedizinischen Dienstleistungen, indem beispielsweise größere Entfernungen zu Fachärzten durch ambulante Versorgungsformen überbrückt werden können. [1] [2]

Kostenträger von medizinischen Behandlungsformen bewerten neue Therapiemöglichkeiten teilweise zurückhaltend, da die Effektivität und Effizienz der neuen Therapieform grundlegende Voraussetzungen sind, um ins Leistungsangebot übernommen zu werden. Dieser Nachweis kann mit einem standardisierten Register, dem Telemedizinregister, durch den jeweiligen Telemedizin-Dienstleister unterstützt werden.

Als konkretes Beispiel einer telemedizinischen Dienstleistung wird die ambulante Parkinsontherapie in der Arbeit detaillierter betrachtet. Die Erkrankung an Morbus Parkinson benötigt oftmals für die Sicherung der Lebensqualität der Patienten im Alltag eine besonders angepasste und individuelle Einstellung der Medikation. Diese erfolgte früher durch mehrwöchige Krankenhaus-Aufenthalte und kann durch die Therapie alternativ beim Patienten ambulant durchgeführt werden. Der Patient erhält eine speziell entwickelte Video-Einheit, die rund um die Uhr für Aufnahmen zur Verfügung steht. Diese werden unmittelbar dem behandelnden Neurologen beziehungsweise Facharzt über eine gesicherte Internetverbindung übertragen. Die Videos werden von diesem bewertet und

ermöglichen somit eine gezielte Anpassung der Medikation. Ein zusätzlich zur Video-Einheit vorhandener Drucker beim Patienten gibt dann den durch den Facharzt angepassten Medikationsplan aus.

1.1 Problemstellung

Der Nachweis der Effektivität und Effizienz gegenüber den Kostenträgern im Gesundheitswesen stellt telemedizinische Dienstleister oftmals vor Probleme, mit welchen Daten dieser Prozess erfolgen soll. Zu einer angebotenen Behandlung muss für den Kostenträger nachvollziehbar sein, wie diese Versorgungsform im einzelnen durchgeführt wird und mit welchem Ergebnis dies im Vergleich zu einer bisherigen Therapie erfolgt. Die Klassifizierung und Qualifizierung von behandlungsrelevanten Daten steht dabei im Mittelpunkt, was in Absprache zwischen Dienstleister und Kostenträger erfolgt. Dabei sind verschiedene Voraussetzungen zu berücksichtigen, um die Beweiskraft der ausgewählten Daten zu unterstützen. Diese müssen zum Beispiel Kriterien der Validität, Authentizität und Revisionssicherheit erfüllen. [3] [4]

Aufgrund der Diversifizierung der Möglichkeiten in den telemedizinischen Behandlungsformen ist das bisherige Verfahren sowohl für den Dienstleister als auch den Kostenträger kompliziert und wenig standardisiert.

Als Nebenerscheinung ist auch die bisherige Auswertung mittels qualitativer Parameter über einen Zeitraum von mehreren Jahren problematisch, wenn die behandlungsrelevanten Daten nur bedingt konsistent erfasst werden. Beispielsweise kann eine Systemumstellung die vom Dienstleister erfassten Datensätze nicht mehr mit früheren Daten vergleichbar machen.

Verursacht durch mögliche Stigmatisierungen, die durch Krankheiten hervorgerufen werden kombiniert mit der weitreichenden Vernetzung und Verfügbarkeit persönlicher Daten ist der Umgang mit den medizinischen Daten besonders sensibel und vorrauschaugend zu bewerten. Ein unautorisierter Zugriff auf erhobene und verarbeitete Daten ist unbedingt auszuschließen. Problematisch dabei ist die bisherige rechtliche Handhabung von medizinischen Daten, welche nicht zentral an einem Ort vorgehalten, sondern in dezentralen Strukturen und verteilten Systemen ausgetauscht werden. Dies ist oftmals

unvermeidlich bei telemedizinischen Dienstleistungen. Besonders dort müssen mit höchster Sorgfaltspflicht die bisherige Gesetzgebung und der momentane Stand der Technik kombiniert werden, um eine hinreichend zuverlässige Schutz- und Sicherungsstufe der gespeicherten und übermittelten Daten zu erreichen. [5]

1.2 Ziele der Diplomarbeit

In dieser Diplomarbeit soll ein Anforderungskatalog für ein Telemedizinregister entwickelt werden, das für verschiedene Dienstleister aus dem Sektor der Telemedizin ein Mittel zur standardisierten Datenspeicherung und damit Datenauswertung für Kostenträger bietet. Dadurch soll besonders der Nachweis der Effektivität und Effizienz gegenüber den Kostenträgern im Gesundheitswesen durch integrierte Standards verbessert werden.

Der Anforderungskatalog berücksichtigt dabei die aktuellen grundlegenden Datenschutzbestimmungen und verschiedene Datenschutz-Modelle der medizinischen Datenverarbeitung. Mittels der Grundlagen-Kapitel wird ein ausreichender Kenntnisstand im Bereich Datenschutz angestrebt, um auch für zukünftige Anpassungen und Entwicklungen im Bereich der Gesetzgebung durch ein differenziertes Grundlagenwissen vorbereitet zu sein.

Die Ausrichtung des Telemedizinregisters erfolgt für den Einsatz im deutschen Gesundheitswesen, berücksichtigt bei den Grundlagen-Kapiteln aber auch bereits vorhandene Regelungen und Standards für den Datenaustausch im internationalen Raum.

1.3 Struktureller Aufbau der Diplomarbeit

Grundlegende Definitionen und Voraussetzungen werden im ersten Teil der Arbeit beschrieben. Dabei ist im Zusammenhang mit der „Verarbeitung von Daten“, soweit nicht anders formuliert, der komplette unter dem Aspekt des Datenschutzes fallende Prozess der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten definiert.

In den ersten fünf Kapiteln werden die theoretischen und rechtlichen Grundlagen zum Telemedizinregister aufgeführt. Dabei sind zur Strukturierung der verschiedenen Telemedizin-Bereiche typische Beispiele eingesetzt, die teilweise schon mehrjährige Erfahrungen in der praktischen Anwendung vorweisen können. Ein besonderer Fokus wird auch auf die datenschutzrechtliche Relevanz gelegt, da diese bei einer Planung frühstmöglich mit eingebunden werden muss. Die hauptsächliche Ausrichtung ergibt sich durch das Bundesdatenschutzgesetz, welches mit zusätzlichen Erweiterungen wie zum Beispiel den jeweils gültigen Landesdatenschutzgesetzen oder auch fachbezogenen Gesetzen den Rahmen für die medizinische Datenverarbeitung bilden.

Zur Klassifizierung verschiedener Registertypen werden im daran anschließenden Kapitel Beispiele für Register aus öffentlicher Hand aufgelistet. Diverse Attribute und strukturelle Aufbauten lassen sich für das zu konstruierende Telemedizin-Register übernehmen.

Die eingesetzten wissenschaftlichen Methoden zur Entwicklung dieser Arbeit sind im 6. Kapitel aufgeführt. Im anschließenden 7. Kapitel werden vorbereitend zur Erstellung der Anforderungslisten und Prozessmodelle des SOLL-Modells verschiedene Anwendungsszenarien beschrieben und eine Übersicht verfügbarer Standards aufgelistet.

Kapitel 8 und 9 bilden dann den Anforderungskatalog und ein SOLL-Modell des Telemedizin-Registers, welches nach der Erstellung mittels eines praxisbezogenen Beispiels getestet und bewertet wird.

In den letzten beiden Kapiteln wird reflektierend über die wissenschaftlichen Methoden und ausgearbeiteten Modelle und daraus sich ergebende Ergebnissen eine Zusammenfassung erarbeitet, welche auf Problemfälle und offene Fragestellungen hinweist. Eine konkrete Implementierung ist nicht Gegenstand dieser Diplomarbeit und könnte sich als weiterführende Arbeit anschließen.

Der Begriff Telemedizinregister ist in der Arbeit mit der Bezeichnung Register gleichbedeutend, falls sich dies im Kontext nicht anders definiert.

2 Grundlagen Telemedizin

In diesem Kapitel werden neben den notwendigen Definitionen und Begriffserläuterungen, die für eine strukturelle Betrachtungsweise der Telemedizin hilfreich sind, wirtschaftliche Aspekte und eine Kategorisierung telemedizinischer Verfahren aufgelistet.

2.1 Definitionen zur Telemedizin

Der Begriff „Telemedizin“ lässt sich folgendermaßen beschreiben [1]:

„Die Telemedizin umfasst alle medizinischen Behandlungen, bei denen zwischen den Akteuren kein unmittelbarer Kontakt besteht und zur Überwindung der räumlichen Distanz technische Hilfsmittel eingesetzt werden.“

Die genannten technischen Hilfsmittel sind beispielsweise:

- Kommunikationstechnologien (DSL, UMTS, etc.)
- Spezialisierte Geräte zur Parametrisierung beim Patienten (zum Beispiel Blutdruckmessgerät mit Bluetooth-Funktionalität)
- Software (zum Beispiel proprietäre Anwendungen zur Auswertung übermittelter Therapiedaten)
- Smartphones (zum Beispiel Übermittlung kardiologischer Parameter)

Anhand der Beispiele lässt sich erkennen, dass sich ein großes Potentialfeld durch die fortlaufend bessere Vernetzung und ausgebauten Kommunikationsmöglichkeiten ergibt, die Bedeutung der Telemedizin in den nächsten Jahren weiter zu stärken.

Als weiterer Begriff in diesem Zusammenhang ist die „Telematik“ zu nennen [1]:

„Telematik setzt sich aus den Begriffen Telekommunikation und Informatik zusammen und beschreibt im Zusammenhang mit dem Gesundheitswesen die Bereitstellung von Daten und Information mittels Überbrückung von Raum und Zeit.“

Die Telematik ist somit eine technisch basierte Definition, abgrenzend zu Begriffsdefinition von „eHealth“ [1]:

„Mit eHealth werden die wirtschaftlichen Zusammenhänge und Komponenten beschrieben, die im dienstleistenden Bereich des Gesundheitswesens auftreten, welche mit Unterstützung moderner Kommunikationstechnologien die Behandlung von Patienten als Ziel haben.“

In diesen Sektor fallen marktwirtschaftliche Leistungen wie zum Beispiel Medikamente, therapeutische Hilfsmittel, verschiedene Formen der Gesundheitsleistungen (ambulant, stationär, kombiniert) und der Umgang mit Gesundheitsdaten. [1] [6]

Je nach Sichtweise lässt sich die Telemedizin der Definition von Telematik und / oder eHealth unterordnen und wird im weiteren Verlauf der Arbeit nicht weiter spezifiziert. Zusammenfassend zeigt diese Definition den interdisziplinären Anwendungsbereich und damit mögliche Entwicklungspotentialfelder der Telemedizin.

Mit der Gesundheitsreform aus dem Jahr 2000 wurde der Begriff „integrierte Versorgung“ definiert [7]:

„Unter integrierter Versorgung (IV) versteht man die fachübergreifende Versorgung von Patienten, für die Leistungsanbieter aus verschiedenen Sektoren abgestimmt zusammenarbeiten. Außer Haus- und Fachärzten können auch Krankenhäuser, Einrichtungen wie etwa Medizinische Versorgungszentren oder nicht-ärztliche Partner wie Apotheker daran teilnehmen. Voraussetzung für ein solches Leistungsangebot ist ein Vertragsabschluss zwischen einer oder mehreren Krankenkassen und deren Leistungserbringern. Für Versicherte ist die Teilnahme freiwillig.“

Mittels dieser neu eingeführten Versorgungsform soll die sektorale Trennung aufgehoben werden, die bisher im deutschen Gesundheitswesen vorlag. Mit den Sektoren werden verschiedene Leistungsformen und Leistungserbringer beschrieben, zum Beispiel Hausärzte, Kliniken, Einrichtungen zur Rehabilitation. Ein exemplarischer Behandlungsablauf nach Sektoren gestaffelt sieht folgendermaßen aus:

1. Der Patient sucht seinen Hausarzt auf
2. Eine Überweisung an einen Facharzt erfolgt durch den Hausarzt
3. Dort erfolgt eine Einweisung in eine Klinik zur stationären Behandlung
4. Entlassung aus der Klinik und anschließende Überweisung an ein Reha-Zentrum

Oftmals ist die Verbindung und Zusammenarbeit zwischen den verschiedenen Sektoren auf eine abschließende Übergabe (zum Beispiel durch einen Arztbrief) beschränkt. Mit

der integrierten Versorgung sollen diese Strukturen verbessert werden, indem die Zusammenarbeit und gemeinsame Behandlung verstärkt werden. Vorteile ergeben sich für den Patienten zum Beispiel durch festgelegte Richtlinien in Sektoren übergreifenden Behandlungsabläufen und damit verbesserten Voraussetzungen für eine optimierte Gesundheitsversorgung durch anwendbares Qualitätsmanagement.

2.2 Beteiligte Partner und Rollenverteilung

Im Gesundheitswesen in Deutschland finden sich speziell auf den Bereich der Telemedizin bezogen folgende Akteure beziehungsweise Partner:

- Patient
- Niedergelassener Arzt (Hausarzt / Facharzt)
- Klinik
- Kostenträger
- Telemedizinischer Dienstleister
- Sonstige Partner (Apotheke, Labor, etc.)

Die primären Ziele im Gesundheitswesen sind einerseits die (akute) Behandlung von Krankheiten zur Heilung beziehungsweise Linderung und andererseits die Vorsorge zur Verhinderung von krankheitsbedingten Therapiemaßnahmen. Diese Ziele müssen unter Berücksichtigung von volkswirtschaftlichen Aspekten verfolgt werden, um auch langfristig einen ausreichenden gesundheitlichen Standard in der Bevölkerung zu sichern.

[1]

Die Zusammenarbeit zwischen den verschiedenen Akteuren in der Telemedizin wird oftmals in 2 Kategorien verallgemeinert [6]:

- **Kategorie doctor-2-doctor**

Hierbei erfolgen die Kommunikation und der Datenaustausch ohne unmittelbare Einbindung des Patienten. Ein Beispiel ist die schon vor mehr als 50 Jahren zum ersten Mal angewandte Teleradiologie, bei der radiologische Behandlungsdaten über ein Kommunikationsmedium zwischen Ärzten oder damit betreuten Einrichtungen ausgetauscht werden. Die beteiligten Partner in dieser Kategorie können aber auch beispielsweise durch ein Arzt und einen Apotheker realisiert

werden. Das markante Merkmal ist daher die telemedizinische Kommunikation ohne direkte Einwirkung eines zu behandelnden Patienten.

- **Kategorie doctor-2-patient**

Im Fokus der Kommunikation steht eine aktive Mitarbeit des Patienten im Behandlungsverlauf durch eine direkte oder indirekte Verbindung zum betreuenden Arzt beziehungsweise ärztlichen Vertreter. Vor allem die verschiedenen Arten des Monitoring, wie zum Beispiel regelmäßige Blutdruckmessungen im kardiologischen Anwendungsbereich oder Überprüfungen des Blutzuckerwertes bei Diabetes, sind typische Umsetzungen in der Telemedizin. Besonders häufig sind hier spezifische Geräte zur einfachen häuslichen Anwendung beim Patienten entwickelt worden, die dann entweder zu festgelegten Zeitpunkten oder auch in Notfall-Situationen Vital-Parameter erheben und zu einem Arzt übermitteln.

Im folgenden Abschnitt werden drei Beispiele für telemedizinische Anwendungen kurz dargestellt, wobei die ersten beiden primär in der Kategorie doctor-2-doctor anzusetzen sind und das letzte Beispiel für eine Anwendung im Bereich patient-2-doctor dient:

- **TEMPiS – Schlaganfallversorgung**

In der bayrischen Süd-Ost-Region wurde 2003 ein Projekt zur Verbesserung in der Schlaganfallversorgung gegründet: TEMPiS – Telemedizinisches Projekt zur integrierten Schlaganfallversorgung. [8]

Dabei sollen die Nachteile verringert werden, welche durch eine vergleichsweise niedrige Spezialisierung im Bereich der Behandlung von Schlaganfällen in ländlichen Gebieten vorhanden ist. Die hoch qualifizierten Stroke Units - spezialisierte Fachabteilungen zur akuten Schlaganfallversorgung - finden sich fast ausschließlich in Ballungsgebieten und stehen somit einem großen Teil der Bevölkerung nicht in zufriedenstellender Zeit zur Verfügung. Durch eine Kooperation dieser Stroke Units mit mittlerweile 17 regionalen Kliniken wird dieser Standortnachteil gemindert, indem bei akuten Notfallsituationen die regionalen Kliniken per Videoverbindung die Expertise der Experten aus den Stroke Units mit einbeziehen können. [8]

- **Parkinson-Erkrankung**

Zur Erkennung von Anzeichen auf eine vorliegende Parkinson-Erkrankung existiert seit einigen Jahren eine videounterstützte Möglichkeit, beim niedergelassenen Neurologen eine beziehungsweise mehrere Aufnahmen per Videokamera vorzunehmen, die mittels angeschlossenen Netzwerk zu ausgesuchten Spezialisten in Kliniken deutschlandweit zur Analyse versendet werden. Diese Zusammenarbeit von Neurologen mit Klinik-Ärzten beziehungsweise Spezialisten auf dem Gebiet Morbus Parkinson erfolgt mit der medizinische Videobeobachtung MVB GmbH, welche die benötigte Hardware und Software zur Verfügung stellt. Dieses Modell dient auch als praktisches Beispiel im späteren Kapitel zur praxisorientierten Untersuchung des entwickelten SOLL-Modells des Telemedizinregisters.

- **Kardiologische Vorsorge**

Deutschlandweit existieren viele Projekte, deren Ziel eine lückenlose Dokumentation im Bereich der kardiologischen Vorsorge und durchgeführten Therapiemaßnahmen ist. Dabei werden Patienten technische Hilfsmittel wie beispielsweise ein simpel bedienbares EKG zur Verfügung gestellt, mit denen kardiologische Parameter dauerhaft oder zu bestimmten Zeitpunkten erfasst werden und an den behandelnden Arzt übermittelt werden. Ein konkretes Beispiel ist die Entwicklung der Segeberger Kliniken zusammen mit der Krankenkasse DAK, bezeichnet mit „Mein Herz“. Patienten mit kardiologischen Problemen wie beispielsweise einer Herzinsuffizienz messen täglich Vitalparameter mit ihnen zur Verfügung gestellten Geräten wie einem EKG, Blutdruckmessgerät und einer Waage. Diese Daten werden an ein medizinisches Zentrum der Segeberger Kliniken übermittelt und veranlassen dort nach einer Analyse gegebenenfalls eine unmittelbare Reaktion, zum Beispiel eine Kontaktaufnahme mit dem Patienten und einer Empfehlung zum Aufsuchen eines Arztes. [9]

Die Rolle des telemedizinischen Dienstleisters ist über die Einbindung in die aktive Mitarbeit im Prozess der Behandlung definiert:

Passive Dienstleister, die rein organisatorische Funktionalitäten übernehmen, indem Verträge und Netzwerke mit den beteiligten Partnern (Ärzten, Kliniken, Kostenträgern, etc.) abgeschlossen werden.

Aktive Dienstleister hingegen verantworten bestimmte Bereiche in dem Behandlungsablauf, indem beispielsweise spezifische Geräte zum Monitoring diverser Vitalparameter entwickelt oder auch Service-Center betrieben werden, bei dem Patienten durch Übermittlung behandlungsrelevanter Parameter direkt mit eingebunden sind.

Limitierungen bestehen in Deutschland bei der Umsetzung telemedizinischer Behandlungen durch verschiedene Gesetzgebungen, welche in der Rollenverteilung beachtet werden müssen. So ist beispielsweise durch die Berufsordnung der Ärzte vorgeschrieben, dass eine Diagnosestellung nur durch einen unmittelbaren Kontakt zwischen Arzt und Patient erlaubt ist. Eine Ferndiagnose, die ein mögliches Potentialfeld in der Telemedizin, besonders im notfallmedizinischen Sektor, darstellt, ist somit gesehen nicht möglich. Auch der Umgang mit medizinischen Daten ist strengen Richtlinien unterworfen, deren Besonderheiten in den folgenden Kapiteln, vor allem bei der Konzeption verschiedener Datenschutz-Modelle, genauer erläutert werden.

2.3 Entwicklung und Verbreitung in Deutschland

Im Jahr 2011 lagen die Ausgaben im deutschen Gesundheitswesen bei 293,8 Milliarden Euro, dies sind anteilig circa 11,3 % des Bruttoinlandsproduktes [10]. Im Vergleich mit anderen europäischen Ländern ist dieser Wert im oberen Bereich der Aufwendungen zur Gesundheitswirtschaft einzuordnen.

Durch die sogenannte „Anschubfinanzierung“ wurde mit der Gesundheitsreform im Jahr 2004 nach § 140a ff. SGB V ein unterstützendes Finanzierungsmodell eingeführt, um die Anzahl der Verträge im Bereich der integrierten Versorgung zu erhöhen. Seit der Einführung der IV im Jahr 2000 gab es bis dahin nur wenige Abschlüsse in diesem Sektor. Konkret gelöst wurde die Finanzierung der Förderung mit einem anteilmäßigen Etat, bei dem 1 % der Gesamtvergütungen zur ambulanten und stationären Versorgung für integrierte Versorgungsformen bereitgestellt wurde. In einer Übergangszeit bis 2009

wurden somit neue IV-Verträge unterstützt, die ab der weiteren Gesundheitsreform im Jahr 2009 finanziell selbstständig tragfähig sein mussten. [11]

Zur Analyse der Entwicklung des telemedizinischen Sektors in Deutschland eignet sich die Anzahl von offiziellen IV-Verträgen, die jährlich zu einem Stichtag gültig sind.

Bei der Anzahl ist zu berücksichtigen, dass die Zählung durch die gemeinsame Registrierungsstelle zur Unterstützung der Umsetzung des § 140 d SGB V nur gemeldete Verträge der einzelnen beteiligten Krankenkassen auflistet und daher auch Doppelzählungen nicht auszuschließen sind. Anhand der Zahlen lässt sich sehr gut die Wirkung durch die Anschubfinanzierung von 2004 bis 2009 erkennen, die insgesamt die Anzahl der IV-Verträge um ein Vielfaches vergrößerte. Die Anzahl der IV-Verträge lag zum Jahreswechsel 2008 / 2009 bei 6183. [12]

Nach dem Auslaufen des Förderprogramms stellte sich unmittelbar eine Stagnation bei den gültigen Verträgen ein, bedingt durch die notwendig gewordene komplette Eigenfinanzierung der jeweiligen Abschlüsse. Eine Änderung ergab sich in dem Zeitraum von 2009 bis 2011 vor allem in der Anzahl der im Rahmen der Verträge behandelten Patienten, die von 1,66 Millionen auf 1,93 Millionen Patienten anwuchs. [12]

Anzahl IV-Verträge

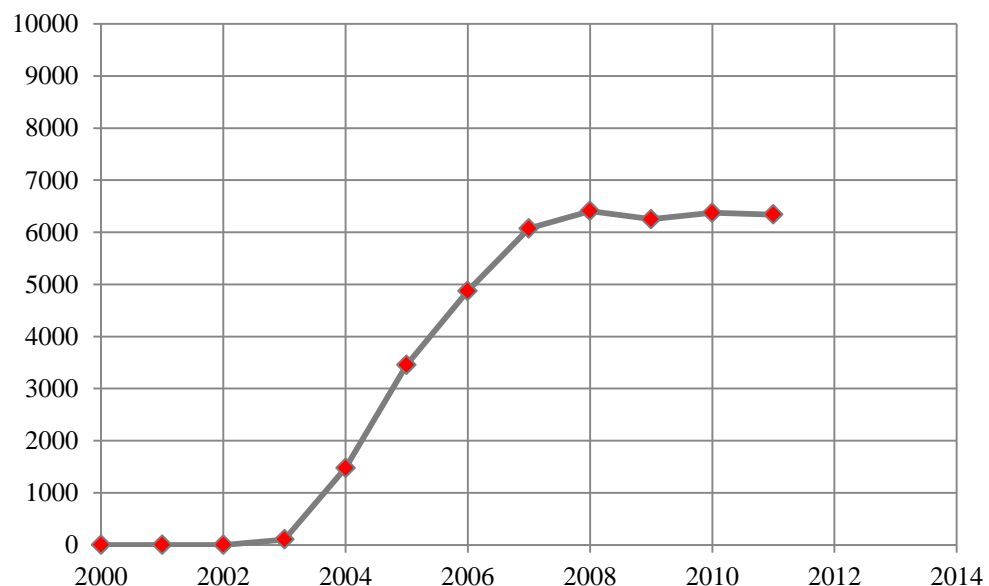


Abbildung 1, Anzahl IV-Verträge [12], [13], [14]

Verallgemeinernd zeigt das Diagramm eine positive Wirkung durch das Förderprogramm aus dem Jahr 2004. In Frühphasen von IV-Verträgen ist eine gezielte Unterstüt-

zung zur Etablierung der Dienstleistungen am Markt hilfreich. Trotz des häufig formulierten Entwicklungspotentials und der zunehmenden Bedeutung des Telemedizin-Sektors ist dieser Bereich marktwirtschaftlichen Risiken unterworfen, die mit dem Telemedizinregister gemindert und der Prozess zur Abrechnung telemedizinischer Behandlungen verbessert und unterstützt werden sollen.

2.4 Internationale Entwicklung und Verbreitung

In anderen europäischen Ländern sind bedingt durch einfachere Strukturen im Gesundheitswesen und Rechtsvorschriften vergleichsweise fortgeschrittene Umsetzungen in der Telemedizin zu finden. Besonders skandinavische Länder verfolgen schon seit mehreren Jahren gezielte Bestrebungen zur Etablierung der Telemedizin. Im folgenden Abschnitt sind zwei Beispiele aufgeführt, die in Europa Anwendung finden:

- **Schweiz : Medgate**

Medgate wurde 1999 in der Schweiz gegründet, um eine bessere telemedizinische Versorgung für die Bevölkerung anzubieten und dem größer werdenden Hausarztmangel entgegenwirken zu können. Bemerkenswert im Vergleich zu ähnlichen Projekten ist die gute Vernetzung und Umsetzung in der alltäglichen Anwendung, zum Beispiel durch eine App für Smartphones, hochqualifizierte telefonische Betreuungsdienste und mehreren größeren Medizin-Zentren für einen direkten Patientenkontakt. Die primäre Kommunikation erfolgt über telefonische Konsultationen, wobei im Vergleich zu anderen Call-Centern bei Medgate ausschließlich Ärzte die Anfragen der Patienten entgegen nehmen. [15]

In den telemedizinischen Zentren in Basel, Zürich und Solothurn sind ärztliche Spezialisten verschiedenster Fachbereiche im Einsatz, die einerseits eine direkte Behandlungsmöglichkeit bieten und andererseits eine Rund-um-die-Uhr Betreuung den Patienten zur Verfügung stellen. [16] Die Vernetzung der Zentren untereinander bietet eine hohe fachliche Kompetenz in den einzelnen Fachgebieten der Medizin.

Die entwickelte App unterstützt den Patienten bei der Auswahl der korrekten Rufnummer (abhängig vom Krankheitsbild) und bietet zusätzliche telemedizinische

sche Dienste wie beispielsweise eine Funktion zur Übermittlung von Fotos zur besseren Erkennung und Einstufung eines Krankheitsbildes. [15]

- **Deutschland / Polen : Telemedizin in der Euroregion Pomerania e.V.**

In Zusammenarbeit mit Deutschland und Polen ist vor einigen Jahren ein telemedizinisches Netzwerk zur verbesserten Versorgung für mehrere medizinische Fachgebiete in der Region Pomerania, bestehend aus Mecklenburg-Vorpommern, Nord-Brandenburg und Westpommern (Polen), entstanden. Die demographische Entwicklung und die damit verbundenen Probleme in der medizinischen Infrastruktur sind besonders in der ländlich geprägten Region Pomerania durch die geringe Bevölkerungsdichte beispielhaft für die mögliche Entwicklung in den kommenden Jahren. Hochqualifizierte medizinische Versorgungsstrukturen sind aufgrund eingeschränkter Kostenmittel vor allem in städtischen Ballungszentren zu finden. Dies verursacht langfristig deutliche Einschränkungen für einen Teil der ländlichen Bevölkerung, wenn der Zugang zu notwendigen medizinischen Anwendungen mit großen Entfernungen verbunden ist.

Der 2007 gegründete Verein „Telemedizin in der Euroregion POMERANIA e.V.“ koordiniert und plant die telemedizinischen Angebote in Zusammenarbeit mit 35 beteiligten Kliniken in Deutschland und Polen. Im Fokus steht dabei die Kommunikation zwischen behandelnden Ärzten, um Expertenmeinungen auch zu Nacht- und Wochenendzeiten über die Region verteilt anbieten zu können. Zusätzlich sind Konsultationen und Konferenzen möglich, um uneingeschränkt Zweitmeinungen von spezialisierten Fachärzten zu Rate ziehen zu können. [17]

Beispielsweise bietet die Universitätsmedizin in Greifswald für mehrere Fachgebiete (Pathologie, HNO, Radiologie, etc.) eine Unterstützung beziehungsweise Beratung für mehrere kleinere Kliniken in der Umgebung an, welche durch die Übermittlung von Videodaten realisiert werden.

Das Projekt wird von der EU durch das INTERREG IV-Programm subventioniert und dient als Modellregion für die Auswertung von Qualität und Quantität verschiedenster telemedizinischer Teilprojekte, basierend auf klinischen Behandlungsdaten. [18]

3 Rechtliche Grundlagen – Datenschutz

In diesem Kapitel werden grundlegende Voraussetzungen für die rechtliche Sicherheit beim Umgang mit personenbezogenen Daten erläutert. Diese Bedingungen sind für medizinische Daten teilweise noch durch strengere Kriterien und Gesetzen definiert und dienen als Basis für den Anforderungskatalog des Telemedizinregisters.

3.1 Definitionen des Datenschutzes

Der Begriff „Datenschutz“ wird im Bundesdatenschutzgesetz (BDSG) folgendermaßen definiert: [19]

„Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten.“

Hervorzuheben sind bei dieser Definition die Begriffe „Einzelnen“ und „personenbezogen“. Die Datenschutz-Gesetze sind in Deutschland auf natürliche Personen anzuwenden, welche bei vielen Registerformen die Datenbasis bilden und auch beim Telemedizinregister die zu verwaltende Datenmenge darstellen. Die Formulierung „personenbezogene Daten“ ist im BDSG definiert: [19] [20]

„Daten über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimm- baren Person (Betroffener).“

Dies führt zu einer Unterscheidung von Daten in drei Kategorien [21]:

- **Daten einer bestimmten Person**
zum Beispiel Vor- und Nachname, Wohn-Adresse
- **Daten einer bestimm- baren Person**
zum Beispiel IP-Adresse, Mitgliedsnummer in einer Krankenversicherung
- **Andere Daten**
Daten, die nicht auf eine Person schließen lassen

Von besonderem Interesse sind somit die ersten beiden Kategorien, durch die Daten einen unmittelbaren Verweis auf Personen enthalten oder mit Kombination weiterer

Datenbestände mittelbar einer Person beizuordnen sind. Diese Daten unterliegen strengeren Richtlinien als unpersönliche Daten, um die Persönlichkeitsrechte der betroffenen Personen nicht zu beeinträchtigen und zu schützen.

Umfassend wird der Schutz der persönlichen Daten auch dadurch gewährleistet, dass nicht nur der Speichervorgang von Daten durch das BDSG reglementiert ist, sondern auch dazugehörige Prozesse der Erhebung, Verarbeitung (Speichern, Verändern, Übermitteln, Sperren, Löschen) und Nutzung der Daten durch das Gesetz definiert sind. [20]

3.1.1 Grundsätze des Datenschutzes

Folgende Prinzipien und Grundsätze im Bereich Datenschutz lassen sich auflisten, die bei Verarbeitungsprozessen von Daten allgemein gültig sind [21] [22]:

- **Verbot mit Erlaubnisvorbehalt**
Grundsätzlich ist die Erhebung, Speicherung und Verarbeitung von fremden personenbezogenen Daten nicht erlaubt. Ausnahmen sind durch eine schriftliche Einwilligungserklärung des Betroffenen oder eine gesetzliche Legitimierung vorgesehen.
- **Auskunfts- und Korrekturrechte**
Betroffene einer Datenverarbeitung können jederzeit Auskunft über ihre gespeicherten Daten erhalten und besitzen gegebenenfalls ein Recht auf Korrektur fehlerhafter Daten.
- **Datensicherheit**
Eine technische Sicherung der Daten vor äußerlichem Zugriff ist notwendig.
- **Datenvermeidung und Datensparsamkeit**
Nur notwendige Daten sollen verarbeitet werden. Des Weiteren sollen nicht mehr benötigte Daten nach einer bestimmten Zeit gelöscht werden.
- **Zweckbindung**
Die Daten sind einem bestimmten Zweck zuzuordnen und sind an diesen gebunden. Geänderte Absichten müssen neu vereinbart werden, zum Beispiel durch aktualisierte Einverständniserklärungen. [23]

- **Rechtliche Risiken**

Verstöße gegen die rechtlichen Vorschriften werden durch Behörden geahndet.

Basierend auf diesen Normen gibt es verschiedene gesetzliche Regelungen, in denen getrennt nach Fachbereichen die Verarbeitung von Daten detailliert geregelt ist. Zum bundesweit gültigen Bundesdatenschutzgesetz gibt es länderweit zusätzliche Landesdatenschutzgesetze, welche vor allem im öffentlichen Sektor Anwendung finden. Dazu kommen noch individuelle Gesetzes-Regelungen, wie das Telemediengesetz (TMG), welches konkrete Vorschriften im Bereich "Datenschutz im Internet" vorgibt. Des Weiteren existieren beispielsweise zu medizinischen Daten fachspezifische Gesetze, wie die ärztliche Schweigepflicht (Verschwiegenheitspflicht, § 203 StGB), die im Umgang mit personenbezogenen Daten bei der Erstellung eines Telemedizinregisters berücksichtigt werden müssen. [19] [24]

Zusammenfassend ergeben sich dadurch je nach Einsatzgebiet komplexe Wirkungszusammenhänge bei der praktischen Anwendung des Datenschutzes. Eine Herangehensweise zur Einhaltung der Vorschriften ist eine frühzeitige Miteinbeziehung der Thematik des Datenschutzes in die Entwicklung von datenverarbeiteten Prozessen. Dabei müssen die zuvor aufgelisteten Grundsätze eingehalten werden und eine Überprüfung der Datenbestände mit den folgenden Punkten zu einem positiven Ergebnis führen:

3.1.2 Die „10 Gebote“ des Datenschutzes

Eine Liste der „10 Gebote“ sollte grundsätzlich auf die geschützten Daten anwendbar sein (als Beispiel auf einen Datenserver bezogen): [25]

- 1. Zugangskontrolle**
Server-Raum mit restriktiver Zugangskontrolle
- 2. Datenträgerkontrolle**
Server in einem abgeschlossenen Bereich
- 3. Speicherkontrolle**
Absicherung des Server-Betriebssystems
- 4. Benutzerkontrolle**
Authentifizierung der Benutzer

5. Zugriffskontrolle

Rechteverwaltung der Benutzer

6. Übermittlungskontrolle

Dokumentation von Übertragungs-Sessions

7. Eingabekontrolle

Revisionskontrolle bei Datenbeständen

8. Auftragskontrolle

Dokumentation über die Verarbeitungsprozesse von Daten

9. Transportkontrolle

Verschlüsselung von zu übertragenden Daten

10. Organisationskontrolle

Datensicherungs-Konzept

Durch die verschiedenen Gesetze und der Anwendung der 10 Gebote ist somit ein Grundgerüst gegeben, schutzbedürftige Daten so zu behandeln, dass keine Persönlichkeitsrechte von Betroffenen eingeschränkt oder verletzt werden. Dies setzt voraus, dass ausgearbeitete Konzepte regelmäßig anhand des aktuellen Stands der Technik überprüft und Aktualisierungen der Maßnahmen vorgenommen werden. Beispielsweise muss die Verschlüsselung von übermittelten personenbezogenen Daten hinreichend vorgenommen werden, so dass eine Entschlüsselung nicht oder nur unter unverhältnismäßig hohem Aufwand vorgenommen möglich ist. Solche Maßnahmen müssen regelmäßig neu bewertet werden, falls beispielsweise Sicherheitslücken verwendeter Algorithmen bekannt werden.

Die Definition der Verhältnismäßigkeit wird dabei durch die Auswirkungen einer Beeinträchtigung der Persönlichkeitsrechte vorgegeben: so sind die zu erwartenden Nachwirkungen einer Entschlüsselung eines Datenbestandes, der Mail-Adressen enthält, allgemein als geringer anzusehen als ein (missbräuchlicher) Datenverlust, der Namen und dazugehörige medizinische Behandlungsdaten betrifft. Besonders sensible Daten wie medizinische oder auch strafrechtliche Daten müssen somit mit höchstmöglicher Sorgfalt gegen einen unautorisierten Zugriff geschützt werden. [26]

3.2 Rechtliche Entwicklung

In Deutschland wurde das erste bundesweite Gesetz zum Thema Datenschutz im Jahr 1977 erlassen, das Bundesdatenschutzgesetz (BDSG). In diesem Gesetz sind grundlegende Regelungen formuliert, die einen automatisierten beziehungsweise elektronisch unterstützten Umgang mit persönlichen Daten definieren. [21]

In mehreren Abschnitten wurden in den folgenden Jahren Erweiterungen und Anpassungen vorgenommen; eine Neufassung im Jahre 1990 und Änderungen in den Jahren 2001, 2003 und 2009. Diese Veränderungen sind notwendig geworden, da einerseits die Anwendung der Verarbeitung personenbezogener Daten durch die rasch ansteigende Anzahl von IT-Systemen in privaten, öffentlichen und wirtschaftlichen Bereichen zugenommen hat und andererseits auch die Forderungen und Sensibilisierungen der Bevölkerung zum Schutz der eigenen Daten gestiegen sind.

Zusätzlich wurde durch die unterschiedlichen Datenschutz-Regelungen im europäischen Wirtschaftsraum und den in den letzten Jahrzehnten fortschreitenden länderübergreifenden Datenaustausch eine allgemeingültige Vorschrift für die EU-Länder notwendig. Diese Richtlinien wurden erstmals 1995 in der Datenschutzrichtlinie (95/46/EG) und zwei Jahre später in der Telekommunikationsrichtlinie (97/66/EG) vorgegeben. Diese wiederum mussten in die jeweiligen nationalen Datenschutzgesetze umgesetzt beziehungsweise integriert werden.

Oftmals wird das sogenannte „Volkszählungsurteil“ des Bundesverfassungsgerichts im Jahr 1983 als Ausgangspunkt der öffentlichen Wahrnehmung der Problematik im Umgang mit persönlichen Daten genannt: mit diesem Urteil verhinderte das Bundesverfassungsgericht eine umfangreiche Erhebung von Daten im Rahmen des Volkszählungsgesetzes. Bundesweit sollten zum Beispiel folgende Daten durch Auskünfte der Bevölkerung und Firmen erhoben werden. [19]

- Informationen zu Einkommen und Beruf
- Klassifizierung der Religionszugehörigkeit
- Auflistung der Gehaltsstrukturen in Firmen

Viele Bereiche der geplanten Datenerfassungen sind laut Bundesverfassungsgesetz nicht zulässig für eine automatisierte Erhebung [21]:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. [...] Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. [...]“

Die dort genannte „informationelle Selbstbestimmung“ prägt auch heute noch wesentlich die Ausrichtung des Bundesdatenschutzgesetzes und damit deren praktische Anwendung. Das Selbstbestimmungsrecht verhindert somit, dass generell ohne Zustimmung des Betroffenen dessen Daten erhoben, gespeichert, verarbeitet oder weitervermittelt werden. Ausnahmen sind Anwendungsfälle, in denen die personenbezogenen Daten unentbehrlich sind. Beispielsweise ist im Rahmen eines Arbeitsverhältnisses die Speicherung von persönlichen Daten (Adresse, Kontodaten, etc.) notwendig, um die korrekte Erfüllung des Vertrages zu gewährleisten. [21]

3.3 Verfahrensweisen im Datenschutz

In der medizinischen Forschung werden schon seit längerem Konzepte zur Datenverarbeitung angewendet, welche datenschutzkonform sind. Dies wird durch den grundlegenden Ansatz erreicht, Datensätze so zu verändern, dass die Persönlichkeitsrechte der Betroffenen beziehungsweise Patienten nicht mehr eingeschränkt oder verletzt werden.

Mittels der Veränderung der personenidentifizierenden Daten wird somit ein Datenmodell erreicht, dass nicht zwingend die Einwilligung der Patienten oder eine gesetzliche Sonderregelung zur Datenübermittlung benötigt.

3.3.1 Pseudonymisierung

Ein häufig angewandtes Schema ist die Pseudonymisierung. Diese ist laut BDSG folgendermaßen definiert [20]:

„Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Re-Identifizierungsrisiken können sich aus dem Verfahren der Pseudonymgenerierung und / oder dem Umfang der Datensätze ergeben.“

Die Generierung der Pseudonyme muss daher so erfolgen, dass bei alleinigem Vorliegen der überarbeiteten Datensätze keine Daten einer bestimmten Person zuzuordnen sind. Zwei verschiedene Techniken werden oftmals dafür eingesetzt: Einerseits eine feste Zuordnung von vorher definierten Werten anstelle der personenidentifizierenden Merkmalen oder andererseits durch die Anwendung einer Hash-Funktion, die ersetzende Daten beziehungsweise Werte aufgrund der vorliegenden Daten berechnet.

Beispiel Zuordnung mittels Hash-Funktion:

Initiale Daten (zum Beispiel Name)	Anwendung Hash-Funktion	Ergebnis
Mustermann, Thomas	→	Fnon&/fnqw
Musterfrau, Anna	→	%sn43Ubn(j
Müller, Manuela	→	Gn83N} }5xi

Abbildung 2, Zuordnung mittels Hash-Funktion

Beispiel Zuordnung mittels fester Werte:

Initiale Daten (zum Beispiel Name)	Zuweisung	Werte-Liste
Mustermann, Thomas	→	00001
Musterfrau, Anna	→	00002
Müller, Manuela	→	00003

Abbildung 3, Zuordnung mittels fester Werte

Die Methode mittels zuvor definierter Werte erfordert demnach zusätzlich eine Speicherung der Zuweisungen in einer Liste, falls nachträglich Änderungen an einem pseudonymisierten Datensatz erforderlich sind oder auch eine Re-Identifizierung ausdrücklich gewünscht wird. [5]

Bei der Methode mit der Hash-Funktion hingegen muss nur die Funktion selbst sicher aufbewahrt werden. Eine erneute Anwendung der Hash-Funktion auf einen ursprünglichen Datensatz ergibt das identische Ergebnis wie zuvor.

3.3.2 Anonymisierung

Bei diesem Konzept sind die veränderten Daten praktisch nicht re-identifizierbar. Damit erstellte Datensätze sind folglich aber auch nicht änderungsfähig oder erweiterbar, falls zum Beispiel eine Patientenakte mit fortlaufenden Behandlungsergebnissen erfasst werden soll.

Definiert wird die Anonymisierung im BDSG wie folgt [20]:

„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.“

Erreicht wird eine sichere Anonymisierung zum Beispiel durch Anwendung mathematischer Funktionen (Falltür-Funktionen, etc.), bei denen eine mehrmalige Anwendung auf einen Datensatz jeweils unterschiedliche Ergebnisse liefert. Dies kann zum Beispiel durch Miteinbeziehung von variierenden Werten wie Uhrzeit, Zufallsgenerator oder ähnlichem erfolgen. Eine Re-Identifizierung kann nur durch eine zusätzliche erfasste Liste und / oder Informationen erfolgen, welche die jeweiligen Veränderungen dokumentieren.

Nachteilig ist aber im medizinischen Bereich die fehlende Möglichkeit, einem zuvor erzeugten anonymen Datensatz weitere Informationen hinzuzufügen, wie es zum Beispiel im Rahmen einer längerfristigen Therapie in der Telemedizin sinnvoll wäre. Daher wird häufiger im medizinischen Sektor eine Pseudonymisierung eingesetzt, welche solche Datenänderungen einfacher verfügbar macht. [27]

3.3.3 Treuhänder

Die bisher aufgeführten Konzepte sind einer zentralen Verarbeitung von Datenbeständen zuzuordnen, deren Umsetzung mehrere Nachteile sowohl in der Anwendung als auch in der datenschutzrechtlichen Relevanz aufweist. Bei einer zentralen Lagerung von originalen und veränderten Datensätzen und den dazugehörigen Verfahren (Hash-Funktion, Zuordnungsliste) ist die Gefahr groß, dass diese Daten missbräuchlich zusammen kombiniert und geforderte Sicherheiten des Datenschutzes aufgehoben werden. Des Weiteren sind die Anwendungsoptionen bei einer zentralen Verwaltung eingeschränkt gegenüber dezentralen beziehungsweise verteilten Lösungen, wenn mehrere Einrichtungen oder Partner beteiligt sind. Besonders diese Situation ist im Bereich der Telemedizin ein oftmals gegebener Zustand, um therapiebezogene Daten einrichtungsübergreifend zu erfassen und verarbeiten zu können. [5] [27]

Daher gibt es bei einer dezentralen Lagerung und Verwaltung der Datenbestände noch die zusätzliche Option eines Treuhänders, der im Auftrag einen Teil der Daten vertrauensvoll aufbewahrt oder zusätzlich in den Prozess der Pseudonymisierung oder Anonymisierung mit eingebunden wird.

Verschiedene detaillierte Konzepte zur Datentreuhänder-Umsetzung sind in Kapitel 4 aufgeführt. Allgemein beschrieben dient der Treuhänder als vertrauenswürdige Vermittlerstelle zwischen einem datenerfassenden Dienstleister und einem datenabfragenden Anwender. Die Daten werden über mehrere voneinander getrennte Bereiche verteilt, welches dem datenschutzrechtlichen Konzept der informationellen Gewaltenteilung entspricht. Dies bedeutet, zu schützende Datenbestände logisch und physisch voneinander zu trennen und in die Verantwortung mehrerer verschiedener Institutionen beziehungsweise Verwaltungen zu übertragen. Beispielsweise lassen sich Behandlungsdaten in identifizierende Patientendaten (IDAT) und in medizinische Behandlungsdaten (MDAT) zerlegen und getrennt aufbewahren. Dadurch wären bei einem partiell vorhandenen Sicherheitsproblem - wie beispielsweise bei einem Datendiebstahl - die Risiken verringert, dass Kenntnisse über medizinische Behandlungen einer Person zugeordnet werden können. [28] [29]

3.4 Datenschutzrechtliche Faktoren in der Medizin

Besonders dem Bereich der Datenerfassung in der Medizin ist in den letzten Jahren besondere Bedeutung durch die zunehmende Vernetzung im Gesundheitswesen und die Sensibilisierung im Umgang mit persönlichen Daten zugewiesen worden.

Zum persönlichen Interesse von Patienten, dass eigene Daten nicht allgemein zugänglich sind, kommt im medizinischen Sektor und dort besonders in der Telemedizin ein verstärktes Schutzbedürfnis erhobener Daten und die Erfordernis strenger Richtlinien zur Reglementierung der Zugriffsmöglichkeiten auf Behandlungsdaten. Im Rahmen einer Behandlung werden unterschiedlichste Daten verarbeitet, die ausschließlich autorisierten Anwendern zur Verfügung stehen dürfen. Diese Notwendigkeiten sind in verschiedenen Konzepten für die Verarbeitung medizinischer Daten berücksichtigt worden, welche als Grundlage bei der Erstellung des Anforderungskataloges in dieser Arbeit mit einbezogen werden.

Vorab werden die wichtigsten Einflussfaktoren beschrieben, die im ärztlichen Umfeld die Datenschutz-Vorschriften zusätzlich zur allgemeinen Gesetzgebung erweitern:

a) **Ärztliche Schweigepflicht**

Im Strafgesetzbuch (StGB) ist im Paragraphen 203 die Verletzung von Privatgeheimnissen definiert. Zusammen mit der Muster-Berufsordnung (MBO) für Ärzte (§ 9) entsteht damit eine ärztliche Schweigepflicht, die auch alle an der medizinischen Behandlung beteiligten Personen dazu verpflichtet, keine anvertrauten Informationen und Geheimnisse des Patienten an Dritte weiterzugeben. Diese Informationen umfassen alle Daten, an deren Geheimhaltung der Patient ein sachlich begründetes und somit schutzwürdiges Interesse besitzt [30]. Diese Verschwiegenheitspflicht kann aufgehoben werden, falls der Patient die konkrete Einwilligung dazu erteilt hat oder der Patient von einer Informationsweitergabe ausgehen muss (stillschweigende Einwilligung) oder von der Einwilligung des Patienten auszugehen ist (mutmaßliche Einwilligung). Diese Aufhebung tritt auch bei Gefahr im Verzug oder offenbarten gravierenden Straftaten des Patienten ein, was hier aber nicht weiter erläutert wird. [30]

b) Umgang mit schützenswerten personenbezogenen Daten, BDSG

Neben dem allgemeinen datenschutzrechtlichen Umgang mit Daten ist im BDSG der medizinischen Bereich genauer definiert durch § 3, Abs. 9: *„Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.“* [20] Gesundheitsdaten unterliegen somit einem besonderen Schutz und benötigen strengere Richtlinien in der Verarbeitung als allgemeine personenbezogene Daten. Im Paragraph 4 des BDSG werden Anforderungen beschrieben, welche notwendig sind. Bezogen auf medizinische Daten ist die Kontrolle durch einen Datenschutzbeauftragten erforderlich, wenn Gesundheitsdaten verarbeitet werden. [30]

c) Dokumentationspflicht

Verpflichtend zu einer Behandlung muss ein Arzt umfassende Dokumentationen erstellen, die einerseits eine beweiskräftige Aussagefähigkeit in strittigen Fällen zwischen Patient und Behandler sicherstellt und andererseits auch Möglichkeiten zur Standardisierung von Verfahren und Qualitätssicherung bietet. Die Vorschriften dazu finden sich beispielsweise in § 10 Abs.1 MBO und anderen Gesetzen (BMV-Ä, EKV, Röntgenverordnung, etc.) [30]. Die Datenerfassung im Rahmen einer Behandlung (Behandlungsvertrag) bedarf keiner expliziten Zustimmung des Patienten, wenn die Daten notwendig zur Durchführung der Behandlung sind. Der Umfang der Dokumentation muss zweckgebunden erfolgen und soll die Grundsätze des Datenschutzes berücksichtigen. Üblicherweise sind mehrjährige Speicherfristen vorgeschrieben. Dies dient vor allem der Sicherung gegenüber Ansprüchen, die seitens des Patienten im Falle einer fehlerhaften Behandlung geltend gemacht werden können. Darüber hinaus gibt es auch Krankheiten, bei denen eine zeitliche Dokumentationshistorie von Vorteil ist. [30]

d) Informationelles Selbstbestimmungsrecht

Ausgehend von einem Urteil des Bundesverfassungsgerichts (Volkszählungsurteil, 1983) wurde der Begriff des informationellen Selbstbestimmungsrechts definiert, welches das Recht des Einzelnen über die Geheimhaltung und Art der Verwendung seiner persönlichen Daten beschreibt. Daraus ergibt sich in der

Medizin folgende Kernaussage: „Aus dem Recht auf informationelle Selbstbestimmung ergeben sich die Auskunftspflichten des Arztes gegenüber dem Patienten. Der Patient hat ein Recht darauf zu erfahren, welche Daten über ihn vorliegen. Dazu gehört auch das Recht auf Kopien seiner Krankenakte. Grundsätzlich ist der Arzt verpflichtet, über den objektiven Teil seiner Aufzeichnungen Auskunft zu geben oder Kopien anzufertigen. Werden dem Patienten Informationen verweigert, so ist unter Umständen plausibel zu begründen warum!“ [31]

e) Wahrung des Patientengeheimnisses

Abgrenzend zur ärztlichen Schweigepflicht lässt sich die Wahrung des Patientengeheimnisses mit Maßnahmen beschreiben, die zur Geheimhaltung der persönlichen Daten dienen. Die ärztliche Schweigepflicht lässt sich als aktiven Prozess betrachten, bei dem keinerlei Daten oder Informationen durch die mit der Behandlung betreuten Personen (aktiv) an Dritte weitergegeben werden dürfen. Des Weiteren ist aber auch eine passive Betrachtungsweise sinnvoll: es muss verhindert werden, dass medizinische Daten Personen zugänglich gemacht werden, die keinen Zugriff darauf besitzen dürfen. Technische Systeme müssen mit ausreichenden Mechanismen versehen werden, die zum Beispiel eine Zugangskontrolle und Verschlüsselungen beinhalten. Diese Vorkehrungen müssen regelmäßig auf Aktualität und hinreichende Umsetzung nach Stand der Technik überprüft werden. [30]

f) Recht auf Dateneinsicht des Patienten

Basierend auf dem informationellen Selbstbestimmungsrecht besitzt jeder Patient generell das Recht auf Auskunft, welche Daten über ihn wo zu welchem Zweck gespeichert sind und wer darauf Zugriff besitzt. Diese nicht zu vernachlässigende Erfordernis wird idealerweise in frühen Phasen der Entwicklung von Datenschutz-Modellen beziehungsweise Projekten mit Inhalten der Verarbeitung medizinischer Daten miteingebunden, um das Auskunftsrecht des Patienten lückenlos erfüllen zu können. Im Unterschied zum allgemeinen Recht auf Auskunft sind in Behandlungen noch Einschränkungen vorhanden: der Patient darf nur objektive Daten im Zusammenhang mit der Behandlung einsehen, subjektive Daten (zum Beispiel persönliche Einschätzungen von einem Arzt) unterliegen nicht diesem Recht. Die Daten beziehungsweise deren Darstellung muss so er-

folgen, dass auch ein Patient ohne größere Schwierigkeiten die ihm vorgelegten Informationen verstehen kann. [30]

Diese Punkte müssen zusätzlich zu den im vorherigen Kapitel erwähnten Grundsätzen des Datenschutzes in der Konzept-Erstellung des Telemedizinregisters berücksichtigt werden und verursachen teilweise einen Interessenskonflikt der beteiligten Personen des Registers. Besonders in der Telemedizin stellt die Übermittlung erfasster Daten ein Schwerpunkt in Verarbeitungsprozessen dar und verletzt bei zu sorgloser Anwendung gegebenenfalls mehrere gesetzliche Richtlinien. So ist es beispielsweise einem behandelnden Arzt bei strenger Auslegung der ärztlichen Schweigepflicht nicht ohne weiteres erlaubt, die von ihm im Rahmen der Behandlung erfassten Daten einem anderen Arzt zu übermitteln, wie dies im Rahmen eines Konsil notwendig ist. Da eine vorab eingeholte pauschale Einwilligung des Patienten zur Übermittlung von Daten datenschutzrechtlich als nicht ausreichend anzusehen ist, muss dieser Interessenskonflikt in der Planung von telemedizinischen Behandlungen sorgfältig berücksichtigt werden. Der Patient muss im Vorfeld der Behandlung so ausführlich wie möglich aufgeklärt sein, welche Daten von ihm verarbeitet werden, um nachträgliche Komplikationen zu verhindern.

Zur Vermeidung allzu komplizierter Ausgangssituationen gibt es für einige Bereiche der Medizin gesetzliche Übermittlungsbefugnisse: beispielsweise ist im Sozialgesetzbuch V (SGB V) die (notwendige) Übermittlung an kassenärztliche Vereinigungen, Krankenkassen und dem medizinischen Dienst genau definiert. [30] Dadurch wird es legitimiert, auch ohne eine ausdrückliche Einverständniserklärung des Patienten Daten der Behandlung, die für Abrechnungsvorgänge notwendig sind, den beteiligten Kostenträgern zu übermitteln. Ein optionales Widerspruchsrecht des Patienten würde ein geregeltes Behandlungsverhältnis nicht ermöglichen und wird daher durch diese definierten gesetzlichen Regelungen aufgehoben. [30]

Der telemedizinische Sektor unterliegt aufgrund disziplinarüberschreitender Ausrichtungen diversen Gesetzen und Einflussfaktoren, die im Vorfeld der Register-Anwendung seitens des telemedizinischen Dienstleisters auf die Einhaltung überprüft und umgesetzt werden müssen. Eine nachträgliche Korrektur durch zum Beispiel erweiterte Einwilligungserklärungen des Patienten bringt erfahrungsgemäß viele Komplikationen mit sich.

4 Auflistung datenschutzrelevanter Modelle

Der Bereich der medizinischen Forschung behandelt schon lange das Thema Datenschutz von medizinischen Daten. Besonders durch die Arbeiten der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) existieren einige grundlegende Überlegungen und daraus resultierende Modelle, die als Konzept auch für die telemedizinischen Anwendungen geeignet sind.

Im Folgenden wird das Hauptmodell des TMF vorgestellt, welches sich thematisch in verschiedene Untermodelle abhängig vom Anwendungsgebiet untergliedern lässt. Die Ziele dieses Datenschutzkonzeptes sind vor allem die Sicherung der Qualität und Verbesserung der Anwendung datenschutzrechtlicher Vorschriften in der medizinischen Forschung. [28] Hierbei sind die Grundlagen für die rechtliche und moralische Anwendung der Forschung in die Modellierung der Konzepte mit einbezogen und dienen als Basis für die Entwicklung eines konkreten Datenschutzmodells.

Die Voraussetzungen der Datenerfassung und Datenspeicherung in der medizinischen Forschung ähneln der Struktur in der Telemedizin und sind daher geeignet, verschiedene Ausgangssituationen schematisch in ein Modell zu überführen. Zusätzlich sind in der Telemedizin einige Anwendungen und Projekte bereits mit der Forschung verbunden und realisieren die Speicherung größerer Datenmengen mit dem Zweck einer anschließenden Verwendung, wenn beispielsweise eine Studiauswertung beabsichtigt wird.

Im Mittelpunkt der TMF-Konzepte steht die Trennung der Behandlungsdaten beziehungsweise Forschungsdaten in zwei Kategorien:

- **IDAT (identifizierende Daten)**

Diese Daten sind personenbezogen und benötigen besondere Schutzvorkehrungen (Verschlüsselung, Pseudonymisierung, Anonymisierung, Sperrung). Beispielsweise sind direkt personenbezogene Daten wie Name, Adresse, Geburtsdatum, etc. Elemente der Menge IDAT, aber auch indirekt identifizierende Daten wie die Krankenkassennummer sind als IDAT zu klassifizieren. [28]

- **MDAT (medizinische Daten)**

Die andere Teilmenge umfasst alle medizinischen Daten, die für sich alleine ausgewertet keine Identifizierung einer Person ermöglichen. Dies sind beispielsweise Daten zur Medikation, Vitalparameter, etc. Nur in Zusammenhang mit passenden Elementen der IDAT-Menge lässt sich eine Zuordnung zu einer Person vornehmen. Daher werden vergleichsweise keine so umfangreichen Schutzmechanismen in den Datenschutz-Modellen wie für die IDAT-Menge benötigt. [28]

Prinzipiell müssen allen Modellen die Voraussetzungen vorhanden sein, medizinische Daten abspeichern zu dürfen. Dies beinhaltet eine datenschutzrechtliche Überprüfung der vorliegenden Betriebsstruktur und vor allem die Einwilligung der betroffenen Patienten zur Datenspeicherung und der eventuell pseudonymisierten Datenweitergabe zum Zweck der Forschung. In diversen medizinischen Bereichen besteht eine Pflicht zur Erfassung der Daten in einem Register, welches beispielsweise bei meldepflichtigen Krankheiten (Seuchen, etc.) gegeben ist. In den meisten Fällen muss aber, falls keine gesetzliche Regelung dazu existiert, eine Einwilligungserklärung der Patienten zur Datenweitergabe vorhanden sein.

Das grundlegende Vorgehen in den Modellen ist nach der Trennung der Datenkategorien in IDAT und MDAT die anschließende Bearbeitung der besonders sensiblen IDAT Menge mit Hilfe einer Pseudonymisierung. Diese kann gegebenenfalls mehrstufig durchgeführt und bei einem Treuhänder umgesetzt werden. [32]

4.1 Datenschutzmodelle des TMF

Das TMF hat basierend auf dem Grundmodell für vier Anwendungszwecke ein jeweils angepasstes Modell entworfen, die unterschiedliche Pseudonymisierungsstufen und Verarbeitungsschritte vornehmen. Die Trennung der Anwendungsbereiche ergibt sich hauptsächlich durch die Art der angewandten Forschung: so gibt es Forschungen mit direktem Patientenbezug, bei dem der Erfasser der Daten zusätzliche Zugriffsmöglichkeiten auf die von ihm abgespeicherten Daten benötigt, beispielsweise bei der Erfassung eines Krankheitsverlaufs für Forschungsbereiche. Dem gegenüber gibt es Forschungs-

umsetzungen, die nur eine einmalige Datenerfassung vorsehen (indirekter Patientenbezug). Beispiele hierfür sind Register für die Erfassung meldepflichtiger Krankheiten, bei denen keine kontinuierliche Datenpflege der abgespeicherten Datensätze notwendig ist.

Im Grundmodell des TMF existieren dazu drei abgegrenzte Bereiche, die am Datenaustausch beziehungsweise der Speicherung für medizinische Forschungszwecke beteiligt sind [28]:

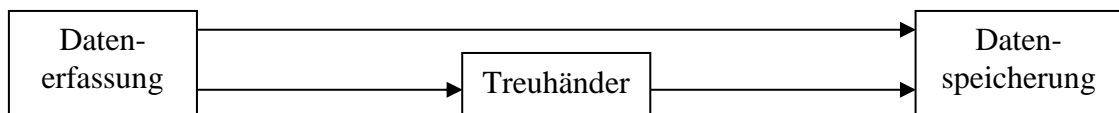


Abbildung 4, TMF Grundmodell [28]

- **Datenerfassung / Anwender**
Umfasst alle Anwender, die in der Behandlung für die Erfassung von medizinischen Daten verantwortlich sind, zum Beispiel Ärzte und Kliniken.
- **Treuhand-er (modellabhängig)**
Zwischen den Bereichen der Datenerfassung und Datenspeicherung ist optional ein Treuhand-er vorgesehen, dessen Aufgabe die sichere Veränderung der IDAT-Menge ist, meist durch Pseudonymisierung. Abhängig vom Modell sind mehrere Zwischenschritte für diesen Prozess vorgesehen, um eine IDAT-Menge für die sichere Datenspeicherung aufzubereiten. Oftmals findet sich in der Literatur die Bezeichnung TTP (Trusted Third Party) als Synonym für den Treuhand-erdienst.
- **Datenspeicherung / Datenbank**
Die erfassten Daten werden in einem zentralen oder dezentralen Datenspeicher abgelegt, der oftmals extern vorgehalten wird. Vor der Speicherung sind Mechanismen zur Pseudonymisierung der IDAT-Menge erforderlich. Eine Verarbeitung der Daten erfolgt entweder durch einen direkten Zugriff (beispielsweise einem Webinterface) oder indirekt durch eine Anfrage und anschließendem Datenexport.

In den Modellen ist der Fokus auf die jeweilige Handhabung mit den Daten gerichtet. Die zusätzlich notwendige Verschlüsselung beim Austausch von Daten (Übermittlung an externe Bereiche) wird bei dieser Betrachtungsweise vorausgesetzt.

4.1.1 TMF – Modell A

Das erste Modell berücksichtigt eine vergleichsweise einfache Struktur des Datenaustauschs. Die dabei verwendeten Datentypen sind MDAT, IDAT und ein Patientenidentifikator (PID), der ein eindeutiges Abbild aus der IDAT-Menge darstellt, vergleichbar mit einem Schlüsselattribut in einer Datenbank. Dieses Modell eignet sich vor allem bei der versorgungsnahen Forschung, bei dem ein direkter Patientenbezug in der Erfassung und Verarbeitung vorhanden ist. [27]

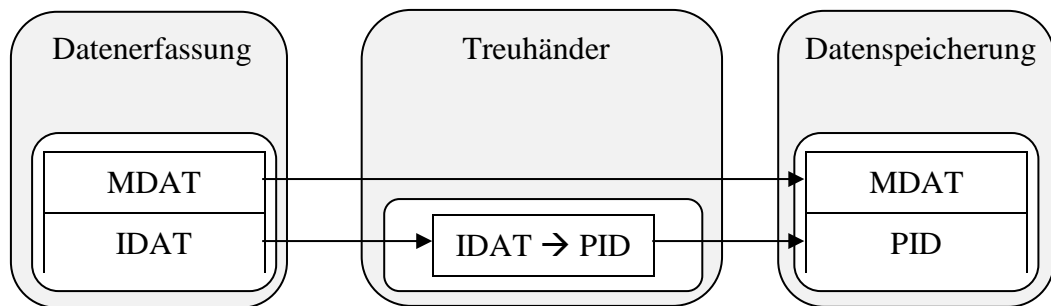


Abbildung 5, TMF – Modell A [27]

Ablauf:

Die anfangs erfassten Daten bei den Anwendern (zum Beispiel Arzt, Labor) dienen als Ausgang zur Daten-Aufbereitung. Dabei werden die Daten der IDAT-Menge einem Treuhänder übermittelt, der anhand eines festgelegten Verfahrens aus den IDAT-Daten einen eindeutigen Identifikator erzeugt, welcher mit PID bezeichnet wird. Dieser wird anschließend zusammen mit den MDAT-Daten in dem Datenspeicher abgelegt. Die Zuordnung IDAT→PID wird in einer Liste beim Treuhänder gespeichert und ist nur diesem zugänglich. [27]

Merkmale:

- Möglichkeit zur Datenpflege beziehungsweise mehrmaligen Verarbeitung durch den Anwender
- Datenqualität muss beim Anwender sichergestellt werden
- Personenbezogener Zugriff für die Anwender auf den Datenspeicher
- Ein direkter Zugriff auf den Datenspeicher durch angeschlossene Forschungsprojekte ist nicht vorgesehen, die Datenweitergabe erfolgt durch Export
- Pseudonym ist nur dem Treuhänder und in dem Datenspeicher bekannt
- MDAT und IDAT sind nur dem jeweiligen Anwender bekannt.

Das Verfahren zur PID-Generierung aus der IDAT-Menge beim Treuhänder, welches in den unterschiedlichen Modellen eingesetzt werden kann, ist in der folgenden Grafik schematisch dargestellt:

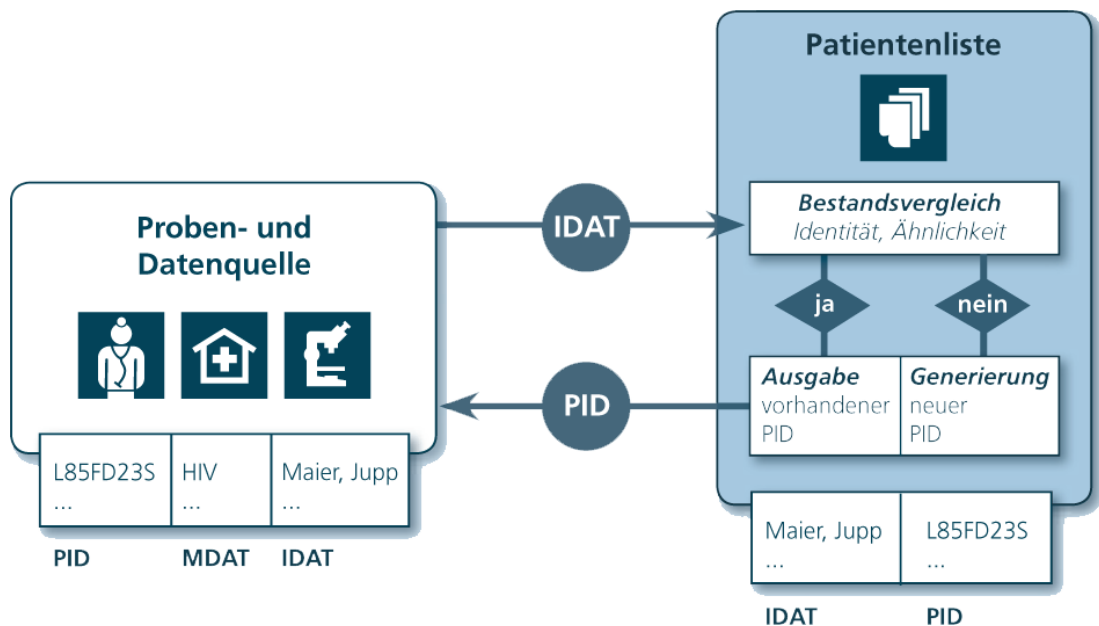


Abbildung 6, Funktionsweise IDAT zu PID [33]

Durch die TMF wurde ein PID-Generator entwickelt, der die notwendigen Schritte zur Pseudonym-Generierung standardisiert in mehreren Schritten vornimmt [33]:

1. Beim Anwender beziehungsweise Erfasser der Patienten-Daten sind die Daten in MDAT und IDAT kategorisiert.
2. Die IDAT-Daten werden an den PID-Generator übermittelt (zum Beispiel bei einem Treuhänder).
3. Dort werden die IDAT-Daten einem fehlertoleranten Matchingverfahren unterzogen, um fehlerhafte Eingaben auszubessern, die zum Beispiel häufig durch unterschiedliche Schreibweisen bei der Erfassung des Patientennamens auftreten.
4. Falls noch kein PID existiert, wird ein neuer PID generiert und die IDAT-Daten mit dem dazugehörigen PID in einer Zuordnungsliste gespeichert. Andernfalls wird die schon vorhandene PID ermittelt.
5. Die PID wird an den Anwender zurückgegeben, der diese für den weiteren Verarbeitungsprozess verwenden kann.

Zu berücksichtigen ist in diesem Verfahren, dass die PID an den Anwender zurück geliefert wird und je nach System diesem zusammen mit den IDAT-Daten und MDAT-Daten bekannt ist.

Bezogen auf das Modell A ist das Verfahren auch so umsetzbar, dass die PID direkt an den Datenspeicher weitergegeben wird und dem Anwender somit nicht mehr zur Verfügung steht. Nur beim Treuhänder und im Datenspeicher sind dann die PID in Verwendung.

4.1.2 TMF – Modell B

Forschungsbereiche ohne direkten Patientenbezug werden im zweiten Modell des TMF behandelt. Eine der größten Unterschiede zum vorherigen Modell ist die eingeschränkte Möglichkeit der Datenverwaltung seitens des Anwenders, da in dem Bereich der Datenspeicherung ein dem Datenerfasser unbekanntes Pseudonym verwendet wird. Diesem ist somit eine einseitige Datenübermittlung gestattet. Weitere datenpflegende Zugriffe, beispielsweise für eine Aktualisierung der im Datenspeicher hinterlegten Daten, sind in diesem Konzept nicht vorgesehen. [32]

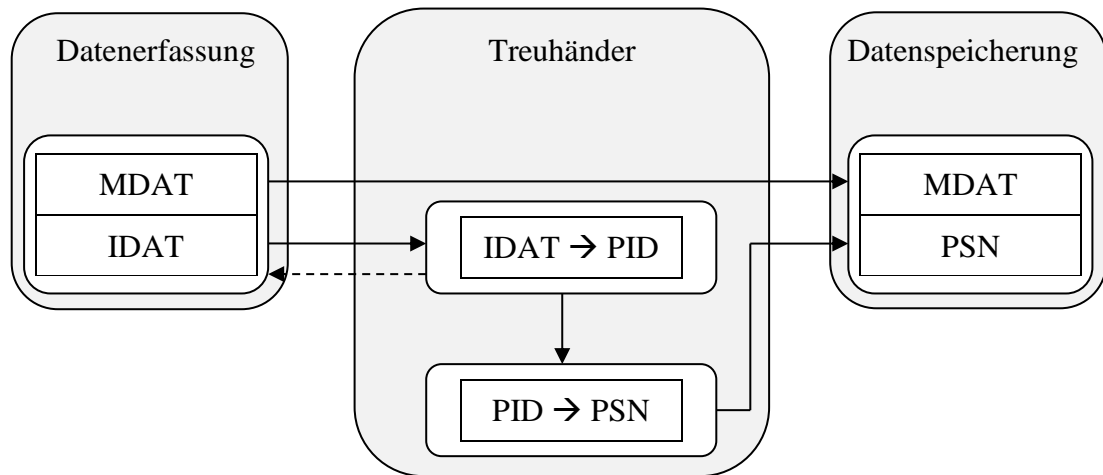


Abbildung 7, TMF – Modell B [32]

Der Vorgang der Pseudonym-Erzeugung erfolgt in diesem Modell mehrstufig. Ausgehend von der auch im ersten Modell verwendeten PID-Generierung wird im zweiten Schritt verschlüsselt ein Pseudonym erzeugt, welches für den Datenspeicher vorgesehen ist.

Ablauf:

Der initiale Ablauf ist mit dem des Modell A vergleichbar. Nach der Generierung des PID gibt es zwei Teilprozesse:

1. Der PID wird an den Anwender zurückgegeben und kann im weiteren Verlauf der Datenverarbeitung verwendet werden.
2. Der PID wird unmittelbar zur Erzeugung des Pseudonyms verwendet. Das Pseudonym wird mit den MDAT-Daten verbunden und an den Datenspeicher übermittelt.

Merkmale:

- Das Verfahren zur Pseudonym-Erzeugung ist nur dem Treuhänder bekannt
- Beim Treuhänder wird eine Liste IDAT→PID und eine Liste PID→PSN verwaltet und ist nur diesem bekannt.
- Das Pseudonym erlaubt keine Rückschlüsse auf die dazugehörige IDAT-Menge und bietet somit eine sichere Speicherung der für die Forschungszwecke benötigten Daten.

- Nachträgliche Änderungen an denen im Datenspeicher abgelegten Datensätzen können nur durch eine De-Pseudonymisierung beim Treuhänder erfolgen.
- Durch das (sichere) Pseudonym können direkte Zugriffe auf den Datenspeicher durch angeschlossene Partner erlaubt werden, ein indirektes Verfahren über einen Export-Vorgang ist nicht zwingend erforderlich.

4.1.3 TMF – Modell Biodatenbanken

Erweiternd zum TMF Modell – B sind im Datenschutz-Modell für Biodatenbanken zusätzliche Parameter zur Kennzeichnung der abgespeicherten Datensätze vorgesehen, da in dieser Struktur zusätzlich zur Erfassung von Forschungsdaten dazugehöriges Material wie beispielsweise Proben eingelagert werden. [34]

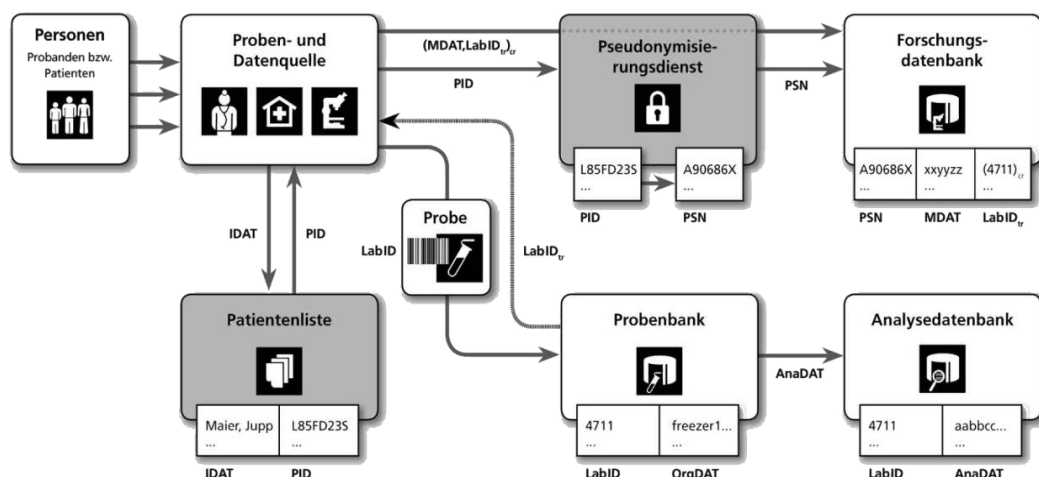


Abbildung 8, TMF – Modell Biodatenbank [34]

Die Kennzeichnung LabID und die pseudonymisierte Kennung LabID_{tr} verbinden die Proben mit den zugehörigen MDAT-Daten. Die Funktionsweise der LabID Pseudonymisierung ist mit der des PID→PSN Generierungsvorgang vergleichbar: die LabID wird an die Probenbank übermittelt und liefert das Pseudonym LabID_{tr} an die datenerfassende Stelle zurück, die das Pseudonym verschlüsselt mit der MDAT-Menge in die Forschungsdatenbank ablegt. Durch die Trennung der ID-Generierungen sind Rückschlüsse auf betroffene Personen deutlich erschwert und bilden somit eine Grundvoraussetzung zur weiteren Datenverarbeitung durch externe Quellen. [34]

Merkmale [34]:

- Physische Trennung von Material (LabID_{tr}) und Daten (MDAT, PSN)
- Trennung von Analysedaten und medizinischen Daten möglich
- LabID beim Erfasser und der Probenbank bekannt
- LabID_{tr} als Parameter zur Speicherung in Forschungsdatenbank
- LabID_{tr} bekannt beim Erfasser, Probenbank, Forschungsdatenbank

4.1.4 TMF Maximalmodell

Als Weiterentwicklung der bisherigen drei Modelle ist vom TMF ein schematisches Modell entworfen worden, das die Funktionsweisen der bisherigen einzelnen Modelle als eigenständige Module bündelt und dadurch eine größere Flexibilität bei der Umsetzung in reale Datenschutz-Projekte bietet, indem ein weiteres zentrales Modul zur Verwaltung der Identitäten integriert wird. [32]

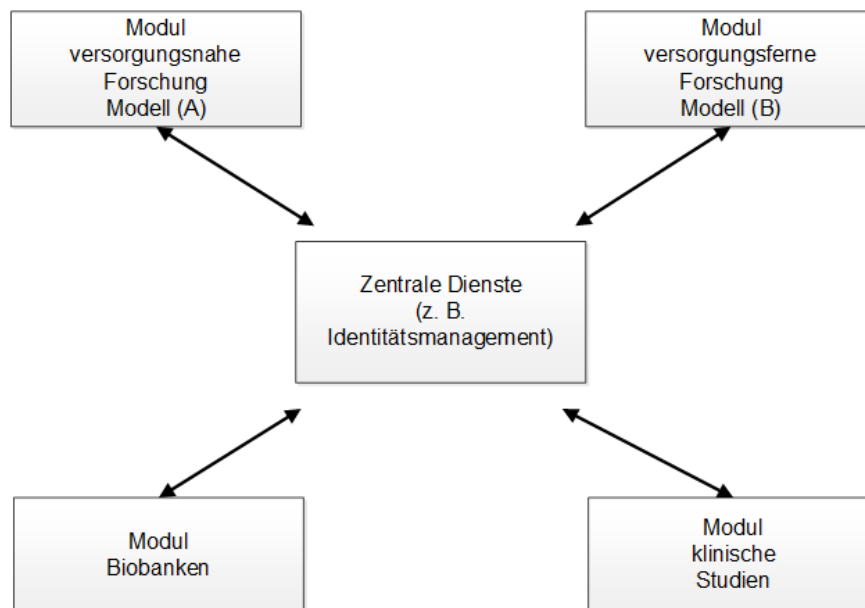


Abbildung 9, Maximalmodell TMF [32]

Des Weiteren ist die Modellierung der datenschutzrechtlichen Verfahren von klinischen Studien in einem eigenständigen Modul umgesetzt.

Merkmale [32]:

- Einheitliches Modell mit modularer, skalierbarer Netzarchitektur
- Größere Anwendbarkeit bei Projektplanungen
- Vereinfachte Umsetzbarkeit durch modularen Aufbau
- Unterschiedliche rechtliche Rahmenbedingungen werden in den Modulen gekapselt
- Modulbauweise ermöglicht bessere informationelle Gewaltenteilung
- Kommunikation erfolgt über zentrale Module

Das zentrale Modul bietet für die angeschlossenen Module zentrale Dienste an, die einerseits für die Kommunikation und andererseits in allen beteiligten Modulen benötigt werden.

Dies sind beispielsweise folgende Dienste [32]:

- **Identitätsmanagement**

Werden in verschiedenen Modulen bestimmte Identitäten (beispielsweise Pseudonyme) benötigt, so bietet sich eine Verwaltung der Identitäten an einer zentralen Stelle an, wie dies mit einem Treuhänder umgesetzt werden kann. Identitäten, die bei nur einem Modul benötigt werden, sollten nur in diesem verwaltet werden. Je weniger Bereiche Kenntnisse über ein Identitätsmanagement besitzen (Zuordnungsliste IDAT→PID), desto sicherer ist die datenschutzrechtliche Bewertung.

- **Rechtmanagement**

Der Zugriff auf gespeicherte Daten unterscheidet sich nach Anwendungsgebiet der Forschung: bei versorgungsnahen Forschungen ist eine Möglichkeit zur Datenpflege oftmals notwendig, bei dem ein Datensatz fortlaufend ergänzt beziehungsweise verändert wird, um zum Beispiel einen Krankheitsverlauf zu dokumentieren. Versorgungsferne Forschungen hingegen können beispielsweise so aufgebaut sein, dass nur eine einmalige Datenerfassung notwendig ist und durch die Rechteverwaltung Zugriffe auf diese Datensätze deutlich limitiert sind.

- **Einwilligungsmanagement**

Als einer der elementarsten Grundvoraussetzungen für die Verarbeitung von medizinischen Daten ist eine vorhandene Einwilligungserklärung des betroffenen Patienten zwingend notwendig, solange keine gesetzliche Regelung für den Datenaustausch vorhanden ist. In dem zentralen Modul werden die Einwilligungen verwaltet, um auch bei gegebenenfalls widerrufenen Einwilligungserklärungen die gespeicherten Datensätze löschen beziehungsweise sperren zu können. Die zentrale Organisation verhindert damit unterschiedliche oder fehlerhafte Versionen des Einwilligungsstatus.

- **Datenqualitätsmanagement**

Bei der Erfassung und Pflege der Daten ist eine Qualitätssicherung vorteilhaft, welche zentral die verarbeiteten Daten auf die Erfüllung festgelegter Kriterien überprüft und somit eine Möglichkeit zur Standardisierung der Prozesse ermöglicht.

4.2 Anwendbarkeit im Bereich der Telemedizin

Die im vorigen Abschnitt vorgestellten TMF-Modelle eignen sich in vielfacher Weise für die Anwendung im telemedizinischen Bereich. Die meisten Problemstellungen sind auch bei Projekten der Telemedizin datenschutzrechtlich zu berücksichtigen und sind durch die oftmals enge Verbindung zu Studien und Forschungen vergleichbar in deren Umsetzung. [35] [36]

Besonders vorteilhaft ist einerseits die differenzierte Betrachtung der Modelle je nach angewandter Versorgungsnähe. In telemedizinischen Projekten wird zumindest das TMF - Modell A der versorgungsnahen Forschung Anwendung finden. Sobald medizinische Daten an externe Partner übermittelt werden und / oder in externen / entfernten Datenspeichern vorgehalten werden, sind Prozesse zur sicheren Pseudonymisierung und gegebenenfalls Anonymisierung identifizierender Daten zwingend anzuwenden.

In dem Anforderungskatalog für das Telemedizinregister ist daher die Anwendung und Weiterentwicklung der vom TMF vorgelegten Modelle sinnvoll, um eine fundierte Grundlage für ein sicheres Datenschutzkonzept umsetzen zu können.

In den folgenden Kapiteln werden verschiedene Struktur-Möglichkeiten in der Telemedizin erläutert, um darauf passende Modifikationen der Modelle vornehmen zu können.

Zu berücksichtigen ist bei der Datenschutz-Umsetzung für ein Telemedizinregister die bisher angewandte Struktur bei der telemedizinischen Anwendung, da bei jedem telemedizinischen Dienstleister ein datenschutzrechtliches Konzept zum Umgang mit medizinischen Daten zu erwarten ist. Daher kann das in dieser Arbeit aufgezeigte Modell als zusätzliche Kontrolle verwendet werden, falls schon ein ausgereiftes Konzept seitens des Dienstleisters vorhanden ist und gegebenenfalls nur partiell ergänzt wird.

Die Modelle des TMF sind in den letzten Jahren mehrfach Revisionen unterworfen worden und werden voraussichtlich noch weitere Änderungen in den nächsten Jahren aufweisen. Daher ist bei der Planung zur Realisierung eines Telemedizinregisters eine Überprüfung auf Aktualität der in Betracht gezogenen Modelle sinnvoll. Auch seitens neuer EU-Richtlinien zum geregelten Datenaustausch über Ländergrenzen hinweg muss mit weiteren Anpassungen und geänderten Anforderungen gerechnet werden. [36]

4.3 Problemfälle

Exemplarisch sind einige bekannte Datenschutz-Probleme aufgeführt, welche in den letzten Jahren im medizinischen Bereich aufgetreten sind. Diese Auflistung erfolgt ohne eigene Bewertung und dient als Hinweis, dass ein exakt definiertes Datenschutz-Konzept Grundvoraussetzung im Bereich der vernetzten Medizin ist, um die Risiken und Gefahren unkontrollierbarer Datenverluste zu verringern:

April 2008

Aufgrund einer privaten Nutzung eines im medizinischen Sektor eingesetzten Rechners gelangten tausende Arztberichte einer spanischen Privatklinik in das öffentliche Internet. [37]

November 2011

Mehr als 2500 sensible Daten von Patienten (Klinikbriefe, medizinische Befunde, psychologische Dokumentationen) sind monatelang über das öffentliche Internet verfügbar.

Die verursachende Lücke existierte bei einem externen Dienstleister, der Datenbanken für mehrere soziale Dienste und Behörden in Deutschland verwaltet. [38]

August 2013

Durch den Datenschutzbeauftragten des Landes Schleswig-Holstein, Thilo Weichert, wurde auf einen Missstand im Umgang mit Patientendaten durch Apothekenzentren in Deutschland hingewiesen. Diese sind berechtigt, einen Handel mit erhobenen Daten aus angeschlossenen Apotheken zu betreiben, unter der Voraussetzung eine ausreichende Anonymisierung der identifizierenden Patientendaten vorzunehmen. Die angewandte Veränderung (64-stelliger Code) ist aber laut Weichert nicht ausreichend und ermöglicht eine Rückentschlüsselung und damit die Gefahr einer missbräuchlichen Profilerstellung von Patienten und deren Nutzungsverhalten von Medikamenten. [39]

Diese drei Beispiele zeigen schon die zahlreichen Problemstellen im Umgang mit sensiblen Daten. Datenschutz-Lücken entstehen oftmals durch Fehlverhalten, bisher unbekanntes Schwachstellen in verwendeten Software-Systemen oder auch mangelhaften Umsetzungen von datenschutzrechtlichen Konzepten. Mit den konzeptionellen Modellen der TMF kann frühzeitig in der Planungsphase ein Großteil möglicher Angriffspunkte und Schwachstellen in der datenschutzrechtlichen Handhabung erkannt und geschlossen werden.

Problematisch in vielen Projekten der Medizin kann ein sich verändernder Zweck der erfassten Daten sein, vor allem wenn marktwirtschaftliche Interessen der eigentlichen sparsamen Erfassung von Daten entgegenwirken. Dadurch könnten Datensätze zum Beispiel das Ziel von Unternehmen werden, die im Bereich der Pharmazie marktwirtschaftliche Interessen besitzen. Diese Gefahren können durch gut überlegte Datenmodelle minimiert werden, die einen aktuellen Stand der Pseudonymisierung und Verschlüsselung berücksichtigen.

5 Grundlagen – Register

Zum besseren Verständnis der verschiedenen Möglichkeiten bei der Strukturierung des Registeraufbaus werden in diesem Kapitel grundlegende Definition und Verfahren aufgelistet, die Anwendung in der Datenspeicherung finden und für die Verwendung des Telemedizinregisters geeignet sind.

Ein Unterschied wird zwischen dem Begriff der Datenbank und einem Register hervorgehoben, welches in der Literatur oftmals synonym verwendet wird:

Die Datenbank eignet sich als Datenspeicher für eine im Vorfeld definierte Art von Daten und deren Verwaltung. Sie ist gegebenenfalls vergleichsweise aufwändig in der Erweiterung für neue Datentypen, welche bei der Planung unberücksichtigt oder zu dem Zeitpunkt unbekannt waren.

In einem Register hingegen ist eine Speicherung verschiedenster Datentypen und Medien möglich, da das Register eine Kombination unterschiedlichster Datenspeicher bietet. Dabei kann eine Datenbank eine übergeordnete Instanz darstellen, um Schlüsselfaktoren zu erfassen und sortieren. Darüber hinaus sind auch Fileserver, physische Speichermöglichkeiten etc. unter dem Begriff Register aufgeführt, womit die unterschiedlichen Voraussetzungen der telemedizinischen Projekte ohne weitreichende Einschränkungen der speicherbaren Datentypen umgesetzt werden können.

5.1 Begriffsdefinitionen Register

Ein Register ist allgemein definiert eine Struktur, in der verschiedene Daten gespeichert und verwaltet werden können. Diese Daten werden zu verschiedenen Zwecken in diesem Register vorgehalten und sind je nach Aufbau des Registers unterschiedlich in ihren Verarbeitungsmöglichkeiten.

Folgende Teilnehmer beziehungsweise Positionen lassen sich in der Registeranwendung unterscheiden:

1. Register

Register ist ein Begriff für eine datenspeichernde Stelle. Dieses umfasst alle möglichen Speicherobjekte, in denen unterschiedliche Datentypen dauerhaft abgelegt werden können.

In dieser Betrachtungsweise beträgt die Anzahl von möglichen Registern genau eins. Dies bedeutet, dass für jedes Register eine getrennte Betrachtung der beteiligten Bereiche notwendig ist.

2. Datenerfassung

Der Bereich der Datenerfassung beschreibt alle verschiedenen Möglichkeiten, mit denen Daten erfasst und als Ziel die Übermittlung und Speicherung im Register haben.

Die Anzahl der möglichen Stellen zur Datenerfassung beträgt mindestens eins. Es sind also mehrere Positionen im Bereich der Datenerfassung möglich. Dies ist auch die häufigste Struktur, die bei einem Register-Aufbau im medizinischen Bereich zu erwarten ist.

3. Datenverarbeitung

Die Datenverarbeitung ist definiert durch alle verschiedenen Möglichkeiten, deren Ziel die Auswertung und weitere Verarbeitung der im Register abgelegten Daten ist.

Vergleichbar mit der Datenerfassung beträgt die Anzahl mindestens eins. Oftmals sind im medizinischen Sektor eine beziehungsweise wenige datenverarbeitende Positionen anzutreffen, die eine Analyse der im Register abgespeicherten Daten vornehmen.

4. Datenverwaltung

Die Datenverwaltung administriert und organisiert die Struktur und deren Verhalten bei der Ein- und Ausgabe der Daten im Register.

Bezogen auf ein Register ist die Anzahl der datenverwaltenden Stellen auch auf genau eins begrenzt. Eventuell ist die verantwortliche Stelle bei der laufenden Pflege des Registers unterschiedlich zu der, welche das Grundkonzept des Registers erstellt und aufgebaut hat. Trotzdem sind in der logischen Sichtweise

beide zu einer Position zusammengefasst, um damit die Abgrenzung zu den Bereichen der Datenerfassung und Datenverarbeitung hervorzuheben.

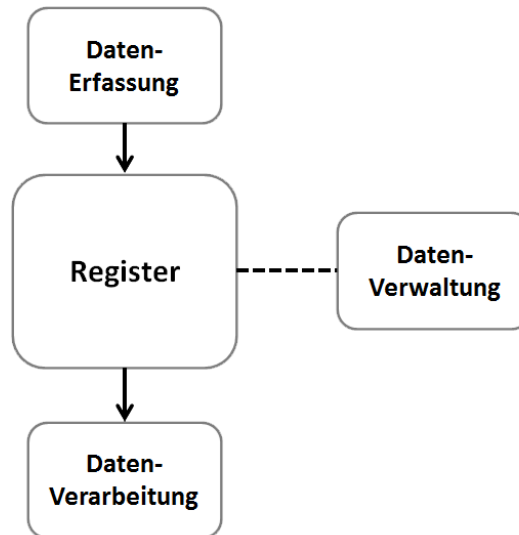


Abbildung 10, Schema Register-Aufbau

Die in der Grafik aufgeführten einzelnen Bereiche müssen nicht zwangsläufig unterschiedlicher Verantwortung unterstehen. So kann beispielsweise die Datenerfassung auch für die Verwaltung der abgespeicherten Daten zuständig sein oder auch die weitere Verarbeitung vornehmen. Eine logische Trennung der Funktionsbereiche vereinfacht aber die Konzeption bei der Erstellung und Wartung eines Registers, vor allem im Bereich der Rechteverwaltung. Diese umfasst alle definierten Regeln, welche Personen beziehungsweise Gruppen Zugriffsrechte auf die unterschiedlichen Datenbereiche besitzen. Diese Regeln sollten frühzeitig bei der Erstellungsphase des Registers definiert werden, da nachträgliche Anpassungen oft mit großem Aufwand verbunden sind.

Als eines der bekanntesten Register ist das Konzept des Krebsregisters in Deutschland zu nennen: schon vor mehreren Jahrzehnten entstand der Bedarf einer Datenspeicherungsmöglichkeit zur Klassifizierung von Krebsfällen, um aussagekräftigere Zahlen zur Verbreitung von Krankheitsfällen unter Berücksichtigung demografischer Faktoren (Alter, Wohnort, etc.) zu gewinnen. Dieses Konzept wird im folgenden Kapitel genauer beschrieben. [40]

Die **Vorhaltung der Register** erfolgt üblicherweise im medizinischen Sektor durch **öffentliche** Verantwortung, wenn dies zum Beispiel durch Gesetze festgelegt wurde.

Die Alternative ist eine **private** Organisation zur Register-Verwaltung, welches aber vorwiegend im marktwirtschaftlichen Sektor zu finden ist.

5.2 Verfahren der Datenübermittlung

Die Datenübermittlung von der datenerfassenden Stelle in das Register lässt sich, je nach Zeitraum und Häufigkeit der Übertragungen, in mehrere Verfahren unterteilen.

a) Einzelne Datenübertragung

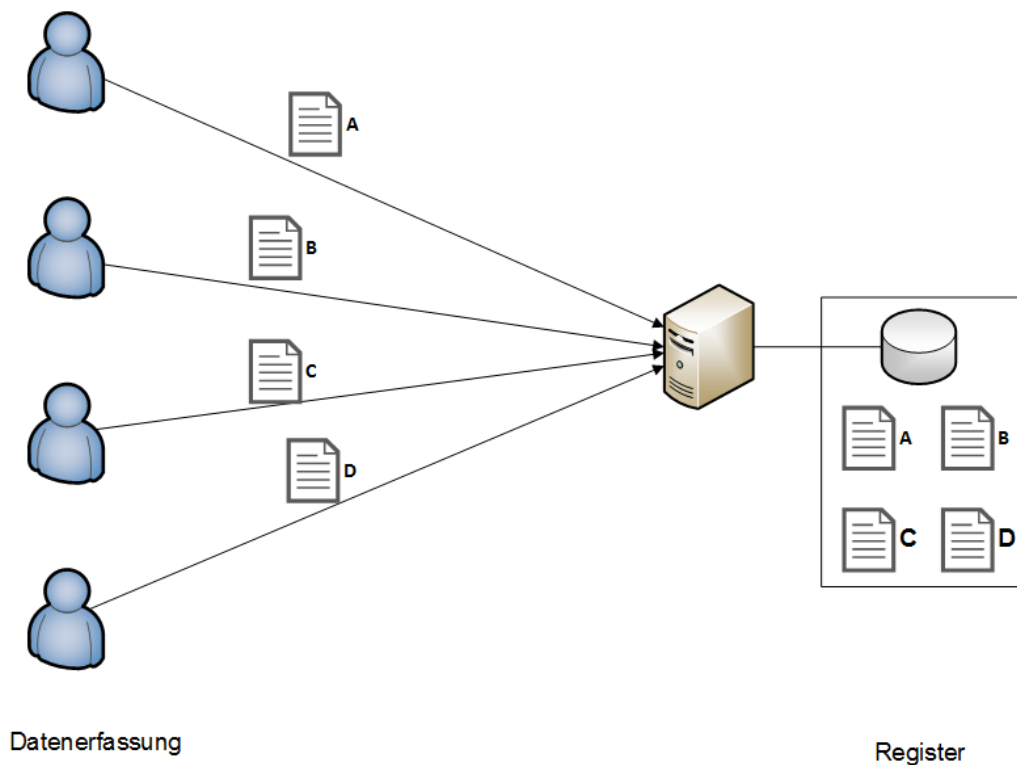


Abbildung 11, Register – einzelne Datenübertragung

Bei der einzelnen Übermittlung von Datensätzen ist die Struktur des Registers vergleichbar mit einer Meldfunktion von Daten. Das Ziel dieses Ablaufs ist die einmalige Erfassung von Ereignissen beziehungsweise Datensätzen, die nachträglich nicht mehr verändert oder ergänzt werden sollen.

Die datenerfassende Stelle benötigt dafür vergleichsweise wenig Rechte zur Datenspeicherung, da Veränderungen nicht vorgesehen sind und Löschungen / Sperrungen entweder automatisiert erfolgen (zum Beispiel nach Ablauf einer Zeitfrist) oder auf Antrag durch das Register erfolgen können.

Im Register ist der Vorgang der Datenannahme und Speicherung um den Prozess eines Datenabgleichs (siehe folgende Varianten) reduziert, da keine Daten zusammengeführt werden müssen.

b) Blockweise Datenübertragung

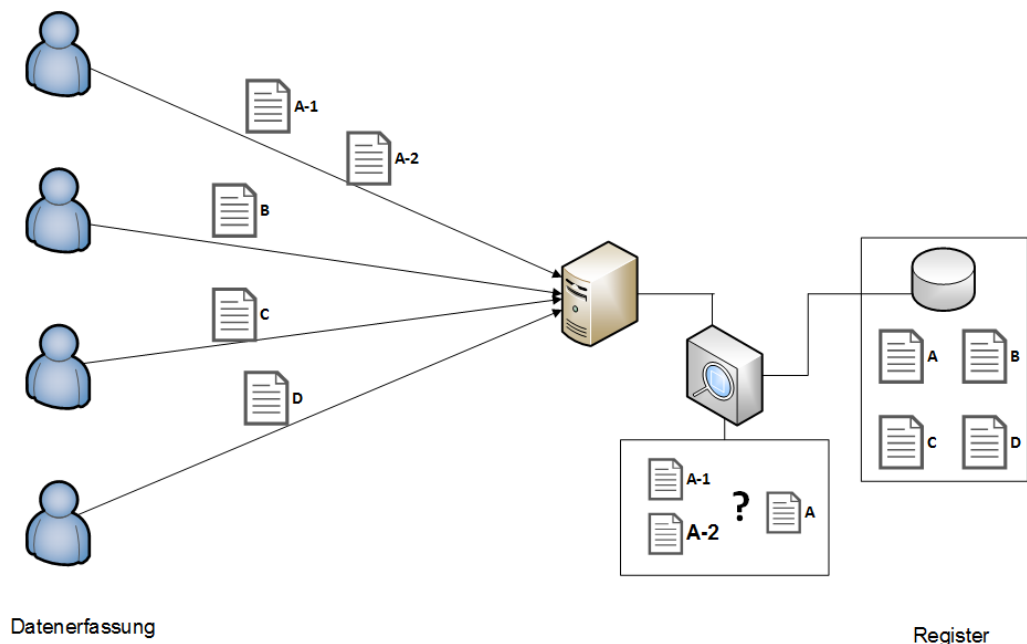


Abbildung 12, Register – blockweise Datenübertragung

Die blockweise Übermittlung von Daten bezeichnet eine Übertragungstechnik, die zu bestimmten Zeitpunkten (periodisch) oder unbestimmten Zeitpunkten (aperiodisch) erfolgt, aber keine permanente Übertragungsmöglichkeit beinhaltet. Beispielsweise werden nach einem initialen Vorgang der Datenanlage im Register über einen definierten Zeitraum hinweg mehrmals ergänzende Daten zu dem Datensatz hinzugefügt.

Die datenerfassende Seite benötigt eine komplexere Rechtezuteilung im Vergleich zur einmaligen Übermittlung, um bereits angelegte Datensätze korrekt erweitern beziehungsweise verändern zu können.

Im Register muss gegebenenfalls vor der Datenspeicherung eine Überprüfung stattfinden, ob ein Datensatz neu angelegt werden muss oder ein bestehender verändert wird. Diese Überprüfung ist vor allem im Bereich der Pseudonymisierung zwingend. Dieser Prozess ist in der Grafik als Zwischenschritt vor der Speicherung im Register aufgeführt. Dabei werden in diesem Prozess eingehende Datensätze anhand einer Identifikationsmöglichkeit überprüft, ob ein schon bereits existierender Datensatz im Register vorhanden ist, welcher mit neuen Daten ergänzt oder verändert werden muss.

c) **Kontinuierliche Datenübertragung**

Bei der kontinuierlichen Datenübertragung ist im Gegensatz zur blockweisen Übertragung eine dauerhafte Verbindung zwischen Datenerfasser und Register vorhanden und macht somit gegebenenfalls eine lokale Zwischenspeicherung von Datensätzen beim Erfasser überflüssig. Daten können in "Echtzeit" in das Register übertragen werden und bieten daher eine höhere Aktualität der abgespeicherten Daten. Nachteile sind hingegen die Notwendigkeit einer stabilen (und ausreichend schnellen) Verbindung und gegebenenfalls größere Verwaltungsaufgaben auf der Seite des Registers. Zum Beispiel ist eine qualitätssichernde Maßnahme zur inhaltlichen Bewertung der Datensätze bei der kontinuierlichen Datenübertragung erst im Register möglich, wobei die beiden vorherigen Verfahren durch eine zeitlich begrenzte Übermittlungstechnik Qualitätssicherungen beim Datenerfasser sinnvoll machen können.

Die Unterschiede in der Datenübermittlung ergeben sich vor allem in der Komplexität der Rechteverwaltung seitens der Zugriffsmöglichkeiten im Register und in der Anwendung von Pseudonymisierungstechnologien. Wird eine sichere Pseudonymisierung vorgenommen, erschwert dieses die Pflege eines bestehenden Datensatzes, wenn mehrere unterschiedliche datenerfassende Bereiche auf einen gemeinsamen Datensatz Zugriff benötigen. Wird die Pseudonymisierung nicht im Register vorgenommen, muss entweder durch eine zusätzliche Stelle die Pseudonymisierung zentral verwaltet werden oder

alle beteiligten Bereiche die gleiche Pseudonymisierung verwenden. Diese Problematik wird im folgenden Kapitel in einem Modell genauer beschrieben.

5.3 Register-Speicherverwaltung

Besonders die Struktur des Registerspeicherorts hat durch eine verbesserte Infrastruktur in der Vernetzung mehr Möglichkeiten erhalten. Wurden früher Register für mehrere Anwender zentral aufgebaut, sind heutzutage auch dezentrale Varianten möglich, die Vorteile gegenüber der zentralen Speicherung bieten.

Zur besseren Abgrenzung sind drei Speicherverwaltungsoptionen definiert: eine zentrale Speicherung, bei der das Register an einem Ort vorgehalten wird und eine dezentrale Speicherung, die sich wiederum in eine dezentrale Struktur mit mehreren verbundenen Speicherorten zusammensetzt und der Cloud-Struktur, deren Verhalten mit einem zentralen Register vergleichbar ist, aber dezentrale Vorteile bietet.

a) Zentrales Register

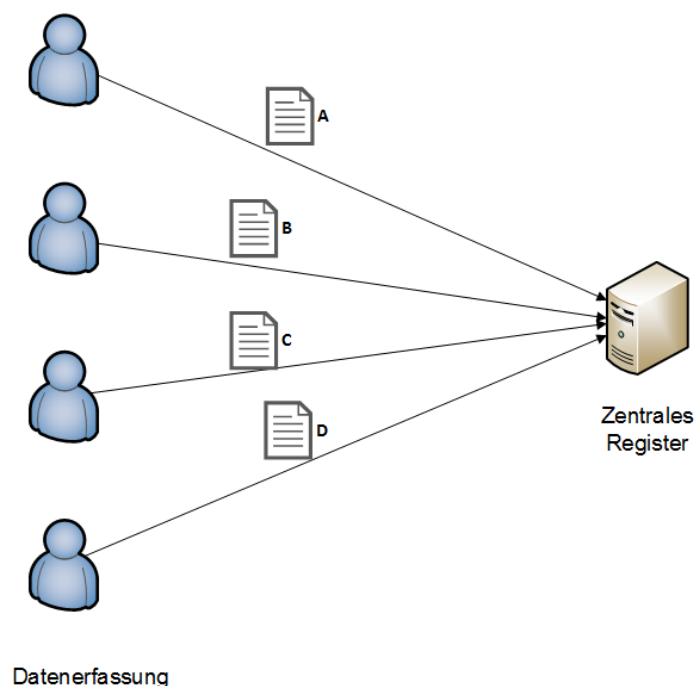


Abbildung 13, zentrales Register

Bei dieser Struktur befindet sich das Register an einem festen, definierten Ort. Alle Anwender des Registers müssen eine Verbindung zu der Schnittstelle des Registers aufbauen. Dieses kann über eine Netzwerk-Verbindung oder auch physisch betrachtet mittels eines Postversands zu Probeneinlagerungen oder nicht digitalen Meldeformularen erfolgen.

Vorteile sind die vergleichsweise einfach zu organisierenden Registermodelle und Rechteverwaltungen, die nur an einem Ort vorgenommen werden müssen. Bei Verarbeitungsprozessen im Register müssen keine Datensätze von verschiedenen Speicherstellen synchronisiert und die Prozesse zur Datenerfassung einfacher strukturiert werden. Nachteile bestehen in der zwingenden Verbindungsherstellung vom Anwender zum Register, welches bei Netzwerk-Ausfällen für Probleme sorgen kann.

b) Dezentrales Register

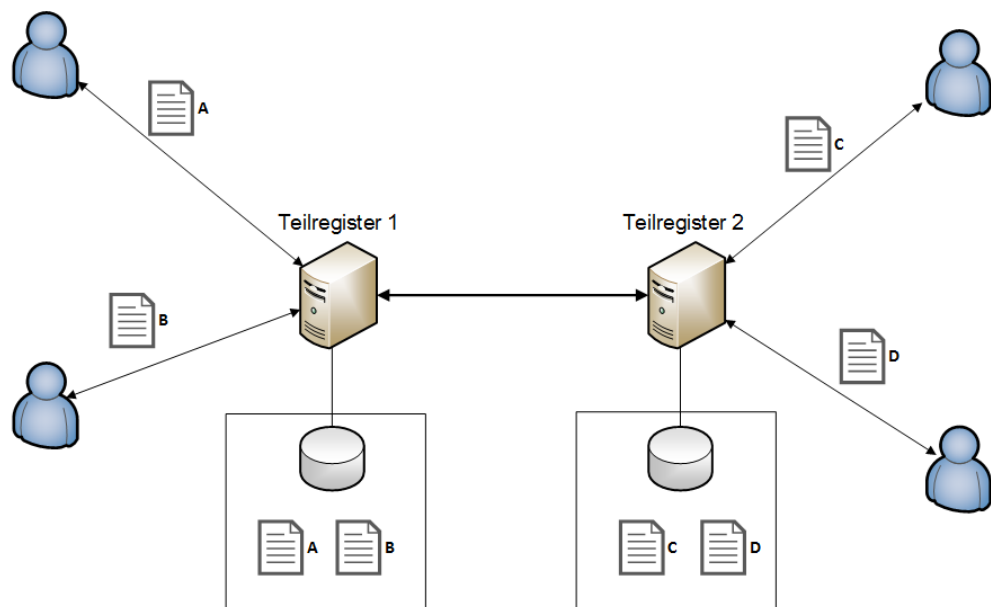


Abbildung 14, dezentrales Register

In dem Beispiel ist das Register in zwei Teilregister zerlegt, die miteinander verbunden sind. Auf die jeweiligen Teilregister greifen Anwender zu, die vorher einem Zugriffspunkt zugeordnet wurden. Daten, die zum Beispiel von dem Anwender A in das Teilregister 1 gespeichert werden, sind physisch nur in dem Teilregister 1 vorhanden und müssen mit zusätzlichen Prozessen dem Teilregister 2 bekannt gemacht werden. Die Verwaltung der Teilregister kann separat oder zentral organisiert sein.

Vorteile sind die Möglichkeiten zur genaueren Differenzierung, welche Anwender auf welche Teilregister einen Zugriff haben. Damit bestehen die Optionen einer spezifischeren Rechteverwaltung und ein geringeres Ausfallrisiko bei Zugriffen auf die Datensätze, da bei Ausfall eines Teilregisters die anderen Bereiche weiterhin zur Verfügung stehen. Je nach Strukturierung können die Teilregister lokal bei einem Anwender vorhanden sein und damit deutlich schnellere Zugriffsoptionen als ein entferntes (zentrales) Register bieten. Nachteilig ist die höhere Komplexität bei der Verwaltung der im Register hinterlegten Daten, wenn die einzelnen Teilregister miteinander verbunden werden müssen und das Risiko für Attacken auf das Register erhöht wird. Mit steigender Anzahl von Registerelementen vergrößert sich auch die Anzahl der Zugriffsmöglichkeiten.

c) Cloud – Register

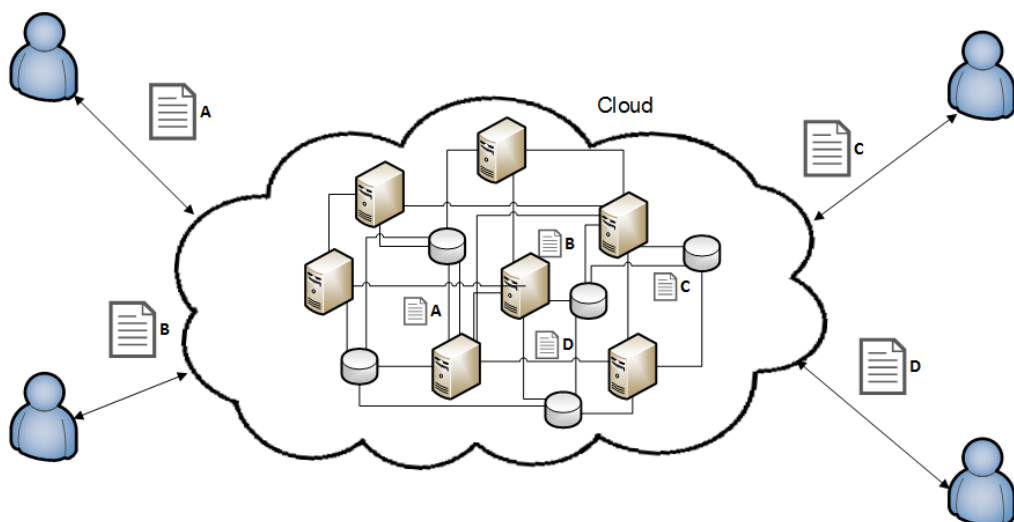


Abbildung 15, Cloud-Register

Eine weitere dezentrale Lösung ist die Cloud-basierte Speicherung von Daten. Mit dem Begriff Cloud werden Rechnernetze bezeichnet, die sich verteilt über größere Distanz dem Anwender vergleichsweise wie ein zentrales Rechnernetz darstellen und die ausgedehnte Struktur verbergen. Zusätzlich zu den Hardware-Lösungen stehen oftmals Software-Dienstleistungen den Anwendern als definierte Services standortunabhängig zur Verfügung.

In der oben aufgeführten Grafik sind in der Cloud zahlreiche Rechner und Speichermöglichkeiten angedeutet, die miteinander verbunden sind und das Rechnernetz darstellen. Die Verantwortung zur Strukturierung unterliegt dem Cloud-Anbieter.

Vorteilhaft ist eine gute Skalierbarkeit, bei der die Ressourcen in der Cloud optimal an die Bedürfnisse angepasst werden kann. Des Weiteren ist die Kombination von Hardware und Software-Diensten nicht standortgebunden und für die jeweiligen Anwender verfügbar und vereinfacht somit die Anwendbarkeit der Dienste. Nachteile sind die Grundstrukturen der Cloud, bei denen Daten in verteilten Rechnernetzen, die meist über das Internet erreichbar sind, gespeichert werden und somit die Zugriffskontrolle erschwert wird. Eigene Lösungen zu Cloud-Installationen, um die Verantwortung über den Cloud-Bereich zu besitzen, bedürfen gegebenenfalls umfangreicher Investitionen in die benötigte Infrastruktur.

Wie schon bei den zuvor erwähnten dezentralen Speichermöglichkeiten muss eine Abwägung zwischen einerseits der sicheren Verwaltung der Daten bei zentralen Lösungen und andererseits der besseren Anwendungsmöglichkeit von dezentralen Speicherräumen vorgenommen werden. In dieser Arbeit ist die Betrachtung vor allem auf die zentrale Speicherorganisation gelegt, da in dieser die Verwaltung und Administration am sichersten durchgeführt werden kann. Je sensibler die zu speichernden Daten sind, desto weniger sollte eine dezentrale beziehungsweise verteilte Lösung in Betracht gezogen werden, da die Risiken eines Datenverlustes mit Anzahl der beteiligten Speicherstellen ansteigt. Diese Situation ist besonders bei der Inanspruchnahme eines kommerziellen Cloud-Dienstes als kritisch zu bewerten, da die Verantwortung über die eingesetzten Systeme, die Zugriffskontrollen und Verbreitung der Daten beim Dienstanbieter der Cloud liegt.

5.4 Projektbeispiele

Der folgende Abschnitt führt einige Beispiele auf, die verschiedene Strukturen zur Datenerfassung und Speicherung verwenden.

Die Beispiele sind aus dem öffentlichen Sektor (Waffenregister und Melderegister).

a) Nationales Waffenregister (NWR)

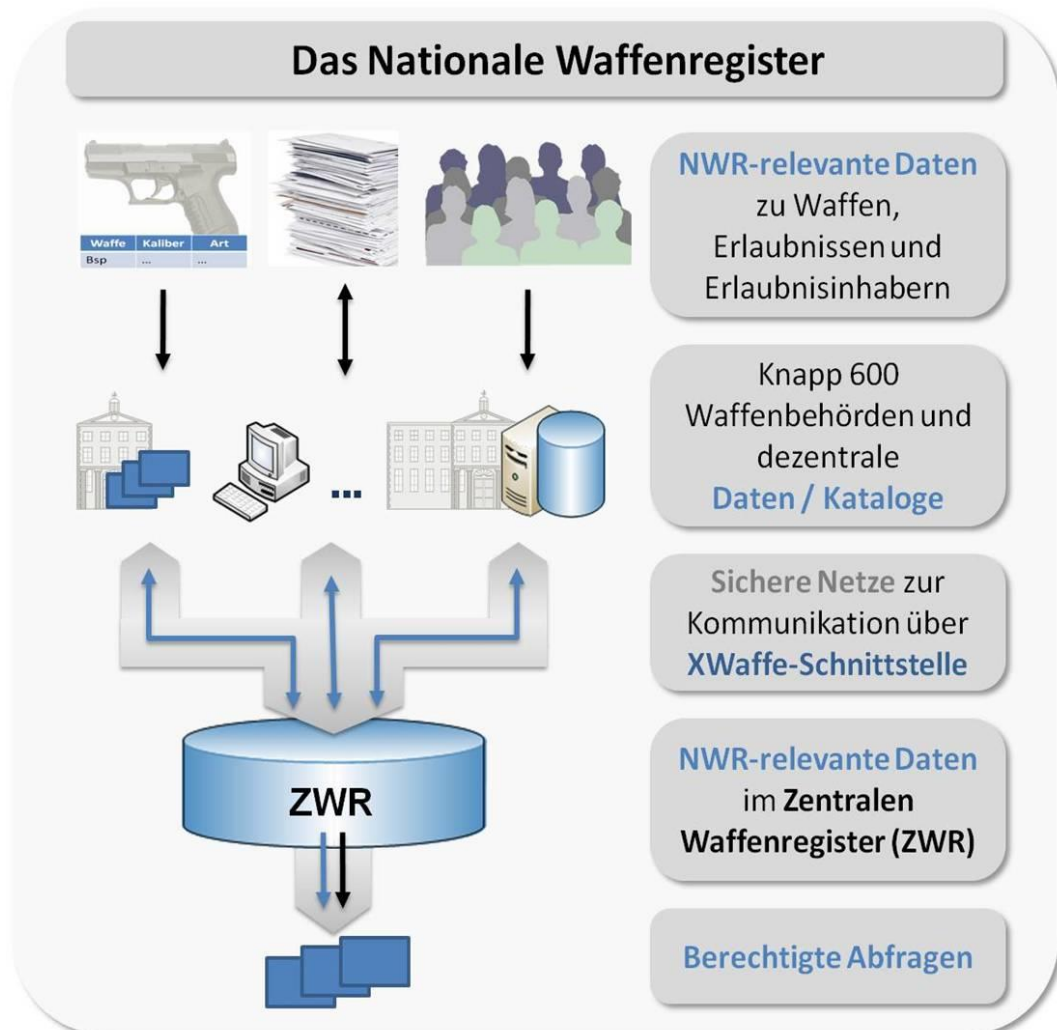


Abbildung 16, Nationales Waffenregister [41]

Anfang 2013 wurde ein neues nationales Waffenregister in Deutschland eingeführt, dessen Ziel die zentrale Speicherung von Informationen zu persönlichen Daten von Waffenhaltern und den Daten zu offiziell registrierten Waffen ist und die bisherigen regional verwalteten Waffenregister ablösen soll.

Die oben dargestellte Abbildung zeigt eine Migration von bisher vielfach vorhandenen lokalen Lösungen zur Datenerfassung (ca. 600 lokale Waffenbehörden in Deutschland) zu einem zentralen und bundesweit gültigem Register. Bis 2013 wurden die Datensätze zu Waffen in den lokalen Waffenbehörden erfasst, welche aber durch eine EU-Richtlinie (2008/51/EG) in ein zentrales oder dezentrales landesweit gültiges Waffenregister überführt werden mussten. [41]

Die heterogene Struktur der Waffenregistrierung, die durch die unterschiedlichen Waffenbehörden entstanden ist, musste in eine einheitliche Struktur überführt werden. Dazu wurde als Schnittstelle zwischen den lokalen Registern und dem nationalen Waffenregister eine XML-Struktur entworfen (XWaffe). Diese berücksichtigt alle notwendigen Parameter, welche im NWR erfasst werden müssen und wird von den lokalen Waffenbehörden als Standard eingesetzt, um die lokalen Datensätze ins NWR zu überführen. Aufgrund der Sensibilität der abgespeicherten Daten (personenidentifizierende Daten) ist das NWR nur aus einem privaten Verwaltungsnetzwerk zugänglich, eine Anbindung an das Internet ist nicht vorgesehen. [41]

b) Krebsregister

Zur Erfassung von meldepflichtigen Krankheiten und der rechtzeitigen Erkennung von drohenden Seuchen werden schon seit langem in der Medizin verschiedene Melderegister und Seuchenregister geführt. [40]

Ein bekanntes Beispiel ist die Erfassung von Krebserkrankungen in einem Register, bei dem auch Forschungsinteressen vorhanden sind. Durch den Gesetzgeber wurden Regelungen verfasst, die den Einsatz eines Krebsregisters definieren, zum Beispiel mit dem Bundeskrebsregisterdatengesetz (BKRGD) aus dem Jahr 2009. [42] Aufgrund unterschiedlicher Landesgesetze, die einen Registeraufbau zu Krebserkrankungen beeinflussen, sind auch hier heterogene Strukturen vorhanden, die in einem nationalen Register zusammengeführt werden sollen.

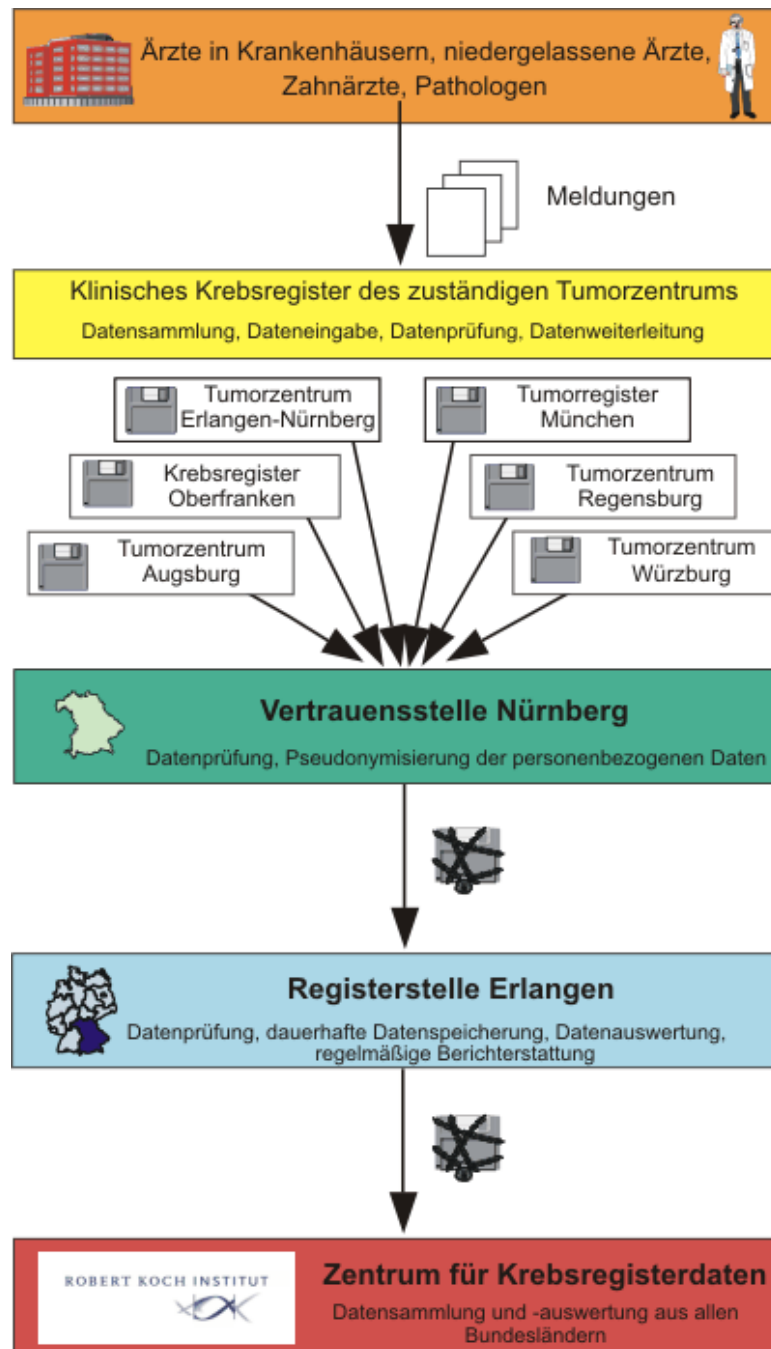


Abbildung 17, Meldeverfahren Krebsregister Bayern [43]

In der vorherigen Grafik ist der Ablauf des Meldeverfahrens skizziert, der bei Krebserkrankungen im Bundesland Bayern vollzogen wird. Dieses Verfahren wird in den anderen Ländern vergleichsweise durchgeführt und zeigt die verschiedenen Schritte zur Aufbereitung der regional erfassten Daten für ein landesweit anwendbares Krebsregister.

In regionalen Zentren (Tumorzentrum) werden von beteiligten Erfassungsstellen (Ärzten, Kliniken, Pathologen) Meldungen dokumentiert, die über zusätzliche Zwischenschritte an das Robert Koch Institut weitergeleitet werden.

Die erste Stelle (Vertrauensstelle Nürnberg) dient als Treuhänder für die Datenaufbereitung. In der darauf folgenden Registerstelle Erlangen werden zentriert für das Bundesland Bayern Datensätze der einzelnen Tumorzentren gespeichert und in einem weiteren Aufbereitungsprozess an das nationale Register übermittelt. [43] [44]

c) Melderegister der Länder

Ein Beispiel für ein dezentrales Speichervorhaben sind die Melderegister in den einzelnen Bundesländern von Deutschland. In jedem der Länder existieren eigene Landesmeldegesetze und bundesweit dazu ein Melderechtsrahmengesetz (MRRG). [45]

Die Registrierung und Erfassung erfolgt bei Einwohnermeldeämtern, die pro Gemeinde und Stadt eingerichtet sind. Derzeit beträgt die Anzahl deutschlandweit über 5000 Meldeeinrichtungen.

Die zentralen Register sind mit der Struktur des Telemedizinregisters vergleichbar, sofern dieses zentral eingerichtet und vorgehalten wird. Verschiedene Anwender sind an das Register angebunden und benutzen wie im Beispiel des Nationalen Waffenregisters standardisierte Methoden zur Datenerfassung und Übermittlung an das Register.

Im Telemedizinregister besteht auch die Option zur Einbindung mehrerer telemedizinischer Dienstleister, die aus unterschiedlichen Datenbeständen eine einheitliche Datenmenge im Register abbilden. Daher wäre bei einer konkreten Systementwicklung des Telemedizinregisters eine detaillierte Analyse der technischen Realisierungen des Waffenregisters ein mögliches Vergleichsmodell.

6 Wissenschaftliche Methodik

Folgend werden die wissenschaftlichen Methoden erläutert, die im Rahmen dieser Diplomarbeit eingesetzt werden. Bei den Methoden sind besonders die Methoden “Desk Research“ und Interviews ausgewählt worden, um neben der umfassenden Einführung in die Telemedizin und den Datenschutz-Grundlagen praxisbezogene Erkenntnisse von beteiligten Dienstleistern und Kostenträgern zu erlangen.

6.1 Grundlegende Methodik

Als grundsätzliches Vorgehen zur Erstellung des Anforderungskataloges wurde aus dem Bereich der Softwaretechnik das Wasserfallmodell ausgewählt, bei dem die ersten beiden Phasen in dieser Diplomarbeit bearbeitet wurden. [46]

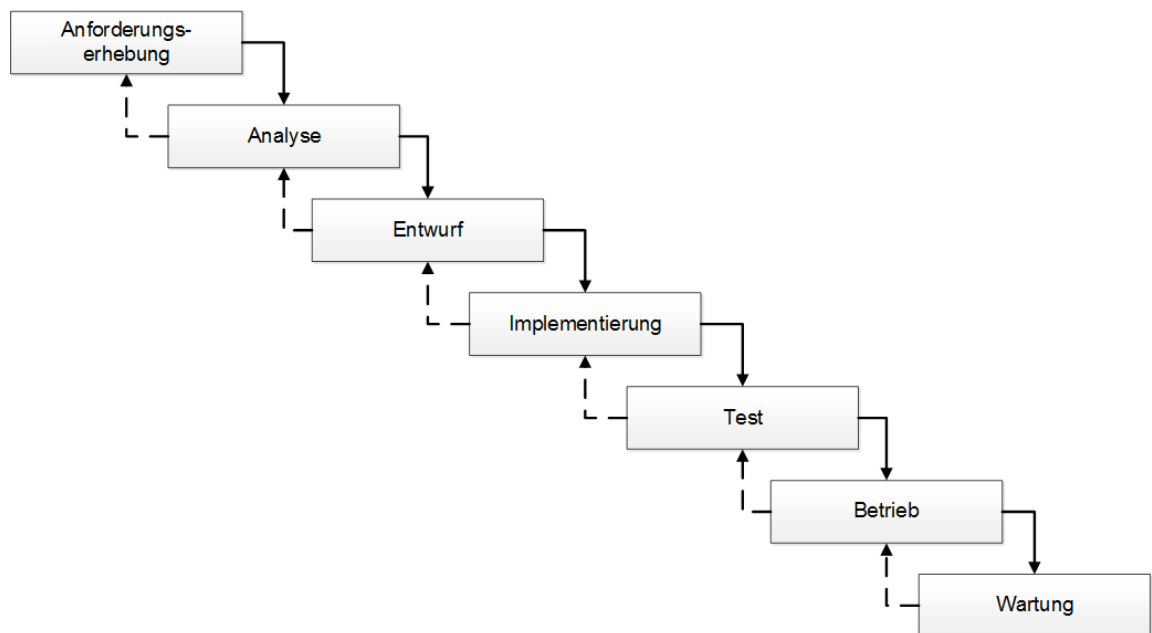


Abbildung 18, Wasserfallmodell [46]

Die Eigenschaft des Wasserfallmodells setzt eine lineare Phasenbearbeitung voraus, bei dem die Prozesse einer neuen Phase erst nach Abschluss der vorherigen Phase durchgeführt werden. Optional sind Rücksprünge zu vorherigen Phasen möglich, da in vielen

Projekten im Laufe der einzelnen Phasenbearbeitungen neue Erkenntnisse und Anforderungen entstehen, die integriert werden müssen. Beispielsweise können nach der abgeschlossenen Anforderungserhebung neue Anforderungen in der Analyse-Phase auftreten, welche in der vorherigen Phase noch nicht erkenntlich waren. Die Phasen werden bis zur Analyse komplett bearbeitet, einen Teil der Phase Entwurf wird in dieser Arbeit mit entwickelt.

Zu den Phasen der Anforderungserhebung und Analyse kommt vorweg noch eine Phase der Einführung, die aufgrund des Umfanges als eigenständige Phase hier aufgeführt wird. Da bisher noch kein vergleichbares System auf dem Markt existiert, muss in die erste Phase der Einführung vergleichsweise viel Zeit investiert werden, um anwendbare Konzepte aus verwandten Gebieten mit in die Planung zur Erstellung des Anforderungskataloges integrieren zu können. Die einzelnen Phasen sind somit [46]:

1. Einführung

Die Einführung umfasst alle vorherigen Kapitel, die grundlegende Voraussetzungen für die Erstellung des Anforderungskataloges darstellen.

Der größte Teil wird dabei mittels Desk-Research als Methode erhoben.

2. Anforderungserhebung

Die Anforderungserhebung hat eine Definition eines Anforderungskataloges als Ziel, welcher vorbereitend für weitere Arbeiten dienen soll.

Zusätzlich zum Desk-Research werden Interviews durchgeführt, die einzelne Bereiche des Anforderungskataloges erweitern sollen.

3. Analyse

Die Analyse der ermittelten Anforderungen wird vor allem anhand eines praktischen Beispiels durchgeführt, um einen ausreichenden Umfang und eventuell weitere Problematiken aufzeigen zu können, die in folgenden Arbeiten als Thema dienen könnten.

4. Entwurf

Aus den vorherigen Phasen und deren Ergebnisse wird ein erster Entwurf konstruiert, der alle Anforderungen an das Telemedizinregister erfüllt. Als Ergebnis steht ein Prototyp des Modells zur Verfügung. Dieser Entwurf ist nicht mehr Teil dieser Arbeit.

5. Implementierung

Der vorherige Entwurf wird in dieser Phase implementiert und liefert somit ein erstes lauffähiges System, welches aber noch weiteren Bearbeitungsschritten unterworfen ist. Dies ist nicht Teil dieser Arbeit.

6. Test

Basierend auf der Implementierung werden in dieser Phase verschiedene Testmodelle entwickelt und durchgeführt, um verschiedene Szenarien der Anwendungsoptionen auf die Vollständigkeit und Robustheit zu überprüfen. Dies ist nicht Teil dieser Arbeit.

7. Betrieb

Nach erfolgreicher Beendigung der Testphasen und der eventuellen Korrektur von Fehlern und weiteren notwendigen Ergänzungen ist das System bereit zum Einsatz. In der Betriebsphase zeigen sich eventuell weitere Anforderungen und notwendige Anpassungen an das System, die in einer Dokumentation erfasst werden. Dies ist nicht Teil der Arbeit.

8. Wartung

Diese Phase ist umfassend mit der Phase des Betriebs zu sehen, da eventuelle Anpassungen, Korrekturen und Erweiterungen in diese Phase fallen. Je nach geplanter Anwendungszeit ist die Phase Wartung abwechselnd mit der Betriebsphase anzuwenden. Dies ist nicht Teil der Arbeit.

6.2 Desk-Research

In den ersten beiden Phasen der Einführung und Anforderungserhebung wird der größte Teil zur Erhebung der Daten mit der Methode Desk-Research durchgeführt. [47] Desk-Research ist definiert mit der Erhebung von Informationen durch Auswertung bestehender Systeme, die auf dem Markt verfügbar sind. Der Unterschied zur normalen Forschung ergibt sich technisch vor allem durch die Untersuchung an bestehenden Quellen, woraus sich auch die alternative Bezeichnung “Sekundärforschung“ ergibt.

Die verwendeten Quellen zur Forschung sind unterschiedlichster Herkunft und sind idealerweise mit wissenschaftlichem Hintergrund verfasst worden. Aber auch die wirtschaftliche Thematik ist bei der Methode von großem Interesse, wobei es dort in der Verwendung von Veröffentlichungen gegebenenfalls zusätzlicher Rechtsklärungen bedarf.

Im Zusammenhang mit dieser Arbeit werden beispielsweise folgende Quellen berücksichtigt:

- Verschiedene Gesetzgebungen
- Internationale Standards für den Austausch medizinischer Daten
- Strukturdiagramme medizinischer Projekte
- Konzeptmodelle zur Anwendung von Datenschutz in der Medizin
- Fachliteratur (Bücher, Magazine)
- Verschiedene Online-Publikationen
- Prozessbeschreibungen
- Informationsbroschüren

Die Einarbeitung in die Thematik der Telemedizin und möglichen vergleichbaren Konzepten aus anderen fachfremden Bereichen bedarf der Kombination der verschiedenen Quellen, um einen anwendungsbezogenen Rahmen für die Diplomarbeit konstruieren zu können.

Aufgrund fachspezifischer Gesetze und rechtlichen Richtlinien ergeben sich für die Phase der Anforderungserhebung und Analyse elementare Anforderungen, die durch praktische Erfahrungen ergänzt werden sollten, deren Erhebung mittels der Interview-Methode geplant ist.

6.3 Interview

Das Interview als ausgewähltes Mittel der Befragungstechnik eignet sich zur Erhebung von spezifischen Anforderungen, die aus bisherigen Erfahrungen der interviewten Personen gewonnen werden. Die Befragung in einem persönlichen Gespräch bietet die zusätzliche Option, auf bestimmte Themengebiete im Laufe des Interviews vertiefend einzugehen.

Die Durchführung eines Interviews kann in unterschiedlichen Variationen stattfinden, wobei für diese Arbeit ein Fragenkatalog als Mittel der Wahl vorbestimmt wurde, um gezielt Erfahrungen und Ansprüche als Ergebnis gewinnen zu können. Zur Vorbereitung der Interviews mussten neben der Bestimmung der Personen vor allem die gewünschten Ergebnisse der Befragung berücksichtigt werden.

Den ausgewählten Dienstleistern und Kostenträgern wird per Mail eine Interviewanfrage gesendet, um eine generelle Bereitschaft für ein Interview zu erfragen und eine anschließende Terminvereinbarung durchführen zu können. Die Interviewanfrage enthält in einem kurzen Absatz die Thematik des geplanten Interviews und eine Erläuterung der Diplomarbeit, um im Vorfeld den Interviewpartner ein besseres Verständnis für eine Gespräch zu ermöglichen.

Aufgrund besonderer Umstände wird auf das Ergebnis der Interviewanfragen im Fazit nochmals genauer eingegangen. Die Fragenkataloge befinden sich im Anhang dieser Arbeit.

6.3.1 Stakeholder

Als Stakeholder werden beteiligte Personen beziehungsweise Gruppen bezeichnet, von denen eine Anwendung beziehungsweise Funktion im Rahmen des Projektes zu erwarten ist. Diese Stakeholder können mit unterschiedlichen Methoden in die Planungs- und Erstellungsphase eines Projekts miteingebunden werden, wobei in dieser Arbeit die Methode des Interviews für diesen Zweck ausgewählt wird.

Zur Durchführung des Interviews werden folgende Stakeholder ausgewählt:

1. Telemedizinische Dienstleister

Zur Analyse von bisherigen Verfahrensweisen bei der Umsetzung von Abrechnungsverfahren werden drei verschiedene Dienstleister aus dem Bereich der Telemedizin ausgewählt. Das Ziel ist vor allem die Erhebung von Kenntnissen, wie bisherige Verfahren in der Abrechnung im Einzelnen durchgeführt werden und welche Problematiken dabei auftreten.

2. Kostenträger

Die andere Gruppe, die beim bisherigen Vorgang des Abrechnungsverfahrens beteiligt ist, stellt die Seite der Kostenträger dar. Dazu sind die drei deutschlandweit größten Krankenkassen für ein Interview ausgewählt, da bei diesen die umfangreichste Erfahrung im Bereich der Telemedizin zu erwarten ist.

3. Datenschutzbeauftragte

Viele der bisherigen Gesetze, die sich auf den Datenschutz beziehen, sind allgemein auf medizinische Sektoren und angeschlossene Forschungsbereiche bezogen. Der Bereich der Telemedizin ist aufgrund vergleichsweise junger Etablierungszeit noch nicht umfassend mit gesetzlichen Richtlinien definiert und kann somit einige Unklarheiten in der Anwendung aufweisen. Dazu wird ein Interview mit dem Datenschutzbeauftragten von Rheinland-Pfalz und Nordrhein-Westfalen beabsichtigt, um eventuelle Aktualisierungen und sich in der Entwicklung befindende gesetzgeberische Verfahren mit in das Konzept einbinden zu können.

Die Interviews für die Stakeholder „Telemedizinischer Dienstleister“ und „Kostenträger“ ähneln sich im strukturellen Aufbau und den beabsichtigten Erkenntnissen.

Die Anzahl der Fragen wird auf maximal 10 Fragen festgesetzt. Die Durchführung soll einen Zeitrahmen von ca. 20 Minuten zur Beantwortung nicht überschreiten. Dadurch besteht optional noch genügend Zeit für eine Ergänzung zusätzlicher Fragen und die Nachfrage zur Vertiefung bestimmter Antworten.

6.3.2 Thematische Struktur

Thematisch ist das **Interview für die Dienstleister und Kostenträger** in drei Abschnitte gegliedert, die wiederum unterteilt einerseits bisherige Erfahrungen in Abrechnungsprozessen abdecken und andererseits die Option für eine Integration gewünschter Änderungen zu den Verfahrensweisen bieten und Erwartungen an das Register erfragen:

1. Verfahrensweise bei bisherigen Nachweisprozessen

Die Fragen in dieser Kategorie haben als Hauptziel die Erfassung, mit welchen Prozess-Schritten bisher ein Prüfungsvorgang zwischen Kostenträger und telemedizinischen Dienstleister vollzogen wird. Dieser Ablauf sollte idealerweise eine Auflistung der verschiedenen Schritte dokumentieren, die bei einer Prüfung nacheinander durchgeführt werden.

2. Datenkategorisierung

Grundsätzlich lassen sich die Daten, die zu einer telemedizinischen Behandlung gehören, in zwei Bereiche einteilen. Einerseits in Daten zur Kosten-Abrechnung und andererseits Daten zur Durchführung, Auswertung und Dokumentation (medizinische Daten). Das Ziel der Befragung zu diesem Thema ist eine detailliertere Erfassung und Einstufung, mit welchen Daten eine Prüfung durchgeführt wird. Dabei sind vor allem die Daten interessant, die unabhängig vom jeweiligen Kostenträger in eine Prüfung miteinbezogen werden.

3. Bisher angewandte Systeme beim Nachweisprozess

Als Ergebnis soll eine Übersicht über technische Systeme bei dieser Kategorie entstehen, die bei den Prüfverfahren eingesetzt werden. Dies können Systeme in allen verschiedenen Bearbeitungsstadien sein, zum Beispiel dem Prozess bei der Datenanfrage, übermittelte Datenauflistungen in Excel, Verschlüsselungsarten bei der Datenübermittlung etc.

Das **Interview mit den Datenschutzbeauftragten** wird mit dem Ziel durchgeführt, gegebenenfalls vergleichbare Ausgangssituationen und Informationen über aktuelle Entwicklungen im gesetzlichen Bereich zur Reglementierung des Umgangs mit medizinischen Daten zu erfahren und in die Anforderungsliste zu integrieren. Eventuell exis-

tieren Ansätze zur weiteren Definition medizinischer Datenverarbeitungsprozesse durch neue Gesetzesvorhaben, welches die Voraussetzung für die Entwicklung des Anforderungskatalogs des Telemedizinregisters beeinflussen würde.

6.4 Rich-Pictures

Ergänzend zur Anforderungsliste des geplanten Telemedizinregisters wird der IST-Zustand und SOLL-Zustand mittels eines Rich-Pictures skizziert, um vorhandene Anwendungsfälle konkreter bestimmen zu können und einen Gesamtüberblick zu erzielen.

Ein Rich-Picture ist definiert mit [48]:

„A Rich Picture is a way to explore, acknowledge and define a situation and express it through diagrams to create a preliminary mental model. A rich picture helps to open discussion and come to a broad, shared understanding of a situation.“

Mit einem Rich-Picture sollen ohne vordefinierte Mittel auf einen Blick ein Zustand eines Systems oder Konzepts dargestellt werden, welches eine Ausgangsposition für weitere Überlegungen und Konkretisierungen sein soll. Mit einfachen Darstellungsmitteln sollen komplexe Zusammenhänge beschrieben werden, bei denen keine detaillierteren Informationen benötigt werden.

7 Anwendungsszenarien für ein Telemedizinregister

Der Bereich Telemedizin, definierbar als medizinische Verfahren mit Datenübermittlung beziehungsweise Datenaustausch zwischen entfernten Beteiligten an einer Behandlung, gilt als noch „junge“ Disziplin im medizinischen Bereich, welche durch eine steigende Vernetzung der Behandler beziehungsweise Einrichtungen und dem stetigen Ausbau von Breitband-Verbindungen große Potentialfelder im Bereich der medizinischen Dienstleistungen bietet. [3] [6]

Deutschlandweit gesehen gibt es viele Projekte der Telemedizin, denen aber oftmals die Etablierung beziehungsweise Anerkennung als eine Regelleistung durch die Kostenträger wie den gesetzlichen Krankenkassen nach Ablauf der Projektphase noch fehlen. Beispielsweise sind ambulante Therapieformen ein geeignetes Mittel, in strukturschwächeren Regionen Patienten eine bessere Verfügbarkeit moderner Therapieverfahren zu bieten und eine Minderung des Fachärzte-Mangels in ländlichen Gebieten herzustellen. [49] Der Prozess zur Anerkennung der telemedizinischen Dienstleistung als Regelleistung durch die Kostenträger ist vergleichsweise langfristig, da neben beweisbaren Studienergebnissen über die Wirksamkeit der Therapieformen (Effektivität) die Kostenträger auch ökonomische Untersuchungen (Effizienz) berücksichtigen müssen. Die Akzeptanz zur Anerkennung einer Leistung ist deutlich höher, wenn neben der Qualität der Therapie auch eine Kosteneffizienz bewiesen werden kann, beispielsweise gegenüber stationär durchgeführten Therapieformen.

Zur Nachweisbarkeit der Effizienz der telemedizinischen Verfahren benötigen die telemedizinischen Dienstleister und Kostenträger ein gesichertes Verfahren, Behandlungsdaten bewerten zu können. Dies soll mit dem Telemedizinregister unterstützt werden, welches eine Datenbasis zu telemedizinischen Behandlungen vorhält und bestimmten Partnern Zugriff auf diese Datensätze erlaubt. Das Register kann als vertrauensbildende Maßnahme bei einem unabhängigen Partner, zum Beispiel dem medizinischen Dienst der Krankenversicherungen (MDK), vorgehalten werden.

Als Beispiel einer seit mehreren Jahren etablierten telemedizinischen Behandlung ist die ambulante Parkinsontherapie der MVB GmbH mit Sitz in Koblenz genannt. Anhand des Beispiels soll auch die Beschreibung der beteiligten Partner beziehungsweise definierbare Rollen der Anwendung des Telemedizinregisters aufgelistet und eine Übersicht der

zu notwendigen Prozessschritten erarbeitet werden. Dazu wird im folgenden Abschnitt neben einer schematischen Darstellung einer Struktur des Telemedizinregisters und den beteiligten Partnern ein IST-Zustand und darauf aufbauend ein SOLL-Zustand beschrieben, der sich aus folgenden Erkenntnissen zusammensetzt:

- eigene Erfahrungswerte des Autors durch die mehrjährige Tätigkeit bei einem telemedizinischen Dienstleister
- die Prozess-Analyse bei der medizinische Videobeobachtung MVB GmbH
- Interview-Anfragen und Ergebnisse an telemedizinische Dienstleister und Kostenträger

Diese beschriebenen IST- und SOLL-Zustände sind abgrenzend zum im Kapitel 9 vorhandenen SOLL-Modell als inhaltliche Situationsdarstellung formuliert und vorbereitend zur Auswahl der Standards zur Übertragung und Verarbeitung medizinischer Daten vorhanden.

7.1 Detaillierte Beschreibung des Telemedizin – Registers

Eine Telemedizinregister-orientierte Darstellung ist in der folgenden Grafik dargestellt:

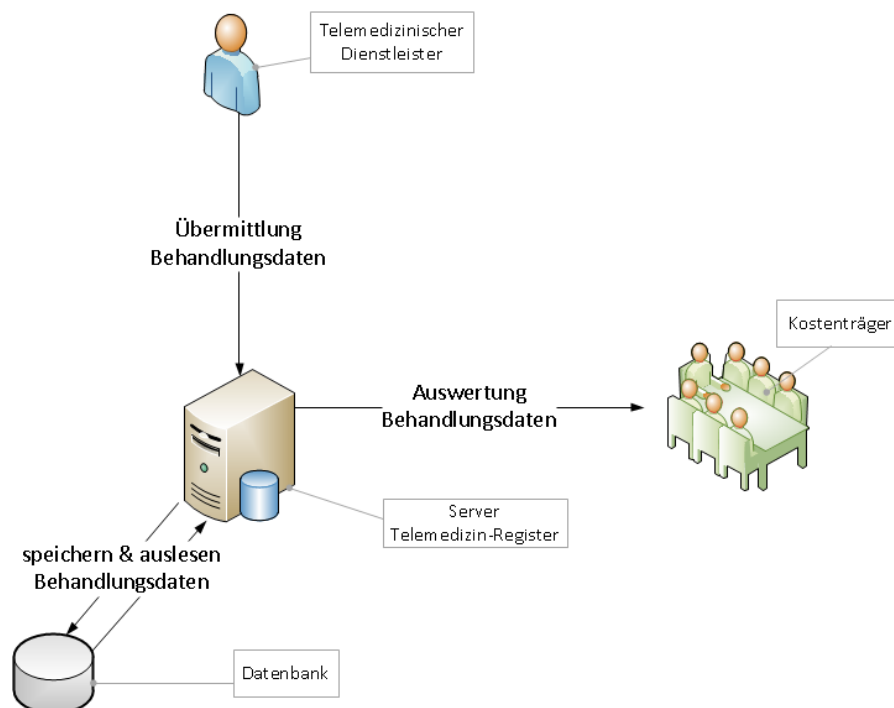


Abbildung 19, Funktionsweise Telemedizinregister

Die wesentlichen Bereiche der Grafik lassen sich in drei Kategorien unterteilen, wobei der Bereich des Registers eine passive Funktion besitzt. Als Schnittstelle zwischen Dienstleister und Kostenträger dient das Telemedizinregister als Speicherstelle von Kopien der für die Abrechnung benötigten Daten und somit als Kontrolle zur Validierung.

Die Stakeholder sind einerseits durch telemedizinische Dienstleister und andererseits durch den Bereich der Kostenträger dargestellt, die alle beteiligten Krankenkassen und sonstige Institutionen, welche für die Abrechnungsvorgänge der Therapien verantwortlich sind, umfassen.

7.1.1 IST-Zustand

Im deutschen Gesundheitswesen werden für die Abrechnungsvorgänge von telemedizinischen Anwendungen im Vergleich zu internationalen Prozessen der Gesundheitsvorsorge wenige Standards eingesetzt. In der Telemedizin werden bei Projektbeginn die notwendigen Parameter zur Datenerfassung festgelegt, die für die erfolgreiche Durchführung des Projektes notwendig sind. Dabei können unterschiedliche Voraussetzungen gegeben sein, welche Institutionen für die Verwaltung der Daten und der dazugehörigen Abrechnung Verantwortung besitzen, beispielsweise wenn mehrere unabhängige Einrichtungen an der Behandlung beteiligt sind.

Aufgrund der vorliegenden Struktur der integrierten Versorgung, die vergleichsweise neu im Gesundheitswesen ist, müssen die einzelnen Prozesse der Datenerfassung, Datenverarbeitung und Abrechnung oftmals individuell entwickelt werden und sind dadurch erschwert auf weiterfolgende Projekte und telemedizinische Anwendungen übertragbar.

Die benötigten Verträge zur integrierten Versorgung (IV-Verträge) werden einzeln mit den beteiligten Partnern ausgehandelt und abgeschlossen. Somit existiert ein wirtschaftlicher Risikofaktor bei dem Ziel zur Etablierung der telemedizinischen Therapien aufgrund der fehlenden Planungssicherheit der Finanzierung, wie es beispielsweise bei Regelleistungen vorgegeben ist. So besteht die Möglichkeit, dass ein beteiligter Kostenträger nach Ablauf eines IV-Vertrages die Verträge nicht verlängert und damit Probleme in der Finanzierung für den Telemedizin-Dienstleister entstehen lässt. Dies kann

besonders bei telemedizinischen Behandlungen auftreten, die ein Projekt-Stadium absolviert haben und eine Etablierung als Dienstleistung im Gesundheitswesen anstreben.

Die Abrechnung und Analyse der Behandlungsdaten erfolgt individuell bei den Kostenträgern, denen seitens der Dienstleister die benötigten Daten auf Anfrage zur Verfügung gestellt werden. Diese Übermittlung kann auf unterschiedliche Weise erfolgen. Dabei besitzen die Kostenträger wenige Möglichkeiten zur Kontrolle der erhaltenen Daten auf Korrektheit und Vollständigkeit.

7.1.2 SOLL-Zustand

Als SOLL-Zustand ist ein standardisierter Katalog zur Einrichtung eines Telemedizinregisters angestrebt, welcher die einzelnen Prozesse und Abläufe mit der Unterstützung standardisierter Maßnahmen beschreibt. Diese Standards sind teilweise im internationalen Gesundheitswesen im Einsatz und auf nationale Gegebenheiten angepasst worden.

Vor der Einrichtung des Telemedizinregisters sollten bei dem telemedizinischen Dienstleister Vorkehrungen getroffen werden, die den Transfer und Austausch der Daten in das Telemedizinregister vereinfachen. Dabei müssen besonders datenschutzrechtliche Grundlagen berücksichtigt werden, zu denen aber erwartungsgemäß bei einem telemedizinischen Projekt bereits individuelle Konzepte entwickelt und umgesetzt worden sind. [50]

Die Datenmenge und Datentypen sollten in Absprache mit den beteiligten Partnern wie beispielsweise den Kostenträgern im Vorfeld der Therapie abgesprochen werden, da besonders bei der Analyse der Therapie-Daten je nach Kostenträger unterschiedliche Bewertungskriterien im Einsatz sind, wie dies im durchgeführten Interview mit der Techniker Krankenkasse deutlich wurde. Der Aufbau des Registers soll nachträgliche Änderungen und Erweiterungen möglich machen, da optional zusätzliche Datentypen (Videoaufnahmen, Audiodateien, etc.) im Verlauf der Therapie erfasst und im Telemedizinregister gespeichert werden soll.

Durch die Integration standardisierter Anwendungen bei der Umsetzung des Telemedizinregisters soll eine verbesserte Ausgangsbasis für die Verhandlungen der IV-Verträge zwischen Dienstleister und Kostenträger hergestellt und damit telemedizinischen Dienstleistern bessere Planungssicherheit gewährleistet werden.

Im europäischen Gesundheitsraum sind in den letzten Jahren viele Projekte im Bereich des eHealth-Sektors entwickelt und durch die EU gefördert worden, bei denen standardisierte Verfahren angewendet werden. Das langfristige Ziel ist die Minderung von regionalen Besonderheiten beziehungsweise Limitierungen in der Verfügbarkeit der Anwendungen zur Gesundheitsversorgung und verbesserte Austauschmöglichkeiten in länderübergreifenden Behandlungen [51]. Die bisherige standortgebundene Versorgung von Patienten soll deutlich flexibler und vielfältiger werden. So könnte zum Beispiel ein in Deutschland lebender Patient auf Versorgungsmöglichkeiten in Frankreich Zugriff erlangen und dem Patienten somit eine deutlich erweiterte Auswahlmöglichkeit in der Umsetzung der individuellen Gesundheitsversorgung bieten.

Dazu werden standardisierte Verfahren benötigt, die einen Austausch von Daten mit Therapiebezug über die Ländergrenzen hinweg ermöglichen. Als ein konkretes Projekt ist epSOS aufgeführt:

Das europäische Projekt **epSOS** (**e**uropean **p**atients **S**mart **O**pen **S**ervices) [51] steht für eine Sammlung von standardisierten Diensten zum Austausch von Patientendaten. Der Fokus ist dabei auf die Entwicklung einer Patientenakte (Patient Summary) und eines elektronischen Rezepts (ePrescription) beziehungsweise einer Medikationsverschreibung (eMedication) gelegt. Für diese Modelle werden standardisierte Prozesse entwickelt, die einen Datenaustausch über Ländergrenzen hinweg innerhalb der EU definieren und unterstützen sollen. [51] [52]

epSOS wurde im Jahr 2007 durch die europäische Kommission gegründet und wird mittlerweile durch 27 Organisationen aus 12 EU-Ländern weiterentwickelt [51]. Basierend auf internationalen Standards wird eine Lösung für die Übermittlung der medizinischen Daten angestrebt, um Patienten und Behandlern eine vereinfachte Anwendung bei der Anlage einer Dokumentation zur Therapie zu ermöglichen. So werden zum Beispiel sprachliche Barrieren umgangen, indem die standardisierte Patientenakte unabhängig vom Datenerfasser in der jeweils gewünschten Sprache zur Verfügung steht. [52]

7.2 Module für Anwendungsszenarien

In den folgenden Anwendungsszenarien werden durch eine modulare Auflistung verschiedene Grundstrukturen von telemedizinischen Behandlungen beschrieben. Dies bedeutet, dass keine Darstellung komplett funktionaler und eigenständiger Anwendungsszenarien erfolgt, sondern eine Teilung in die einzelnen Funktionsbereiche vorgenommen wird. Aus den einzelnen Teilmodulen zusammengesetzt lassen sich unterschiedliche funktionale Anwendungsszenario abbilden.

Die Teilung erfolgt in die Module:

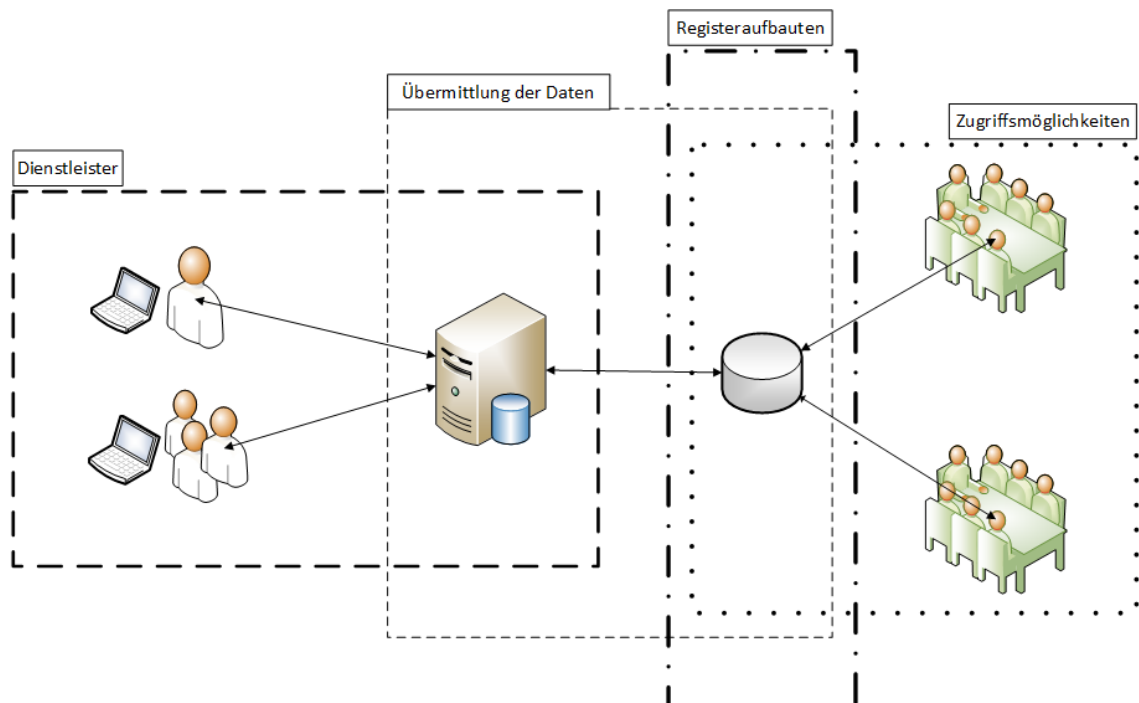


Abbildung 20, Gliederung Anwendungsszenario

a) Dienstleister

Die Differenzierung der beteiligten Dienstleister erfolgt in die Anzahl der unabhängigen Positionen, die Daten in das Register übertragen. Die Menge beträgt mindestens eine datenübertragende Position. Zu erwarten ist bei einigen telemedizinischen Projekten eine größere Anzahl von datenerfassenden Stellen, die unabhängig voneinander die erfassten Daten in einen definierten Bereich speichern, beispielsweise einer Datenbank. Auf das Register bezogen ist der Unter-

schied vor allem in der Anbindung an das Register zu betrachten: entweder werden die Daten durch eine zentrale Einrichtung an das Register übermittelt oder durch mehrere, voneinander unabhängige Positionen.

b) Übermittlung der Daten

Die Differenzierung erfolgt nach der Art der verwendeten Übertragungsprozesse und den damit verbundenen standardisierten Funktionsbeschreibungen. Die Übertragungen sind entweder singulär, periodisch oder permanent (siehe Kapitel 5.2, Verfahren der Datenübermittlung). Eine sichere Verbindung ist die wichtigste Voraussetzung bei der Übermittlung und muss gegenüber unerlaubten Zugriffen geschützt sein.

c) Registeraufbauten

Die Differenzierung wird mit verschiedenen Registeraufbauten und Unterteilungen anhand der zu erfassenden Datenkategorisierungen vorgenommen. Die Mindestmenge beträgt ein Register-Abschnitt. Je nach Komplexität der zu verwaltenden telemedizinischen Daten sind auch mehrere Register-Abschnitte möglich. Allgemein gilt, dass pro telemedizinischen Dienstleister genau ein Telemedizinregister geführt wird.

d) Zugriffsmöglichkeiten auf das Register

Die Differenzierung ist die Anzahl der beteiligten Positionen, welche einen Zugriff auf das Register und damit eventuell erweiterten Analyse-Funktionen erhalten. Die Mindestmenge beträgt eins.

Die vier folgenden Anwendungsszenarien sind aus den aufgeführten Modulen konstruiert und bilden typische Strukturen telemedizinischer Behandlungen ab:

Aufbau Szenario A:

- Ein Dienstleister
- Singuläre Übertragung
- Ein Registerabschnitt
- Eine Zugriffsmöglichkeit

Dieses Szenario bildet die vergleichsweise einfachste Struktur ab, die bei der Anwendung des Telemedizinregisters auftreten kann. Die Anzahl der möglichen Optionen in den einzelnen Bereichen ist auf das Minimum reduziert und ermöglicht somit eine klar abgrenzbare Rechteverwaltung im Telemedizinregister. Die singuläre Übertragung ist vergleichbar mit der Struktur eines einfachen Melderegisters, bei dem nur einmalig eine Datenübertragung ins Register durch eine zentrale datenerfassende Stelle erfolgt.

Aufbau Szenario B:

- Mehrere Dienstleister
- Singuläre Übertragung
- Ein Registerabschnitt
- Mehrere Zugriffsmöglichkeiten

In diesem Szenario ist die Komplexität der Verwaltung des Registers durch mehrere Dienstleister und mehrere Zugriffsmöglichkeiten gegenüber dem Szenario A erweitert. Diese Struktur bildet die Zusammenarbeit von mehreren Dienstleistern ab, die an einer Therapie beteiligt sind. Ein Beispiel dafür wäre eine initiale Untersuchung beim jeweiligen Hausarzt, die im Vorfeld zur Eignungsüberprüfung eines Patienten für eine Therapie stattfindet und die Expertise von mehreren Spezialisten berücksichtigt.

Aufbau Szenario C:

- Ein Dienstleister
- Permanente Übertragung
- Ein Registerabschnitt
- Mehrere Zugriffsmöglichkeiten

Bei dieser Ausgangssituation wird vor allem die permanente Datenübertragung seitens des Dienstleisters an das Telemedizinregister in den Mittelpunkt gestellt, was bei vielen telemedizinischen Behandlungen eine vergleichbare Ausgangssituation darstellt. So wäre die regelmäßige Überprüfung und Erfassung kardiologischer Werte beim Patienten zu Hause ein reales Beispiel für dieses Szenario, bei dem über einen zentralen Sammelpunkt beim verantwortlichen Dienstleister die vorhandenen Behandlungsdaten kontinuierlich an das Telemedizinregister übermittelt

werden. Neben den beteiligten Kostenträgern besitzen zusätzlich kardiologische Forschungsnetzwerke eingeschränkte Zugriffsmöglichkeiten zur Datenanalyse auf die im Register hinterlegten Daten.

Aufbau Szenario D:

- Mehrere Dienstleister
- Verschiedene Übertragungstechniken
- Mehrere Registerabschnitte
- Mehrere Zugriffsmöglichkeiten

Im komplexesten Szenario D sind die Optionsmöglichkeiten der beteiligten Partner maximal gewertet, indem verschiedene Dienstleister auch verschiedene Arten von Daten zu unterschiedlichen Zeitpunkten an das Register übermitteln. Aufgrund der angenommenen größeren Datenmenge sind auch im Register mehrere Unterteilungen vorgesehen, auf die verschiedenste Zugriffsmöglichkeiten existieren können. Dieses Szenario dient somit der Beschreibung aller anwendbaren Techniken beziehungsweise Methoden, um das Telemedizinregister aufzubauen und weiterverwenden zu können.

Der größte Unterschied in den Szenarien entsteht durch die Komplexität der Rechteverwaltung, mit der die Zugriffe auf das Telemedizinregister definiert werden. Je mehr beteiligte Positionen an der Datenspeicherung und der weiteren Verarbeitung beteiligt sind, desto umfangreicher ist die Anzahl der benötigten Rollen und damit verbundenen Konten im Register. Die Aufbereitung der Daten hingegen unterscheidet sich vor allem in der Art der verwendeten Datentypen und der Übertragungstechnik.

Für die Entwicklung der Prozesse in den folgenden Kapiteln wurde das **Szenario C** ausgewählt, da dieses allgemein betrachtet viele telemedizinische Behandlungen beschreibt. Des Weiteren ist das für die Überprüfung der Prozesse ausgesuchte praktische Beispiel ebenfalls vom Typ Szenario C. Die dort entwickelten Modelle lassen sich weitestgehend auf die Szenarien A, B und D übertragen, da die verwendeten Standards eine Skalierung beteiligter Positionen berücksichtigen.

7.3 IHE – Standards

Die Maßnahmen und Prozesse, die beispielsweise für das zuvor beschriebene epSOS – Projekt eingesetzt werden, basieren grundlegend auf IHE – Standards (Integrating the Healthcare Enterprise) [53]. Diese werden seit 1997 in Zusammenarbeit von medizinischen Produkteherstellern, Kliniken und weiteren Behandlern definiert und haben als Ziel die verbesserte Austauschmöglichkeit von medizinischen Daten im internationalen Gesundheitssektor. [52]

Mittels dieser Standards, die teilweise auch auf nationale Gegebenheiten angepasst sind, soll der Datenaustausch bei den Prozessen des Telemedizinregisters unterstützend beschrieben und modelliert werden. Die Vorteile bei der Anwendung der IHE-Standards sind

- Möglichkeiten zur besseren Weiterentwicklung und Anpassung des Registers für zukünftige Aufgaben und Funktionen
- Berücksichtigung nationaler Besonderheiten bei der Auswahl der angepassten Standards
- Erwartung einer höheren Akzeptanz des Register-Modells
- Miteinbeziehung von Erfahrungswerten durch revidierte Standards

Die IHE-Initiative fördert die aktive Zusammenarbeit von Verantwortlichen im Gesundheitswesen mit beteiligten Herstellern, um Verbesserungen im technischen Bereich des Gesundheitswesens erzielen zu können [53]. Dazu werden bekannte Standards wie DICOM und HL7 als Ausgangsbasis zur Entwicklung spezifischer Standards benutzt, deren Hauptziel die verbesserte Behandlung von Patienten darstellt. Vorliegende Standards werden also in Koordination von Behandlern und Geräteherstellern so angepasst, dass eine vereinfachte Kommunikation möglich ist. [53]

In der folgenden Grafik ist die Vorgehensweise zur Definition eines IHE-Standards schematisch dargestellt:

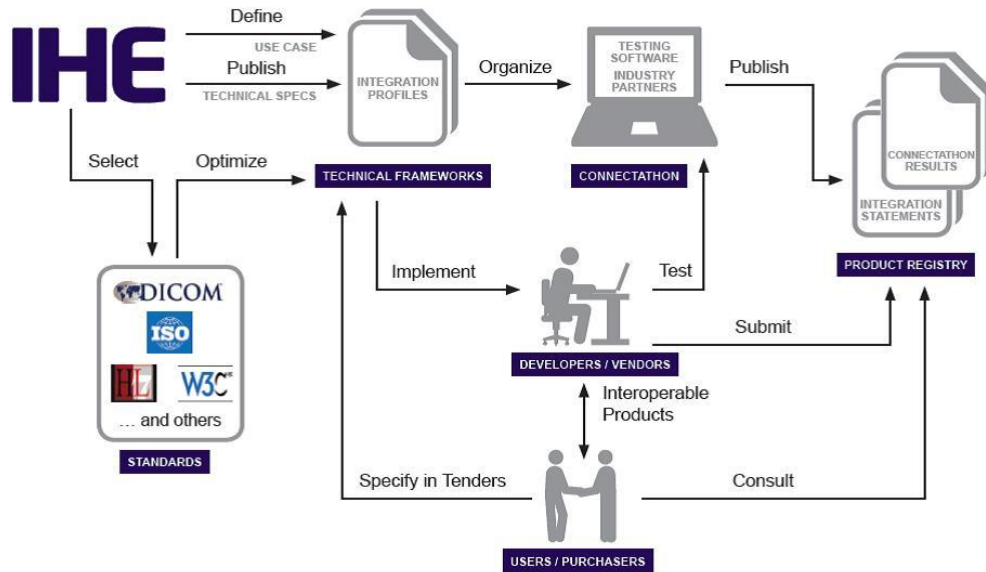


Abbildung 21, Funktionsweise IHE [53]

Ablauf [53]:

Die IHE sucht aus vorhandenen Standards, die nicht zwingend aus dem medizinischen Bereich sein müssen, verwendbare Profile aus und passt diese auf zusätzliche Anforderungen an. Diese Umsetzungen werden in einem Technical Framework gebündelt und stehen somit Entwicklern und Anwendern zur Verfügung. Diese wiederum kooperieren bei den technischen Umsetzungen des Frameworks und veröffentlichen diese Ergebnisse. Zusammen mit durch die IHE definierten Anforderungen und Spezifikationen entstehen Standardisierungs-Profile, in die neben den grundlegenden Voraussetzungen auch anwendungsspezifische Informationen (Erfahrungswerte, Herstellerspezifische Anforderungen, etc.) miteinfließen.

Die IHE hat den Prozess in folgende vier Schritte aufgeteilt [53]:

1. Medizinische und technische Experten definieren in Zusammenarbeit Anwendungsfälle, die einen Austausch von medizinischen Daten beschreiben.
2. Mittels vorhandener Standards werden durch technische Experten spezifische Anforderungen erhoben, die beim Austausch von Daten mit den verwendeten Systemen und Geräten berücksichtigt werden müssen.
3. Diese Anforderungen, "IHE Profile", werden von Herstellern und Entwicklern in den Geräten und Systemen umgesetzt. Die Bezeichnung **HIT System**

(“Healthcare Information Technology“) steht dabei für die eingesetzten Geräte und Systeme.

4. In jährlich stattfindenden Testdurchgängen (“Connectathons“) werden die Profile auf ihre Praxistauglichkeit untersucht.

Diese Vorgehensweise erzeugt somit Standardisierungsprofile, die für reale Umsetzungen im medizinischen Sektor, vor allem der Telemedizin, sehr gut geeignet sind aufgrund der Interoperabilität und heterogenen Entwicklungsweise. Des Weiteren werden Aktualisierungen in den Anforderungen und Neuentwicklungen in den Standards durch die jährlichen Connectathons in die Profile miteingearbeitet und bieten einen zuverlässigen Stand der Veröffentlichungen.

Die von der IHE veröffentlichten Technical Frameworks sind in mindestens zwei Abschnitte unterteilt, den Integration Profiles und den Transactions. Je nach Framework kann die Unterteilung noch zusätzliche Abschnitte umfassen. [52] [53] In den Integration Profiles sind die technischen Anforderungen definiert und in dem Abschnitt Transactions werden detailliert die Prozesse beim Austauschvorgang zwischen beteiligten Partnern beschrieben.

Eine thematische Trennung der Profile erfolgt bei der IHE durch eine Einteilung in verschiedene Domains [53]:

- Anatomic Pathology
- Cardiology
- Dental
- Endoscopy
- Eye Care
- IT Infrastructure
- Laboratory
- Patient Care Coordination
- Patient Care Devices
- Pharmacy
- Quality, Research and Public Health
- Radiation Oncology
- Radiology

Für jeden dieser Bereiche werden Technical Frameworks veröffentlicht und regelmäßig überarbeitet. Von besonderem Interesse für die Modellierung des Telemedizinregisters ist die Domain "IT Infrastructure", da in dieser sektorenübergreifend Prozesse zum Datenaustausch zwischen Behandlern standardisiert zusammengefasst sind. Die Domain selbst ist wiederum in mehrere Bereiche unterteilt, beispielsweise die Domain Patient Care Coordination [52]:

- ATNA: Audit Trail and Node Authentication
- BPPC: Basic Patient Privacy Consents
- CT: Consistent Time
- XDM: Cross-Enterprise Document Media Interchange
- XDR: Cross-Enterprise Document Reliable Interchange
- XDS.b: Cross-Enterprise Document Sharing
- PAM: Patient Administration Management
- PDQ: Patient Demographic Query
- PIX: Patient Identifier Cross-Referencing

Als grundlegende Standards bei der Beschreibung des Telemedizinregisters werden die Profile **XDS.b**, **ATNA**, **PIX** und **XDM** eingesetzt, welche teilweise auf die nationalen Gegebenheiten (BDSG, Berufsverordnungen, etc.) angepasst wurden.

Im folgenden Abschnitt wird das Profil XDS.b genauer beschrieben, da der elementare Aufbau des Telemedizinregisters unter Zuhilfenahme der XDS.b-Standards erfolgt. Die weiteren eingesetzten Profile (ATNA, PIX, XDM) werden bei der erstmaligen Verwendung erläutert.

Die einzelnen Umsetzungen der Spezifikation erfolgt mit verschiedenen Standards und technischen Schnittstellen zur Konnektivität und Übertragung von Informationen, unter anderem mit Web Services, SOAP, MTOM / XOP und ebXML. Teilweise gibt es bei den Standards die Möglichkeit, zur besseren Kompatibilität unterschiedliche Versionen einzusetzen, welches die Einbindung von älteren Systemen erleichtert. Beispielsweise existieren bei der Transaktion "Patient Identity Feed" zwei Versionen zur Verwendung: einerseits die Version mit Berücksichtigung des HL7 v2-Standards mit der Bezeichnung ITI-8 und andererseits die auf dem HL7 v3 basierenden Standard bezeichnete Transaktionskennung ITI-44. Die HL7 v2 Standards benutzen TCP-Sockets zur Verbindung, bei HL7 v3 erfolgt dies über HTTP(s)-Ports [54].

7.4 Profil XDS.b - Cross-Enterprise Document Sharing

Im Katalog XDS werden die Registrierung, Verteilung und Verarbeitung von elektronischen Patienten-Dokumenten beschrieben, die bei einer Interaktion zwischen beteiligten Versorgern auftreten können. Das Ziel ist die standardisierte Beschreibung von Prozessen des Datenaustauschs, die bei Bedarf auf nationale Gegebenheiten angepasst werden können. Wie im Titel beschrieben ist das primäre Objekt bei den Prozessen ein Dokument mit Patienteninformationen, das in unterschiedlichen Datentypen (Textdokument, Bild, etc.) vorliegen kann. [55]

Elementar bei dem XDS Profil ist die Trennung der Dokumenten-Verarbeitung in vier Sektionen, auch als Akteure bezeichnet [54]:

1. Document Repository

Hier werden die Dokumente gespeichert, die im Rahmen des Aufbaus einer elektronischen Patientenakte erfasst werden (physischer Speicherort).

2. Document Registry

In der Registrierung werden die Dokumente verwaltet, die im Document Repository gespeichert sind (virtueller Speicherort). Diese Registrierung ist somit das zentrale Element in der Struktur, über welches Dokumente registriert und gesucht werden können. Anstatt der kompletten Dokumente werden einzig die zugehörigen Metadaten in der Registry gespeichert und verwaltet.

3. Document Sources

Bezeichnung für die datenspeichernden Stellen, von denen mehrere in einer Struktur vorhanden sein können. Von der Document Source werden Dokumente in das Document Repository gespeichert, welche dann im Document Registry angemeldet werden.

4. Document Consumers

Bezeichnung für Positionen, die gespeicherte Dokumente verarbeiten. In einer Struktur können mehrere Konsumenten vorhanden sein, die auf Daten zugreifen können. Dabei wird vom Document Consumer eine Anfrage an die Document

Registry gestellt (Metadaten-Suche), die dann im weiteren Verlauf die angeforderten Dokumente mit Einbindung des Document Repository zurückliefern.

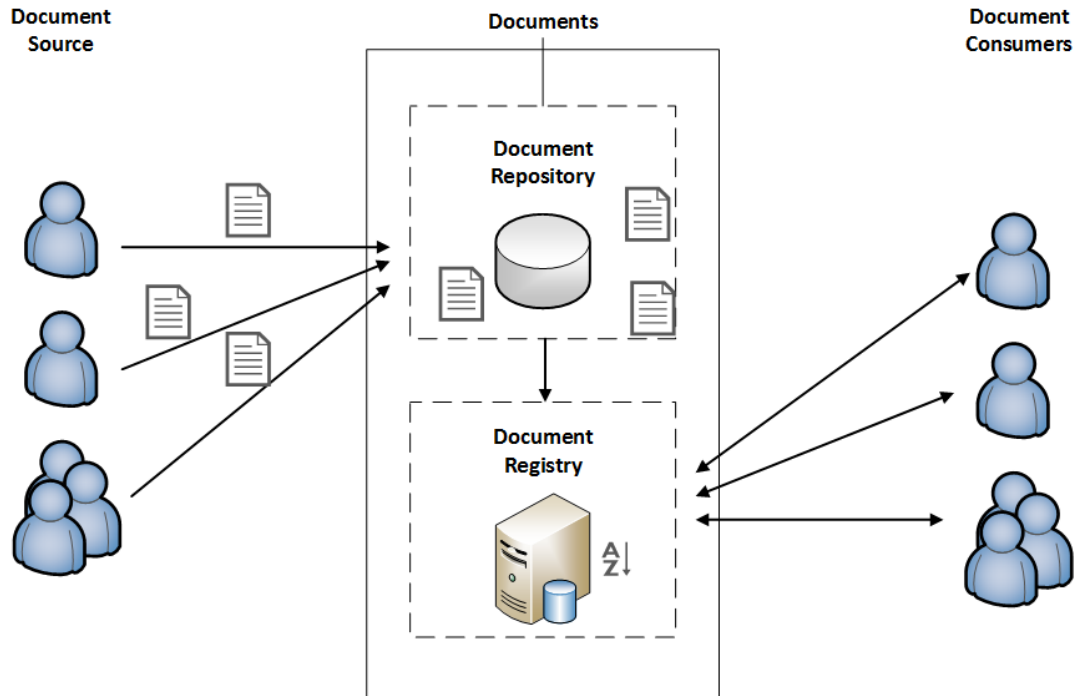


Abbildung 22, Funktionsweise XDS [54]

Diese Struktur, bei der Daten und Metadaten der Dokumente getrennt gespeichert werden, bietet mehrere Vorteile gegenüber einer einfacheren, komplett zentralen Speicherung:

- Optionale Filterung von Dokumenten durch die separate Verwaltung in der Document Registry
- Vereinfachter dezentraler Aufbau von Netzwerken möglich (Standort von Document Repository und Document Registry können über große Entfernung voneinander getrennt sein)
- Verbesserte Skalierbarkeit bei zusätzlichen Partnern (Source, Consumer)
- Optionale Möglichkeit, die Rechteverwaltung exakter zu definieren

Derzeit aktuell ist das Profil XDS.b, welches im Jahr 2009 das erste XDS Profil (XDS.a) ablöste [54]. Eine Übersicht der beteiligten Akteure und Transaktionen ist in der folgenden Grafik dargestellt:

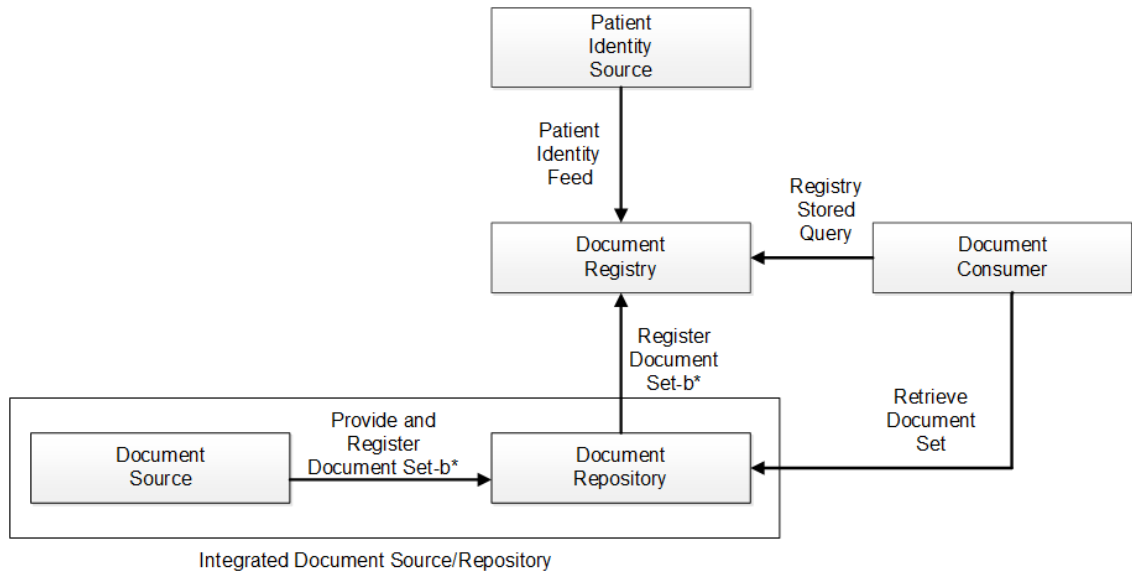


Abbildung 23, IHE-D XDS.b Actors and Transactions [54]

Ausgehend von der Abbildung 19 (Funktionsweise XDS) ist in der Grafik die Verwaltung der Dokumente mit einem zusätzlichen Akteur beschrieben, der Patient Identity Source.

Die bisherige Darstellung betrachtet ausschließlich die Dokumenten-Speicherung und Verwaltung, die aber bei realer Anwendung noch weitere Anbindungen benötigt: Die Trennung von identifizierenden Daten (IDAT) und medizinischen Daten (MDAT) bedingt bei der Verwaltung der Dokumente (MDAT) in der Document Registry eine Integration von patientenbezogenen Daten, der sogenannten Patient Identity Source (PID). Mittels dieser ist in der Umgebung ein eindeutiger Identifikator vorhanden, der die Verwaltung der Daten vereinfacht. [55]

7.4.1 Akteure bei der Verwendung des XDS.b-Profiles

Bei der Umsetzung des XDS.b-Profiles gibt es einige vordefinierte Akteure, zwischen denen die Transaktionen erfolgen. Erweiternd zu den bereits zuvor erwähnten elementaren Sektionen / Akteuren beim Dokumentenaustausch sind folgende Akteure für die Erstellung des Telemedizinregisters verfügbar [54]:

- **Patient Identity Source**
Akteur mit Patienteninformation, zum Beispiel behandelnde Einrichtung
- **Patient Identifier Cross-Reference Manager (PIX Manager)**
Akteur, der zentral in einer Affinity Domain verschiedene Patienten-ID verwaltet und Auskunft gibt
- **Patient Identifier Cross-Reference Consumer**
Akteur, der beim PIX Manager Anfragen zu hinterlegten Patienten-Informationen erfragt
- **Document Registry**
Zentraler Akteur in einer Affinity Domain, bei dem Dokumente registriert und abgefragt werden können (vgl. mit einer zentralen Datenbank)
- **Document Repository**
Akteur, der in einer Affinity Domain Dokumente entgegennimmt, speichert und die Metadaten zur Registrierung an die Document Registry weiterleitet
- **Document Consumer**
Akteur, der Anfragen nach hinterlegten Dokumenten an die Document Registry stellt und Dokumente verarbeitet, zum Beispiel ein Behandler als Konsil
- **Document Source**
Akteur, der Dokumente in die Affinity Domain einbringt und oftmals auch mit einer Patient Identity Source verbunden ist, zum Beispiel eine behandelnde Einrichtung
- **Image Document Consumer**
Akteur, der Anfragen nach hinterlegten Bilddaten an die Document Registry stellt und Dokumente verarbeitet, zum Beispiel ein Behandler als Konsil
- **Image Document Source**
Akteur, der Information zu Bilddaten in die Affinity Domain einbringt und Bilddaten aufgrund großer Datenmengen zum Abruf bereithält

- **Patient Demographics Consumer**
Akteur, der mit demographischen Werten Anfragen an den Patient Demographics Supplier zur Suche nach Patienteninformationen stellt
- **Patient Demographics Supplier**
Akteur, der demographische Werte zu Patienten speichert und Anfragen dazu entgegen nimmt, oftmals mit dem PIX Manager verbunden
- **Provider Information Directory**
Akteur, der zentral Informationen zu den verschiedenen Akteuren beziehungsweise Behandler und Einrichtungen der Affinity Domain speichert und verwaltet
- **Provider Information Source**
Akteur, der an den Akteur Provider Information Directory Informationen zu seiner Identität als Behandler / Einrichtung übermittelt
- **Provider Information Consumer**
Akteur, der beim Provider Information Directory Information zu den hinterlegten Provider-Daten (Behandler, Einrichtungen) anfragt
- **Time Client**
Akteur, der beim Time Server Information zur aktuellen Zeit anfragt
- **Time Server**
Akteur, der zentral in einer Affinity Domain die Zeit-Informationen verwaltet
- **Audit Repository**
Akteur, der zentral in einer Affinity Domain Informationen zur Protokollierung von Aktionen der beteiligten Akteure speichert und verwaltet

Mittels dieser Akteure werden im Kapitel 9 detailliert Prozesse formuliert, indem die am Telemedizinregister beteiligten Partner die Funktionalitäten der aufgelisteten Akteure zugewiesen bekommen. Dabei kann beispielsweise ein Dienstleister gleichzeitig mehrere Rollen einnehmen, wenn durch ihn Dokumente und Patienteninformationen sowohl in das Register gespeichert als auch gelesen werden (Source und Consumer).

7.4.2 Transaktionen bei der Verwendung des XDS.b-Profiles

Im folgenden Abschnitt werden die einzelnen Transaktionen des XDS.b Profils aufgelistet, welche im Telemedizinregister Verwendung finden. Als erstes erfolgt die Bezeichnung der Transaktion und die dazugehörige Transaktionskennung (Standardisierungs-Nummer). Sollten verschiedene Versionen (basierend auf unterschiedlichen HL7-Standards) existieren, werden mehrere Transaktionskennungen aufgeführt. Im zugehörigen Absatz werden die Funktionen der Transaktionen aufgelistet und detailliert beschrieben [54]:

- **Patient Identity Feed, ITI – 44, ITI – 8**

Transaktion zur Übermittlung von Patientendaten an verschiedene Akteure.

Beteiligte Akteure: Patient Identity Source, Document Registry

Die Übermittlung der persönlichen Patientendaten an die in der Domain verwendete Document Registry erfolgt durch diese Transaktion. Verantwortlich für die Transaktion ist der Akteur Patient Identity Source. [54]

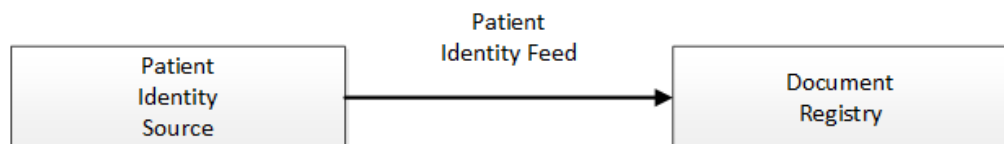


Abbildung 24, Transaktion Patient Identity Feed [54]

- **Provide and Register Document Set-b, ITI – 41**

Transaktion zur Speicherung und Registrierung der Dokumente.

Beteiligte Akteure: Document Source, Document Repository

Durch eine Document Source wird ein Dokument zusammen mit Metadaten an das Document Repository zum Speichervorgang übermittelt. [54]

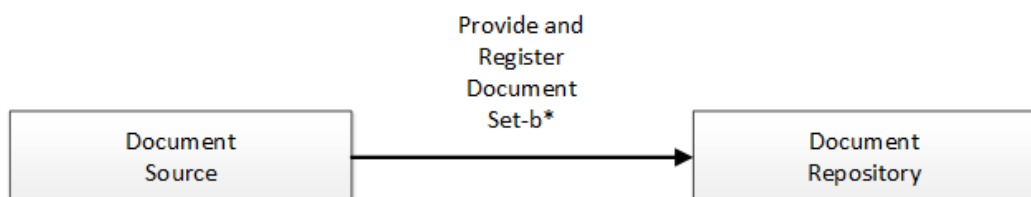


Abbildung 25, Transaktion Provide and Register Document Set-b [54]

- **Register Document Set-b**, ITI – 42

Transaktion zur Registrierung von Dokumenten.

Beteiligte Akteure: Document Repository, Document Registry

Als fortführender Prozess der Transaktion Provide and Register Document Set-b erfolgt die Registrierung (Metadaten-Übermittlung) in der Document Registry durch die Document Repository. [54]

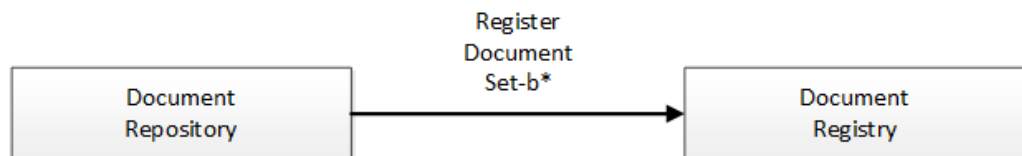


Abbildung 26, Transaktion Register Document Set-b [54]

- **Registry Stored Query**, ITI – 18

Transaktion zur Suche nach registrierten Dokumenten.

Beteiligte Akteure: Document Consumer, Document Registry

Eine Suche nach Dokumenten erfolgt durch einen Document Consumer, der mit dieser Transaktion die Suche an die Document Registry richtet, von der genau eine in der Struktur ("Affinity Domain") vorhanden ist. Anstatt verschiedene Repositories auf der Suche nach Dokumenten anzufragen, wird die Anfrage durch die Registry zentral verarbeitet. [54]

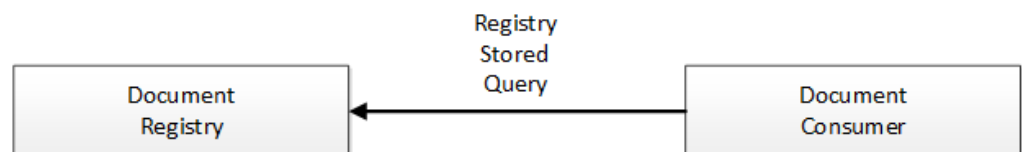


Abbildung 27, Transaktion Registry Stored Query [54]

- **Retrieve Document Set**, ITI – 43

Transaktion zum Erhalt von angefragten Dokumenten

Beteiligte Akteure: Document Registry, Document Consumer

Nach der erfolgreichen Bearbeitung der Transaktion Registry Stored Query erfolgt mit dieser Transaktion der Transfer der ermittelten Dokumente. Aufgrund

der Option von mehreren übermittelten Dokumenten wird die Transaktion mit “Document Set“ beschrieben. [54]

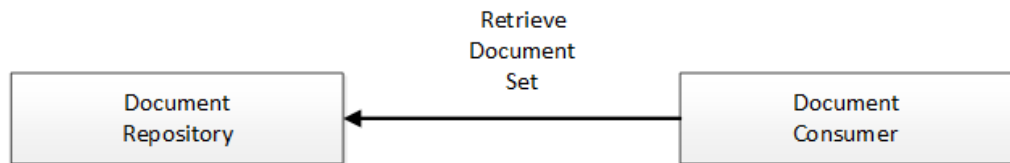


Abbildung 28, Transaktion Retrieve Document Set [54]

- **Provide and Register Imaging Document Set**, MTOM/XOP RAD – 68

Transaktion zur Registrierung speicherintensiven Bilddaten (XDS-I).

Beteiligte Akteure: Image Document Source, Document Repository, Document Registry

Dateien mit einem großen Bedarf an Speicherplatz werden im Gegensatz zu normalen Dokumenten nicht als Kopie an das Document Repository gesendet, sondern verbleiben bei der Image Document Source. Einzig Metadaten werden an das Document Repository übermittelt. Die in diesem Fall spezielle Aufbereitung der Metadaten wird Key Object Selection (KOS) genannt. Dieses Objekt wird im Document Repository gespeichert und die dazugehörigen Metadaten an die Document Registry übermittelt. [54]

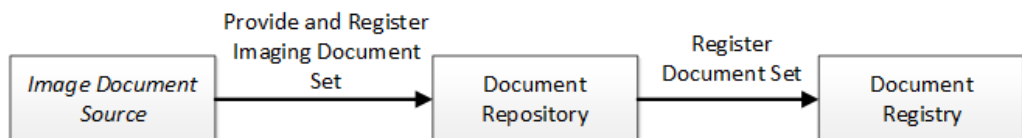


Abbildung 29, Transaktion Provide and Register Imaging Document Set [54]

- **WADO Retrieve**, RAD – 55

Transaktion zum Erhalt von Bilddaten über http (XDS-I).

Beteiligte Akteure: Image Document Consumer, Image Document Source

Die Transaktion WADO (“Web Access to DICOM Persistent Objects“) Retrieve ist eine von mehreren Möglichkeiten, die Bilddaten direkt von der Image Document Source zu laden. Bei dieser Möglichkeit wird der DICOM Standards WADO als Variante zum Download verwendet. Der Image Document Consumer erhält auf eine Anfrage die Verweise auf KOS-Objekte in den entsprechenden Document Repository. Diese verweisen wiederum auf die Speicherorte der

hinterlegten Bilddaten. Von dort erfolgt der Download der gewünschten Bilddaten. [54]

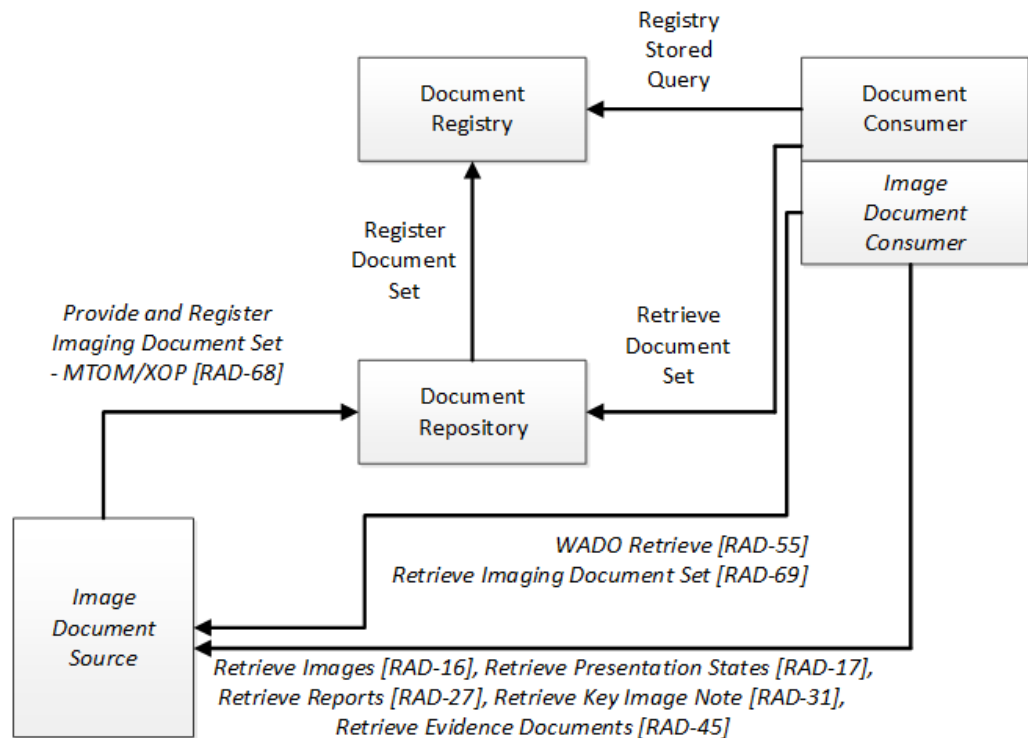


Abbildung 30, Transaktionen Image Document [54]

- **Retrieve Imaging Document Set, RAD – 69**

Transaktion zum Erhalt von Bilddaten durch eine modifizierte Transaktion Retrieve Document Set (XDS-I).

Beteiligte Akteure: Image Document Consumer, Image Document Source

Eine weitere Alternative zum Download der Bilddaten ist diese Transaktion, deren Funktionsweise mit der Transaktion Retrieve Document Set vergleichbar ist. Die Unterschiede in den Übermittlungsvarianten sind durch die eingesetzten Protokolle definiert, um eine bessere Kompatibilität mit bereits verwendeten Verfahren zu erreichen. [54] (Siehe Abbildung 30, Transaktionen Image Document)

- **Weitere Retrieve Images Transaktionen**, RAD – 16, RAD – 17, RAD – 27, RAD – 31, RAD – 45

Transaktionen zum Erhalt von Bilddaten verschiedener Datentypen (XDS-I).

Die weiteren Alternativen zum Download der Bilddaten sind spezifisch aufgeteilt nach Art der Daten: zum Beispiel Bilder (RAD – 16), Befunde (RAD – 27) [54] (Siehe Abbildung 30, Transaktionen Image Document)

- **Update Document Set**, ITI – 57

Transaktion zur Veränderung von Metadaten der Dokumente

Beteiligte Akteure: Document Administrator, Document Registry

Die Transaktion ermöglicht Änderungen der hinterlegten Metadaten in der Document Registry. Dazu wird ein weiterer Akteur mit der Bezeichnung Document Administrator benötigt, der Modifizierungen an Metadaten der gespeicherten Dokumente, Folder oder Assoziationen durchführen kann. Des Weiteren sind auch Änderungen in der Verfügbarkeit der durch die Document Registry verwalteten Objekte möglich. [54]

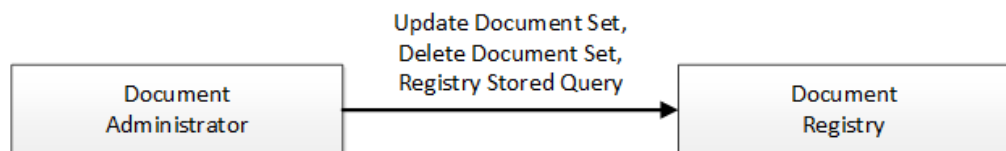


Abbildung 31, Transaktionen Update und Delete Document Set [54]

- **Delete Data**, ITI – 62

Transaktion zur Löschung von Metadaten.

Beteiligte Akteure: Document Administrator, Document Registry

Ergänzend zur Änderung von Metadaten ist auch eine Transaktion zur kompletten Löschung bestimmter Metadaten vorhergesehen. [54]

(Siehe Abbildung 31, Transaktionen Update und Delete Document Set)

- **PIX – Query, ITI – 45**

Transaktion zur Abfrage von Patienten-IDs (PIX).

Beteiligte Akteure: PIX Manager, PIX Consumer

Mit der Anfrage wird eine Patienten-ID ermittelt, welche in unterschiedlichen Varianten innerhalb einer Affinity Domain auftreten kann. PIX ist die Abkürzung für Patient Identifier Cross-Reference. Je nach Struktur der beteiligten Behandlern können sowohl lokale als auch für die Domain globale Patienten-IDs vorhanden sein, deren Verwaltung durch einen PIX Manager durchgeführt wird. Dieser erhält die Informationen zu Patienten und den dazugehörigen IDs über die jeweilig angeschlossenen Patient Identity Sources. Oftmals wird durch den PIX Manager eine eindeutige und in der Affinity Domain globale Patienten-ID vergeben, die sogenannte Master Patient ID (XAD – Pid). Die lokal verwendeten IDs werden durch die Patient Identity Source dem PIX Manager bekannt gemacht und von diesem miteinander verknüpft. Somit kann ein PIX – Consumer eine Anfrage an den PIX – Manager zur Ermittlung der bekannten ID-Informationen stellen. [54]

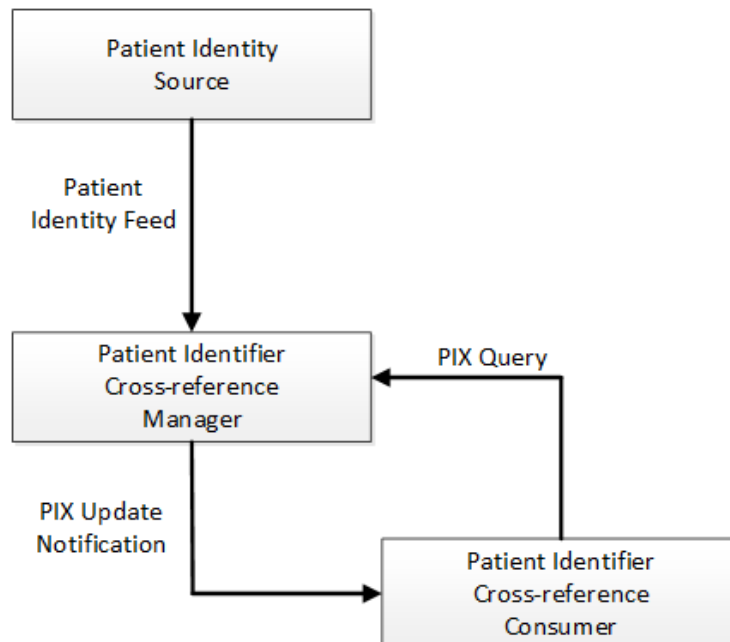


Abbildung 32, Transaktionen ID-Management [54]

- **Patient Demographics Query**, ITI – 47, ITI – 21

Transaktion zur Ermittlung von Patienten mittels demographischer Werte.

Beteiligte Akteure: Patient Demographics Consumer, Patient Demographics Supplier

Eine Abfrage zur Ermittlung von Patienten kann zusätzlich zur gezielten ID-Abfrage auch mit demographischen Werten durchgeführt werden, womit auch identifizierende Daten wie Vorname, Nachname, Adresse, Alter etc. zur Suche eingesetzt werden können. Diese durch den Patient Demographics Supplier verwalteten Daten sind oftmals mit einem PIX Manager innerhalb der Affinity Domain verbunden. [54]

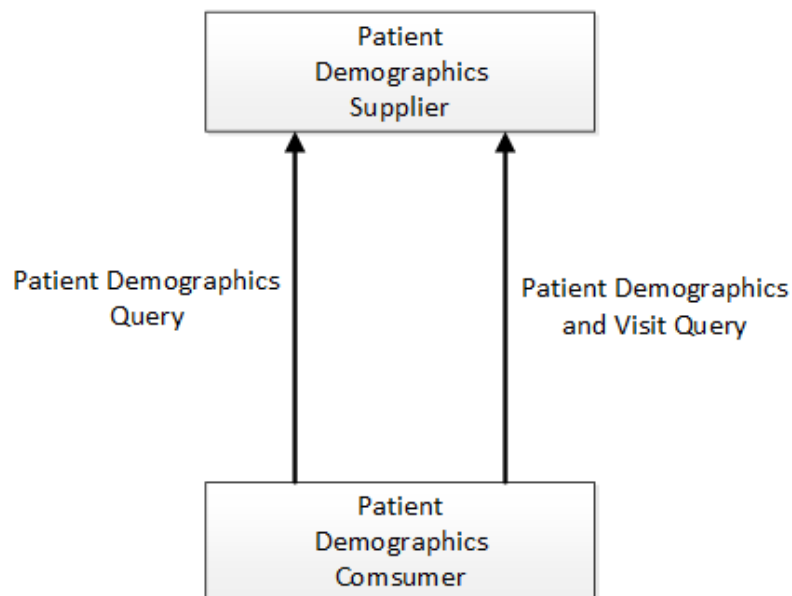


Abbildung 33, Transaktionen Demographics Query [54]

- **Provider Information Feed**

Transaktion zur Informationsübermittlung von Behandler-Daten.

Beteiligte Akteure: Provider Information Source, Provider Information Directory

Die Bezeichnung Provider beschreibt alle Behandler beziehungsweise Leistungserbringer, die an der Behandlung mitwirken. Die Informationen über diese Personen und Einrichtungen werden durch diese Transaktion an ein Provider Information Directory gesendet. Neben der Funktion der Datenübermittlung wer-

den auch Änderungen und Lösch-Vorgänge von Provider-Daten hierdurch erledigt. [54]

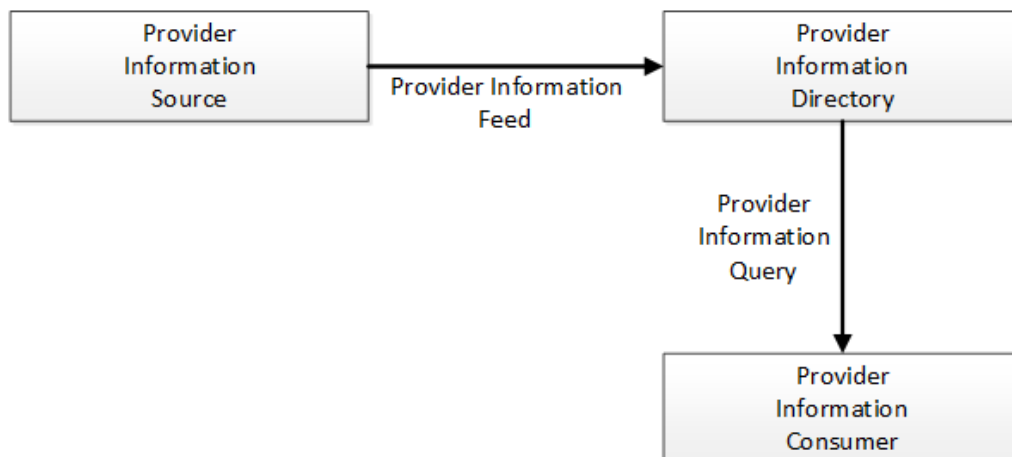


Abbildung 34, Transaktionen Provider Informations [54]

- **Provider Information Query, ITI – 58**

Transaktion zur Abfrage von Behandler-Informationen.

Beteiligte Akteure: Provider Information Consumer, Provider Information Directory

Eine Anfrage an das Provider Information Directory wird mit dieser Transaktion durchgeführt, und liefert die hinterlegten Daten zum Provider zurück. Eine Besonderheit ist die Option zur Kategorisierung im Provider Information Directory, bei dem die Beziehungen von erfassten Behandlern abgebildet werden können, falls beteiligte Einrichtungen zum Beispiel in einer Hierarchie angeordnet sind. [54]

(Siehe Abbildung 34, Transaktionen Provider Informations)

Die aufgelisteten Transaktionen und Beschreibungen der Akteure des XDS.b – Profils eignen sich aufgrund der modularen Bauweise und unterschiedlichen Verarbeitungsmöglichkeiten medizinischer Daten zur weiteren Verwendung bei der Erstellung des Telemedizinregisters, bei dem durch die Voraussetzungen der unterschiedlichen telemedizinischen Dienstleistungen eine hohe Anpassungsfähigkeit sinnvoll ist.

7.5 Anwendungsszenarien aus sektorenfernen Projekten

Die Realisierung des Telemedizinregisters bietet gegebenenfalls weitere Potentialfelder im Bereich eHealth, insofern die rechtlichen Bedingungen dafür vorhanden sind. Vorab ist erneut darauf hinzuweisen, dass eine Erfassung und Verarbeitung medizinischer Daten strengen Richtlinien unterworfen ist, welche in den einführenden Kapiteln dieser Arbeit aufgeführt sind. Weitere Verwendungszwecke der im Register hinterlegten Daten müssen vor der Einrichtung legitimiert werden.

Sobald Daten erfasst werden, die eine Re-Identifizierung ermöglichen oder in anderer Weise Grundrechte von Betroffenen einschränken, müssen gesetzliche Kriterien eingehalten werden. Entweder durch ein fachspezifisches Gesetz, welches die Datenerfassung und Datenverarbeitung definiert oder es muss eine Einwilligungserklärung der Betroffenen vorhanden sein, die umfassend und zweckgebunden über die Verwendung der Daten aufklärt. Folglich lassen sich nachträgliche Erweiterungen in der Datenverarbeitung des Registers nur durchführen, falls ein Gesetz dies ausdrücklich erlaubt oder die Einwilligungserklärungen erweitert und aktualisiert werden. Die Methode der Anonymisierung der verwendeten Daten ist mit Risiken verbunden, da sich eventuell zukünftig durch die Kombination mit anderen Datenbeständen bisher nicht absehbare Re-Identifizierungsrisiken ergeben können. Beispielsweise ist die Kombination von Medikations-Daten aus einer Behandlung mit Erwerbs-Daten einer Apotheke als eine kritische Kombination anzusehen, falls durch zusätzliche Faktoren wie einer seltenen Erkrankung die Re-Identifizierung deutlich einfacher wird. [56] [57]

Ausgehend von einer aller Kriterien entsprechenden Situation mit Berechtigungen zur weiteren Datenverarbeitung wären folgende Szenarien denkbar:

I. Anbindung des Registers an eine elektronische Patientenakte

Die elektronische Patientenakte ist eine Digitalisierung der medizinischen Daten, welche im Rahmen von Behandlungen, Überweisungen, Rezeptausstellungen etc. vorliegen. Die Vorteile liegen besonders im vereinfachten Austausch der erfassten Daten zwischen verschiedenen Behandlern und damit verbundenen geringeren Doppeluntersuchungen und einem lückenloseren Therapieverlauf. Darüber hinaus ist für den Patienten eine verbesserte Möglichkeit gegeben, sich selbstständig über den Fortschritt und Umfang von angewandten Therapien zu

informieren und die Weitergabe von medizinischen Daten zu autorisieren. [58]
[59]

II. Archivierungsfunktionen

Die Daten im Register können als Archivdaten für Behandlungen eingesetzt werden, unter der Berücksichtigung der eingesetzten Pseudonyme. Mittels einer Funktion, die den Pseudonymen zweifelsfrei die realen Daten wieder zuordnet und einer ausreichend langfristigen Speicherungsplanung wären die Voraussetzungen gegeben, die Datenverarbeitung im Register als eine Archivierungsfunktion anzusehen. Diese Kopie der Daten im Telemedizinregister würde somit ein sicheres Konzept der Datenarchivierung beziehungsweise Backup-Vorgängen ergänzen, in Abhängigkeit des Umfangs der im Register hinterlegten Daten. [29]

III. Verknüpfung mit der medizinischen Forschung

Das größte Potential würde bei der Nutzung der im Register hinterlegten Daten zur medizinischen Forschung entstehen, wobei dort die aufwendigsten Kriterien zur Datenverarbeitung eingehalten werden müssen. Der Patient muss mit der weiteren Nutzung der Daten einverstanden sein und das Recht zum Widerruf der Erklärung beziehungsweise Korrektur der Daten besitzen. Die im Register vorhandenen pseudonymisierten Daten müssen in weiteren Schritten entweder komplett anonymisiert oder durch zusätzliche Pseudonymisierungs-Prozesse so verändert werden, dass keine Rückschlüsse oder Re-Identifizierungen möglich sind. Die Trennung und Kategorisierung der im Register gespeicherten Daten ermöglicht eine gezielte Auswahl von Datenmengen, welche für eine Forschung von Relevanz sein könnten. [60] [24]

Zusammenfassend sind weitere Prozesse zur Aufbereitung der Daten im Register notwendig, bevor eine der Szenarien umgesetzt werden kann. Besonders die Modifikation der Pseudonyme in identifizierende Daten für die digitale Patientenakte und Archivierungsfunktion ist an umfangreiche Maßnahmen geknüpft. Die Anonymisierung der Pseudonyme zur Verwendung in der medizinischen Forschung wäre durch die Datenreduzierung vergleichsweise effizient durchzuführen.

8 Anforderungen an ein Telemedizin – Register

In diesem Kapitel werden detailliert Anforderungen beschrieben, die an das Telemedizinregister gestellt werden. Dazu werden Grundbedingungen aus den vorherigen Kapiteln, insbesondere die rechtlichen Anforderungen, zusammen mit Erkenntnissen aus den Interviews und der ersten Beschreibung des Registers zusammengeführt und zur Konkretisierung von Anwendungsfällen eingesetzt.

Aus diesen ergeben sich Anforderungslisten, welche in funktionale und nicht funktionale Anforderungen getrennt sind. Des Weiteren werden in diesem Kapitel Datenmodelle und deren Verwendungen im Telemedizinregister aufgeführt, die eine Basis für die Modellierungen der verschiedenen Prozesse darstellen.

8.1 Rich-Pictures des IST- und SOLL-Zustands

Die aufgeführten Rich-Pictures orientieren sich am Anwendungsszenario C, bei dem die beteiligten Stakeholder in Gruppen dargestellt werden. Mittels dieser Visualisierung wird der Unterschied zwischen dem aktuellen Zustand und dem geplanten Zustand durch die Erweiterung des Modells mit einem Telemedizinregister erkennbar, indem das Rich-Picture eines IST-Zustands mit einem Rich-Picture eines SOLL-Zustands ergänzt wird.

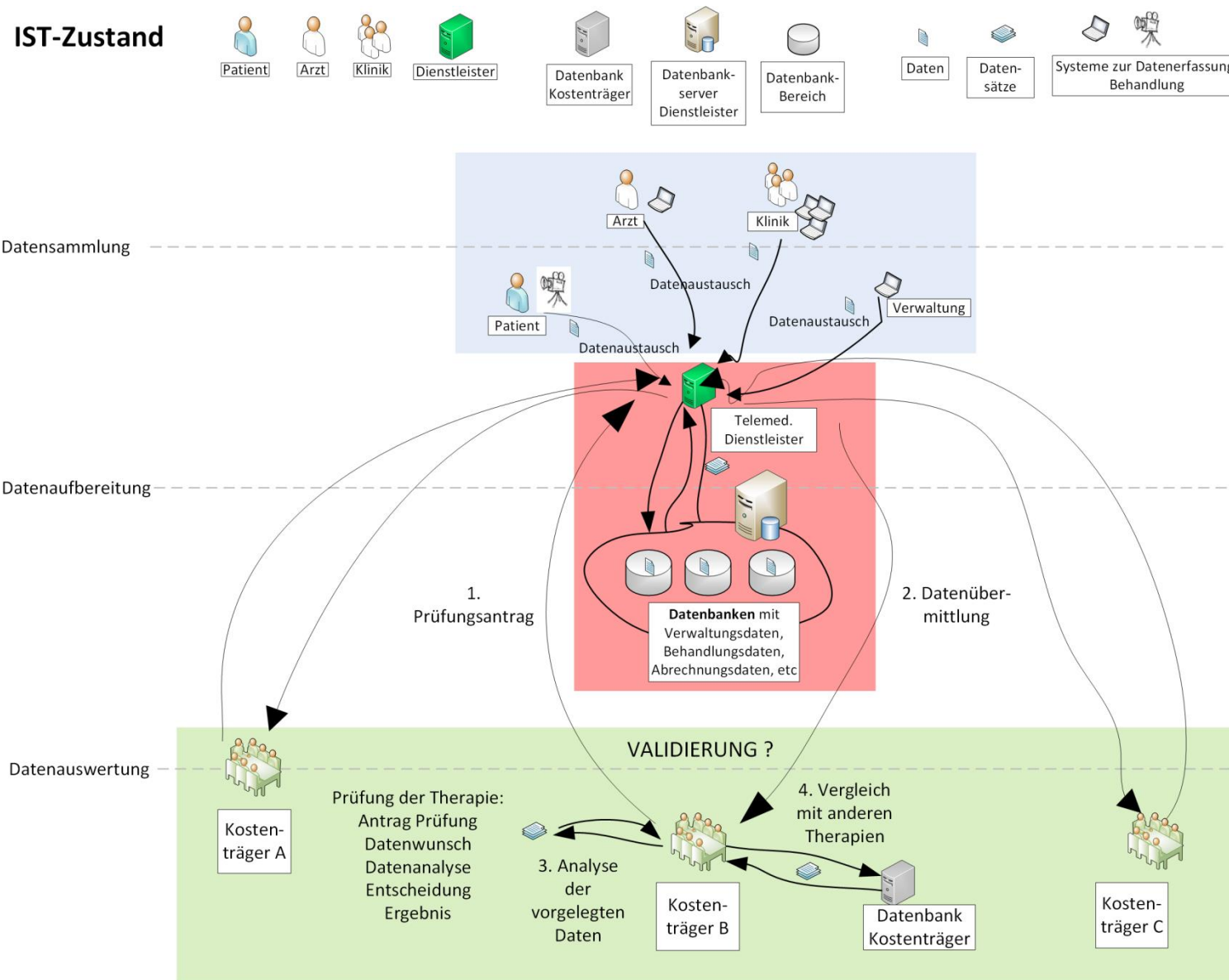


Abbildung 35, Rich-Picture IST-Zustand

Der IST-Zustand entspricht einem Beispiel eines telemedizinischen Dienstleisters, der zentral Daten von verschiedenen an der Therapie beteiligten Einrichtungen erfasst und speichert. Diese Einrichtungen können mit unterschiedlichen Geräten arbeiten, um Behandlungsdaten zu erfassen und an den Dienstleister zu übertragen. Beispielsweise mit einem anwendungsoptimierten Gerät zur einfachen Anwendung durch den Patienten im häuslichen Umfeld oder komplexen klinischen Systemen, die mit dem Dienstleister verbunden sind. Die Struktur der an der Therapie direkt beteiligten Partner ist blau hinterlegt, mit dem Dienstleister als zentrales Bindeglied. Der Übersicht wegen ist nur ein Rechner stellvertretend für den Dienstleister in dieser Teilstruktur aufgeführt, welcher die komplette Infrastruktur (Server-Systeme, Client-Systeme und Netzwerke) beim Dienstleister abbildet.

Die zweite Teilstruktur ist rot hinterlegt und beschreibt die bisherige Speicherorganisation zur Verarbeitung der erfassten Therapiedaten durch den telemedizinischen Dienstleister. Zu erwarten sind mehrere verschiedene Speichermöglichkeiten, die für die unterschiedlichen Datenkategorien verwendet werden, zum Beispiel Datenbanken für Verwaltungsdaten, Abrechnungsdaten und Behandlungsdaten, Fileserver für Dokumente, Audio und Videodaten. Mit dieser Teilstruktur sind auch alle verarbeitenden Prozesse dargestellt, die im Rahmen der Therapie durch den Dienstleister erfolgen.

Die Datenauswertung durch die Kostenträger wird in der dritten Teilstruktur mit der grünen Markierung abgebildet. Generell sind bedingt durch die Vielzahl von verschiedenen Krankenkassen in Deutschland für telemedizinische Projekte auch eine dementsprechend hohe Anzahl von Kostenträgern in den Prozess der Abrechnungsvorgänge involviert. Die individuellen Kostenträger stellen an den Dienstleister Anfragen zum Erhalt der Therapiedaten und werten diese meist selbstständig aus. Vor allem dieser Zustand beeinflusst den Umfang der im Telemedizinregister hinterlegten Daten. Sind die Kostenträger daran interessiert, die Analyse der Daten in eigener Verantwortung vorzunehmen, wird der Bedarf an zu empfangenden Daten größer sein als im Vergleich zur Situation, bei der vor einer Datenerfassung bestimmte Kriterien und Verfahren zur Durchführung der Analyse gefiltert werden.

SOLL-Zustand

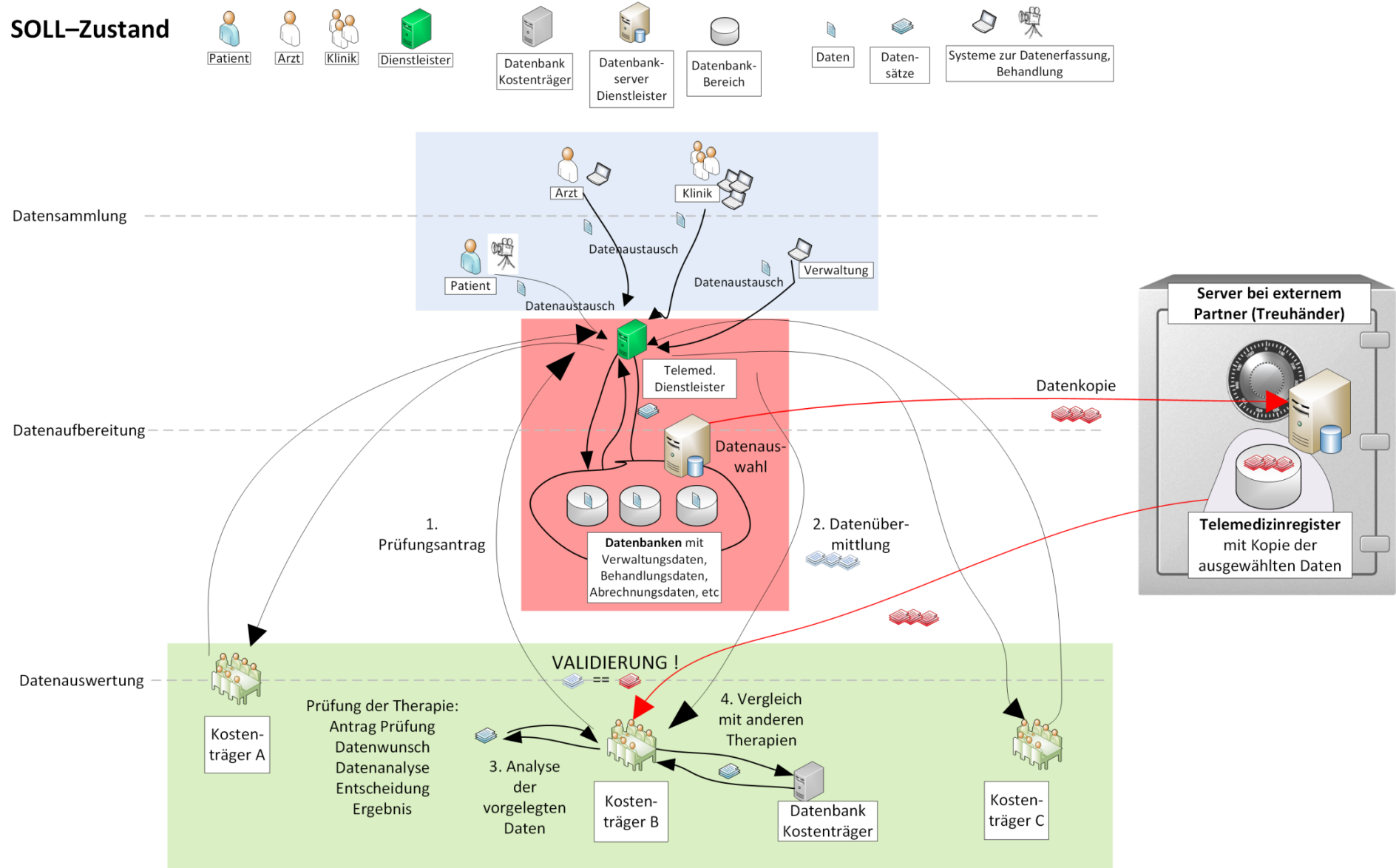


Abbildung 36, Rich – Picture SOLL-Zustand

Der SOLL-Zustand, welcher im obigen Rich-Picture dargestellt ist, zeigt die Integration des Telemedizinregisters in die bisherigen Abläufe der Therapiedurchführung und Abrechnungsvorgänge. Parallel zu den Daten, die ein Kostenträger durch den Dienstleister nach einer Anfrage erhält, stehen zur Validierung oder stichprobenweisen Überprüfung Datensätze aus dem Telemedizinregister zur Verfügung.

Damit ist eine Erweiterung der Arbeitsprozesse auch für aktuell laufende telemedizinische Projekte realisierbar, indem die therapierelevanten Daten für die Speicherung und Verarbeitung in dem Telemedizinregister ausgewählt und aufbereitet werden.

Der Unterschied der Datensätze, welche beim Dienstleister oder im Telemedizinregister vorhanden sind, ergibt sich in der notwendigen Pseudonymisierung der an das Register übermittelten Daten. Eine unveränderte Kopie der Daten in das Register zu übertragen wäre aufgrund gesetzlicher Einschränkungen mit einem sehr hohen technischen Aufwand verbunden und erhöht die Risiken eines möglichen Datenverlusts deutlich. Zusätzlich könnten andere potentielle Anwendungsfelder durch das Telemedizinregister nur eingeschränkt zur Verfügung stehen, da eine weitere Verarbeitung der Daten erst nach aufwendigen Aufbereitungsprozessen möglich wäre.

8.2 Datenkategorien

Zur Bestimmung der möglichen Anwendungsfälle bei der Einrichtung und Nutzung eines Telemedizinregisters wird ein konkretes Anwendungsszenario detailliert untersucht, um praxisnah die einzelnen Schritte und Voraussetzungen des Ablaufs zu erfassen.

Hierzu dient das in Kapitel 7 beschriebene Anwendungsszenario C. Bei diesem werden durch ein Dienstleister kontinuierlich Daten in das Telemedizinregister übertragen, welches von mehreren Kostenträgern als Validierungsmöglichkeit genutzt werden kann. Dieses Schema wird auf viele telemedizinische Projekte zutreffen. Die Abweichungen der anderen Szenarien werden zusätzlich danach aufgeführt und untersucht.

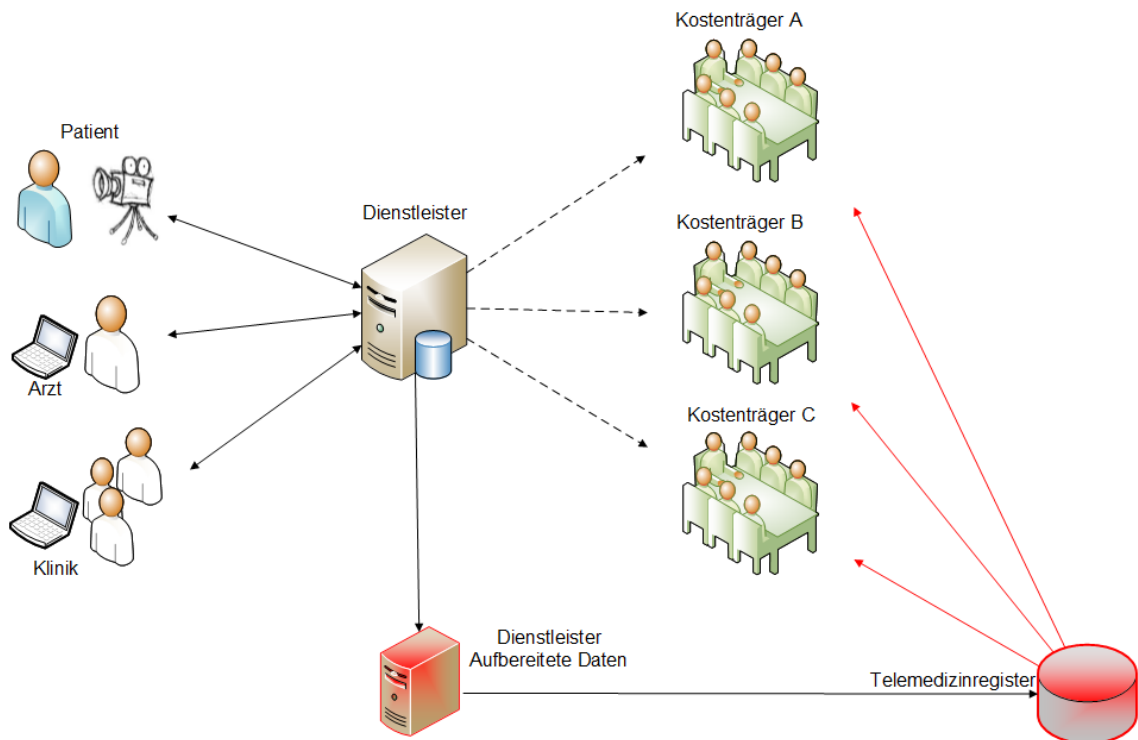


Abbildung 37, Anwendungsszenario C

Als datenerfassende Einrichtungen sind drei verschiedene Positionen aufgeführt: der Patient, der behandelnde Arzt und die Klinik. Durch diese werden separat Daten erfasst und an den telemedizinischen Dienstleister übertragen.

Für die beteiligten Kostenträger sind für Abrechnungszwecke nun zwei Möglichkeiten vorhanden, Therapiedaten zu erhalten: Einerseits ein direkter Weg mit der Anfrage an den telemedizinischen Dienstleister und andererseits durch die Anfrage an das Telemedizinregister. Hierzu müssen die Daten durch den Dienstleister vor der Speicherung im Register spezifisch ausgewählt und bearbeitet werden, um vor allem datenschutzrechtliche Kriterien für die externe Speicherung und Verarbeitung von Daten einzuhalten.

Die Anzahl der Kostenträger ist in diesem Szenario auf drei limitiert, um die Handhabung unterschiedlicher Anforderungen durch den jeweiligen Kostenträger darstellen zu können. Die Auswahl der Daten, welche eine Krankenkasse für ihre Analysen der Effizienz und Effektivität der Therapie im Vorfeld trifft, ist in dieser Arbeit nur schematisch beschreibbar, ohne exakte Datenanforderungen auflisten zu können. Dieser Prozess muss vor Einrichtung des Telemedizinregisters abgeschlossen sein.

Die verwendeten Datentypen lassen sich neben den zuvor erwähnten IDAT und MDAT in weitere Kategorien gliedern:

1. IDAT

Diese Daten sind identifizierende Daten, welche eine direkte oder indirekte Verbindung zu Patienten aufweisen. Dazu zählen beispielsweise folgende Daten [61]:

- Name
- Vorname
- Adresse
- Geburtsdatum
- Mitgliedsnummer Krankenkasse
- Pseudonym

2. MDAT

Daten mit einem medizinischen Bezug werden der MDAT – Kategorie zugeordnet, wobei im Verlauf der Prozesse nochmals eine Unterteilung vorgenommen wird, die sich aufgrund dem benötigtem Speicherplatz ergeben. So sind bestimmte medizinische Daten so umfangreich, dass deren Speicherung nur bei der datenerfassenden Einrichtung erfolgt und Anfragen für diese Daten zusätzliche Bearbeitungsschritte benötigen (siehe Transaktion Provide and Register Imaging Document Set des XDS.b – Profils).

Beispiele für MDAT [61]:

- Medikationsdaten
- Befunde
- Rezepte
- Videoaufnahmen
- Audioaufnahmen
- Röntgenbilder
- Laborergebnisse

3. Metadaten

Mittels der Metadaten werden die medizinischen Daten (MDAT) klassifiziert und für die Verarbeitung im Telemedizinregister benötigt. Besonders im Prozess

der Registrierung, Speicherung und Suche nach medizinischen Daten beziehungsweise Dokumenten werden die Metadaten vorausgesetzt. Die Metadaten werden zusammen mit den an das Register übermittelten Dokumenten und Objekten übertragen und können beispielsweise in einem Container-ähnlichen Format zusätzliche Informationen zur Verwaltung enthalten.

4. Verwaltungsdaten

Als zusätzliche Kategorie von Daten werden den Abrechnungsdaten alle Informationen zugeordnet, die für betriebswirtschaftliche Abläufe zur Abrechnung der Therapie zwischen Leistungserbringer und Kostenträger verwendet werden. Diese Daten sind nicht Gegenstand der Speicherung im Telemedizinregister und sollen einzig bei Dienstleistern und beteiligten Kostenträgern verwendet werden. Beispiele hierfür sind:

- Rechnungen
- Verwaltende Daten zur Therapiedauer
- Leistungsbeschreibungen

Bei der Verarbeitung und Speicherung der Datentypen sind zwei grundlegende Abschnitte zu unterteilen, welche im Verlauf der Erstellung und Nutzung eines Telemedizinregisters vorhanden sind: der Bereich der Datenaufbereitung beim Dienstleister und die Verarbeitung der Daten im Telemedizinregister. Diese Trennung ist sinnvoll, da ein Telemedizinregister auch für schon laufende Projekte und Dienstleistungen angewendet werden soll, bei denen aber unterschiedlichste Systeme und Prozesse bei der Datenverarbeitung zu erwarten sind. Daher ist eine Beschreibung der Aufbereitung von Daten für das Telemedizinregister im folgenden Abschnitt aufgeführt, welches einen Weg zu standardisierten Daten aufzeigen soll.

Das Ergebnis dieser Aufbereitung kann an das Telemedizinregister übermittelt und dort gespeichert werden, welches der zweite grundlegende Abschnitt in der Verarbeitung und Speicherung darstellt. Diese Prozesse lassen sich aufgrund der vorhandenen Standardisierung in dieser Arbeit ausführlicher beschreiben und sollen für alle Dienstleister, die ein Telemedizinregister anwenden, als Vorlage eine Verwendung in der Struktur des Registers finden. Eine Auflistung der verwendeten Datenkategorien findet sich in den zwei folgenden Unterkapiteln, welche in Abbildungen den Bezug der Daten untereinander darstellen.

8.2.1 Auswahl und Aufbereitung der Daten beim Dienstleister

Der folgende Abschnitt zeigt die verwendeten Datenmodelle und den daraus resultierenden Datenfluss, der durch die Aufbereitung der Therapie-Daten durch den telemedizinischen Dienstleister entsteht.

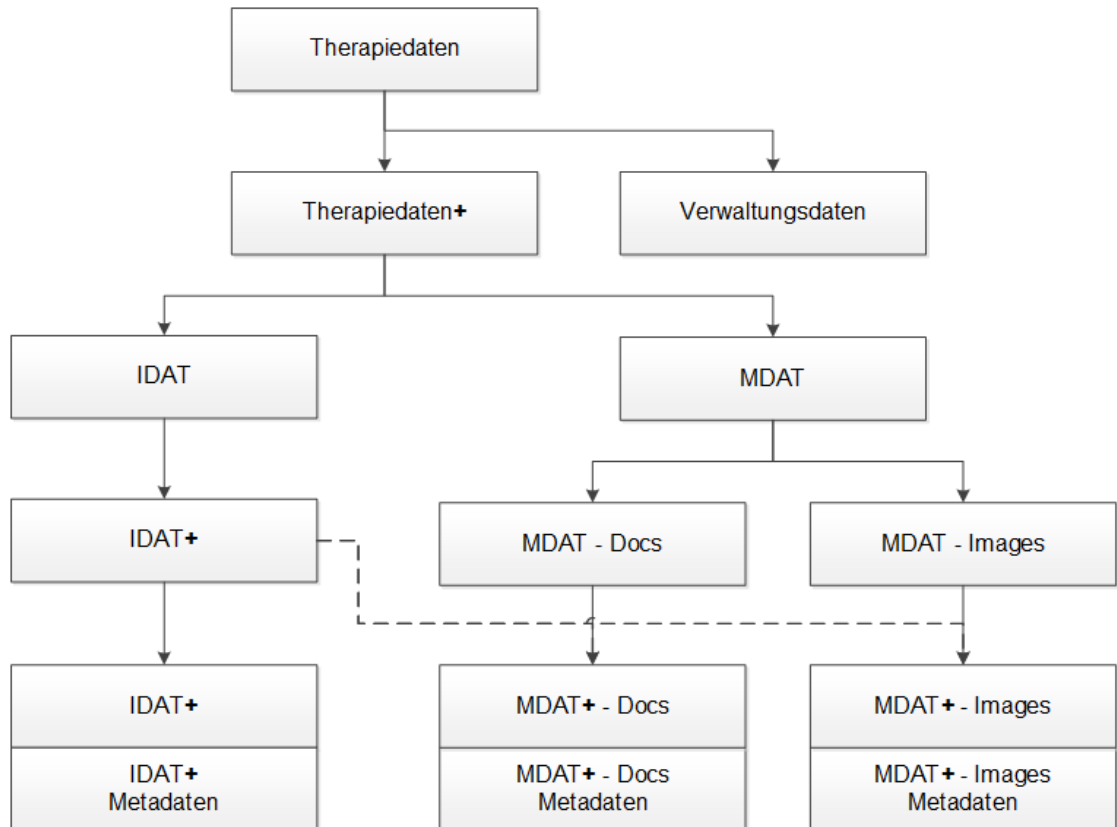


Abbildung 38, Datenaufbereitung beim Dienstleister

- **Therapiedaten**
Datenmenge aller beim Dienstleister vorhanden Daten zur Therapie.
- **Therapiedaten+**
Datenmenge, die nach dem Auswahl-Prozess des Dienstleisters in Zusammenarbeit mit den Kostenträgern entsteht.
- **Verwaltungsdaten**
Menge aller Daten, die ein Dienstleister nicht für die medizinische Behandlung benötigt und daher nicht im Register erfasst werden.

- **IDAT**
Datenmenge, die alle identifizierenden Daten (persönliche Daten) umfasst.
- **IDAT+**
Datenmenge, die nach der Pseudonymisierung aus IDAT entsteht, d.h. ohne reale Daten, die eine direkte Identifizierung erlauben.
- **IDAT+ Metadaten**
Die Metadaten von IDAT+ werden für die Verwaltung der IDAT+ im Telemedizinregister benötigt.
- **MDAT**
Datenmenge, die alle medizinischen Daten (Informationen, Dokumente, Bilder, etc.) beschreibt.
- **MDAT – Docs**
Teilmenge von MDAT, die alle Daten (Informationen, Dokumente, etc.) umfasst, welche in das Telemedizinregister übertragen werden.
- **MDAT – Images**
Teilmenge von MDAT, die alle Daten (Bilder, Videos, Audio, etc.) beschreibt, welche nicht direkt ins Telemedizinregister übertragen werden, aufgrund der hohen Datenmengen. Beispielsweise sind die Dateien bei radiologischen Untersuchungen vergleichsweise sehr speicherintensiv, daher werden nur Metadaten in das Register übertragen.
- **MDAT+ - Docs**
Aufbereitete Datenmenge, die aus MDAT – Docs entsteht und Elemente von IDAT+ miteinbindet. Dabei werden IDAT - Informationen in der MDAT – Doc Menge durch IDAT+ - Information (Pseudonyme) ersetzt, soweit dies möglich ist.
- **MDAT+ - Images**
Aufbereitete Datenmenge, die aus MDAT – Images entsteht und Elemente von IDAT+ miteinbindet. Dabei werden IDAT - Informationen in der MDAT –

Images Menge durch IDAT+ - Information (Pseudonyme) ersetzt, soweit dies möglich ist.

- **MDAT+ - Docs Metadaten**

Die Metadaten von MDAT+ - Docs werden für die Verwaltung der MDAT+ im Telemedizinregister benötigt.

- **MDAT+ - Images Metadaten**

Die Metadaten von MDAT+ - Images werden für die Verwaltung der MDAT+ im Telemedizinregister benötigt und als spezielles Objekt übertragen.

8.2.2 Speicherung und Verarbeitung der Daten im Register

An den Prozess der Aufbereitung angeschlossen erfolgt die Übermittlung, Speicherung und Verarbeitung der Daten im Telemedizinregister, welche für die Verwendung im Register bearbeitet sind.

Neben der Kopie der therapierelevanten Daten (IDAT, MDAT) in das Register werden für die Verwaltung und Protokollierung zwei weitere Datentypen benötigt, die mit USER und AUDIT bezeichnet sind. Deren Zugriffsmöglichkeiten sind gegenüber den anderen Daten deutlich eingeschränkt und sind in administrativer Verantwortung.

- **USER**

Daten zur Verwaltung der zugriffsberechtigten Konten und Identitäten.

- **AUDIT**

Datenmenge, durch die alle Zugriffe (speichern, lesen, ändern, löschen, administrative Zugriffe) protokolliert und auswertbar sind.

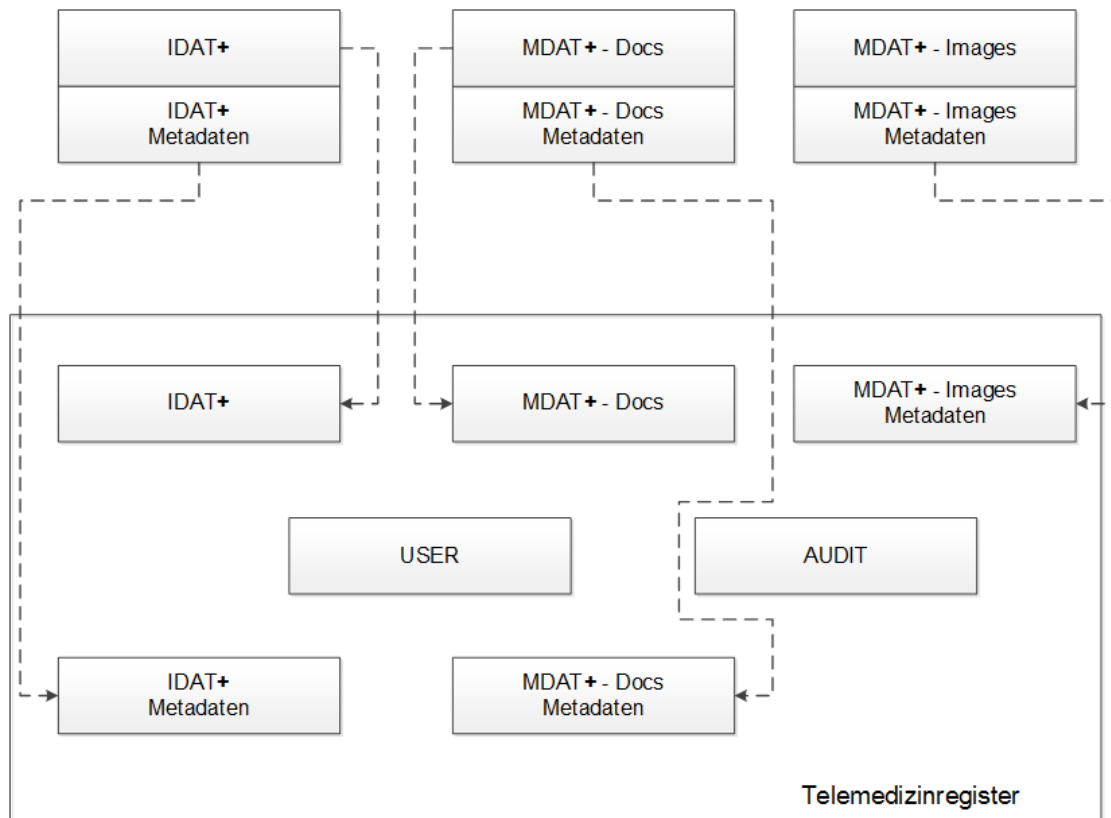


Abbildung 39, Datentypen im Register

Die bei der Aufbereitung entstehenden MDAT+ - Images werden bei der jeweiligen Einrichtung vorgehalten, die für die Speicherung der Daten in das Register verantwortlich ist.

Auf detaillierte Datenmodelle wird in dieser Beschreibung bewusst verzichtet, um die verschiedenen Voraussetzungen bei den telemedizinischen Behandlungen allgemein erfassen zu können. Erwartungsgemäß wird die Schnittmenge der Daten zwischen verschiedenen Dienstleistern nicht umfangreich sein, da es unzählige verschiedene Optionen zur Datenerfassung und Datenspeicherung bei Dienstleistern gibt. Daher muss individuell der Aufbereitungsprozess beim Dienstleister durchgeführt und bereits vorhandene Strukturen in diese Prozesse miteinbezogen werden. Unter günstigen Voraussetzungen sind bei einem telemedizinischen Dienstleister bereits standardisierte Verfahren im Einsatz, welche eine Weiterverwendung der erfassten Datenmenge erleichtern.

Als Beispiel für die Aufbereitung der Daten werden im 9. Kapitel mittels einiger reduzierten Datenmengen die Teilprozesse der Aufbereitung und Speicherung im Telemedizinregister dargestellt.

8.3 Anwendungsfälle

Die Prozesse und Abläufe zur Einrichtung des Telemedizinregisters sind durch zwei Anwendungsfälle unterteilt, um die Bereiche der Datenaufbereitung und der eigentlichen Verarbeitung im Telemedizinregister voneinander zu trennen.

1. Anwendungsfall Datenaufbereitung

Die Speicherung der Daten benötigt mehrere vorbereitende Schritte, um bei vorhandenen telemedizinischen Projekten die datenschutzrechtlichen Voraussetzungen zur Speicherung der Daten bei externen Partnern ausreichend vorzubereiten. Daher ist dieser Ablauf in einem eigenen Anwendungsfall dargestellt, der die Aufbereitung der vorhandenen Therapiedaten in mehreren Abschnitten definiert.

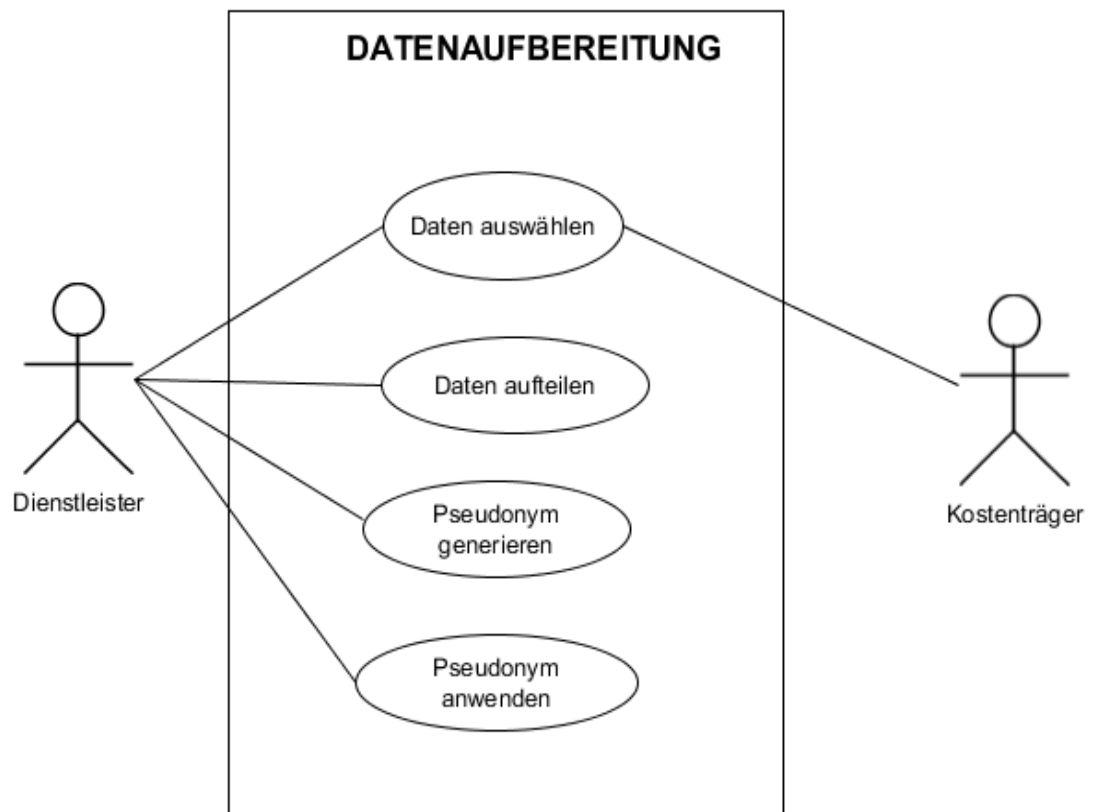


Abbildung 40, Anwendungsfall Datenaufbereitung

Die beteiligten Akteure sind der Dienstleister und der Kostenträger, welche initial in Kooperation die relevanten Daten der Therapie festlegen (Daten auswählen). Diese werden in folgenden Prozessen (Daten aufteilen, Pseudonym generieren, Pseudonym anwenden) für die Speicherung aufbereitet.

- **Daten auswählen**

Der telemedizinische Dienstleister und die jeweiligen Kostenträger bestimmen zusammen eine Auswahl der beim Dienstleister vorhandenen Daten, welche in das Telemedizinregister übertragen werden sollen. Die verwendeten Datentypen sind Therapiedaten, Therapiedaten+ und Verwaltungsdaten. Das Ziel der Auswahl ist ein für den Kostenträger ausreichender Datenbestand im Telemedizinregister, der für die Validierung der Analyse und Bewertung verwendet werden kann.

- **Daten aufteilen**

Nach der Auswahl der Daten wird die gefilterte Datenmenge (Therapiedaten+) in zwei Kategorien geteilt, den identifizierenden Daten (IDAT) und den medizinischen Daten (MDAT). Aus der Menge der medizinischen Daten lassen sich wiederum zwei Teilmengen bilden, die MDAT-Docs und die MDAT-Images, deren Unterschied in dem Umfang des benötigten Speicherplatzes besteht.

- **Pseudonym generieren**

Die IDAT-Menge wird mittels Pseudonymisierungsschritten zur IDAT+ - Menge verändert. Das Ziel besteht darin, die persönlichen Daten in einem oder mehreren Pseudonymisierungsvorgängen so zu verändern, dass keine Re-Identifizierungen bei einem Datenverlust oder unautorisiertem Zugriff auf die bearbeiteten Telemedizinregister-Daten möglich ist.

- **Pseudonym anwenden**

Die Informationen aus der IDAT+ - Menge werden auf die dazugehörigen MDAT-Datenmengen angewendet, bei denen auch identifizierende Daten vorhanden sein können. Diese Änderungen sollen soweit wie möglich umgesetzt werden. So sind beispielsweise Änderungen bei Dateinamen einfacher durchführbar, IDAT-Bezeichner in medizinischen Befunden hingegen sind nur mit erhöhtem Aufwand beziehungsweise bei Bildern (Röntgenaufnahmen) nicht gegen die generierten IDAT+ - Bezeichner austauschbar. Sind bei medizinischen Text-Dokumenten die persönlichen Daten verhältnismäßig effizient austauschbar, so sollten hingegen in der Datenaufbereitung für nicht editierbare Objekte Maßnahmen ergriffen werden, um eine erhöhte Sicherheit gegen Datenverlust und

unautorisierten Zugriff zu gewährleisten. Bei unverhältnismäßig hohem Aufwand der Änderungsvorgänge kann die Verschlüsselung ein alternatives Verfahren zur Sicherung darstellen.

2. Anwendungsfall Telemedizinregister

Nachdem Daten durch den Dienstleister für die Speicherung in dem Register vorbereitet wurden, sind die wesentliche Prozesse des Registers definierbar:

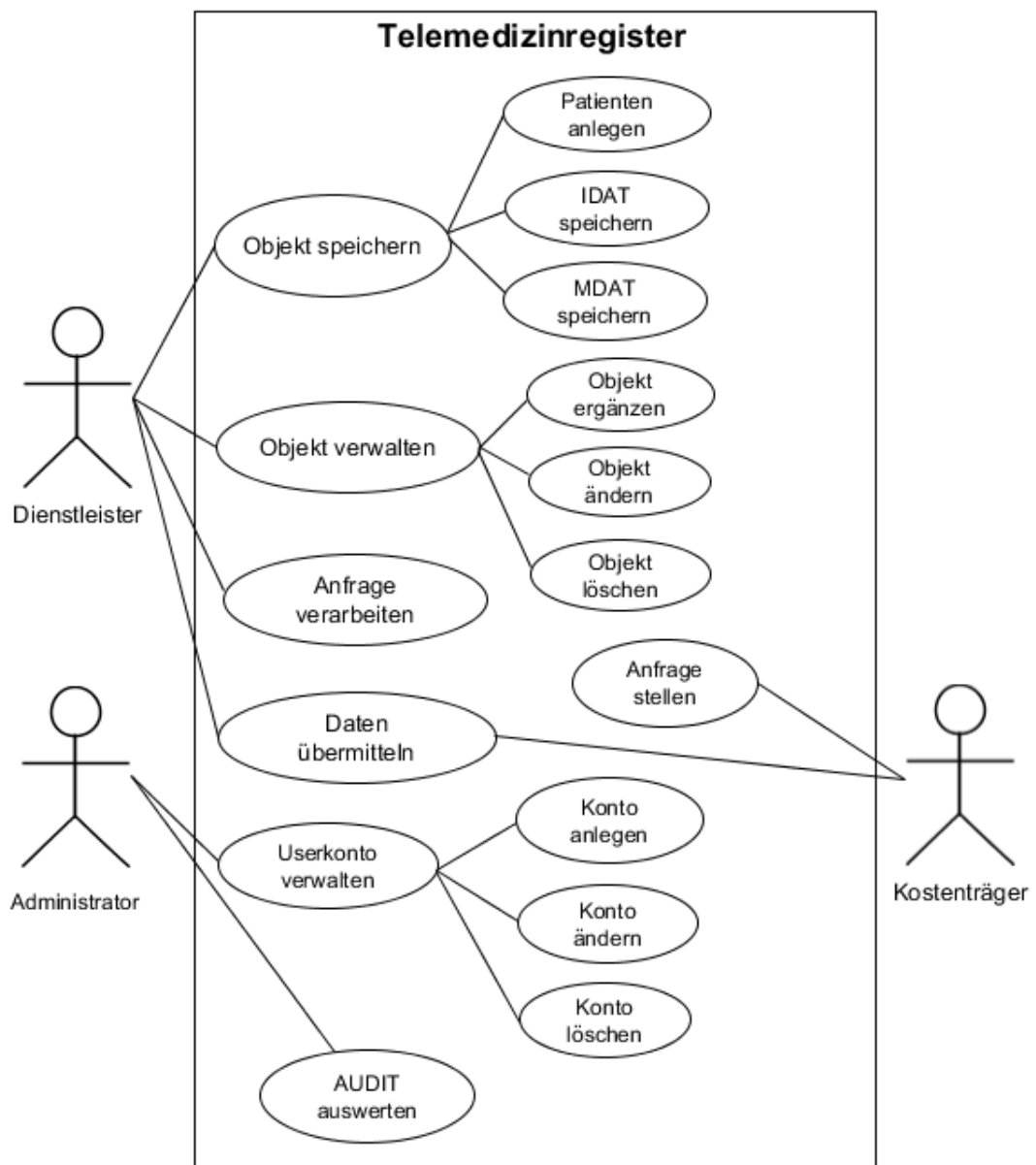


Abbildung 41, Anwendungsfall Telemedizinregister

Als weiteren Akteur im Vergleich zum vorherigen Anwendungsfall ist der Administrator aufgeführt, der administrative Funktionen im Telemedizinregister besitzt. Diese bestehen in der Anlage und Verwaltung der zugriffsberechtigten Konten (USER) und Funktionen zur Auswertung von AUDIT-Informationen. Mittels dieser werden Protokollierungen und Zugriffsinformationen gespeichert, um eine lückenlose Historie der Zugriffe in den verschiedenen Anwendungen des Telemedizinregisters zu sichern.

- **Objekt speichern**

Mit der Bezeichnung Objekt werden die verschiedenen Elemente bezeichnet, welche für die Speicherung der therapielevanten Daten im Telemedizinregister benötigt werden. Darunter fallen die Daten der IDAT+ - Menge und MDAT+ - Menge, welche kombiniert eine Patientenakte darstellt. Dazugehörig sind auch Metadaten, mit denen die Verwaltung und Suche im Register strukturiert ist. Die Funktion Objekt speichern beschreibt die unterschiedlichen Teilfunktionen zur erstmaligen Speicherung der Daten.

- **Objekt verwalten**

Je nach Therapieform werden die Daten, die im Telemedizinregister angelegt werden, in weiteren Schritten verarbeitet. Dies sind die Funktionen ergänzen, ändern und löschen von Objekten. Dabei werden durch den Dienstleister Veränderungen an bereits existierenden Objekten vorgenommen, die vor allem Metadaten bei Korrekturen, beispielsweise Adressänderungen bei Patienten, und MDAT+ bei ergänzenden Objekten betreffen (beispielsweise das hinzufügen von medizinischen Dokumenten).

- **Anfrage stellen**

Durch den Akteur Kostenträger werden Anfragen mit der Absicht an das Telemedizinregister gestellt, bestimmte oder alle Daten einer Therapie zu erhalten beziehungsweise in Absprache mit dem Dienstleister übermittelt zu bekommen. Mittels dieser Anfrage wird eine Datenmenge ausgewählt, die anhand bestimmter Zeiträume, spezifischer demografischer Kriterien oder allgemein definiert ist.

- **Anfrage verarbeiten**

Nach dem Eingang einer Anfrage durch den Kostenträger muss diese auf Legitimation, Korrektheit und Erfüllbarkeit untersucht werden, welches durch den Akteur Administrator durchgeführt wird. Werden die zuvor genannten Kriterien erfüllt, muss im nächsten Schritt die Auswahl der angefragten Daten erfolgen, an welche sich die Übermittlung an Kostenträger und Information an den Dienstleister anschließen.

- **Daten übermitteln**

Die Übermittlung der angefragten Datenmenge kann grundsätzlich auf zwei verschiedene Arten erfolgen: einerseits durch eine Bereitstellung, Aufbereitung und Anzeige der Daten mittels einer Oberfläche, auf die der Kostenträger Zugriff besitzt und Möglichkeiten zur weiteren Suche und Filterung aufweisen kann.

Andererseits ist ein Datenexport vom Telemedizinregister zum Kostenträger, bei dem zusätzliche Mechanismen zur Sicherung der Übertragung vorgenommen werden müssen. Des Weiteren muss seitens des Kostenträgers ein Verfahren zum Import der erhaltenen Daten zur weiteren Analyse erfolgen, damit die übertragenen Informationen durch den Kostenträger genutzt werden können. Die standardisierte Speicherung und Verarbeitung der Daten im Telemedizinregister bietet Möglichkeiten zur Entwicklung einer Schnittstelle, welche die Prozesse des Exports vereinfachen würde.

- **Userkonto verwalten**

Durch den Akteur Administrator werden zentral in dem Telemedizinregister die Benutzerkonten verwaltet, welche Zugriff und damit verbundene Aktionen auf das Register besitzen. Dies ist die Hauptaufgabe des Administrators, der vorher definierte Rollen und Konten im Register anlegt, ändern und löschen kann, mit Berücksichtigung des Akteurs Dienstleister. Auch grundlegende technische Vorgänge zur Durchführung der verschiedenen Aktionen im Register sind in der Verantwortung des Administrators, dessen Aufgabengebiet mit dem eines Datenbank-Administrators vergleichbar ist.

- **AUDIT auswerten**

Der Administrator verwaltet darüber hinaus die Protokollierung der Zugriffe und ausgeführten Aktionen, die durch Akteure im Telemedizinregister erfolgen. Diese Zugriffsstatistiken müssen bei Anfragen und routinemäßigen Stichproben - beispielsweise einem Kriterium des Qualitätsmanagement - auswertbar sein, um eine lückenlose Historie der Aktionen im Register zur Überprüfung darstellbar zu machen. Nur durch diese unverfälschte Protokollierung ist sichergestellt, dass ein Kostenträger korrekte Daten zur Analyse erhalten und mittels dieser eine Validierung der Therapiedaten vornehmen kann. Darüber hinaus ist die Protokollierung datenschutzrechtlich vorgeschrieben und kombinierbar mit dem Auskunftsrecht von Patienten.

8.4 Anforderungsliste

Die Anforderungsliste enthält eine Gliederung der Anforderungstypen, getrennt nach Funktionsbereichen; funktional und nicht funktional. Des Weiteren sind in den Funktionsbereichen noch weitere Unterteilungen vorhanden, um die Anforderungen thematisch zu gliedern. Die Anforderungsbeschreibungen werden eine allgemeine Darstellung aufweisen und technische Details nur im Zusammenhang mit den verwendeten Standards besitzen.

Zusätzlich zur Beschreibung der Anforderung erfolgt in tabellarischer Form eine Nummerierung, ein eindeutiger Bezeichner, eine Priorisierung in drei Stufen (MUSS, SOLL, KANN) und die Referenz, welche die Begründung oder die Voraussetzung für die Anforderung angibt.

Mit der Bezeichnung Objekt werden alle Informationen umschrieben, die im Register für die Speicherung und Verwaltung der Patientendaten notwendig sind. Dies können zum Beispiel Datenbankeinträge (Adresse), medizinische Dokumente (Befund) oder auch Metadaten zur Verwaltung der Informationen sein.

Allgemein sollte das System Telemedizinregister neben den spezifischen Anforderungen folgende Kriterien der Software-Technik allgemein berücksichtigen [46]:

- **Korrektheit**

Die Speicherung der Daten und anschließende Verarbeitung müssen ausnahmslos korrekte Daten verwenden, zu keiner Zeit dürfen unvollständige oder fehlerhafte Daten im Register vorhanden sein.

- **Erweiterbarkeit**

Das System soll für verschiedenste telemedizinische Dienstleistungen eingesetzt werden und benötigt daher eine modulare Bauweise, die für spezifische Anforderungen erweitert werden kann. Dieses kann mit standardisierten Profilen zur Datenübermittlung und Datenverarbeitung unterstützt werden.

- **Verifizierbarkeit**

In das System sollen Funktionen integriert werden, die eine Überprüfung auf Korrektheit und Vollständigkeit von übermittelten, gespeicherten und verarbeiteten Daten automatisiert durchführt, um eine fehlerfreie Datenverarbeitung zu ermöglichen.

- **Dokumentation**

Neben der Dokumentation der eingesetzten Verfahren und Techniken zur Verbesserung der Portabilität und Wiederverwendbarkeit sind auch Protokollierungen aller Zugriffe, Aktionen und Funktionen von hoher Priorität, um mit der lückenlosen Historie der Datenverarbeitung die notwendigen datenschutzrechtlichen Vorgaben zu erfüllen.

Damit ergibt sich eine Anforderungsliste, die neben den in der Arbeit erhobenen Anforderungen auch allgemeingültige Kriterien auflistet, die an ein Software- und Hardware-System gestellt werden. [62]

8.4.1 Funktionale Anforderungen

Nr..	Bezeichner	Beschreibung	Priorität			Referenz
			MUSS	SOLL	KANN	
FA1	Generelle Anforderungen des Systems					
FA1.1	Objekt-Speicherung	Objekte können gespeichert werden.	x			IDAT - und MDAT – Objekte werden im Register gespeichert
FA1.2	Objekt-Konstante	Objekte können konstant angelegt werden.	x			Objekte wie die ID werden als Konstante gespeichert
FA1.3	Objekt-Änderungen	Objekte können verändert werden	x			Recht des Patienten auf Änderung evtl. fehlerhafter Daten und Erweiterung IDAT + MDAT
FA1.4	Objekt-Sperrungen	Objekte können gesperrt werden für weitere Zugriffe.	x			Recht des Patienten auf Sperrung von ihm erfasster Daten
FA1.5	Objekt-Löschung	Objekte können gelöscht werden.		x		Recht des Patienten auf Löschung von ihm erfasster Daten (abhängig vom Konzept)
FA1.6	Objekt-Historie	Zugriffe auf Objekte müssen lückenlos protokolliert werden.	x			Auskunftsrecht des Patienten
FA1.7	Konstante Historie	Die Historie darf nicht veränderbar sein.	x			Vertrauensbildende Maßnahme gegenüber Kostenträger (valide Daten)
FA2	Bereich Daten					
FA2.1	Objekt-Kategorie	Objekte können einem Datentyp zugeordnet werden.	x			Einteilung der abzuspeichernden Daten in MDAT oder IDAT
FA2.2	Datentypen	Es können verschiedene Datentypen zur Auswahl angelegt werden.	x			Vereinfachte Bedienung zur Unterscheidung verschiedener MDAT-Typen
FA2.3	Datentypen-Änderung	Es können vorhandene Datentypen geändert und gelöscht werden.			x	Erweiterung oder Änderung der verwendeten Datentypen im Register (neue MDAT – Typen z.B.)
FA2.4	Objekt-Besitzer	Objekte werden einem Besitzer zugeordnet.	x			Rechteinhaber notwendig zur Verwaltung der gespeicherten Daten
FA2.5	Verschlüsselung	Objekte können verschlüsselt werden.		x		Bei nicht pseudonymisierbaren MDAT-Images und Export der Daten an Kostenträger

FA3		Prozess-Ausführung			
FA3.1	Atomare Funktionen	Funktionen (Änderungen, Erweiterungen, etc.) an Objekten müssen atomar erfolgen.	x		Berücksichtigung bei der Beteiligung mehrerer zugriffsberechtigter Dienstleister auf die im Register gespeicherten Objekte.
FA3.2	Funktion-Definition	Durch einen Administrator können Funktionen definiert werden.		x	Vorgänge können standardisiert den Anwendern zur Verfügung gestellt werden.
FA3.3	Funktion-Überprüfung	Das Ergebnis der ausgeführten Funktionen ist auf Korrektheit überprüfbar.	x		Die vorliegenden Daten müssen zu jedem Zeitpunkt korrekt sein.
FA3.4	Funktions-Historie	Ausgeführte Funktionen werden lückenlos protokolliert.	x		Teilschritte von Funktionen werden protokolliert, um Korrektheit des Ergebnisses nachweisen zu können.
FA4		Fehlerbehandlung			
FA4.1	Fehlerfrei	Gespeicherte Objekte müssen fehlerfrei sein.	x		Fehlerfrei in Bezug auf die beim Dienstleister vorhandenen Daten (Kontrolldaten)
FA4.2	Fehlerhafte Daten	Fehlerhafte Daten werden neu übertragen.	x		Vermeidung der Speicherung teilweiser korrekter Daten
FA4.3	Prüfung	Die Übertragung von Objekten muss auf Korrektheit überprüft werden.	x		Beispielsweise mittels Prüfsummen zur Sicherstellung der Unverfälschtheit
FA4.4	Fehler-Protokoll	Alle Fehler werden protokolliert.	x		Notwendig für Fehlerbehebungen und Kontrolle auf unberechtigte Zugriffsversuche
FA5		Rechteverwaltung			
FA5.1	Rollen-Anlage	Es können verschiedene Rollen zur Nutzung angelegt werden.	x		Zugriffsmöglichkeit durch Dienstleister und Kostenträger
FA5.2	Rollen-Änderung	Die angelegten Rollen können verändert werden (Zugriffsrechte).		x	Bei mehreren Dienstleistern notwendig im Fall einer Verantwortungsänderung
FA5.3	Administrator	Mindestens eine Rolle besitzt administrative Rechte zur Verwaltung der Konten.	x		Administrator mit erweiterten Rechten
FA5.4	Anzahl Konten	Je nach Rolle können mehrere Konten existieren.		x	Beteiligung mehrerer Dienstleister und Kostenträger ist möglich
FA5.5	Zugehörigkeit	Ein Konto kann mehrere Rollen besitzen.		x	Gegebenenfalls Dienstleister mit einigen administrativen Rechten
FA5.6	Zuweisung	Bei Anlage eines Kontos muss eine Rolle zugewiesen werden.	x		Vermeidung nicht autorisierter Zugriffe durch unbedingte Rollenzuweisung bei einer Kontoeinrichtung

FA6		Qualität				
FA6.1	Prüfung	Die Qualität der eingegebenen Daten werden durch das System überprüft.	x			Qualitätskontrollen der im Register hinterlegten Daten (Qualitätsmanagement)
FA6.2	Qualitätsrichtlinien	Für gespeicherte Objekte sind qualitative Richtlinien definierbar.		x		Anpassungsmöglichkeiten der automatischen Qualitätskontrolle
FA6.3	Protokollierung	Die Überprüfung der Qualität kann durch die Protokollierungsfunktion unterstützt werden.			x	Durch den Administrator können Protokollierungsdaten zur Qualitätskontrolle zur Verfügung gestellt werden.

8.4.2 Nichtfunktionale Anforderungen

Nr..	Bezeichner	Beschreibung	Priorität			Referenz
			MUSS	SOLL	KANN	
NFA1		Sicherheit				
NFA1.1	Erreichbarkeit	Das System darf nicht öffentlich zugänglich sein.	x			Sicherheitskriterium zur Risiko-Minimierung unautorisierter Zugriffsversuchen
NFA1.2	Authentifizierung	Nur autorisierten Benutzern ist der Zugriff gestattet.	x			Sensible Daten dürfen nur von autorisierten Anwendern eingesehen werden
NFA1.3	Zugangssicherung	Die Authentifizierung sollte in einem zweistufigen Verfahren erfolgen.		x		Erhöhte Sicherheit der korrekten Authentifizierung
NFA1.4	Manipulation	Das System ist gegen Manipulationen gesichert (Einschränkung Zugriffsrechte)	x			Schutz der sensiblen Daten
NFA1.4	Zugriffs-Historie	Alle Zugriffe und Zugriffsversuche müssen protokolliert werden.	x			Risiko-Minimierung unautorisierter Zugriffe
NFA2		Zuverlässigkeit				
NFA2.1	Verfügbarkeit	Das System ist permanent erreichbar und nutzbar.		x		Vermeidung längerfristiger Ausfallzeiten, notwendig bei permanenter Datenübertragung
NFA2.2	Backup	Das System verwendet Techniken zur regelmäßigen Datensicherung.	x			Sicherung gegenüber technischen und anderen Fehlern
NFA2.3	Ausfall-Szenario	Diverse Ausfall-Szenarien werden berücksichtigt und Lösungen zur kompletten Wiederherstellung entwickelt.	x			Differenzierung der Maßnahmen anhand einer Risiko-Klassifizierung

NFA3		Anwenderfreundlichkeit				
NFA3.1	Oberfläche	Das System bietet Konfigurationsmöglichkeiten zur spezifischen Anpassung von Benutzeroberflächen.		x		Optimierte Anwendungsmöglichkeiten bei verschiedenen Anwendern
NFA3.2	Kompatibilität	Die Oberfläche zur Anwendung des Systems lässt sich mit verschiedenen Betriebssystemen anwenden.		x		Verbesserte Integration in vorhandene Strukturen bei Dienstleister und Kostenträger
NFA3.3	Demo-Bereich	Zu Trainings- und Testzwecken gibt es einen Demobereich mit Dummy-Daten, der gefahrlos genutzt werden kann.			x	Für Schulungs- und Testzwecke
NFA3.4	Hilfe	Zu den einzelnen Bereichen des Systems stehen Hilfe-Informationen zur Verfügung.	x			Verbesserte Anwendung und Fehlerreduzierung für Anwender mit seltenen Zugriffen
NFA3.5	Verzögerungen	Aufwendige Aktionen und Verzögerungen des Systems bei der Verarbeitung werden dem Anwender mitgeteilt.	x			Informationen aufgrund der externen Speicherung und möglichen Verzögerungen bei ausgeführten Aktionen
NFA4		Effizienz				
NFA4.1	Reaktion	Eingaben des Benutzers werden in angemessener Zeit verarbeitet.	x			Abhängig von konkreten Systementwürfen können die Zeiten präzise definiert werden
NFA5		Schnittstellen				
NFA5.1	System-Interface	Das System wird über ein eigenes Interface für den Anwender verfügbar gemacht	x			Die Interface-Umsetzung verbessert die Anwendung des Systems in vorhandenen Systemen
NFA5.2	Stapelverarbeitung	Daten können mit einer Stapelverarbeitungsfunktion an das System übermittelt werden.			x	Die Objekte können gebündelt an das Register übertragen werden, um die Übermittlungen teilweise zu automatisieren
NFA5.3	Export	Zum Export der Daten nach einer Anfrage existiert ein eigenes Interface.	x			Für die Kostenträger wird ein eigenes Interface benötigt, welches neben der Such- und Ergebnis-Darstellung Optionen zum Export anbietet

9 SOLL – Modell eines Telemedizin – Registers

In diesem Kapitel werden einzelne Prozessbereiche zur Anwendung des Telemedizinregisters detailliert beschrieben, die mit den Erkenntnissen der vorherigen Kapitel entwickelt werden. Aufgrund der notwendigen Berücksichtigung unterschiedlichster Strukturen, welche bei telemedizinischen Dienstleistern erwartungsgemäß vorliegen, sind die Prozessmodelle allgemein formuliert und integrieren die Datenmodelle aus dem vorherigen Kapitel.

Der komplette Prozess zur Speicherung und Verwaltung der Daten im Telemedizinregister ist inhaltlich in sieben Teilprozesse gegliedert, welche teilweise aufeinander aufbauen.

Nach der Beschreibung der einzelnen Prozessbereiche erfolgt mittels eines realen Beispiels die Überprüfung und Analyse der vorgestellten Modelle.

9.1 Struktur der Funktionsbereiche

Zur Erstellung des Anforderungskatalogs für ein Telemedizinregister sind die einzelnen Abläufe und Prozesse gegliedert in:

- I. Auswahl der Daten beim Dienstleister**
- II. Aufbereitung der Daten für das Register**
- III. Übermittlung der Daten an das Register**
- IV. Speicherung der Daten im Register**
- V. Änderung von Daten im Register**
- VI. Verarbeitung von Anfragen der Kostenträger**
- VII. Übermittlung der angefragten Daten**

Diese Bereiche werden separat betrachtet und dazugehörige Prozessmodelle in einer Grafik dargestellt. Zusammen mit den rechtlichen Grundlagen werden Prozessabläufe und gegebenenfalls dazugehörige Datenmodelle entworfen, in welche Standards des IHE, vor allem dem XDS.b – Profil, miteingearbeitet werden können.

Basierend auf der Auflistung der verschiedenen Akteure im XDS.b – Profil (siehe Kapitel 7.4.1) ist die Einteilung für das Telemedizinregister und die drei Positionen Dienstleister, Telemedizinregister und Kostenträger folgendermaßen:

Der **Dienstleister** entspricht den Akteuren:

- Patient Identity Source (PID Source)
- Patient Identifier Cross-Reference Consumer (PIX Consumer)
- Provider Information Source (PVI Source)
- Provider Information Consumer (PVI Consumer)
- Document Source
- Image Document Source
- Time Client

Seitens des telemedizinischen Dienstleisters werden Informationen zu den Patienten-Daten und Provider-Daten an das Register übermittelt (PID Source, PVI Source) und sind für weitere Aktionen aus dem Register abrufbar (PIX Consumer, PVI Consumer). Die Hauptaufgabe besteht in der Übermittlung der Dokumente, die im Telemedizinregister verwaltet werden (Document Source, Image Document Source). Bei einer Beteiligung mehrerer telemedizinischer Dienstleister ist die Anzahl der jeweiligen Sources und Consumer dementsprechend erweitert. Gegebenenfalls ist bei einem einzelnen Dienstleister die Anzahl der Akteure reduziert, falls keine verwaltenden Instanzen zu Provider-Informationen erfasst werden müssen.

Im **Telemedizinregister** sind folgende Akteure abgebildet:

- Patient Identifier Cross-Reference Manager (PIX Manager)
- Document Repository
- Document Registry
- Patient Demographics Supplier
- Provider Information Directory (PVI Directory)
- Time Server
- Audit Repository

Das Telemedizinregister übernimmt die Verwaltung der eingestellten Informationen zu den Patienten und Provider (PIX Manager, PVI Directory). Neben den verschiedenen Document Repositories und einer zentralen Document Registry ist mit dem Audit Repo-

sitory eine Funktion zur Protokollierung der Zugriffe vorgesehen. Die Anzahl der Document Repositories kann vorab anhand der Unterscheidung eingesetzter Dokumenten-Typen bestimmt werden: eine Struktur, bei der für jeden Datentyp ein definiertes Document Repository zum Einsatz kommt, vereinfacht nachträgliche Anpassungen in der Verwaltung der einzelnen Datentypen. So wäre beispielsweise ein Document Repository für pseudonymisierte PDF-Dateien und ein Document Repository für nicht pseudonymisierbare, aber verschlüsselte PDF-Dateien in der Aufbereitung und der Datenweitergabe an die Kostenträger sinnvoll. Somit können die Aufbereitungsprozesse für Kostenträger individuell an die in der Document Repository gespeicherten Daten angepasst werden.

Der **Kostenträger** wird die Funktion folgender Akteure enthalten:

- Patient Identifier Cross-Reference Consumer
- Document Consumer
- Image Document Consumer
- Patient Demographics Consumer
- Provider Information Consumer

Durch den Kostenträger werden nur lesende Aktionen durchgeführt, wodurch die Consumer-Akteure diesem zuzuordnen sind. Diese bieten neben der Möglichkeit eines kompletten Exports der Datensätze im Register auch Optionen zur gezielten Suche nach abgespeicherten Therapiedaten. Je nach hinterlegter Datenmenge ist auch eine Suche nach demographischen Werten möglich, falls zum Beispiel bestimmte Altersgruppen das Ziel einer Analyse seitens des Kostenträgers darstellen.

9.2 Prozess – Modelle

Bei allen aufgeführten Teilprozessen ab der dritten Prozesskategorie sind die Vorgänge zur Protokollierung und Speicherung der AUDIT-Informationen automatisch durchzuführen, damit jede Aktion im Telemedizinregister erfasst und durch den Administrator eingesehen werden kann. Die Aufbereitung der Daten beim Dienstleister muss nicht zwingend für die Anwendung des Telemedizinregisters protokolliert werden.

9.2.1 I Auswahl der Daten beim Dienstleister

Die vor der Erstellung des Telemedizinregisters ausgewählten Daten beim Dienstleister sind durch zwei maßgebliche Faktoren bestimmt:

1. Auswahl der Daten durch Absprache mit beteiligten Kostenträgern

Damit sollen die Datenmengen der beim Dienstleister erfassten Therapiedaten auf die für den Kostenträger interessanten Datenmengen reduziert werden, welches Vorteile beim Umfang der Verarbeitung der zu übertragenden Datenmengen ins Register aufweist und zusätzlich den Grundsatz des Datenschutzes "Datensparsamkeit und Datenvermeidung" berücksichtigt.

2. Auswahl der Daten durch Reduzierung der Verwaltungsdaten

Ein telemedizinischer Dienstleister wird zusätzlich zu den Therapiedaten, welche aus der IDAT-Menge und MDAT-Menge bestehen, für eigene verwaltende Vorgänge Verwaltungsdaten erfassen und speichern, die aber nicht Gegenstand der Datenmenge im Telemedizinregister sein sollen. Dabei sind dies vor allem Daten zur betriebswirtschaftlichen Durchführung von Prozessen wie beispielsweise allgemeine Abrechnungsprozesse zwischen Dienstleister und Kostenträger und Daten zur Kundenverwaltung.

Diese Datenauswahl kann durch Erfahrungswerte bei vergleichbaren Projekten unterstützt werden, wird aber erwartungsgemäß eine umfangreiche Kommunikation zwischen Dienstleister und Kostenträger benötigen.

9.2.2 II Aufbereitung der Daten für das Register

Prozess Therapiedaten aufteilen

Das Ziel dieses Prozesses ist die Teilung und Markierung vorgegebener Datenmengen in die zwei unterschiedlichen Bereiche von IDAT und MDAT.

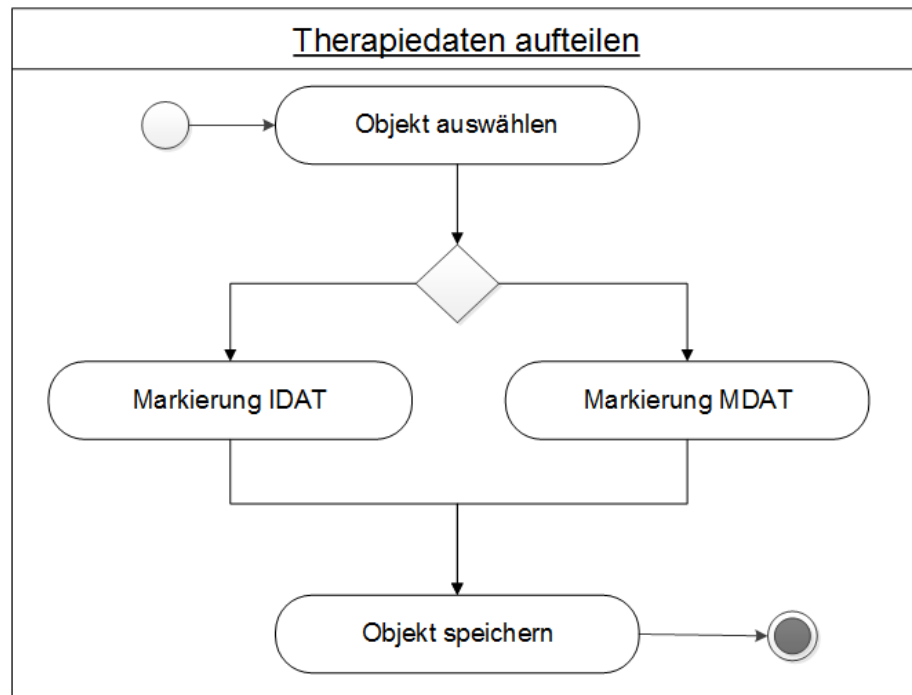


Abbildung 42, Prozess Therapiedaten aufteilen

Anfangs wird ein Objekt ausgewählt, welches zusammenhängende Informationen einer Behandlung umfasst und als allgemeiner Bezeichner für ein Datenobjekt dient, vergleichbar mit einer Patientenakte. Diese besteht überwiegend aus verschiedenen medizinischen Informationen und Dokumenten (MDAT) und den persönlichen Informationen (IDAT). Neben der Trennung des Objekts besteht auch die Möglichkeit, dass ein Objekt nur einer Kategorie zugewiesen wird. Nach der Teilung wird durch die Markierung eine Kategorisierung vorgenommen und anschließend als überarbeitetes Objekt wieder gespeichert. Eine Möglichkeit zur Objekterweiterung durch die Markierung wäre beispielsweise eine Speicherung in einem Container-ähnlichen Dateiformat (XML), bei dem zusätzlich zu den ursprünglichen Daten weitere Informationen angegeben werden können.

Prozess IDAT pseudonymisieren

Die Pseudonymisierung ist aus datenschutzrechtlicher Sicht der wichtigste Schritt in der Datenaufbereitung vor der Übermittlung an das Telemedizinregister.

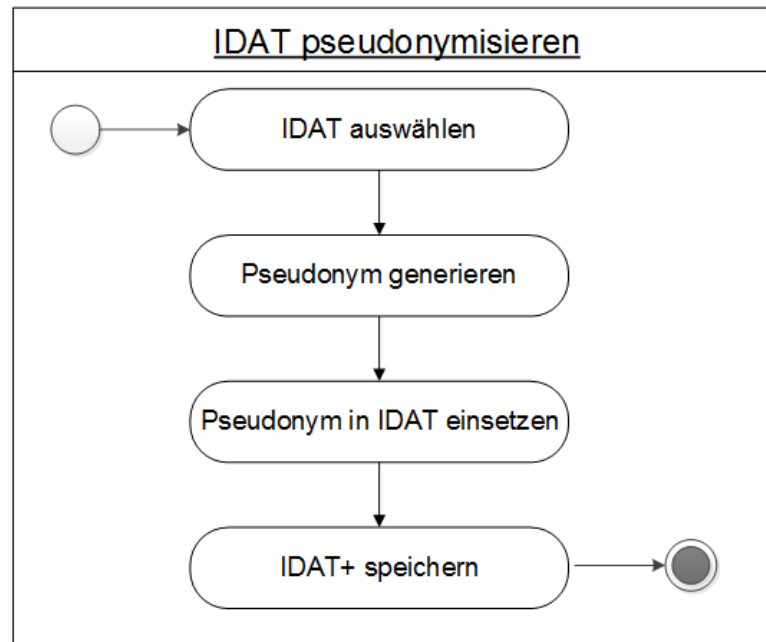


Abbildung 43, Prozess IDAT pseudonymisieren

Um die Gefahren eines unautorisierten Zugriffs auf die Datenmenge im Register auf das Minimum zu reduzieren, müssen alle identifizierenden Daten verändert werden, welche eine Re-Identifizierung ermöglichen. Die in einem Objekt markierten IDAT-Bereiche werden mit einem erzeugten Pseudonym ersetzt und als neues Objekt mit der Markierung IDAT+ abgespeichert.

Ein Unterschied bei den Pseudonymisierungsverfahren ergibt sich in der Anzahl der beteiligten Dienstleister und den damit verbundenen Stellen, die eine Pseudonymisierung durchführen wollen. Bezogen auf das Anwendungsszenario C (siehe Kapitel 7.2, Module für Anwendungsszenarien) ist die Koordinierung der verwendeten Pseudonymisierungsstellen einfacher zu handhaben, wenn nur ein Dienstleister beteiligt ist. Bei diesem kann in einem System eine Funktion zur Generierung von Pseudonymen eingesetzt werden, welche die Pseudonyme erzeugt und die Verwaltung mitsamt Protokollierung übernimmt. Sind zu einem Objekt schon pseudonymisierte Daten (PID) vorhanden, können diese im System ermittelt und verwendet werden.

Sind hingegen mehrere Dienstleister beteiligt, ist ein separates Pseudonymisierungssystem bei einem Treuhänder zu empfehlen, welches zentral alle Anfragen nach Pseudonymen verwaltet und den Dienstleistern die Verwendung einheitlicher IDAT+ Daten ermöglicht. Diese Variante würde auch für die Anwendung bei einem einzelnen Dienst-

leister eine erhöhte Sicherheit durch die informationelle Gewaltenteilung ergeben, wobei sich jedoch Nachteile durch die umfangreichere Verwaltung und den zusätzlichen Übermittlungsprozess zur Pseudonymgenerierung ergeben.

Prozess MDAT+ erzeugen

In diesem Prozess sind analog zur Erzeugung der IDAT+ Menge die Vorgänge zur Pseudonymisierung von MDAT-Informationen beschrieben.

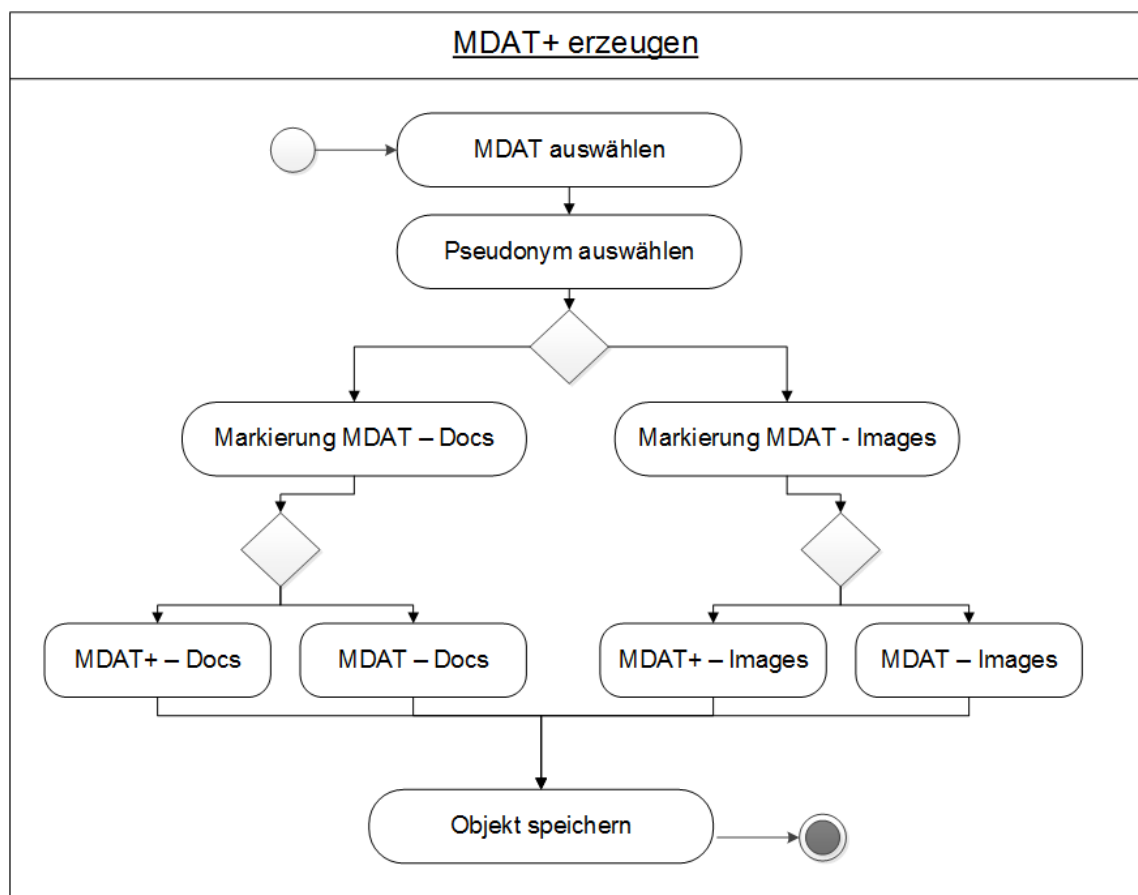


Abbildung 44, Prozess MDAT+ erzeugen

In medizinischen Dokumenten sind oftmals auch persönliche Daten hinterlegt, die eine Re-Identifizierung der Patienten ermöglichen. Beispielsweise ist in Text-Dokumenten bei der Befundung der Name des Patienten vorhanden. Eine Änderung und Anpassung der persönlichen Daten an das bei der IDAT+ - Menge verwendete Pseudonym ist wünschenswert, um auch bei der MDAT Datenmenge die Risiken und Gefahren eines unkontrollierten Datenzugriffs zu mindern. Problematisch dabei kann die Suche und

Änderungen von Information in bildbasierten Dokumenten sein, beispielsweise in Röntgen-Aufnahmen. Eine dortige Änderung wird unverhältnismäßig viele Arbeitsschritte und Ressourcen benötigen. Daher ist alternativ eine Verschlüsselung der nicht veränderten Dokumente mit identifizierenden Daten umzusetzen.

In der oben aufgeführten Grafik sind am Ende des Prozesses vier unterschiedliche Kategorien von medizinischen Daten vorhanden. Einerseits die mit Pseudonymen angepassten Daten von MDAT+ - Docs und MDAT+ - Images, die für eine Registerübertragung aufbereitet sind. Andererseits die zwei Kategorien MDAT – Docs und MDAT – Images, bei denen Pseudonyme nicht integrierbar sind. Diese Daten müssen vor der Übertragung in das Register zusätzlich aufbereitet werden, um keine realen Daten im Register zu verwenden beziehungsweise zur Verfügung zu stellen.

Daher sollten bei der Aufbereitung der Daten für das Register die verwendeten Dokument-Arten auf Möglichkeiten zur Pseudonymisierung untersucht werden und unter Berücksichtigung des notwendigen Aufwands so weit wie möglich mit den generierten Pseudonymen geändert werden. Sind Informationen vorhanden, die eine Re-Identifizierung ermöglichen, aber nicht verändert werden können, müssen Alternativen zur Sicherung der Informationen wie zum Beispiel Verschlüsselung der Dokumente in Erwägung gezogen werden.

Prozess Metadaten generieren

Zur Verwaltung der Daten im Register sind zusätzliche Metadaten der abgespeicherten Dokumente und Informationen notwendig, welche mit diesem Prozess generiert werden. Alternativ kann dieser Prozess auch vor der Pseudonymisierung eingesetzt werden, wobei dann die Integration der generierten Pseudonyme in die Metadaten mitberücksichtigt werden muss.

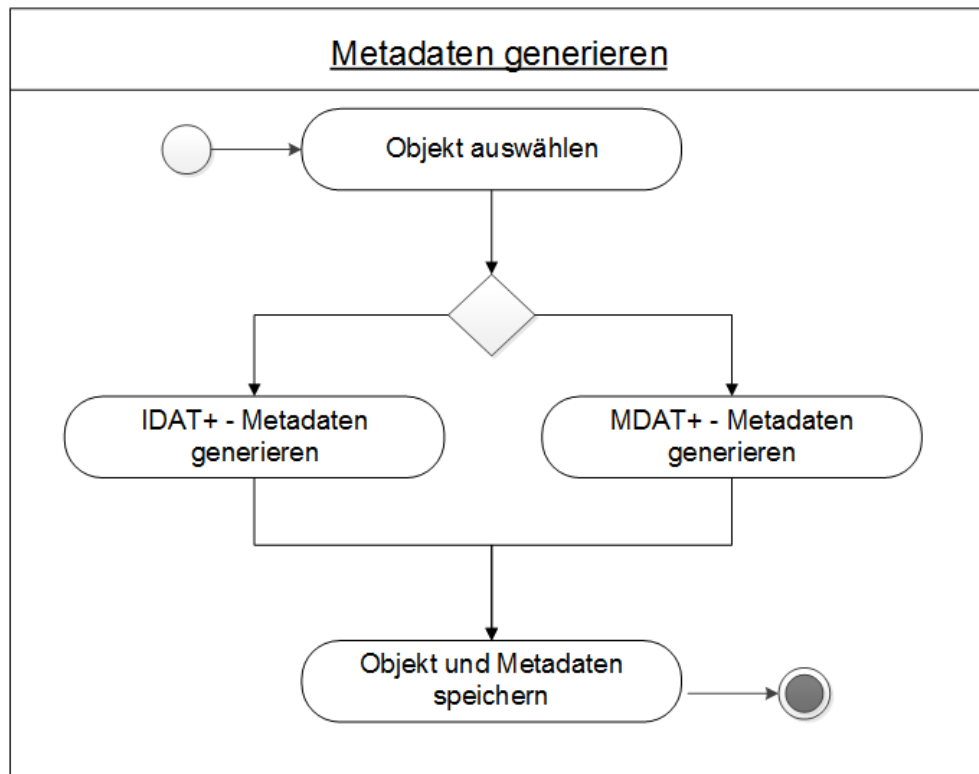


Abbildung 45, Prozess Metadaten generieren

In dem Telemedizinregister wird zusätzlich zu den abgespeicherten Dokumenten eine zentrale Document Registry eingesetzt, in der alle Informationen zu vorhandenen Dokumenten mittels Metadaten gespeichert und verwaltet werden. Dokumente werden zusammen mit Metadaten an das Telemedizinregister übermittelt und dort in dem jeweiligen Document Repository gespeichert. Die Metadaten werden anschließend an die Document Registry gesendet und gespeichert.

Daher sind für die im Register zu hinterlegenden Objekte passende Metadaten zu erzeugen, sofern dieser Prozess automatisierbar ist. Aus den Objekten, die schon Pseudonyme enthalten, sind Informationen zu Dokumenten-Typ, Rechteinhaber, etc. auslesbar und in Metadaten zu speichern. Dieser Prozess ist vor allem für die unterschiedlichen medizinischen Daten elementar, da speicherplatz-intensive Bilddaten nicht als komplette Datei, sondern nur durch die Metadaten zu den Objekten an das Register übermittelt werden. Daher müssen in den Metadaten alle Informationen eingebettet sein, welche für die Verwaltung und besonders für die Suche nach Dokumenten benötigt werden.

9.2.3 III Übermittlung der Daten an das Register

Prozess Userkonten erstellen

Administrativ werden im Telemedizinregister Userkonten erstellt und verwaltet, mit denen der Zugriff auf das Telemedizinregister geregelt ist.

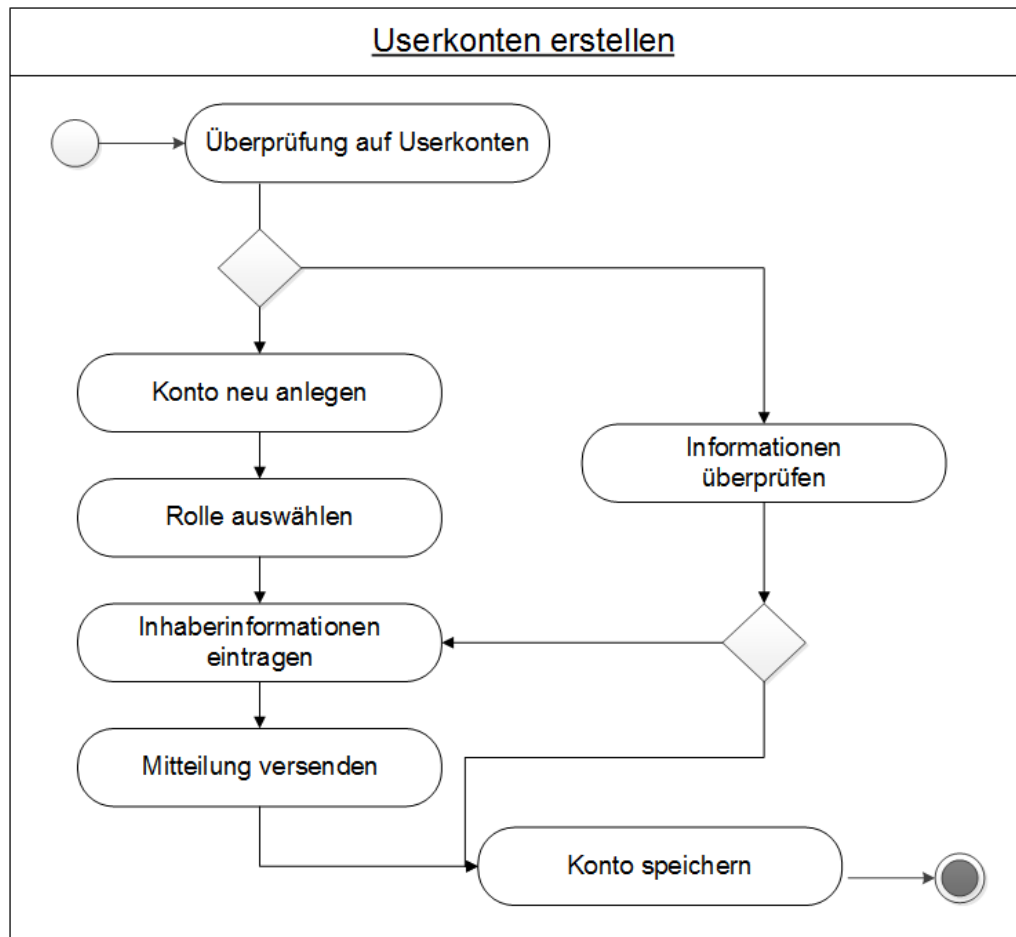


Abbildung 46, Prozess Userkonten erstellen

Durch einen Administrator werden im Telemedizinregister Userkonten angelegt und verwaltet. Die Userkonten bekommen eine oder gegebenenfalls mehrere Rollen zugewiesen, welche den Zugriff auf die im Register gespeicherten Daten reglementieren. Als Abstufung der Zugriffsrechte sind mindestens drei verschiedene Rollen vorhergesehen:

- **Administrator**
volle administrative Rechte für die Verwaltung der Benutzerkonten und verwaltungstechnische Vorgänge im Register, zum Beispiel Fehlerbehebungen, Ein-

richtung von Erweiterungen, Definition von ausführbaren Funktionen und Auswertung der Protokollierungen

- **Dienstleister**

besitzt Anwenderfunktionalität für die Speicherung, Erweiterung, Änderung und gegebenenfalls Löschung / Sperrung der im Register gespeicherten Daten

- **Kostenträger**

vergleichsweise geringe Rechte, da seitens des Kostenträgers nur die Einsicht und der Empfang von Register-Daten zur Analyse vorgesehen ist

Der Prozess der Kontoerstellung prüft bei einem Antrag auf Kontoeinrichtung im ersten Schritt, ob ein Konto mit den einzutragenden Daten vorhanden ist. Wenn dies zutrifft, werden die im Register hinterlegten Daten mit den neu übermittelten Daten verglichen und gegebenenfalls Aktualisierungen vorgenommen.

Sollte noch kein Konto bestehen, wird ein neues Konto mit den übermittelten Informationen eingerichtet und standardmäßig deaktiviert. Dieses sichert das Register gegen unautorisierte Zugriffe, indem eine Aktivierung des Kontos verbunden mit einer Rollenzuweisung erst nach Prüfung der Antragsdaten erfolgt. Automatisierte Neu-Anlagen von Konten, die sofortige Zugriffsrechte auf Daten im Register besitzen, sind unbedingt zu vermeiden.

Am Ende der Kontoerstellung wird der Kontoinhaber über die Einrichtung beziehungsweise Aktualisierung der Kontodaten mit einer Mitteilung informiert und nach einer weiteren Legitimation das Konto freigeschaltet.

Prozess Sichere Verbindung herstellen

Der Prozess zur Herstellung einer sicheren Verbindung vor der Übermittlung von Daten an das Register sollte mit mehreren Autorisierungs-Schritten verbunden sein, um größere Sicherheit gegenüber Attacken auf das System zu bieten.

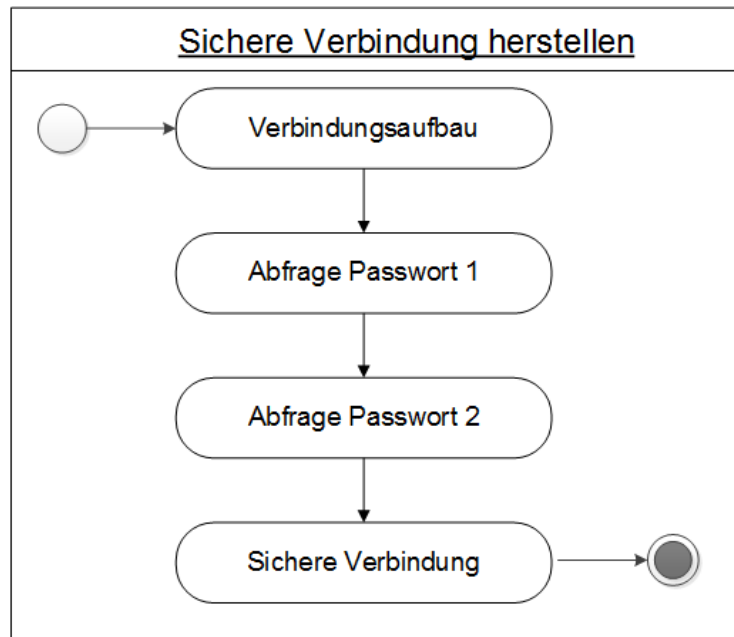


Abbildung 47, Prozess Sichere Verbindung herstellen

Die Übermittlung der Daten an das Telemedizinregister wird aufgrund der Distanz zwischen Dienstleister und Telemedizinregister eine Übertragung über das Internet berücksichtigen müssen. Daher sind Mechanismen einzuplanen, welche einerseits die sichere Übertragung der Daten über das Internet gewährleisten, beispielsweise VPN-Verbindungen mit einer optionalen zusätzlichen Verschlüsselung der übertragenen Daten und andererseits die Verbindungsherstellung gegenüber nicht autorisierten Zugriffen absichern. [63] [64]

Daher sollte bei der Verbindungsherstellung die Abfrage zur Authentizität in mehreren Schritten erfolgen, da dieses Vorgehen die Gefahr eines unerlaubten Zugriffs minimiert. Neben der üblichen Autorisierung mittels Kennung und Passwort kann ein zusätzliches Passwort-Verfahren integriert werden, bei dem stetig ändernde Passwörter verwendet werden, beispielsweise mittels Hardware-Token. Alternativ würde sich auch die Einbindung personengebundener Zertifizierungs-Verfahren anbieten, wie dies zum Beispiel mit einem Heilbehandler-Ausweis möglich wäre. [58]

Die Erreichbarkeit des Registers darf nur über geschlossene Netzwerke erfolgen, welches mittels VPN-Techniken erreicht werden kann. Keinesfalls darf das Register über eine ungesicherte öffentlich zugängliche Schnittstelle erreichbar sein.

Prozess Übermittlung der Daten

Der Prozess zur Übertragung der ausgewählten Daten an das Register überprüft die versendeten Dateien auf Korrektheit und Vollständigkeit.

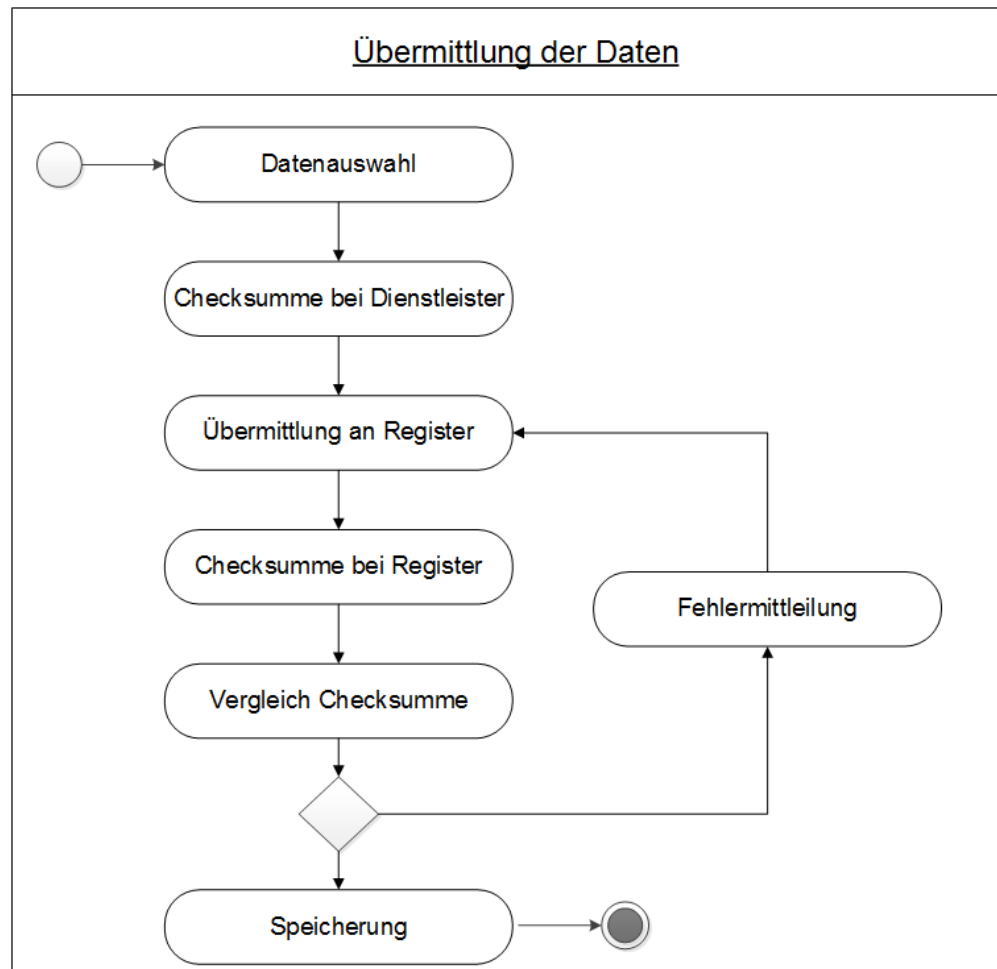


Abbildung 48, Prozess Übermittlung der Daten

Die übermittelten Daten sollen vor der Speicherung im Register auf die Korrektheit und Vollständigkeit überprüft werden, um Manipulationen oder Fehler bei der Übertragung zu beheben. Dafür werden vor dem Versand bei dem Dienstleister Checksummen beziehungsweise Prüfsummen errechnet, welche nach der Übertragung im Telemedizinregister mit der empfangenen Datenmenge erneut berechnet und anschließend zu vergleichen sind. Treten bei diesem Vergleich Differenzen auf, so sind die Dateien erneut zu übermitteln und mit einer Mitteilung an den Dienstleister erfolgt ein Fehlerhinweis.

9.2.4 IV Speicherung der Daten im Register

Prozess Speicherung der Daten

Nach der erfolgreichen Übertragung der Daten an das Telemedizinregister erfolgt der Prozess der Speicherung der Datensätze.

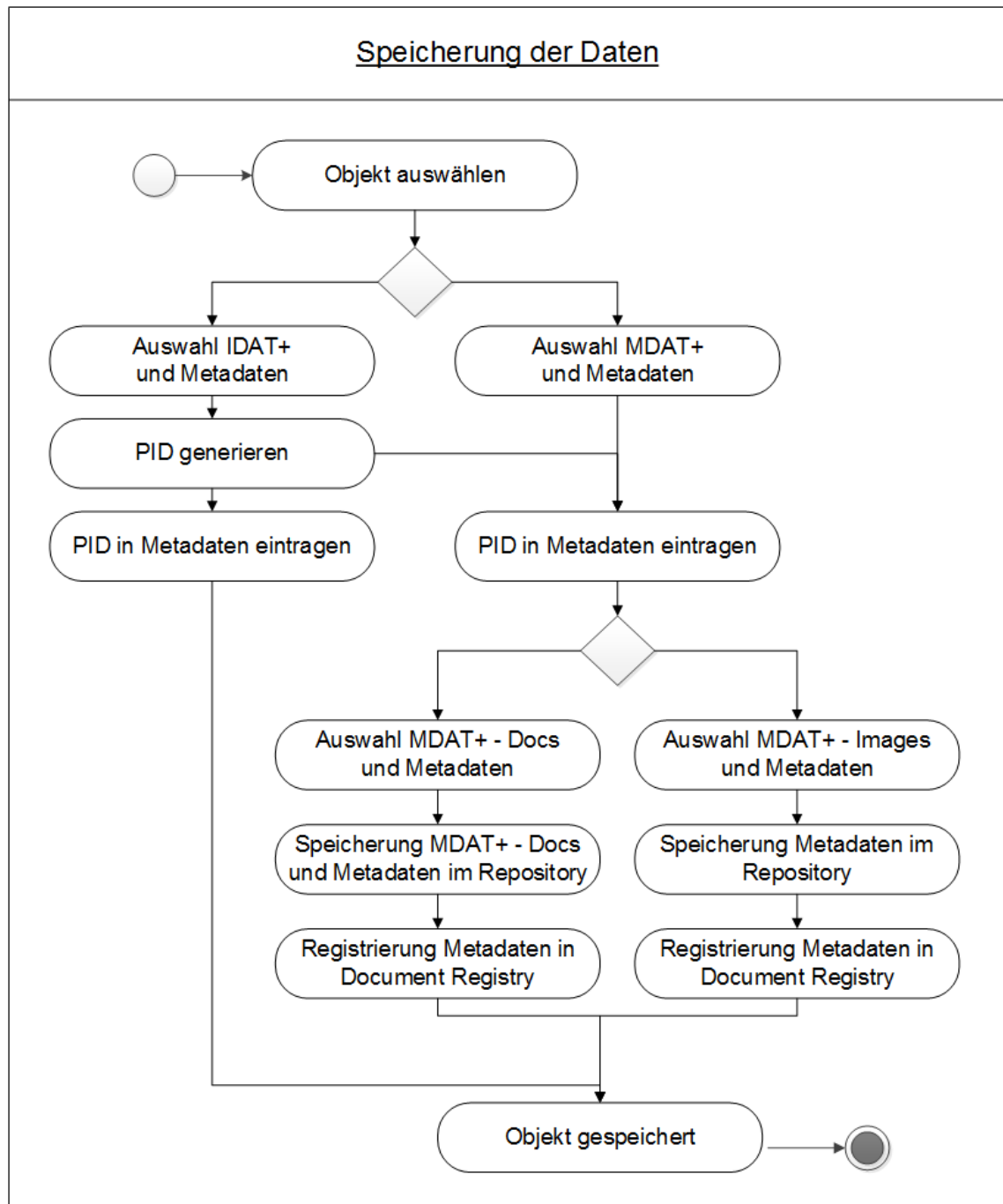


Abbildung 49, Prozess Speicherung der Daten

In diesem Prozess werden die erstmaligen Speichervorgänge von Patientendaten und Informationen zu der Behandlung betrachtet. Die Bearbeitung von bereits vorhandenen

Patientendatensätzen, beispielsweise Änderungen und Ergänzungen, werden in separaten Prozessen beschreiben.

Im ersten Schritt wird ein Objekt ausgewählt und gegebenenfalls eine Teilung der Daten in IDAT+ und MDAT+ mit den dazugehörigen Metadaten vorgenommen. Mittels der IDAT+ - Daten erfolgt eine Identifizierung des ausgewählten Objekts. An dieser Stelle bietet sich optional eine weitere verwaltende Einheit im Register an, in der Identifikationsdaten zentral verwaltet werden können, den PIX Manager (Patient Identifier Cross-Reference Manager). Sollten bei der Datenspeicherung im Register mehrere (unabhängige) Dienstleister beteiligt sein, welche zusammen an einer telemedizinischen Behandlung agieren und keine einheitliche ID für Patienten verwenden, lässt sich die Zusammenführung der unterschiedlichen lokalen IDs durch eine einheitliche Master ID verwirklichen. In dem oben aufgeführten Prozess-Modell ist diese optionale Einheit angenommen und bietet zentrale Dienste zur Verwaltung von Patienten-IDs. Hierbei sei nochmals auf den Unterschied zwischen den beim Dienstleister oder Treuhänder generierten Pseudonym und der im Register verwendeten ID hingewiesen: das Pseudonym soll die Verwendung realer Daten im Register verhindern, da Datenverluste oder unautorisierte Datenzugriffe im Register nie auszuschließen sind. Die im Register verwendete ID hingegen zielt auf eine zentrale Verwaltung unterschiedlich verwendeter Personendaten (Pseudonyme) hin, um eine verbesserte Zusammenführung der Datensätze zu ermöglichen.

Ist zu einem Objekt die ID generiert beziehungsweise passende ID ermittelt, werden die zu speichernden Dokumente mit der ID versehen, beispielsweise durch eine Erweiterung der Metadaten. Anschließend erfolgt analog zum XDS.b-Profil die unterschiedliche Vorgehensweise bei der Speicherung und Registrierung der MDAT+ - Daten. Sind die MDAT+ - Daten vergleichsweise gering im Speicherplatzbedarf, sind diese der Kategorie MDAT+ - Docs zugeordnet und als komplette Kopie im Register speicherbar. Der Dienstleister übernimmt dabei im Register die Funktion Document Source. Bei Speicherplatz-intensiven MDAT+ - Typen erfolgt eine Markierung als MDAT+ - Image. Diese nicht ausschließlich bildbasierten Dokumente werden nicht komplett als Kopie an das Register übertragen, sondern mit Hilfe der Metadaten im Telemedizinregister verwaltet. Diese Metadaten enthalten Verweise auf den Speicherort der MDAT+ - Images beim jeweiligen Dienstleister. Dieser ist somit gleichzeitig neben einer Document Source auch eine Image Document Source.

Die Prozessschritte ab dem Document Repository sind für die verschiedenen MDAT+ - Daten vergleichbar: die Metadaten der MDAT+ - Documents und MDAT+ - Images werden an die Document Registry gesendet und dort für die Registrierung der Dokumente ausgewertet.

Die Speicherung der IDAT+ - Daten wird im PIX – Manager vorgenommen, der als zentrale Speicherstelle die Identifikationsdaten verwaltet. Je nach Datenmenge können die IDAT+ - Daten komplett im PIX – Manager organisiert oder in einer zusätzlichen Document Repository für IDAT+ - Daten gespeichert werden. Eine Registrierung in der zentralen Document Registry wäre aber aufgrund des PIX – Managers nicht notwendig.

Folgende Transaktionen aus dem XDS.b – Profil können für die Speicherung von Objekten eingesetzt werden:

- **Einheitliche PID erzeugen (ITI – 44)**

Der Dienstleister veranlasst vor der Speicherung der übermittelten Daten im Register die Generierung einer PID, welche im Register für diese Daten und gegebenenfalls weitere Ergänzungen verwendet wird

- **Ein Dokument an Repository senden und in Registry eintragen (ITI – 41)**

Für die Speicherung der Dokumente im Register können mehrere Document Repositories eingesetzt werden, um zum Beispiel eine Trennung unterschiedlicher Dokumenten-Typen umzusetzen.

- **Mehrere Dokumente an Repository senden und in Registry eintragen (ITI – 41)**

Erweiternd zur vorherigen Transaktion ist auch die gebündelte Übertragung mehrerer Dokumente an ein Repository vorhergesehen.

- **Bild-Dokumente in der Registry anmelden (RAD – 68)**

Diese Transaktion veranlasst die Anmeldung der MDAT+ - Images in der zentralen Document Registry.

9.2.5 V Änderungen von Daten im Register

Prozess Datensätze ergänzen

In diesem Prozess wird die Ergänzung von Datensätzen beziehungsweise Objekten dargestellt, die bereits im Telemedizinregister vorhanden sind.

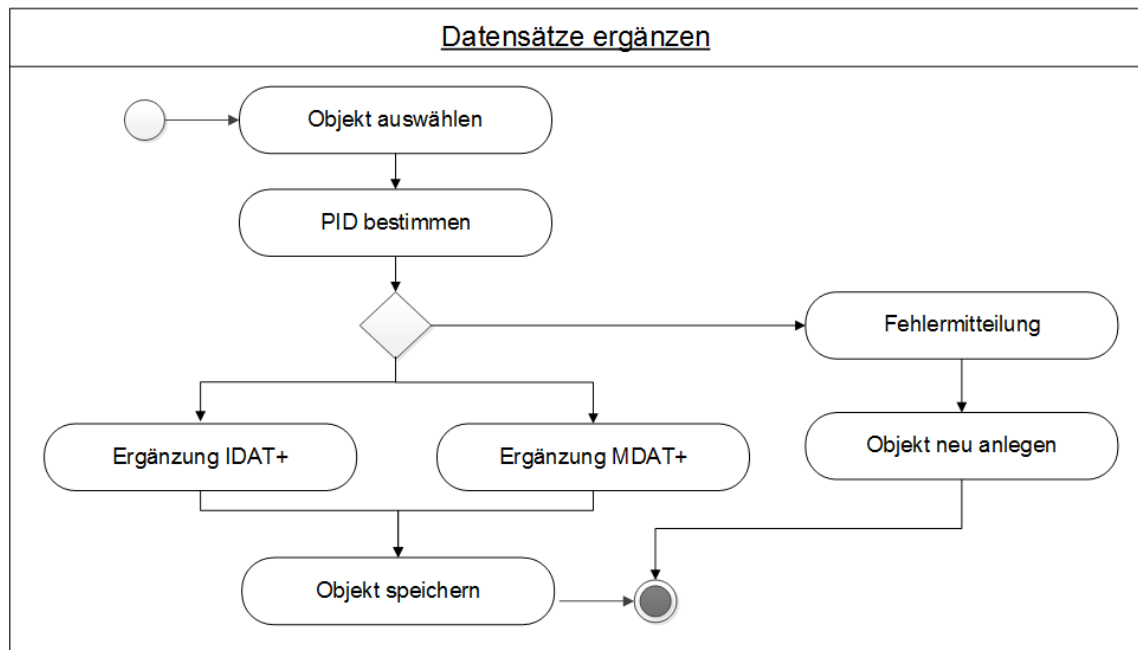


Abbildung 50, Prozess Datensätze ergänzen

Zu einem ausgewählten Objekt wird die im Register verwendete PID bestimmt, die bei der erstmaligen Speicherung von Daten des Patienten angelegt wurde. Daraufhin werden die übermittelten Daten nach IDAT+ und MDAT+ getrennt und die zu ändernden Informationen in den passenden Speicherstellen ergänzt.

Sollte gegebenenfalls bei einer gebündelten Übermittlung von mehreren zu ändernden Objekten zu einem noch kein Eintrag im Register vorhanden sein, muss dieser Fall separat behandelt werden, indem eine Fehlermitteilung an den einstellenden Dienstleister erfolgt und darauf der Prozess zur Neuanlage eines Objektes durchgeführt wird.

Prozess Datensätze ändern

Prozessbeschreibung zur Änderung bereits vorhandener Objekte, welches beispielsweise bei Fehlerkorrekturen notwendig ist.

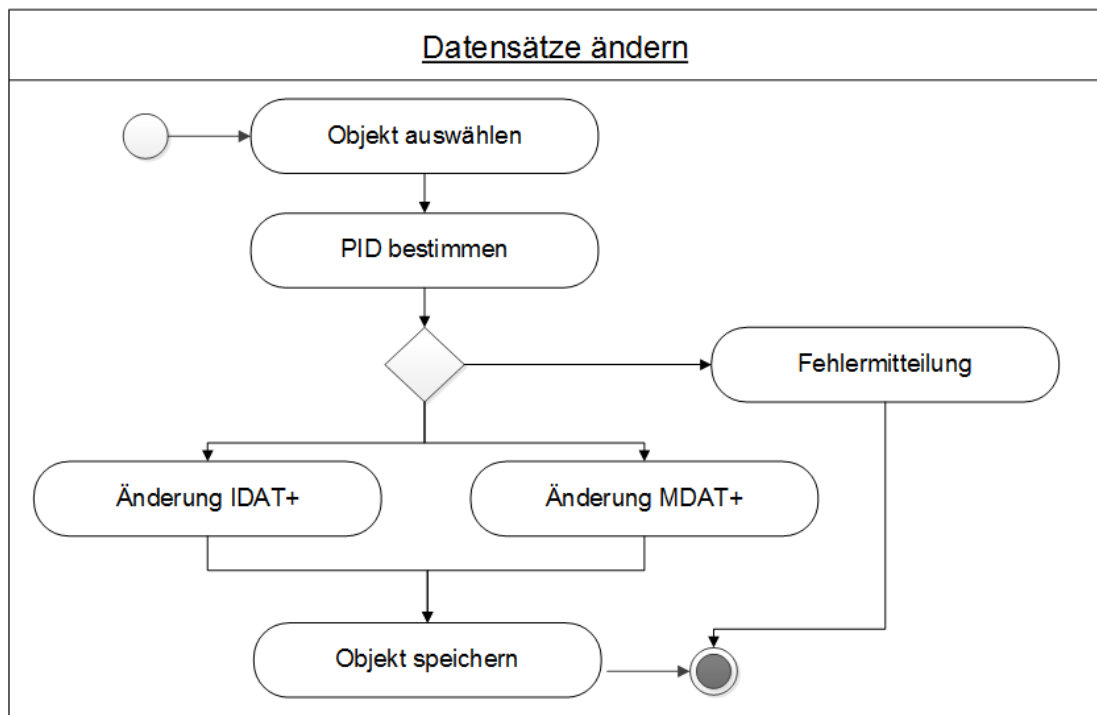


Abbildung 51, Prozess Datensätze ändern

Die Änderung von Objekten ist vergleichbar mit der Ergänzung von Objekten, wobei im Fall einer unbekanntem PID keine automatische Neuanlage erfolgt. Wird durch den Dienstleister eine Änderung eines Objektes beabsichtigt, welches nicht im Telemedizinregister vorhanden ist oder nicht zugeordnet werden kann, muss dieser Prozess abgebrochen werden.

Die Änderungen der IDAT+ und MDAT+ - Informationen werden getrennt voneinander durchgeführt. Der Vorgang der Änderung von Informationen benötigt gegebenenfalls erweiterte Rechte und wäre durch die administrative Rolle umsetzbar. Dieses würde die Authentizität der im Telemedizinregister hinterlegten Daten unterstützen, falls Änderungen nur mit erweiterten Rechten durchführbar sind. Alternativ wäre die zeitliche oder Objekt-basierte Erweiterung der Rechte des Dienstleisters eine Option, falls Änderungen nicht mit den Standard-Rechten des Dienstleisters durchgeführt werden können.

Prozess Datensätze löschen

Mit diesem Prozess werden Objekte gelöscht oder gesperrt, abhängig von der definierten Handhabung im Register.

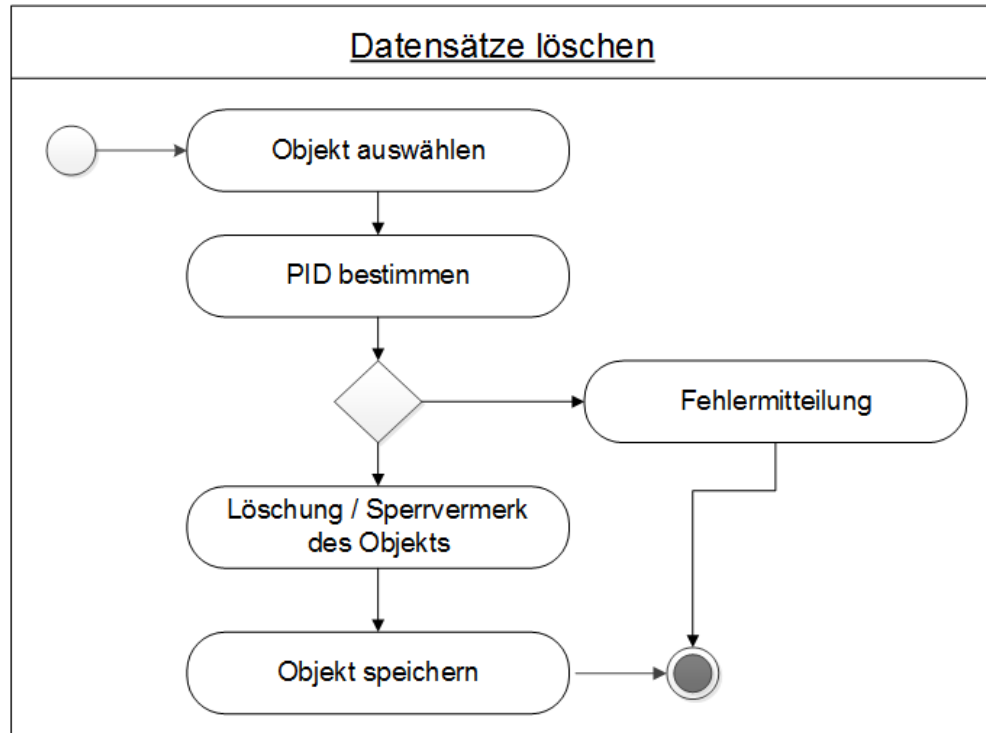


Abbildung 52, Prozess Datensätze löschen

Abhängig von der vorab definierten Richtlinie zum Umgang mit Objekten, die nicht mehr im Telemedizinregister zur weiteren Verarbeitung zur Verfügung stehen sollen, können Objekte komplett gelöscht oder zumindest mit einem Sperrvermerk versehen werden.

Im Umgang mit medizinischen Daten ist oftmals aufgrund gesetzlicher Vorschriften eine Löschung nicht möglich, falls beispielsweise die Dokumentationspflicht eines Arztes diesem Interesse entgegenpricht. Daher sollte vorab bei der Register-Erstellung festgelegt werden, welche Datentypen rückstandlos entfernt oder für weitere Zugriffe gesperrt werden sollen. Diese Aktionen sollten ebenfalls nur mit erweiterten Rechten durchführbar sein und durch eine administrative Freigabe gesichert werden.

9.2.6 VI Verarbeitung von Anfragen der Kostenträger

Prozess Anfrage verarbeiten

Die Anfrage durch einen Kostenträger an das Register zum Erhalt von gespeicherten Daten wird in diesem Prozess dargestellt.

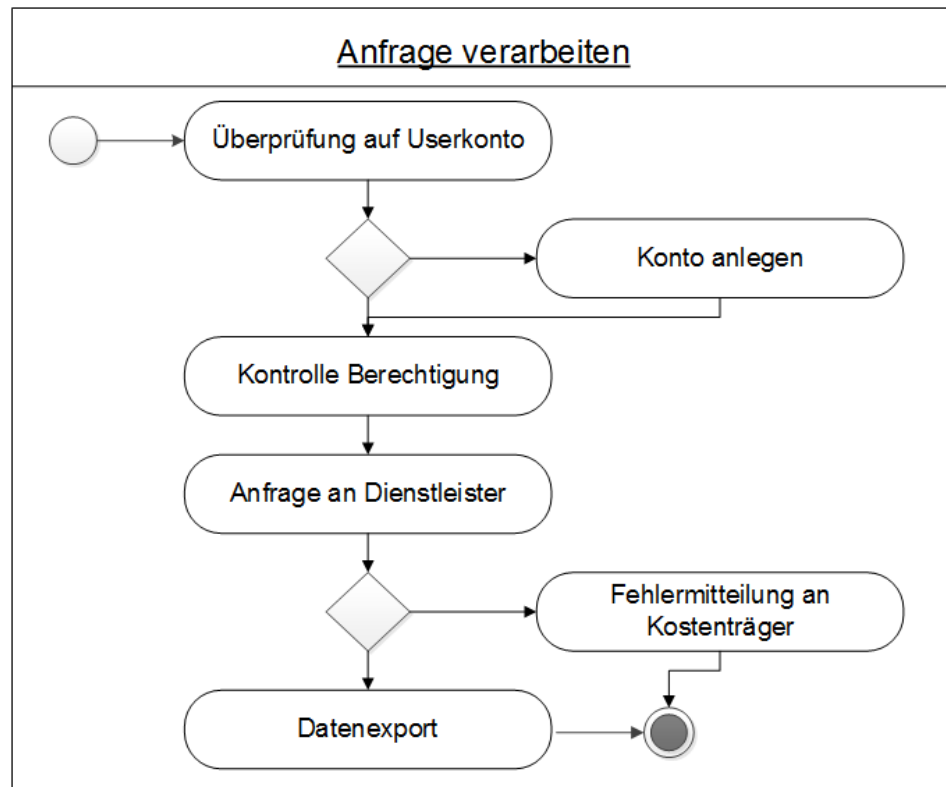


Abbildung 53, Prozess Anfrage verarbeiten

Ist ein Kostenträger an den im Telemedizinregister hinterlegten Daten interessiert, muss für diesen ein Konto eingerichtet werden, welches lesende Rechte auf die Daten besitzt. Am Anfang der Bearbeitungsschritte einer an das Register gesendeten Anfrage wird überprüft, ob ein Konto zum anfragenden Kostenträger existiert. Nach der Kontrolle auf Berechtigungen, welche in den gespeicherten Datenobjekten den Zugriff auf die Daten reglementieren, wird zusätzlich der verantwortliche telemedizinische Dienstleister über die Anfrage informiert.

Sollte dieser einverstanden sein, kann der weitere Ablauf zum Export der Daten an den Kostenträger durchgeführt werden. Optional kann aber der Dienstleister, der für die Speicherung und Verwaltung der Daten im Register verantwortlich ist, eine Anfrage ablehnen, welches eine Fehlermitteilung an den Kostenträger auslöst.

9.2.7 VII Übermittlung der angefragten Daten

Prozess Export von Daten

In diesem Prozess wird der Ablauf des Datenexports an einen berechtigten Kostenträger beschrieben.

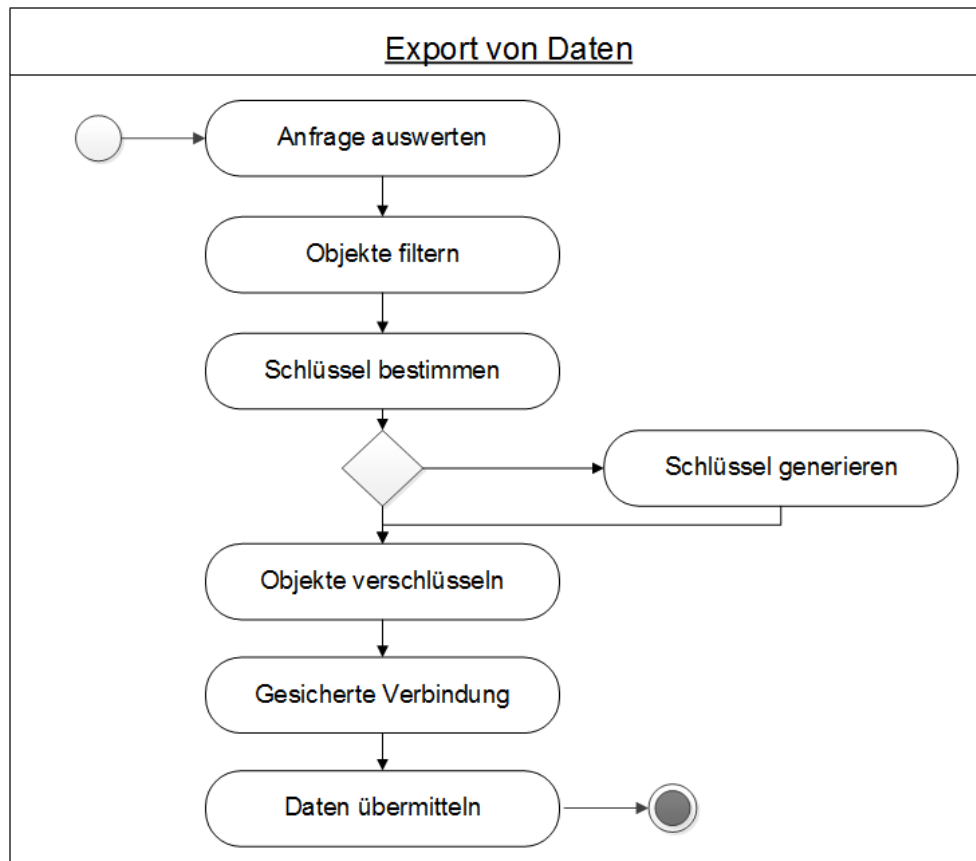


Abbildung 54, Prozess Export von Daten

Wurde eine Anfrage eines Kostenträgers durch den verantwortlichen Dienstleister positiv gewertet, erfolgt der Datenexport aus dem Register an den Kostenträger. Dabei stehen unterschiedliche Methoden zur Verfügung:

- **Kompletter Datenexport**

Kostenträger analysieren selbstständig eine Datenmenge anhand individueller Parameter und benötigen dafür gegebenenfalls alle zur Verfügung stehenden Datensätze zu einer Behandlung. Daher sollte das Register eine Export-Funktion anbieten, die alle registrierten medizinischen Dokumente mitsamt den IDAT+ - Daten zum Export aufbereitet.

- **Selektiver Datenexport**

Des Weiteren soll ein selektiver Datenexport möglich sein, bei dem anhand der Anfrage-Parameter eine Filterung der Daten durchgeführt werden kann. Dabei ist wie beim kompletten Datenexport die Funktion des Kostenträgers bei der Export-Aufbereitung passiv. Als Reaktion auf eine erfolgreiche Anfrage werden dem Kostenträger nach Auswahl und Aufbereitung der Daten durch das Register die Export-Daten zugesendet.

- **Selektive Suche und anschließender Export**

Vergleichbar mit der Speicherung und weiteren Verwaltung der Daten durch den Dienstleister über ein Interface ist eine spezielle Oberfläche mit Suchfunktionen und Lesemöglichkeiten für die Kostenträger möglich. Dabei erhält dieser Zugangsinformationen und sucht selbstständig nach gewünschten Daten im Register. Mittels einer Funktion zum Export beziehungsweise lesendem Zugriff auf die Daten kann der Kostenträger gezielt nach Objekten suchen. Dabei muss diesem eine Zuordnung mit verwendeten Pseudonymen und realen Identifikationsdaten zur Verfügung gestellt werden.

Unabhängig von der eingesetzten Methode sollen die Daten vor der Übermittlung an den Kostenträger zusätzlich verschlüsselt werden, um die Risiken und Gefahren eines missbräuchlichen Datenzugriffs zu verringern und auch den Kostenträger mit in die Verantwortung im Umgang mit den ausgehändigten Daten zu nehmen. Dazu bietet sich beispielsweise eine symmetrische Verschlüsselung an.

Der Prozess der Übertragung zwischen Telemedizinregister und Kostenträger ist vergleichbar mit der Übertragung vom Dienstleister zum Register. Eine sichere Verbindung (beispielsweise VPN) ist zwingend notwendig.

9.3 Praxisbezogene Überprüfung des SOLL – Modells am Beispiel der MVB GmbH

Die in den vorherigen Abschnitten aufgezeigten Prozessmodelle und strukturellen Entwürfe des Telemedizinregisters und den damit verbundenen Datenverarbeitungsschritten werden folgend exemplarisch mit simulierten Datenmengen überprüft.

Dabei dienen Datenstrukturen und Betriebsstrukturen der medizinischen Videobeobachtung MVB GmbH als Ausgangsbasis für die Beispiele, welche für die einzelnen Prozess-Schritte verwendet werden. Die angenommene Datenbasis ist aus Gründen der Wettbewerbssituation und durch Einhaltung von Betriebsgeheimnissen auf ein Modell reduziert, welches bedenkenlos veröffentlicht werden kann. Die exemplarische Vorgehensweise dient neben der Überprüfung auf die Prozess-Funktionalität auch der Offenlegung weiterer Potentialfelder in der Entwicklung des Telemedizinregisters.

Die medizinische Videobeobachtung MVB GmbH [65] ist als Dienstleister in der ambulanten Therapie für Parkinsonpatienten tätig und wurde im Jahr 2002 in Koblenz gegründet. Die Therapie ist eine Form der integrierten Versorgung und somit vertragsabhängig von an der Behandlung beteiligten Kostenträger.

Vorbereitend zur Überprüfung der Prozesse erfolgt vorab eine Vorstellung der vorhandenen System-Strukturen und verwendeten Datentypen:

Beteiligte Positionen:

- MVB GmbH: telemedizinischer Dienstleister
- Patienten
- Hausärzte der Patienten
- Neurologen der Patienten
- Konsil-Kliniken beziehungsweise Konsil-Neurologen
- Kostenträger

9.3.1 Bestandsanalyse der MVB GmbH

Folgende Abbildung zeigt die Struktur der ambulanten Videotherapie bei Parkinson-Patienten:

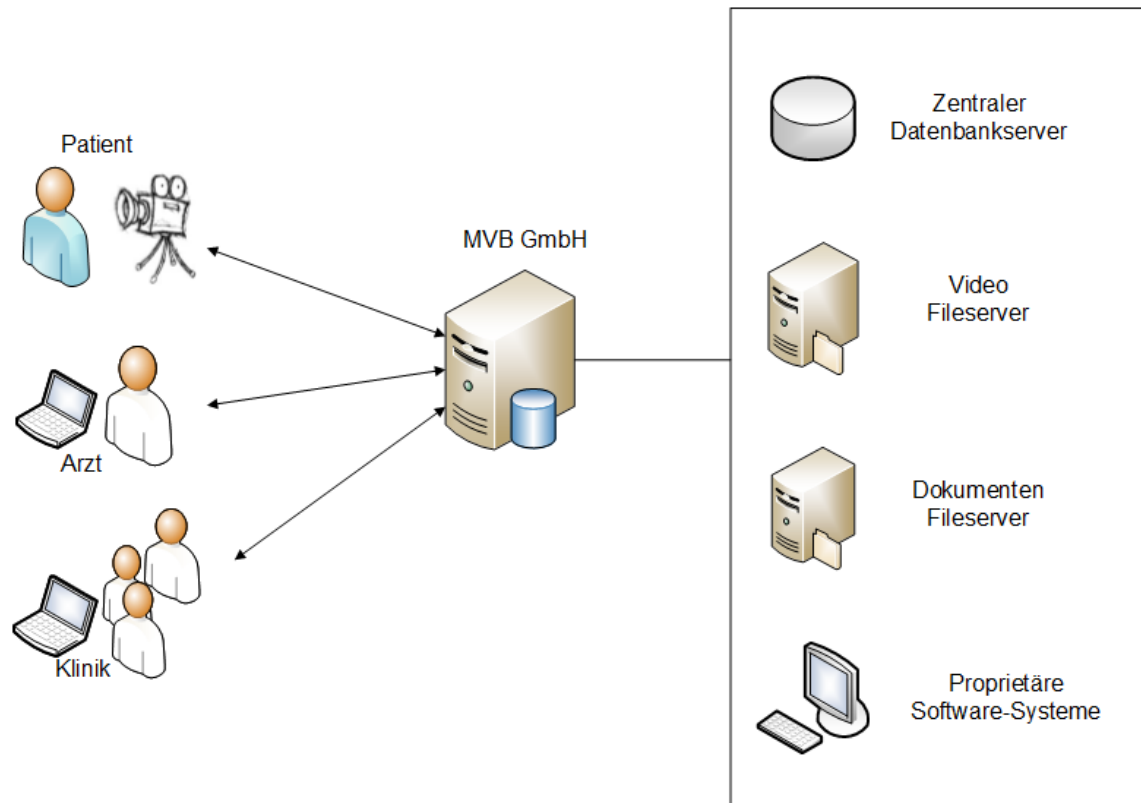


Abbildung 55, Systemmodell MVB GmbH

Die Funktionsweise der Therapie - vereinfacht dargestellt – basiert auf den beim Patienten vorgenommenen Videoaufnahmen, welche dieser selbstständig über einen Zeitraum von 30 Tagen rund um die Uhr an einem speziell dafür entwickelten Gerät auslösen kann. Diese Aufnahmen werden verschlüsselt an die MVB GmbH übermittelt und an die beteiligten Ärzte und gegebenenfalls Konsil-Kliniken weitergereicht. Durch diese erfolgt die Begutachtung der Aufnahmen und eine gezielte Anpassung der Medikationspläne mittels einer proprietären Software. Die geänderten Medikationspläne werden anschließend beim Patienten vor Ort ausgedruckt.

Somit sind bei der MVB GmbH als telemedizinischer Dienstleister unterschiedlichste Datentypen vorhanden, welche darüber hinaus in verschiedenen Systemen gespeichert

und verwaltet werden. Zur besseren Darstellungsweise sind die Systeme in vier Kategorien eingeteilt:

- **Datenbank**

Die Datenbank dient als zentrales Verwaltungsinstrument in der Durchführung der Behandlung. In dieser werden überwiegend die Daten der Therapie erfasst und durch die Anbindung der proprietären Software-Systeme die Daten für weitere Funktionalitäten (Medikationsplan-Änderung, Erstellung Druck-Dokument) vorgehalten. Die verwendeten Datensätze enthalten sowohl IDAT - als auch MDAT – Informationen.

- **Video Fileserver**

Die einzelnen Videoaufnahmen werden bei der MVB GmbH zwischengespeichert und durch Synchronisierungs-Funktionen den beteiligten Ärzten zur Verfügung gestellt. Diese Datentypen sind vergleichsweise speicherintensiv und daher der Kategorie MDAT – Images zuzuordnen.

- **Dokumenten Fileserver**

Zusätzlich werden bei der Therapie Dokumente benötigt, die beispielsweise Befunde, Arztbriefe oder vergleichbare Datentypen sind. Beispielsweise sind im Rahmen der Anmeldung der Therapie einige digitale Dokumente und die Einwilligungserklärung des Patienten notwendig, um die Therapie vorbereiten zu können. Diese meist im PDF-Format vorliegenden Dokumente werden auf dem Dokumenten Fileserver gespeichert. Die vorliegenden Datentypen sind somit überwiegend als MDAT einzusortieren, enthalten aber auch zusätzliche IDAT – Informationen.

- **Proprietäre Software-Systeme**

Alle weiteren eingesetzten Systeme, die vor allem im Bereich der betriebswirtschaftlichen Anwendung eingesetzt werden, können diesem Sektor zugeteilt werden. Dabei liegen vor allem Verwaltungsdaten vor, welche nicht in das Telemedizinregister übertragen werden sollen.

In der Datenbank sind auf das Beispiel bezogen folgende Schemata vorhanden:

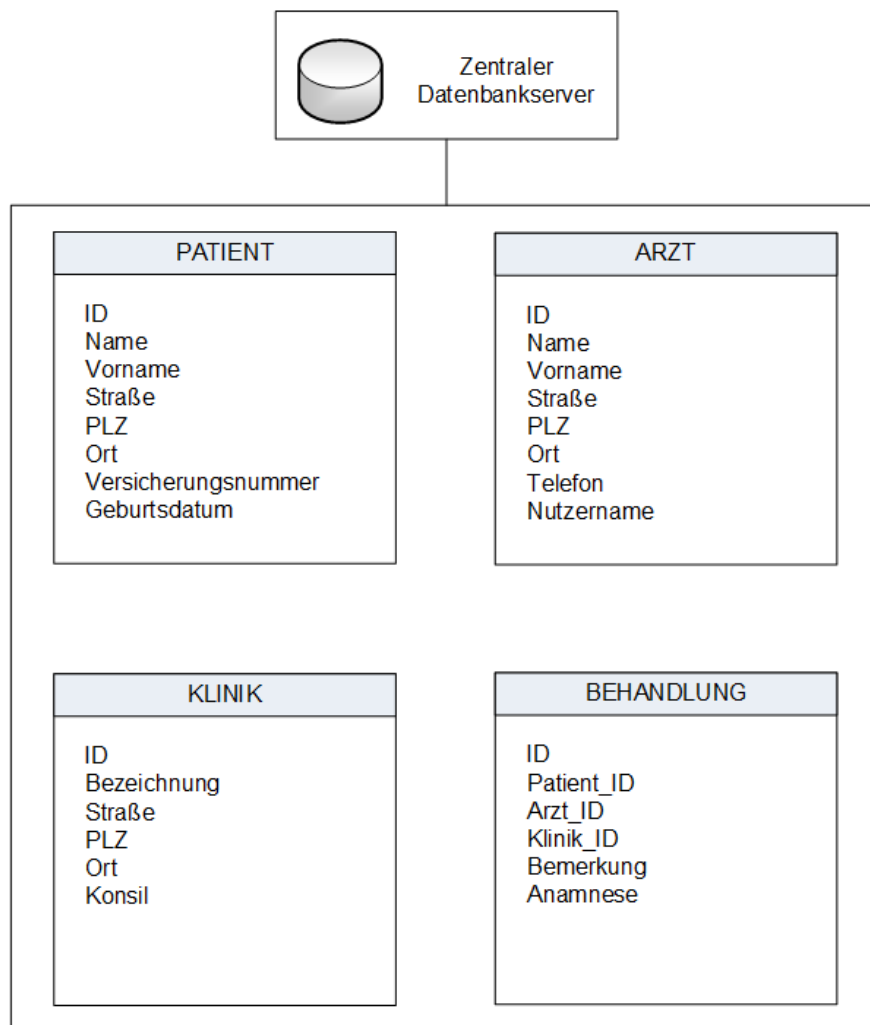


Abbildung 56, Datenbankschema MVB GmbH

Diese Darstellung ist gegenüber dem realen Vorbild deutlich reduziert bei der Auflistung der vorhandenen Datenbank-Strukturen und dient lediglich der Betrachtung verschiedener Vorgänge zur Aufbereitung vorhandener Datensätze.

Die Abschnitte PATIENT, ARZT und KLINIK sind aufgrund der enthaltenen Informationen der Kategorie IDAT zuzuordnen und müssen vor der Übermittlung an das Register veränderte Werte durch eine Pseudonymisierung erhalten. Der Abschnitt BEHANDLUNG hingegen enthält neben den Verweisen auf die beteiligten Personen und Einrichtungen auch Daten der MDAT – Kategorie.

9.3.2 Überprüfung der einzelnen Prozessabschnitte

In diesem Abschnitt werden die einzelnen Prozessabschnitte mit der vorgegeben Bestandssituation überprüft.

I. Auswahl der Daten beim Dienstleister

Bei diesem Szenario wird angenommen, dass in Absprache mit den beteiligten Kostenträgern alle zur Therapie vorhandenen medizinischen Daten an das Telemedizinregister übertragen werden. Die einzige Ausnahme stellen dabei die Daten zur eigenen betriebswirtschaftlichen Durchführung der Prozesse dar, die keine unmittelbare medizinische Relevanz aufweisen, beispielsweise Systeme zur Kunden- und Kontaktpflege.

II. Aufbereitung der Daten für das Register

Der erste Schritt in der Aufbereitung ist durch den Prozess **Therapiedaten aufteilen** definiert:

Als Objekte sind in diesem Beispiele vorhanden:

- Datensätze aus der Datenbank
- Video-Dateien vom Video Fileserver
- Verschiedene Dokument-Typen vom Dokumenten Fileserver

Die Objekte aus der Datenbank sind folgendermaßen markiert:

- PATIENT: Markierung als IDAT
- ARZT: Markierung als IDAT
- KLINIK: Markierung als IDAT
- BEHANDLUNG: Markierung als MDAT

Videos, die von einem Patienten aufgenommen werden, sind als MDAT einzustufen. Eine Datei-Bezeichnung kann identifizierende Daten enthalten, ist aber vergleichsweise einfach zu ändern. Videos stellen aber einen besonderen Fall bei der Bewertung dar: eine Weitergabe der Videos zu Zwecken der medizinischen Forschung ist nicht realisierbar, da die Person durch die Videoaufnahmen identifiziert indirekt werden könnten.

Da Änderungen der Videodaten nicht ohne größeren Aufwand zu bewerkstelligen sind, muss eine zusätzliche Verschlüsselung vor der eventuellen Weitergabe an die Kostenträger erfolgen. Eine detaillierte Betrachtung erfolgt bei der Einstufung der verschiedenen MDAT-Unterkategorien.

Die vorhandenen Text-Dokumente in diesem Beispiel sind auf änderungsfähige Text-Dokumente (Mail, Word, Excel, etc.) und nicht änderungsfähige Text-Dokumente (PDF, geschützte Word-Dateien, etc.) begrenzt. Die änderungsfähigen Text-Dokumente werden nach Inhalt in IDAT oder MDAT klassifiziert. Zu erwarten sind einzelne identifizierende Angaben, beispielsweise im Briefkopf und namentliche Nennungen im Textverlauf und überwiegende medizinische Angaben, die für sich alleine gestellt keine bestimmte Person identifizieren.

Die nicht änderungsfähigen Dokumente sind identisch zu behandeln, werden aber bei der folgenden Unterteilung der IDAT – und MDAT-Unterkategorien eine gesonderte Bearbeitung erfordern. Diese Dokumente müssen mehrstufig aufbereitet werden.

Der folgende Prozess **IDAT pseudonymisieren** verändert alle identifizierenden Daten in den Objekten, die vorher mit IDAT gekennzeichnet wurden. Dies betrifft Objekte, die keine zusätzlichen MDAT – Informationen enthalten.

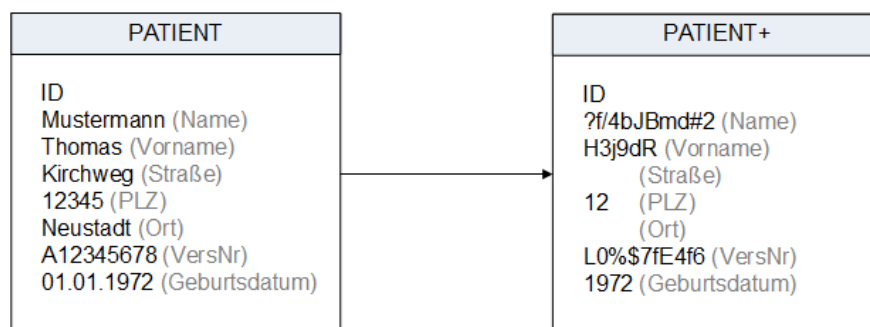


Abbildung 57, Beispiel Pseudonym Datenbank

Die Pseudonymisierung kann auf verschiedene Weisen umgesetzt werden: im obigen Beispiel sind die eindeutigen Faktoren wie Name und Versicherungsnummer mit durch eine Funktion berechnete Zeichenfolgen ersetzt worden. Alternativ wird durch eine Zuordnungsliste, in der reelle Daten und zugehörige Pseudonyme verwaltet werden, eine spätere autorisierte Re-Identifizierung ermöglicht. Daher können weitere Parameter (Straße, Ort) in der IDAT+ - Liste ausgelassen werden.

Demografische Faktoren (Region, Altersgruppen, etc.) lassen sich reduziert in der IDAT+ - Menge abbilden, falls die verringerte Information keine erweiterten Rückschlüsse auf eine Person erlauben. Bezogen auf die oben durchgeführte Variante mit der Angabe der PLZ mit zwei Stellen und dem Geburtsjahr ist die Anzahl der möglichen Personen mit diesen Parametern erwartungsgemäß so umfangreich, dass keine gezielten Re-Identifizierungen damit durchführbar sind. Bei besonders sensiblen Daten ist auch die Reduzierung der Datenmenge auf eine einzelne eindeutige ID möglich, mit der alle personenidentifizierenden Merkmale gebündelt werden.

Das System beziehungsweise Modul, welches die Pseudonyme generiert, sollte eine geringe Quote von doppelten Pseudonym-Erzeugungen aufweisen, die bei der Benutzung von unterschiedlichen Schreibweisen des gleichen Namens auftreten können. "Müller" und "Mueller" sollten bei identischen anderen eindeutig identifizierenden Parametern das gleiche Pseudonym erzeugen beziehungsweise einen Hinweis auf Kontrolle bei bereits durchgeführten Pseudonymisierungsvorgängen liefern.

Mit dem neu generierten Pseudonym können die weiteren Objekte bearbeitet werden, soweit bei den IDAT – Informationen die Änderungen durchführbar sind. In einem Textdokument mit der Anschrift und dem Namen des Patienten sollten nach der Änderung die zuvor berechneten Parameter eingesetzt werden, unter Berücksichtigung eventueller Platzhalter bei den reduzierten Parametern (Straße, Ort).

Der Teilprozess **MDAT+ erzeugen** nimmt eine weitere Unterteilung der zu bearbeitenden MDAT – Menge vor:

Dokumente des Fileservers stellen ein auswählbares Objekt dar. Ein änderungsfähiges Text-Dokument würde zuerst als MDAT – Document markiert und darauf als MDAT+ - Document markiert. Für diesen Übergang müssen einerseits die im medizinischen Dokument enthaltenen IDAT – Daten des Patienten mit dem zuvor generierten Pseudonym ersetzt werden und andererseits auf weitere identifizierende Merkmale (beispielsweise dem Arzt) untersucht und gegebenenfalls erneut verändert werden. Das Ziel nach den Bearbeitungsschritten ist ein Dokument, welches keine identifizierenden Merkmale mehr aufweist und betreffende IDAT-Stellen mit Pseudonymen und Platzhaltern ersetzt wurden. Nicht änderungsfähige Dokumente beziehungsweise Objekte müssen eine spezielle Markierung erhalten und in einem weiteren Prozess für eine Übermittlung an das Register verschlüsselt werden.

Der folgenden Teilprozess **Metadaten generieren** unterstützt die Speicherung und Verarbeitung der Objekte im Telemedizinregister und ist bei der Anwendung der IHE-Standardprofile notwendig. Nach den vorherigen Prozessen existiert die Datenstruktur:

- Pseudonymisierte Datensätze in einer Datenbank
- Video-Dateien vom Video Fileserver
- Geänderte Dokumente mit Pseudonymen auf dem Fileserver
- Verschlüsselte, nicht änderbare Dokumente mit identifizierenden Merkmalen auf dem Fileserver

Die Generierung der Metadaten ist für die Übermittlung der Video-Dateien von besonderer Bedeutung, da nur dessen Metadaten an das Register übermittelt werden. Daher ist auch keine zusätzliche Verschlüsselung der Video-Dokumente für das Telemedizinregister selbst notwendig, da die Veränderung der realen Dateninformationen durch die Verwendung der dazugehörigen Pseudonyme in den Metadaten erfolgen kann. Die Metadaten sollten mit pseudonymisierten Parametern versehen werden und zusätzliche Daten enthalten, welche bei Suchvorgängen und Verarbeitungsprozessen erforderlich sind.

Für jeden einzelnen Objekttyp ist ein separater Vorgang zur Generierung der Metadaten notwendig und bedarf umfangreicher Planungen.

III. Übermittlung der Daten an das Register

Vor der ersten Speicherung der Daten im Register müssen administrative Prozesse durchgeführt werden, indem Zugriffsrollen und Konten angelegt werden. In diesem Beispiel werden vorab Konten für die MVB GmbH und die jeweiligen Kostenträger angelegt. Dabei besitzt die MVB GmbH schreibende Rechte, die für bestimmte Änderungsvorgänge aber noch eine temporäre oder zweckgebundene Berechtigungserweiterung durch den Administrator voraussetzt. Die Kostenträger dürfen Anfragen mit dem Zweck an das Register stellen, gezielte Datensätze zur eigenen Analyse zu erhalten (lesende Rechte). Der Administrator hingegen besitzt die umfangreichsten Rechte und sollte mit einer unabhängigen Position besetzt werden, beispielsweise durch die Vorhaltung des Telemedizinregisters beim medizinischen Dienst der Krankenkassen (MDK) und der Zuweisung der Rolle an einen qualifizierten Mitarbeiter.

Der Prozess **Userkonten erstellen** erfolgt vor der Anwendung des Registers und benötigt identifizierende Daten zur Kontoanlegung. Diese Daten werden neben der Zugriffsberechtigung für die Durchführung der Protokollierung aller Vorgänge im Register benötigt, um zweifelsfrei Aktionen einem Verantwortlichen zuordnen zu können. Diese Protokollierung beschränkt sich aufgrund der Rechteverteilung in diesem Beispiel auf die Erfassung einer Historie.

Mittels der Daten für die Kontenerstellung können auch für den Prozess **Sichere Verbindung herstellen** Zertifikate für die Verbindungsherstellung erzeugt werden, die beispielsweise bei einer VPN-Verbindung eingesetzt werden können. Die Authentifizierung sollte auf jeden Fall zumindest in einem zweistufigen Verfahren erfolgen, bei dem unterschiedliche Mechanismen der Überprüfung eingesetzt werden. Verwendete Passwörter sollten regelmäßig geändert werden.

Die im Register gespeicherten Daten müssen exakt dem Umfang und Inhalt der aufbereiteten Daten beim Dienstleister entsprechen, welches mit dem Teilprozess **Übermittlung der Daten** sichergestellt werden soll. Das eingesetzte System sollte Verfahren zur Prüfung der übermittelten Daten bereitstellen und fehlerhafte Datensätze neu übertragen. Die Daten werden vor der Speicherung im Register gepuffert und erst nach erfolgreicher Überprüfung zur Speicherung der Daten freigegeben.

IV. Speicherung der Daten im Register

Die Struktur des Telemedizinregisters setzt sich aus der beim Dienstleister eingesetzten Struktur und den notwendigen Elementen zur Integration der Standardisierungs-Profile zusammen. Dies ergibt folgenden schematischen Aufbau des Telemedizinregisters bei der Umsetzung dieses Beispiels:

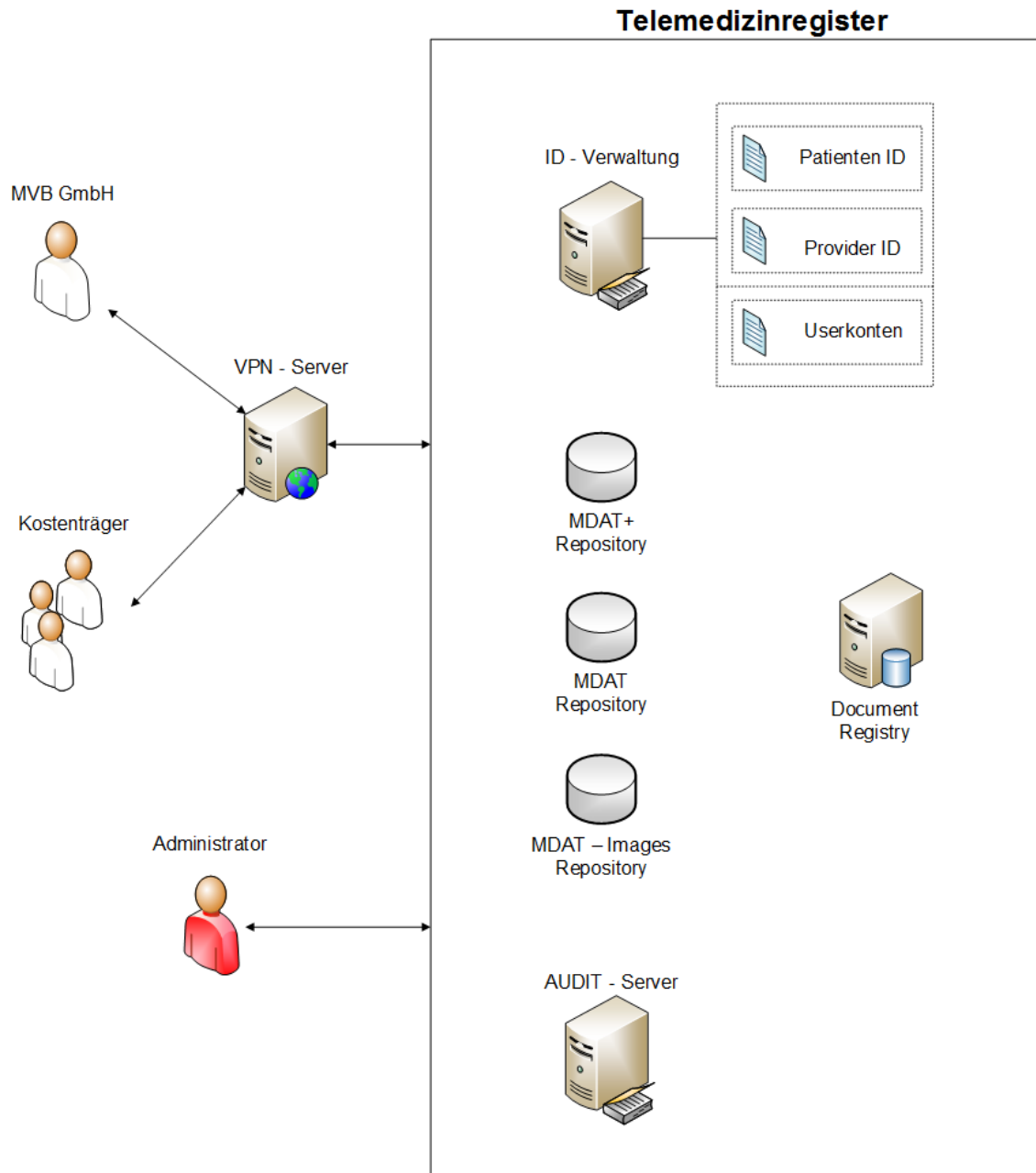


Abbildung 58, Struktur Telemedizinregister für MVB GmbH

Die zu speichernden Objekte werden mit im Register verwendeten IDs ergänzt, die eindeutige Bezeichner für die an den Behandlungen involvierten Patienten, Ärzte, Kliniken und Dienstleister darstellen. Diese Erweiterung bietet zusätzliche Optionen bei den durchführbaren Aktionen im Register, da zum Beispiel nachträgliche Datenergänzungen einfacher zugeordnet werden können.

Die mit IDs versehenen Objekte sind entweder der Kategorie IDAT+, MDAT+ oder MDAT zugeordnet. Die IDAT+ - Objekte werden an den PIX Manager übermittelt. MDAT+ und MDAT – Objekte werden an die entsprechenden Repositories mit den

passenden Transaktionen übermittelt. In diesem Beispiel existiert jeweils ein Document Repository für:

- MDAT+ - Dokumente
- MDAT - Dokumente (verschlüsselt)
- MDAT - Images

Diese sind alle mit der zentralen Document Registry verbunden. Für jedes einzelne Objekt wird eine Protokollierung beziehungsweise Historie im AUDIT-Modul eröffnet, die unter anderem folgende Informationen enthält:

- Objekt-ID
- Durchgeführte Transaktion (zum Beispiel Speicherung)
- Zeitstempel der Transaktion
- Zugeordneter Besitzer
- Gegebenenfalls durchgeführte Änderungen

Die erfassten Protokollierungen sind nur durch den Administrator einsehbar und nicht editierbar. Eine Funktion zur Aufbereitung erstellt eine auswertbare Liste und kann den Kostenträgern zusätzlich zu dem Datenexport der angefragten Objekte ausgehändigt werden. Das Ziel besteht darin, den Kostenträgern bei Bedarf alle Zugriffe, wobei ändernde oder löschende Aktionen besonders hervorzuheben sind, zur Verfügung zu stellen, um die Validierbarkeit der Daten zu unterstützen.

V. Änderungen von Daten im Register

Die Änderungen der Daten können in drei verschiedenen Teilprozessen durchgeführt werden:

- **Datensätze ergänzen**

Die MVB GmbH besitzt alle Rechte zur Ergänzung bereits vorhandener Datensätze. Dies wird durch die über einen längeren Zeitraum andauernde Therapieform notwendig, bei der ein initialer Datensatz im Telemedizinregister mit neuen Daten (Videos, Befunde, etc.) ergänzt wird. Die an das Register übermittelten Objekte sind mit dem gleichen Pseudonym versehen wie das initial gespeicherte Objekt, wodurch weniger Komplikationen bei der Datenergänzung zu erwarten

sind. Dieses Pseudonym wird zur Bestimmung der eindeutigen ID im Register verwendet, welches auch eine Kontrolle auf das Vorhandensein eines zu ergänzenden Objektes beinhaltet. Sollte bei dieser Überprüfung festgestellt werden, dass bisher kein Objekt mit dem Pseudonym / der ID vorhanden ist, besteht die Option einer Neuanlage der Daten und der Mitteilung an die MVB GmbH. Alternativ könnte der Prozess als nicht durchführbar beendet werden.

- **Datensätze ändern**

Die Änderung bereits hinterlegter Daten ist nicht ohne eine weitere Legitimation durch den Administrator möglich. Die Transaktion Update Document Set zur Modifizierung hinterlegter Metadaten muss durch die MVB GmbH mit einer Begründung beantragt und durch den Administrator entweder zeitlich beschränkt oder Objekt-gebunden freigeschaltet werden. Diese Sicherung dient der Vertrauensbildung gegenüber den Kostenträgern, die alle Änderungen über die Protokollierung nachvollziehen können.

- **Datensätze löschen**

Besonders restriktiv muss der Vorgang zur Löschung von Objekten durchgeführt werden, was in diesem Beispiel mit einer vorübergehenden Sperrung des Objekts kombiniert wird. Soll ein Objekt nicht mehr Gegenstand der im Telemedizinregister hinterlegten Datenmenge sein, muss ein Antrag mit Begründung an den Administrator gestellt werden. Nur dieser kann bei positiver Bewertung eine Sperrung des Objekts veranlassen, womit das Objekt für die MVB GmbH und die Kostenträger nicht mehr sichtbar ist. Nach angemessener Wartezeit erfolgt die komplette Löschung der Daten aus dem Register. Bei der Protokollierung sollten auch die Verweise auf das Objekt in eine separate Liste überführt werden. Der Vorgang der Löschung beziehungsweise Sperrung kann beispielsweise durch nicht mehr gültige Einverständniserklärungen eines Patienten erforderlich werden und ist im Register miteinzuplanen.

VI. Verarbeitung von Anfragen der Kostenträger

Ein Kostenträger stellt an das Telemedizinregister gezielte Anfragen nach Datensätzen beziehungsweise Objekten, die als Kontrolldaten dienen sollen im Vergleich mit direkt zwischen der MVB GmbH und dem Kostenträger ausgetauschten Datensätzen. Denkbar ist auch ein Szenario, bei dem die Kostenträger ausschließlich die Daten aus dem Register für analytische Prozesse verwenden, dies ist aber in diesem Beispiel nicht vorgesehen. Eine gezielte Anfrage benötigt Parameter zur Suche im Register, welche dem Kostenträger durch die bei der MVB GmbH vorgenommene Pseudonymisierung und Reduzierung der identifizierenden Daten aber nur eingeschränkt (zum Beispiel demografische Parameter wie Alter) bekannt sind. Daher muss analog zum anfänglichen Prozess der Datenauswahl eine Kommunikation zwischen der MVB GmbH und dem Kostenträger erfolgen:

1. Der Kostenträger beabsichtigt eine Analyse der Therapie.
2. Eine erste Anfrage an das Register informiert auch die MVB GmbH über die beabsichtigten Datenanfragen.
3. Die MVB GmbH informiert den Kostenträger über die im Register vorhandenen Datensätze und übermittelt diesem gegebenenfalls die notwendigen Pseudonyme.
4. Der Kostenträger stellt eine gezielte Anfrage an das Register mit einer Auflistung der gewünschten Datensätze beziehungsweise Objekte, basierend auf dem Pseudonym.

VII. Übermittlung der angefragten Daten

Im Register werden die in der Anfrage enthaltenen Objekte für die Übermittlung an den Kostenträger bereitgestellt, wobei der Teilprozess **Sichere Verbindung herstellen** auch hier zum Einsatz kommt. Mittels einer zusätzlichen Verschlüsselung vor der Übermittlung der ausgewählten Daten ist eine nicht autorisierte Verwendung der Datensätze verhindert, indem der Schlüssel zur Dechiffrierung dem Kostenträger durch die MVB GmbH ausgehändigt wird. Ein System, dass die Dechiffrierung zeitlich begrenzt, erweitert die Möglichkeit zur Limitierung der Verwendung durch das Register ausgehändigter Daten.

10 Diskussion und Empfehlungen

Inhalt dieses Kapitels sind die Reflektion und kritische Betrachtung der eingesetzten wissenschaftlichen Methoden und Verfahrensweisen. Daran anschließend ist auch eine Beschreibung der durchgeführten Änderungen in dem Struktur-Aufbau der Diplomarbeit, welche im Laufe der Datenerhebung notwendig wurden.

Besonders die Interview-Methode wird nochmals betrachtet. Wettbewerbstechnische Gründe verhindern eine ausreichende Auswertung der erhobenen Interview-Daten. Da die Datenmenge der Antworten zu gering ist, besonders im Hinblick auf die Möglichkeiten der Analyse verschiedener Auswertungsmethoden, kann die Interview-Methode für diese Arbeit nur sehr eingeschränkt eingesetzt werden.

10.1 Reflektion

Die anfangs geplante Diplomarbeit benötigte zur Datenerhebung neben der Methode Desk Research auch praxisorientierte Interviews mit Datenschutzbeauftragten und beteiligten Stakeholdern, um frühzeitig in die Planungsphase des Telemedizinregisters bekannte Problematiken der bisherigen Abrechnungsverfahren und Möglichkeiten zur Mitgestaltung der Funktionalitäten durch im Interview abgefragte Erwartungshaltungen miteinzubinden.

Die Kombination der Daten aus dem Desk Research, den Interviews und zusätzlichen Analysen der Prozesse in dem Betrieb MVB GmbH als konkretes Beispiel eines Dienstleisters im telemedizinischen Bereich sollte einen umfassenden Anforderungskatalog ergeben, in dem die Erfahrungen aus bisherigen Prozessen der Abrechnungsvorgänge einen großen inhaltlichen Teil einnehmen.

Bei der Vorbereitung zur Durchführung der Interviews wurden repräsentativ für die beteiligten Stakeholder drei Kostenträger und drei telemedizinische Dienstleister ausgewählt. Die Wahl der drei Kostenträger fiel auf die aktuell drei größten Kostenträger im deutschen Gesundheitswesen, bei den drei telemedizinischen Dienstleistern wurde neben der MVB GmbH noch zwei weitere Dienstleister mit Hilfe eines Telemedizinpor-

tals ausgewählt [66]. An die Datenschutzbeauftragten der Länder Rheinland-Pfalz und Nordrhein-Westfalen wurden ebenfalls Anfragen gerichtet.

Die Interview-Anfragen wurden per Mail versendet und eine kurze inhaltliche Beschreibung der Thematik hinzugefügt, um in einem weiteren Gespräch eine gemeinsame thematische Ausgangsbasis zu besitzen. Seitens der telemedizinischen Dienstleister gab es keine Rückmeldung auf die Anfragen, auch erneute Anfragen blieben unbeantwortet. Dieser Zustand erklärt sich eventuell mit den vorliegenden Antworten der Kostenträger: sowohl die AOK Rheinland als auch die BARMER GEK verwiesen in ihren Antworten darauf, dass sie aus Gründen des Wettbewerbs keinerlei inhaltliche Informationen über Geschäfts- und Abrechnungsprozesse mitteilen wollen. Einzig die Techniker als Kostenträger beantwortete die Anfrage mit einem Terminvorschlag für ein Interview, welches telefonisch durchgeführt wurde. Vorab wurden die in dieser Arbeit im Anhang hinterlegten Interviewfragen dem Interviewpartner zugestellt, damit durch diesen eine Vorbereitung auf das Interview vorgenommen werden konnte. Im Telefonat wurde jedoch durch den Interviewpartner inhaltlich nicht auf die gestellten Fragen eingegangen, sondern die Thematik allgemein beantwortet. Das Fazit des Gesprächs lieferte als Ergebnis die bereits zuvor angenommene Ausgangssituation bei den Kostenträgern: individuell werden die Analyse und Abrechnungsvorgänge im Rahmen der integrierten Versorgungsform mit den beteiligten Vertragspartnern abgesprochen und durchgeführt. Weitere Informationen sind aus Wettbewerbsgründen nicht zu erheben. Eine Standardisierung dieser Prozesse beziehungsweise schematische Abbildung der Vorgänge ließ sich somit nicht wie erwartet in diese Arbeit integrieren. Anstatt der erwarteten Kooperation bei der Datenerhebung konnte durch die Interviews keinerlei konstruktive Informationen zur Erstellung des Anforderungskataloges erhoben werden.

Die Anfragen an die Datenschutzbeauftragten lieferten ebenfalls keine in der Arbeit verwertbaren Informationen, da in einem Fall die Interview-Anfrage abgelehnt und im anderen Fall nicht beantwortet wurde.

Aufgrund dieser fehlenden jedoch eingeplanten Daten wurde die Ausrichtung der Diplomarbeit auf die Schwerpunkte Datenschutz und Einbindung internationaler Standards des eHealth-Sektors angepasst. Diese Änderungen konnten mit der Methodik Desk Research umfangreich vorgenommen werden. Um die theoretischen Modelle des Registers zu überprüfen, wurde eine praxisorientierte Beispielanwendung mit Hilfe der Struktur

der MVB GmbH durchgeführt. Somit konnten zu den einzelnen Prozessbeschreibungen des SOLL-Modells auch einige Datenbeispiele aufgelistet werden.

10.2 Offene Fragen und Problemfälle

Einer der offenen Fragen ist durch die fehlende Einbindung der bisherigen Erfahrungen seitens der telemedizinischen Dienstleister und Kostenträger vorhanden. Ein System zur Standardisierung und Vereinfachung von Abrechnungsvorgängen sollte möglichst Anforderungen durch die Informationen bisher durchgeführter Prozesse enthalten, um etwaige Problematiken in der bisherigen Verfahrensweise frühzeitig zu erkennen und zu beheben. Diese Integration bestimmter Problemfälle ist in der Diplomarbeit mangels fehlender Interview-Daten nicht möglich gewesen, sollte aber für die weitere Entwicklung des Registers nicht unberücksichtigt bleiben.

Die verwendeten Datentypen im Register sind verallgemeinernd aufgeführt, da bei jedem Dienstleister unterschiedliche Voraussetzungen und eingesetzte Systeme zu erwarten sind. Eine präzisere und detailliertere Angabe der Datenmodelle ist somit von weiteren Informationen abhängig, die dazu erschwerend aus unterschiedlich eingesetzten Systemen gewonnen werden müssen. Besonders im Bereich der telemedizinischen Dienstleistungen sind eigenentwickelte Software und Hardwaresysteme im Einsatz, welche oftmals auf einen spezialisierten Datenaustausch hin entwickelt werden. Die Verwendung und Aufbereitung der verschiedenen Daten kann mit Hilfe von Standards, besonders derer mit Bezug des Datenaustauschs, umgesetzt werden, um die Kompatibilität der dadurch entwickelten Systeme zu erweitern. Zusätzlich sind durch die zahlreichen Einflussfaktoren im Bereich des Datenschutzes noch einige offene Fragen zur legitimen Anwendung und Weiterverwendung medizinischer Daten aufgetreten. Einerseits ist durch den Gesetzgeber die Verarbeitung von medizinischen Daten zu Abrechnungsvorgängen erlaubt, andererseits ist durch das Register eine nicht zwingend notwendige Datenverarbeitung gegeben. Durch die Pseudonymisierung ist eine Vorkehrung getroffen worden, die externe Speicherung von medizinischen Daten mit geringeren Risiken durchzuführen. Trotz der Struktur eines geschlossenen Systems, bei dem keine öffentlichen Zugriffe eingeplant sind, ist von einer Verwendung realer Daten unbedingt abzuraten, da verwendete Software-Systeme niemals als fehlerfrei und sicher

gegen Attacken eingestuft werden können. Durch neuere Entwicklungen in der Gesetzgebung kann sich die Ausgangssituation entscheidend verändern, welche Rechte zur Verarbeitung von medizinischen Daten existieren.

10.3 Empfehlungen für weitere Anwendungsbereiche

Die zuvor genannten Problematiken und Themenbereiche eignen sich aufgrund der Komplexität für weitere Arbeiten. So bietet sich die Integration bereits definierter Standards, zum Beispiel durch die IHE, in Prozesse zur Durchführung telemedizinischer Dienstleistungen an. Besonders der Fokus auf die Einbindung international angewandter Standard-Kataloge der IHE und damit umgesetzten Standards von HL7, ISO, etc. soll zukunftsweisende Potentiale in der Realisierung des Telemedizinregisters aufweisen, womit auch die Kompatibilität und Schnittstellen-Funktionalität für weitere Anwendungsfelder erhöht wird. Bisher ist das Konzept des Telemedizinregisters auf den deutschen Gesundheitsmarkt beschränkt, durch die internationalen Standards existieren aber Möglichkeiten zum grenzüberschreitenden Datenaustausch des telemedizinischen Sektors bei der Nutzung des Registers. Je früher eine standardisierte Vorgehensweise bei der Anwendung der Therapie in Bezug auf die Datenverarbeitung vorgenommen wird, desto besser lassen sich anschließende Prozesse weiterentwickeln und integrieren. Die Thematik der Datenerfassung zur Bildung aufschlussreicher Patientenakten wird sich in den nächsten Jahren erwartungsweise erweitern, um die aktuelle Situation der heterogener Datenspeicherung und Verarbeitung zu verbessern. Eine digitale Patientenakte fördert neben der einfacheren Verwendung und Weitergabe erfasster Daten auch die Selbstbestimmung des Patienten, der optional in die Datenverarbeitungsprozesse Einsicht erhält und eigenständig über die Verwendung der Daten bestimmt. Beispielsweise bietet die standardisierte Verarbeitung der Therapiedaten im Telemedizinregister weitere Möglichkeiten zur Anbindung an eine digitalisierte Patientenakte, welches in Kapitel 7 bei den anwendungsfernen Szenarien bereits thematisiert wurde. Aufgrund der verwendeten Techniken zur Pseudonymisierung und weiteren Schritten beim Export der Daten ist eine optionale Verwendung für medizinische Forschungsfelder von Relevanz, sofern die datenschutzrechtlichen Voraussetzungen dafür berücksichtigt werden. Die Speicherung der Daten, vor allem die Verwendung von zusätzlichen Metadaten in

Kombination mit demografischen Faktoren, bietet die Möglichkeit zur weiteren Verwendung aufbereiteter Daten in der medizinischen Forschung.

Bei der Verwendung von beispielsweise treuhänderischen Verfahren zur Pseudonymisierung und anschließender Re-Pseudonymisierung wären auch Voraussetzungen für Archivierungsfunktionen und Backup-Diensten vorhanden, falls die im Register erfassten medizinischen Daten identisch mit denen beim Dienstleister vorhandenen Datensätzen sind. Durch gesetzliche Richtlinien ist es notwendig, über lange Zeiträume, die bis zu 30 Jahren betragen können, Informationen und Dokumente zu durchgeführten Behandlungen vorzuhalten. Die Pseudonymisierung mit Möglichkeiten zur Re-Identifizierung und Verschlüsselung von Daten im Telemedizinregister könnten diese Umsetzungen unterstützen.

Ein weiterer interessanter Aspekt ergibt sich durch die vorbereitenden Prozesse bei der Aufbereitung der Dienstleister-Daten für das Register. Unterstützend durch die vom Dienstleister eingesetzten Standardisierungs-Profile beim Verarbeitungsprozess der Daten und weiteren Maßnahmen wie beispielsweise der Abnahme einer telemedizinischen Datenstruktur durch einen auf diesen Bereich spezialisierten Datenschutzbeauftragten sind Möglichkeiten zu einer Zertifizierung vorhanden. Dies könnte sowohl bei Kostenträgern als auch bei Patienten eine erweiterte Akzeptanz hervorrufen und die telemedizinischen Dienstleister gegenüber rechtlichen Problematiken absichern. Diese Entwicklung der Zertifizierungs-Maßnahmen würde sich in Zusammenhang mit der Einrichtung eines Telemedizinregisters anbieten, um den Prozess der Datenaufbereitung für das Register zu vereinfachen.

11 Fazit und Ausblick

Die Zielsetzung der verfassten Diplomarbeit war die Erstellung eines Anforderungskataloges, der für ein Telemedizinregister benötigt wird. Neben diesem primären Ziel waren auch die ausführliche Grundlagen-Beschreibung der aktuellen Datenschutz-Situation und die praxisorientierte Darstellung des telemedizinischen Sektors weitere Ziele, um die komplexe Thematik der zu berücksichtigenden Einflussfaktoren miteinzubinden. Mit Hilfe von Standardisierungs-Profilen sollte diese Beschreibung auch einen Bezug auf internationale Umsetzungen enthalten.

Die heterogenen Strukturen im deutschen Gesundheitswesen, vor allem die unterschiedlichen Verfahren der Datenerfassung und Abrechnungsprozesse zwischen telemedizinischen Dienstleistern und Kostenträgern, sollten mit Hilfe der Interviews erfasst und exemplarisch mitgestaltende Faktoren bei der Anforderungslistenenerstellung generieren. Die geplanten Interviews lieferten wie zuvor beschrieben aber keine verwertbaren Daten, um die unterschiedlichen Ausgangssituationen in dem Anforderungskatalog berücksichtigen zu können. Zur Etablierung eines allgemeingültigen Telemedizinregisters sind diese Informationen, welche sich aus bisherigen Erfahrungen und zukünftigen Erwartungen zusammensetzen, jedoch eine wichtige Komponente, um den theoretischen Status des Telemedizinregisters in ein Praxis-Stadium weiterentwickeln zu können.

Dieser vorliegende Anforderungskatalog kann für weitere Arbeiten in dem Bereich der Entwicklung des Telemedizinregisters eingesetzt werden: Einerseits könnte die technische Umsetzung anhand eines konkreten telemedizinischen Projekts in Absprache mit einem oder mehreren Kostenträger erfolgen, wobei mit dieser Vorgehensweise weitere Erkenntnisse und praxisorientierte Anforderungen diesen Anforderungskatalog ergänzen würden. Andererseits würde eine Analyse verschiedener telemedizinischer Dienstleistungen und Abrechnungsprozesse die theoretische Modellierung eines allgemeingültigen Anforderungskatalogs erweitern können, bei dem der Fokus auf ein standardisiertes Vorgehen für telemedizinische Dienstleister gelegt wird.

Des Weiteren ist die Bearbeitung und Forschung auf dem Gebiet der im vorherigen Kapitel aufgeführten offenen Fragestellungen eine Möglichkeit, basierend auf dieser Diplomarbeit weitere wissenschaftliche Arbeiten zu definieren. Zu erwarten sind weitere rechtliche Reglementierungen und Anpassungen im Bereich des Datenschutzes, bezo-

gen auf den Umgang mit (sensiblen) medizinischen Daten, welches die Grundvoraussetzungen bei der Erstellung des Telemedizinregisters deutlich ändern könnte. Die Verwendung und Weitergabe der Daten, auch im anonymisierten oder zumindest ausreichend pseudonymisierten Zustand, sollte als äußerst sensibel angesehen werden, um Problematiken bei der Kombination scheinbar ungefährlicher Datensätze zu berücksichtigen. Gesundheitsdaten unterliegen dabei einem besonderen Schutzbedürfnis, wodurch die Anbindung der medizinischen Forschung an ein Telemedizinregister weiterer sorgfältiger Planungen bedarf.

Zusammenfassend ist die Erstellung eines standardisierten Telemedizinregisters, welches durch verschiedene Dienstleister in der Telemedizin eingesetzt werden könnte, von sehr aufwendigen Prozessen zur Aufbereitung der vorhandenen Daten abhängig. Zur Realisierung des Registers für einen Dienstleister sind die vorliegenden Datenmodelle und Prozessabläufe auf die jeweils vorhandenen Strukturen anzupassen und somit erschwert übertragbar auf andere Umsetzungen. Des Weiteren deuten die Ergebnisse der Interview-Anfragen darauf hin, dass weitere Maßnahmen zur besseren Akzeptanzbildung für ein standardisiertes Verfahren unter Berücksichtigung wettbewerbstechnischer Einschränkungen notwendig sind. Ein allgemein anwendbares Telemedizinregister sollte mit Hilfe der beteiligten Stakeholder möglichst bereits ab der ersten Planungsphase deren Erfahrungen und Erwartungen in den Aufbau integrieren.

Die zahlreichen Einflussfaktoren, die maßgeblich durch datenschutzrechtliche Vorgaben und den Strukturen im Gesundheitswesen die Ausrichtung dieser Arbeit bestimmen, werden sich in den nächsten Jahren erwartungsgemäß verändern und weitere Entwicklungsmöglichkeiten auf dem Gebiet der standardisierten Erfassung und Verarbeitung medizinischer Daten entstehen lassen.

Literaturverzeichnis

- [1]. **Häcker, Joachim, Reichwein, Barbara und Turad, Nicole.** *Telemedizin.* München : Oldenbourg Verlag, 2008.
- [2]. **Busse, Prof. Dr. med. Reinhard.** eHealth. *Management im Gesundheitswesen III, Industrie.* [Online] 28. Januar 2013. http://www.mig.tu-berlin.de/fileadmin/a38331600/2012.teaching.ws/Modul_Einfuehrung/2013_01_28_eHealth_UA_.pdf.
- [3]. **Burchert, Heiko.** Telemedizin-Controlling: Aufgaben, Instrumente und Vorgaben. [Buchverf.] Frank Duesberg. *e-Health 2010.* Solingen : medical future Verlag, 2009.
- [4]. **Bartmann, F.-J., Blettner, M. und Heuschmann, P. U.** *Telemedizinische Methoden in der Patientenversorgung.* Köln : Deutscher Ärzte-Verlag, 2012.
- [5]. **Hund, H., et al.** Sichere Pseudonymisierung durch Datentreuhänder. *Fachschaft Medizinische Informatik, Universität Heidelberg, Hochschule Heilbronn.* [Online] April 2013. <https://download.mi.hs-heilbronn.de/conhit-2013/datentreuhaender.pdf>.
- [6]. **Klusen, Norbert und Meusch, Andreas.** *Gesundheitstelematik.* Baden-Baden : Nomos Verlagsgesellschaft, 2002.
- [7]. **Versorgung, Integrierte.** Ärzte Zeitung online. *ABC des Gesundheitswesens.* [Online] 09. September 2009. [Zitat vom: 15. Oktober 2013.] http://www.aerztezeitung.de/politik_gesellschaft/gp_specials/abc_gesundheitswesen/article/564714/integrierte-versorgung.html.
- [8]. **TEMPiS.** Telemedizinisches Projekt zur integrierten Schlaganfallversorgung. [Online] 2010. [Zitat vom: 12. November 2013.] <http://www.tempis.de/>.
- [9]. **Quentin, Robert.** Home monitoring für Herzranke. *Mein Herz.* [Online] 2012. [Zitat vom: 14. November 2013.] <http://www.segebergerkliniken.de/files/skg/content/patienten/herzzentrum/pdf/jahrbuchsh-2011-12-mein-herz.pdf>.
- [10]. **D STATIS, Statistisches Bundesamt.** Gesundheitsausgaben im Jahr 2011. *Pressemitteilung.* [Online] 04. April 2013. [Zitat vom: 13. November 2013.]

https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2013/04/PD13_128_23611.html.

[11]. **Egbert, Nicole, et al.** Integrierte und vernetzte Versorgung der Krankenhäuser in Deutschland und Österreich. [Buchverf.] Frank Duesberg. *e-Health 2012*. Solingen : medical future Verlag, 2011.

[12]. **Laschet, Helmut.** An IV-Verträgen scheiden sich die Geister. *ÄrzteZeitung*. [Online] 03. Januar 2013. [Zitat vom: 23. November 2013.]

http://www.aerztezeitung.de/politik_gesellschaft/krankenkassen/article/828406/wachsen-de-skepsis-iv-vertraegen-scheiden-geister.html.

[13]. **Grothaus, Franz-Josef.** Entwicklung der integrierten Versorgung in der Bundesrepublik Deutschland 2004 - 2008. *Gemeinsame Regisitrierungsstelle zur Unterstützung der Umsetzung des § 140 d SGB V*. [Online] 30. Juni 2009. [Zitat vom: 23. November 2013.] <http://www.bqs-register140d.de/dokumente/bericht-140d.pdf>.

[14]. **Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen.** Ergebnisse einer Befragung zur integrierten Versorgung nach § 140a-d SGB. *SVR Gesundheit*. [Online] 13. November 2013. [Zitat vom: 23. November 2013.] <http://www.svr-gesundheit.de/index.php?id=436>.

[15]. **Medgate.** 360° Healthcare. [Online] 2013. [Zitat vom: 02. Dezember 2013.] www.medgate.ch.

[16]. **news Aktuell (Schweiz) AG.** Medgate: Zukunftsweisendes Gesundheitszentrum für Zürich-Nord. *na presseportal*. [Online] 02. September 2013. [Zitat vom: 02. Dezember 2013.] <http://www.presseportal.ch/de/pm/100001063/100743108/medgate-zukunftsweisendes-gesundheitszentrum-fuer-zuerich-nord-bild>.

[17]. **Telemedizin in der Euroregion POMERANIA e. V.** Netzwerk Pomerania Telemedizin. [Online] Oktober 2012. [Zitat vom: 04. Dezember 2013.] <http://www.idw-online.de/de/attachmentdata26622.pdf>.

[18]. **Steinke, Constanze.** Deutsch-polnisches Telemedizinprojekt startet in die Betriebsphase. *idw - Informationsdienst Wissenschaft*. [Online] 12. April 2013. [Zitat vom: 04. Dezember 2013.] <http://www.idw-online.de/de/news528185>.

- [19]. **Witt, Bernhard C.** *Datenschutz kompakt und verständlich*. Wiesbaden : Vieweg + Teubner Verlag, 2010.
- [20]. **Bundesministerium der Justiz und für Verbraucherschutz.** Bundesdatenschutzgesetz. *juris - Gesetze im Internet*. [Online] 1990. [Zitat vom: 28. Januar 2014.] http://www.gesetze-im-internet.de/bdsg_1990/.
- [21]. **Schröder, Georg F.** *Datenschutzrecht für die Praxis*. München : Deutscher Taschenbuch Verlag, 2012.
- [22]. **Gesundheitsministerium, NRW.** Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen. *Gesundheitsdatenschutzgesetz - GDSG NRW*. [Online] Dezember 1999. <http://www.duesseldorf.de/datenschutz/rechtsgrundlagen/gdsg.pdf>.
- [23]. **Prof. Dr. Pommerening, Klaus; Dr. Drepper, Johannes.** Datenschutz in der medizinischen Forschung 04. *Patienteninformation und Einwilligungserklärung*. [Online] 28. September 2011. http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=13309&PortalId=0.
- [24]. **Prof. Dr. Pommerening, Klaus und Dr. Drepper, Johannes.** Datenschutz in der medizinischen Forschung 02. *Rechtliche Grundlagen der medizinischen Forschung*. [Online] 28. September 2011. http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=13307&PortalId=0.
- [25]. **Witt, Thorsten.** Die 10 Gebote des Datenschutzes. [Online] März 2005. <http://www.wissen4free.org/Material/Datenbank/allgemeinbildung/Die%2010%20Gebote%20des%20Datenschutzes.pdf>.
- [26]. **Spitzer, Michael und Ückert, Frank.** Datenschutzanforderungen in der nationalen medizinischen Forschung am Beispiel der Teleradiologie-Plattform MDPE. [Buchverf.] Frank Duesberg. *e-Health 2010*. Solingen : medical future Verlag, 2009.
- [27]. **Prof. Dr. Pommerening, Klaus; Dr. Drepper, Johannes.** Datenschutz in der medizinischen Forschung 03. *Anonymisierung und Pseudonymisierung*. [Online] 28. September 2011. <http://www.tmf->

ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=13308&PortalId=0.

[28]. **Prof. Dr. Pommerening, Klaus, et al.** Pseudonymisierung in der medizinischen Forschung - das generische TMF-Datenschutzkonzept. *gms - german medical science*. [Online] 6. Dezember 2005. <http://www.egms.de/static/en/journals/mibe/2005-1/mibe000017.shtml>.

[29]. **Prof. Dr. Pommerening, Klaus; Dr. Drepper, Johannes.** Datenschutz in der medizinischen Forschung 06. *Praktisches Vorgehen*. [Online] 28. September 2011. http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=133011&PortalId=0.

[30]. **Kassenärztliche Bundesvereinigung; Bundesärztekammer;** Bekanntmachungen: Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. *aerzteblatt.de*. [Online] Mai 2008. <http://www.aerzteblatt.de/archiv/60114/Bekanntmachungen-Empfehlungen-zur-aerztlichen-Schweigepflicht-Datenschutz-und-Datenverarbeitung-in-der-Arztpraxis>.

[31]. **Dr. Höpken, Andreas und Neumann, Helmut.** *Datenschutz in der Arztpraxis*. Frechen : DATAKONTEXT GmbH, 2008.

[32]. **Pommerening, Univ.-Prof. Dr. Klaus.** Die aktualisierten Konzepte der TMF zum Datenschutz für die medizinische Verbundforschung. *TMF Jahreskongress 2012*. [Online] März 2012. http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=15790&PortalId=0.

[33]. **Telematikplattform für Medizinische Forschungszwecke e.V.** Datenschutz und medizinische Forschung sind vereinbar: Konzepte, Tools und Services der TMF. *Pseudonymisierung*. [Online] 2006. <http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?EntryId=2341&PortalId=0>.

[34]. **Prof. Dr. Pommerening, Klaus; Dr. Drepper, Johannes.** Datenschutz in der medizinischen Forschung 05. *Die Datenschutzkonzepte der TMF*. [Online] 28. September 2011. <http://www.tmf->

ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=13310&PortalId=0.

[35]. **Bultmann, Marion, et al.** Datenschutz und Telemedizin - Anforderungen an Medizinetze. *Konferenz der Datenschutzbeauftragten des Bundes und der Länder.*

[Online] Oktober 2002. [Zitat vom: 26. September 2013.]

http://www.datenschutz.rlp.de/downloads/oh/dsb_oh_telemedizin.pdf.

[36]. **Hofstädter, F. und Klinkhammer-Schalke, M.** Klinische Krebsregister - Neue Entwicklungen nach der nationalen Krebskonferenz. *Kooperationsverbund*

Qualitätssicherung durch Klinische Krebsregister (KoQK). [Online] Mai 2010.

http://www.koqk.de/tl_files/Daten/Publikationen/201002_Forum_DKG_Klinische_Krebsregister.pdf.

[37]. **DPA.** Tausende Arztberichte ins Internet gelangt. *stern online.* [Online] 25. April 2008. [Zitat vom: 15. Oktober 2013.]

<http://www.stern.de/panorama/datenschutzskandal-tausende-arztberichte-ins-internet-gelangt-618475.html>.

[38]. **DPA, Lübeck.** Schwere Panne: 2500 Patientendaten online. *ÄrzteZeitung, Politik & Gesellschaft.* [Online] 04. November 2011. [Zitat vom: 15. Oktober 2013.]

http://www.aerztezeitung.de/politik_gesellschaft/article/677461/schwere-panne-2500-patientendaten-online.html.

[39]. **Himmelein, Gerarld.** Bericht: Apotheke verkaufen unenügend anonymisierte Patientendaten. *heise online.* [Online] 19. August 2013. [Zitat vom: 15. Oktober 2013.]

<http://www.heise.de/newsticker/meldung/Bericht-Apotheken-verkaufen-ungenuegend-anonymisierte-Patientendaten-1937568.html>.

[40]. **Alber, Winfrid.** Klinische Krebsregister aus politischer Sicht. *MedReport Nr. 7.*

[Online] März 2006. http://www.koqk.de/tl_files/Daten/Publikationen/alber_2006.pdf.

[41]. **Bundesministerium des Inneren.** Das Vorhaben "Nationales Waffenregister".

[Online] BMI, 2013.

http://www.bmi.bund.de/DE/Themen/Sicherheit/Waffenrecht/Nationales-Waffenregister/nationales-waffenregister_node.html.

- [42]. **Bundesministerium, Justiz.** Bundeskrebsregisterdatengesetz. *Gesetze im Internet*. [Online] 10. August 2009. [Zitat vom: 22. September 2013.] <http://www.gesetze-im-internet.de/bundesrecht/bkrg/gesamt.pdf>.
- [43]. **Meyer, Martin.** Bevölkerungsbezogenes Krebsregister Bayern. *Meldeverfahren*. [Online] 17. November 2011. <http://www.krebsregister-bayern.de/Informationen-Melden.html>.
- [44]. **Klinkhammer-Schalke, M., Marschner, N. und Hofstädter, F.** Register in der onkologischen Versorgungsforschung. *Onkologie 2012*. [Online] 27. Januar 2012. http://www.tumorzentren.de/tl_files/dokumente/Veroeffentlichungen_Artikel/Register%20in%20der%20Onkol.VF.pdf.
- [45]. **Bundesministerium des Inneren.** Meldewesen. [Online] BMI, 2014. <http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/PolitikGesellschaft/Meldewesen/14.html>.
- [46]. **Balzer, Helmut.** *Lehrbuch der Software-Technik*. Berlin : Spektrum Akademischer Verlag, 2000.
- [47]. **Schwinn, Hans.** *Requirements Engineering*. München : Oldenbourg Verlag, 2011.
- [48]. **Stevens, Kaye.** Rich Pictures. *BetterEvaluation*. [Online] Juli 2012. <http://betterevaluation.org/evaluation-options/richpictures>.
- [49]. **Trill, Roland.** E-Health als Pfeiler in der Gesundheitsregion NORD (GRN). [Buchverf.] Frank Duesberg. *e-Health 2010*. Solingen : medical future Verlag, 2009.
- [50]. **Idris, Tarik, et al.** Eine standardisierte Sicherheitsarchitektur für den einrichtungsübergreifenden Datenaustausch. [Buchverf.] Frank Duesberg. *e-Health 2013*. Solingen : medical future Verlag, 2012.
- [51]. **epSOS.** epSOS - the European eHealth Project. [Online] European Commission, Februar 2014. <http://www.epsos.eu/>.
- [52]. **IHE Deutschland e.V.** IHE Deutschland. [Online] IHE Deutschland e.V., Februar 2014. <http://www.ihe-d.de/>.
- [53]. **IHE.** Integrating the Healthcare Enterprise. [Online] IHE International, 2013. <http://www.ihe.net/>.

- [54]. **HL7**. IHE-D Cookbook. *HL7 Wiki*. [Online] 12. November 2013.
http://wiki.hl7.de/index.php/IHE_DE_Cookbook.
- [55]. **IHE Wiki**. Cross-Enterprise Document Sharing. [Online] 5. April 2013.
http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing.
- [56]. **Bundesministerium, Justiz und Bundesministerium, Gesundheit**. Patientenrechte in Deutschland. *Verbraucherzentrale Bundesverband*. [Online] 17. Oktober 2002.
http://www.vzbv.de/mediapics/1034864605Patientenrechte_10_2002.pdf.
- [57]. **Weichert, Thilo**. Datenschutz und medizinische Forschung. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*. [Online] 19. April 2011.
<https://www.datenschutzzentrum.de/vortraege/20110419-weichert-datenschutz-und-medizinische-forschung.pdf>.
- [58]. **Geis, Ivo**. Das elektronische Gesundheitssystem - elektronische Patientenakte und elektronische Gesundheitskarte: eine datenschutzrechtliche Bewertung. [Buchverf.] Frank Duesberg. *e-Health 2010*. Solingen : medical future Verlag, 2009.
- [59]. **Rispens, Dr. Sybe**. Die elektronische Gesundheitskarte - whitepaper Sicherheit. [Online] 18. Juni 2008.
http://www.bwkg.de/index.php?eID=tx_nawsecuredl&u=0&file=uploads/media/gematik_whitepaper_sicherheit_3571-1.pdf&t=1382524197&hash=2896a908005d7d455eafe657bd84651f112232f7.
- [60]. **Prof. Dr. Pommerening, Klaus; Dr. Drepper, Johannes**. Datenschutz in der medizinischen Forschung 01. *Szenario und Anwendungsfälle*. [Online] 28. September 2011. http://www.tmf-ev.de/DesktopModules/Bring2mind/DMX/Download.aspx?Method=attachment&Command=Core_Download&EntryId=13306&PortalId=0.
- [61]. **Datenschutzbeauftragter, Bundesland Bayern**. Orientierungshilfe: Pseudonymisierung in der medizinischen Forschung. *Veröffentlichungen des bayrischen Landesbeauftragten für den Datenschutz*. [Online] 29. November 2005.
http://www.datenschutz-bayern.de/technik/orient/ohilfe_psn_03.html.

- [62]. **Konferenz der Datenschutzbeauftragten, Bund und Länder.** Orientierungshilfe Krankenhausinformationssysteme. *Unterarbeitsgruppe Krankenhausinformationssysteme, Arbeitskreis Gesundheit und Soziales.* [Online] März 2011.
http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Orientierungshilfe_Krankenhausinformationssysteme.pdf.
- [63]. **Eckert, Claudia.** *IT-Sicherheit.* München : Oldenbourg Verlag, 2008.
- [64]. **Bauer, Johannes, Liebscher, Albrecht und Thielking-Riechert, Klaus.** *OpenVPN.* Heidelberg : dpunkt.verlag, 2006.
- [65]. **medizinische Videobeobachtung MVB GmbH.** ambulante Parkinsontherapie. [Online] Oktober 2013. <http://mvb-parkinson.de/pages/de/startseite.php>.
- [66]. **Fraunhofer FOKUS.** Deutsches Telemedizinportal. [Online] November 2012. <http://telemedizin.fokus.fraunhofer.de/>.

Anhang

I Interview-Fragen

Interview-Fragen an die telemedizinischen Dienstleister

- 1.1. In welche Verfahrensschritte lässt sich eine Prüfung gliedern, die durch einen Kostenträger bei Ihnen durchgeführt wurde? (Auflistung in sequenzieller Form beziehungsweise Beschreibung in mehreren Sätzen)
- 1.2. Welche Probleme sind bei dieser Vorgehensweise aufgetreten?
- 1.3. Wie sollen zukünftig die Prüfungen vollzogen werden beziehungsweise welche Änderungen sind in Planung, das Nachweisverfahren zu ändern?
- 2.1.1. Welche Daten(-typen) wurden bei bisherigen Prüfungen beim Dienstleister angefordert, wenn die Kosten der Behandlungen untersucht wurden?
- 2.1.2. Mit welchen Daten(-typen) erfolgte bisher eine Untersuchung der medizinischer Wirksamkeit einer Therapie?
- 2.2. Welche Probleme sind bei der Datenauswahl und Datenauswertung aufgetreten?
- 2.3. Sind Änderungen in der Auswahl und Auswertung der Daten in zukünftigen Prüfverfahren vorgesehen beziehungsweise notwendig?

- 3.1. Welche technischen Systeme und Programme sind bei den bisherigen Prüfungen in Zusammenarbeit mit dem Dienstleister eingesetzt worden? (*Eventuell punktuelle Auflistung vom Prozessablauf in Frage 1.1 einsetzen*)
- 3.2. Welche Probleme gab es in der Anwendung der eingesetzten Systeme beziehungsweise Programme?
- 3.3. Welche Systeme beziehungsweise Programme sollen zukünftig in den Prüfungsvorgängen eingesetzt werden und gegebenenfalls aus welchem Grund wird ein anderes System eingesetzt?

Interview-Fragen an die Kostenträger

- 1.1. In welche Verfahrensschritte lässt sich eine Prüfung gliedern, die durch einen Kostenträger bei Ihnen durchgeführt wurde? (Auflistung in sequenzieller Form beziehungsweise Beschreibung in mehreren Sätzen)
- 1.2. Welche Probleme sind bei dieser Vorgehensweise aufgetreten?
- 1.3. Wie sollen zukünftig die Prüfungen vollzogen werden beziehungsweise welche Änderungen sind in Planung, das Nachweisverfahren zu ändern?
- 2.1.1. Welche Daten(-typen) wurden bei bisherigen Prüfungen beim Dienstleister angefordert, wenn die Kosten der Behandlungen untersucht wurden?
- 2.1.2. Mit welchen Daten(-typen) erfolgte bisher eine Untersuchung der medizinischen Wirksamkeit einer Therapie?

- 2.2. Welche Probleme sind bei der Datenauswahl und Datenauswertung aufgetreten?
- 2.3. Sind Änderungen in der Auswahl und Auswertung der Daten in zukünftigen Prüfverfahren vorgesehen beziehungsweise notwendig?

- 3.1. Welche technischen Systeme und Programme sind bei den bisherigen Prüfungen in Zusammenarbeit mit dem Dienstleister eingesetzt worden? (*Eventuell punktuelle Auflistung vom Prozessablauf in Frage 1.1 einsetzen*)
- 3.2. Welche Probleme gab es in der Anwendung der eingesetzten Systeme beziehungsweise Programme?
- 3.3. Welche Systeme beziehungsweise Programme sollen zukünftig in den Prüfungsvorgängen eingesetzt werden und gegebenenfalls aus welchem Grund wird ein anderes System eingesetzt?

Interview-Fragen an die Datenschutzbeauftragten

1. Welche Gesetze zum Datenschutz beeinflussen die Konzeption eines Telemedizinregisters, das deutschlandweit Gültigkeit besitzen soll und vor allem die externe Datenspeicherung von medizinischen Daten als Inhalt besitzt?
2. Sind Ihnen standardisierte Verfahren bzw. Richtlinien bekannt, die eine Übermittlung und Speicherung von medizinischen Daten an eine externe Speichermöglichkeit reglementieren?
3. Bei einer Pseudonymisierung bzw. Anonymisierung von identifizierenden Daten in der Medizin sind direkte Rückschlüsse auf die betroffene Person

nicht möglich bzw. sehr aufwendig. Dürfen solch ausreichend veränderte Daten, die ohne zusätzliche Informationen keine Re-Identifizierung erlauben, für andere Bereiche, z.B. medizinische Forschung, ohne die Einwilligung der betroffenen Personen verwendet werden?

4. Können Sie mir Problemfälle im Datenschutz schildern, die in den letzten Jahren im Bereich der Verarbeitung von medizinischen Daten aufgetreten sind?
5. Sind Ihnen Projekte / Bestrebungen bekannt, deren Ziel eine erweiterte Reglementierung im Umgang mit medizinischen Daten ist, bezogen auf externe Speicherung und Übermittlung?