UNIVERSITÄT LEIPZIG

Medizinische Fakultät

Institut für Medizinische Informatik, Statistik und Epidemiologie (IMISE)

3LGM^2-basiertes Referenzmodell für die digitale Archivierung von Patientenunterlagen

Diplomarbeit

Leipzig, Oktober 2006

vorgelegt von:

Sabine Lehmann
geb. am: 09.09.1978

Betreuer:

Prof. Dr. Anke Häber
Prof. Dr. Alfred Winter

Zusammenfassung

Bei der Einführung eines digitalen Archivs in einem Krankenhaus steht der Informationsmanager vor einer schwierigen Aufgabe. Auf dem Markt gibt es eine Vielzahl von Produkten, die für die digitale Archivierung angeboten werden. Da die Anbieter zum einen keine einheitliche Terminologie und zum anderen auch unterschiedliche Techniken und Lösungsarchitekturen verwenden, ist ein Vergleich der einzelnen Produkte schwierig. Das Ziel der Diplomarbeit bestand darin, ein Referenzmodell für die digitale Archivierung von Patientenunterlagen mit Hilfe des 3LGM^2-Baukastens zu erstellen. Aus dem Referenzmodell kann der Informationsmanager durch Konkretisierung spezielle Modelle ableiten. Unter Bezugnahme auf das Referenzmodell ist somit ein Vergleich der einzelnen Produkte möglich. Weiterhin ist erkennbar, wie sich das digitale Archiv in das vorhandene Informationssystem eines Krankenhauses einfügen würde.

Um zu zeigen, dass sich aus dem Referenzmodell spezielle Modelle ableiten lassen, wurden die zur digitalen Archivierung angebotenen Produkte der Firmen d.velop AG, Heydt-Verlags-GmbH, forcont business technology GmbH und EMC^2 mit dem 3LGM^2-Baukasten modelliert. Die Modellierung erwies sich trotz des vorhandenen Referenzmodells als schwierig. Dies lag zum einen daran, dass die Firmen zur Beschreibung ihrer Produkte firmenspezifische Namen verwenden, aus denen nicht immer klar erkennbar ist, welche Komponente sich eigentlich dahinter verbirgt. Zum anderen waren für die Modellierung zusätzliche Informationen notwendig.

Zum Abschluss erfolgte ein Vergleich dieser Produkte mit dem Referenzmodell. Bei diesem Vergleich war zu erkennen, dass das Produkt EMC Centera als Ergänzung zu den Produkten d.3, HYDMedia und forcont factory zu sehen ist. Die Unterschiede zwischen den Produkten d.3, HYDMedia und forcont factory waren vor allem auf der logischen Werkzeugebene zu finden. Während das d.3-System und HYDMedia zusätzliche Module anbieten, ist beim Produkt forcont factory unter Umständen der Kauf von Modulen eines Drittanbieters erforderlich. Auf der fachlichen Ebene im 3LGM^2-Modell sind mit Ausnahme auf zwei Aufgaben keine Unterschiede bei der Erledigung der Aufgaben zwischen den einzelnen Produkten festzustellen. Die Produkte verfügen somit über ähnliche Funktionalitäten. Da die Produkte d.3, HYDMedia und forcont factory reine Softwareprodukte sind, ist kein Unterschied auf der physischen Werkzeugebene feststellbar.

Inhaltsverzeichnis

Begriffs- und Abkürzungsverzeichnis

ADT.....	Admission, Discharge and Transfer
AKH.....	Allgemeines Krankenhaus Wien
AO.....	Abgabenordnung
ASCII…….....	American Standard Code for Information Interchange
BDSG.....	Bundesdatenschutzgesetz
BGB.....	Bürgerliches Gesetzbuch
BLOB.....	Binary-Large-Object
BMWA.....	Bundesministerium für Wirtschaft und Arbeit
BSI.....	Bundesamt für Sicherheit in der Informationstechnik
CA.....	Content Adresse
CAS.....	Content-Adressed Storage
CDF.....	C-Clip Deskriptor File
COLD.....	Computer Output to Laser Disk
CPR-System.....	Computer-based Patient Record System
DICOM…….....	Digital Imaging and Communications in Medicine
DLT.....	Digital Linear Tape
DMAS.....	elektronisches Dokumentenmanagement- und Archivierungssystem
EPA.....	Elektronische Patientenakte
GoB.....	Grundsätze ordnungsgemäßer Buchführung
GoBS.....	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
HCM.....	Hospital Communication Module
HGB.....	Handelsgesetzbuch
HL7.....	Health Level Seven
IOM.....	Institute of Medicine
IS-H.....	Industry Solution-Hospital
i.s.h.med.....	Industry Solution-Hospital/Medical
IKS.....	Internes Kontrollsystem
JPEG.....	Joint Photographic Experts Group
KAS.....	Klinisches Arbeitsplatzsystem
KDMS.....	Klinisches Dokumentations- und Managementsystem
KIS.....	Krankenhausinformationssysteme
LDSG.....	Landesdatenschutzgesetz
LIS.....	Laborinformationssystem

LKHG..... Landeskrankenhausgesetz

LTO..... Linear-Tape-Open

MBO-Ä……..... Musterberufsordnung für die deutschen Ärztinnen und Ärzte

NAS..... Network Attached Storage

NCI..... Non Coded Information

NEMA..... National Electrical Manufacturers Association

OCR..... Optical Character Recognition

PACS……..... Picture Archiving and Communication System

PDF..... Portable Document Format

PDMS..... Patientendatenmanagementsystem

PVS..... Patientenverwaltungssystem

RAID……..... Redundant Array of Inexpensive Disks

RIS..... Radiologieinformationssystem

RöVo……..... Röntgenverordnung

S/MIME……..... Secure Multipurpose Internet Mail Extensions

SAN..... Storage Area Network

TIFF..... Tagged Image File Format

UDO..... Ultra Density Optical

ULD..... Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

VCS..... VDAP Communication Standard

VDAP..... Verband Deutscher Arztinformationssystemhersteller und Provider e.V.

VOI..... Verband für Organisations- und Informationssysteme e.V.

WORM……..... Write Once Read Many

ZPO..... Zivilprozessordnung

ZTD..... Zertifizierungsdiensteanbieter

1 Einleitung

1.1 Gegenstand und Motivation

1.1.1 Gegenstand

Am Universitätsklinikum Leipzig werden laut [Winter 2004] jährlich 6 Millionen Seiten an papierbasierten Dokumenten erzeugt. Das entspricht ca. 1,5 laufende km neue Patientenakten pro Jahr, die gemäß gesetzlicher Aufbewahrungspflichten und Verjährungsfristen bis zu 30 Jahre lang aufbewahrt werden müssen [Zaiß et al. 2005]. Für das Universitätsklinikum Leipzig und für viele Krankenhäuser bedeutet das eine große Herausforderung, denn es muss ausreichend Platz für die Archivierung der papierbasierten Patientenakten vorgehalten werden. Schon heute sind viele konventionelle Archive überfüllt. Da die Patientenakten auch verwaltet werden müssen, entstehen zusätzlich zu dem Raumproblem Personal- und Sachkosten. Darüber hinaus muss sichergestellt sein, dass die Patientenakten bei Anforderungen schnell zur Verfügung stehen. Um dies zu gewährleisten, werden zunehmend rechnerbasierte Werkzeuge für die Archivierung und die Archivverwaltung eingesetzt.

Bereits heute wird eine Vielzahl von Dokumenten elektronisch erzeugt. Um zukünftig vermehrt auf den Ausdruck von Patientenunterlagen zu verzichten, bietet sich der Aufbau einer Elektronischen Patientenakte (EPA) an. Die Elektronische Patientenakte entsteht durch das Einscannen und Indexieren von papierbasierten Patientenunterlagen und durch die Übernahme der bereits in elektronischer Form vorliegenden Dokumente [Häber et al. 2005]. Es existieren zwei unterschiedliche Ansätze für die Elektronische Patientenakte:

1. Bei der Elektronischen Patientenakte handelt es sich um ein digitales Archiv. Dabei wird die Einhaltung der rechtlichen Pflichten nicht automatisch gewährleistet. Es muss u.a. sichergestellt sein, dass die Daten und Dokumente nachträglich nicht geändert werden können und bis zu 30 Jahre lang lesbar sind (was z.B. bei Worddokumenten nicht gewährleistet ist).
2. Nach Abschluss der Behandlung eines Patienten muss die Elektronische Patientenakte archiviert werden. Dazu wird die Elektronische Patientenakte in einem digitalen Archiv abgelegt, welches die Einhaltung der rechtlichen Pflichten gewährleistet.

Die EPA bietet eine Vielzahl von Vorteilen:

- mehrere Nutzer können gleichzeitig und von verschiedenen PCs innerhalb des Krankenhauses auf die Patientenakte zugreifen
- zeitnaher Zugriff auf die Patientenunterlagen
- je nach Personengruppe und Informationsbedürfnis sind verschiedene Sichten auf die Daten möglich
- Möglichkeit der Nutzung von Such- und Sortierfunktionen
- Reduzierung des Personalaufwandes, der z.B. durch den Aktentransport entsteht
- Akte kann nicht verlegt werden.

Die digitale Archivierung einer Patientenakte ermöglicht, dass auch die archivierten Patientenunterlagen innerhalb der gesetzlich vorgeschriebenen Aufbewahrungsdauer schnell und zeitnah zur Verfügung stehen und nicht erst manuell aus Archiven herausgesucht werden müssen. Weiterhin beansprucht die Archivierung der Elektronischen Patientenakte in einem digitalen Archiv wenig Raum und der Einsatz digitaler Medien ist laut [Häber et al. 2005] kostengünstiger im Vergleich zur konventionellen Archivierung. Allerdings ist es nicht ausreichend, wenn die Patientenunterlagen in elektronischer Form auf digitalen Datenträgern abgelegt werden. Es muss

zusätzlich sichergestellt sein, dass die Daten und Dokumente ordnungsgemäß, revisionssicher und rechtlich anerkannt aufbewahrt werden [Häber et al. 2005].

Jedoch stehen die Entwicklung und der Einsatz der Elektronischen Patientenakte in deutschen Krankenhäusern erst am Anfang [Häber et al. 2005]. Das trifft auch für den Einsatz digitaler Archive zu. Nach Einschätzung der Arbeitsgruppe „Archivierung von Krankenunterlagen“ der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V. gibt es zurzeit (Stand Mitte 2005):

- ca. 25 Krankenhäuser, die bereits ein vollständig integriertes digitales Archiv einsetzen und die sowohl bei der Dokumentation als auch bei der Archivierung weitestgehend papierlos arbeiten.
- ca. 300 Krankenhäuser, die für die digitale Archivierung vermehrt digitale Online-Dokumentation und -Speicherung oder hybride Dienstleistungsverfahren wie z.B. Scannen und/oder Mikroverfilmung einsetzen. Hierbei wird aber überwiegend noch Papier als Medium genutzt.
- ca. 300 Krankenhäuser, die ein Bildspeicher- und Kommunikationssystem (Picture Archiving and Communication System, PACS) in unterschiedlicher Ausprägung in der diagnostischen Radiologie einsetzen [Häber et al. 2005].

Bei der Entscheidung für den Einsatz eines digitalen Archivs steht der Informationsmanager eines Krankenhauses vor einer schwierigen Aufgabe. Es gibt eine Vielzahl von Lösungen, die zur digitalen Archivierung angeboten werden. Um eine optimale Lösung für das eigene Krankenhaus zu finden, kann zur Orientierung ein Leitfaden der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. für das rechnerunterstützte Dokumentenmanagement und die digitale Archivierung von Patientenunterlagen verwendet werden.

1.1.2 Problematik

Auf dem Markt wird eine Vielzahl von Lösungen für die digitale Archivierung angeboten. Der Informationsmanager eines Krankenhauses hat die Aufgabe, die am Markt und in der Literatur angebotenen Lösungsvorschläge zu vergleichen. Dabei wird er mit dem Problem konfrontiert, dass die Anbieter keine einheitliche Terminologie, aber auch unterschiedliche Techniken und Lösungsarchitekturen verwenden. Damit sind die Lösungen schwer vergleichbar. Oft sind die angebotenen Funktionalitäten kaum identifizierbar. Aus diesem Grund ist auch nur schwer erkennbar, in welcher Form bereits eingesetzte Anwendungsbausteine im eigenen Krankenhaus Funktionen ergänzen oder unnötig duplizieren. Insbesondere stellt sich die Frage, wie die ordnungsgemäße, revisionssichere und rechtlich anerkannte Aufbewahrung von Patientenunterlagen in einem digitalen Archiv umgesetzt wird. Einige Anbieter werben z.B. mit dem Argument, dass durch den Einsatz ihres Produktes eine rechtssichere Archivierung gewährleistet ist, wobei sie sich mit dieser Aussage meist nur auf die eingesetzten Speichermedien beziehen [Häber et al. 2005]. Der Einsatz von nur einmal beschreibbaren Speichermedien reicht in der Regel nicht aus, um eine rechtssichere Archivierung sicherzustellen. Außerdem ist auch nicht hinreichend geklärt, welche Anforderungen sich an die Langzeitarchivierung von elektronisch signierten Dokumenten ergeben.

Ein Hilfsmittel zum Verständnis und zur Vergleichbarkeit könnte eine Modellierung der Architekturen im 3LGM^2-Modell sein. Die Darstellung der einzelnen digitalen Archive ist jedoch mit viel Aufwand verbunden. Zum einen liegt das daran, dass die Anbieter unterschiedliche Terminologien verwenden, zum anderen sind auch nur unzureichende Details über die einzelnen digitalen Archive verfügbar. In dieser Arbeit soll nun versucht werden, die für ein digitales Archiv angebotenen Hard- und Softwareprodukte der Firmen d.velop AG, forcont business technology GmbH, Heydt-Verlags-GmbH und EMC^2 mit Hilfe des 3LGM^2-Modells zu beschreiben.

Der von der GMDS-Arbeitsgruppe „Archivierung von Krankenunterlagen“ erarbeitete Leitfaden bietet einen guten Überblick, worauf bei der Einführung eines digitalen Archivs zu achten ist. Jedoch ist dieser Leitfaden nicht ausreichend. Es fehlt im deutschen Gesundheitswesen und in der Medizinischen Informatik ein Referenzmodell für die digitale Archivierung von Patientenunterlagen. Unter Bezugnahme auf dieses Referenzmodell wäre ein Vergleich der angebotenen digitalen Archive möglich und der Informationsmanager könnte ein konkretes Modell für sein Informationssystem

erstellen. Anhand dieses konkreten Modells kann er genau feststellen, wie sich das digitale Archiv in sein vorhandenes Informationssystem einfügen würde.

Im Rahmen dieser Diplomarbeit sollen auch internationale Bestrebungen für die digitale Archivierung von Patientenunterlagen mit einbezogen werden.

1.1.3 Motivation

Die Entwicklung eines Referenzmodells für die digitale Archivierung von Patientenunterlagen ist notwendig, um den Informationsmanager eines Krankenhauses bei der Einführung eines digitalen Archivs zukünftig unterstützen zu können. Da die verschiedensten Lösungen für ein digitales Archiv angeboten werden, ist es schwierig, zu entscheiden, welche Lösung für das eigene Krankenhaus optimal ist. Das Referenzmodell bietet zur Unterstützung zwei wichtige Funktionalitäten an:

1. Mit Hilfe eines Referenzmodells können die einzelnen digitalen Archivlösungen bezüglich der Unterschiede und Gemeinsamkeiten verglichen und bewertet werden. Dadurch wird die Entscheidung für oder gegen ein digitales Archiv von einem bestimmten Anbieter einfacher.
2. Ein weiterer wichtiger Aspekt ist die Integration des digitalen Archivs in das vorhandene Informationssystem eines Krankenhauses. Das Referenzmodell kann als Vorlage dienen, um ein konkretes Modell für die digitale Archivierung im eigenen Krankenhaus zu modellieren. Dabei werden aus dem Referenzmodell zunächst die Aufgaben abgeleitet, die das eigene digitale Archiv unterstützen sollte. Zusätzliche Aufgaben können im konkreten Modell noch hinzugefügt werden. Im nächsten Schritt ist festzustellen, ob bestimmte Aufgaben bereits durch andere Anwendungsbausteine im Informationssystem erledigt werden. Damit erhält der Informationsmanager einen Überblick, welche Komponenten für das digitale Archiv einzukaufen sind.

Ohne das Referenzmodell sind die angebotenen digitalen Archive der einzelnen Anbieter nur schwer zu vergleichen. Das Referenzmodell soll dem Informationsmanager dazu dienen, das für sein Krankenhaus am besten geeignete digitale Archiv zu finden. Gleichzeitig sollte auch erkennbar sein, wie sich das digitale Archiv in das vorhandene Krankenhausinformationssystem einfügt. Vor allem soll verhindert werden, dass die gleichen Funktionalitäten von verschiedenen Anwendungsbausteinen mehrfach ausgeführt werden.

1.2 Problemstellung

Problem P1: Zurzeit gibt es kein Referenzmodell für die digitale Archivierung von Patientenunterlagen, das zur Orientierung oder für Vergleichszwecke herangezogen werden kann.

Problem P2: Auf dem Markt und in der Literatur gibt es eine Vielzahl von Lösungsvorschlägen zur digitalen Archivierung, die kaum vergleichbar sind.

1.3 Zielsetzung

Aus den oben genannten Problemen lassen sich folgende Ziele für die Diplomarbeit ableiten:

Angestrebtes Ziel für Problem P1:

Z1: Ziel dieser Arbeit ist: ein 3LGM^2-basiertes Referenzmodell für die digitale Archivierung von Patientenunterlagen.

Angestrebtes Ziel für Problem P2:

Z2: Ziel dieser Arbeit ist: ein Vergleich ausgewählter Hard- und Softwareprodukte für die digitale Archivierung von 4 Anbietern mit diesem Referenzmodell.

1.4 Aufgaben-/Fragestellungen

Fragen zu Ziel 1:

F1: Wie lässt sich mit Hilfe des 3LGM^2-Baukastens ein Referenzmodell erstellen?

F1.1: Welche Aufgaben und Funktionalitäten sollte ein digitales Archiv unterstützen?

F1.2: Welche Verfahren und Methoden zur digitalen Archivierung von Patientenunterlagen werden zurzeit in Krankenhäusern eingesetzt?

F1.3: Welche Aufgaben und Objekttypen sind auf der fachlichen Ebene des 3LGM^2-Modells zu modellieren?

F1.4: Welche Werkzeuge unterstützen die Erledigung dieser Aufgaben auf der logischen Werkzeugebene?

F1.5: Wie sieht die physische Werkzeugebene aus?

F1.6: Inwieweit ist es notwendig, zusätzlich zum 3LGM^2-Modell noch andere Modellierungsmethoden und -werkzeuge einzusetzen, um die erforderlichen Aussagen in einem Referenzmodell treffen zu können?

F1.7: Welche Notwendigkeiten ergeben sich, das 3LGM^2-Modell zu erweitern?

Aufgaben zu Ziel 2:

F2: Wie lassen sich aus dem 3LGM^2-basierten Referenzmodell spezielle Modelle von vier ausgewählten Anbietern ableiten?

A2.1: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma d.velop AG mit Hilfe des 3LGM^2-Baukastens

A2.2: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma Heydt-Verlags-GmbH mit Hilfe des 3LGM^2-Baukastens

A2.3: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma forcont business technology GmbH mit Hilfe des 3LGM^2-Baukastens

A2.4: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma EMC^2 mit Hilfe des 3LGM^2-Baukastens

F2.5: Was bieten diese Firmen an zusätzlichen Funktionalitäten an?

1.5 Vorgehensweise und Aufbau der Arbeit

Die Diplomarbeit gliedert sich in neun Kapitel. Im Kapitel 1 wurden bereits der Gegenstand, die Problematik und die Motivation der Arbeit erläutert. Um eine einheitliche Begriffsbasis zu schaffen, werden im Kapitel 2 die Grundlagen geklärt, die für das weitere Verständnis der Arbeit erforderlich sind.

Das Kapitel 3 enthält eine Beschreibung der Funktionen, die ein digitales Archiv anbieten sollte. Aus den Funktionen lassen sich die einzelnen Aufgaben ableiten.

Im Kapitel 4 erfolgt die schrittweise Erstellung des Referenzmodells mit Hilfe des 3LGM^2-Baukastens.

Im Kapitel 5 werden aus dem Referenzmodell die für die digitale Archivierung angebotenen Hard- und Softwareprodukte von den Anbietern d.velop AG, Heydt-Verlags-GmbH, forcont business technology GmbH und EMC^2 abgeleitet. Ein Vergleich dieser Produkte mit dem Referenzmodell erfolgt im Kapitel 6. Dabei werden die einzelnen Ebenen der 3LGM^2-Modelle gegenübergestellt.

Das Kapitel 7 enthält einige Betrachtungen und Herangehensweisen zur Archivierung in den Ländern Belgien, Österreich und USA.

Die Ergebnisse der Arbeit werden im Kapitel 8 diskutiert. Anhand der eingangs gestellten Fragen wird überprüft, ob die Ziele der Arbeit erreicht wurden. Zum Abschluss wird ein Ausblick auf zukünftige Entwicklungen gegeben.

Das Kapitel 9 beinhaltet den Anhang.

2 Grundlagen

In diesem Abschnitt sollen zunächst die theoretischen Grundlagen geklärt werden, die für das weitere Verständnis der Arbeit erforderlich sind.

2.1 Patientenunterlagen

Der Begriff Patientenunterlagen bezieht sich auf alle Daten und Dokumente, die im Zusammenhang mit der Behandlung eines Patienten erzeugt werden. Dazu gehören z.B. Arztbriefe, Befunde, Bilder, Anamnesen, klinische Dokumentationen (z.B. die ärztliche und pflegerische Dokumentation), Medikamentenanordnungen, Leistungsanforderungen, Signale, Filme, aber auch Abrechnungsunterlagen [Häber et al. 2005].

2.2 Klinisches Arbeitsplatzsystem

Klinische Arbeitsplatzsysteme (KAS) unterstützen das ärztliche und pflegerische Personal auf den Stationen und in den Ambulanzen bei der Erledigung ihrer Aufgaben. Auf einem Arbeitsplatzrechner stehen dem medizinischen Personal die für die jeweiligen Aufgaben erforderlichen Anwendungsbausteine zur Verfügung [Winter et al. 2005]. Nach [Haux et al. 2004] besteht ein KAS aus einem mobilen oder stationären PC zusammen mit den darauf installierten Anwendungsbausteinen und den damit unterstützten Aufgaben. Das KAS unterstützt nach [Winter et al. 2005] u.a. die folgenden Aufgaben:

- Klinische Dokumentation
- Arztbriefschreibung
- Leistungsdokumentation
- Stationsmanagement
- Pflege.

Weiterhin sollte das KAS den Zugang zu aktuellem medizinischen Wissen bereitstellen.

Ein KAS stellt ein Subsystem des Krankenhausinformationssystems dar.

2.3 Krankenhausinformationssysteme

In einem Krankenhaus werden Informationen in unterschiedlichen Bereichen (z.B. Station, Ambulanz, Radiologie, Labor, Sekretariat, Verwaltung) durch verschiedene Personengruppen (z.B. Ärzte, Pflegekräfte, Verwaltungspersonal) erzeugt und bearbeitet. Für eine optimale Pflege und Behandlung eines Patienten ist es erforderlich, dass diese Informationen zwischen den einzelnen Personengruppen und Bereichen ausgetauscht werden. Oftmals werden die Informationen an einem anderen Ort erfasst, wo sie später verarbeitet werden. Durch geeignete Werkzeuge kann der Austausch und die Verarbeitung dieser Informationen unterstützt werden.

Ein Krankenhausinformationssystem ist:

„… das soziotechnische Teilsystem eines Krankenhauses, das alle informationsverarbeitenden (und –speichernden) Prozesse und die an ihnen beteiligten menschlichen und maschinellen Handlungsträger in ihrer informationsverabeitenden Rolle umfasst. Das KIS dient dazu, die Mitarbeiter des Krankenhauses bei der Erledigung der Aufgaben zu unterstützen. Es umfasst daher

- *alle Bereiche des Krankenhauses*
- *alle Gebäude des Krankenhauses und*
- *alle Personengruppen, die im Krankenhaus tätig sind.“* [Winter et al. 2005, Seite 552]

Nach dieser Definition besitzt jedes Krankenhaus ein KIS, das je nach dessen Größe und Ausrichtung von unterschiedlicher Komplexität sein kann.

Ein KIS umfasst sowohl den rechnerunterstützten als auch den nicht-rechnerunterstützten Teil eines Krankenhauses. Der rechnerunterstützte Teil des KIS setzt rechnerbasierte Werkzeuge für die Informationsverarbeitung ein. Dazu gehören z.B. PCs, Datenbanken, Kommunikations- und Dokumentationssysteme. Obwohl immer mehr rechnerbasierte Werkzeuge zum Einsatz kommen, wird eine Vielzahl von konventionellen Werkzeugen genutzt, die den nicht-rechnerunterstützten Teil des KIS bilden. Zu diesen Werkzeugen zählen z.B. die papierbasierte Patientenakte, Schreibmaschine, Kopierer und Formulare.

Das Ziel eines KIS ist es, die Aufgaben eines Krankenhauses zu unterstützen. Zu den primären Aufgaben eines Krankenhauses gehören die Patientenaufnahme, die Behandlungsplanung, die Leistungskommunikation, die Durchführung von Maßnahmen, die klinische Dokumentation sowie die Entlassung und Weiterleitung eines Patienten. Nach [Haux et al. 2004] stellt das KIS

- berechtigten Personen Patienteninformationen vollständig, zum richtigen Zeitpunkt, am richtigen Ort und in der richtigen Form,
- Wissen über Krankheiten und Nebenwirkungen zur Unterstützung der Diagnose und Therapie,
- Informationen über die Qualität der Patientenversorgung, Leistungen und Kosten innerhalb eines Krankenhauses

zur Verfügung.

Zur Unterstützung dieser Aufgaben können für den rechnerunterstützten Teil des KIS Anwendungsbausteine gekauft werden. So werden z.B. für die klinische Dokumentation Klinische Dokumentations- und Managementsysteme, für die Radiologie Radiologieinformationssysteme, für das Labor Laborinformationssysteme und für den operativen Bereich OP-Planungs- und Dokumentationssysteme auf dem Markt angeboten. Im Allgemeinen stammen die in einem Krankenhaus eingesetzten rechnerbasierten Anwendungsbausteine, die auf Softwareprodukten basieren, von unterschiedlichen Herstellern oder sind zum Teil auch Eigenentwicklungen. Bei der Einführung eines neuen Anwendungsbausteins ist also darauf zu achten, dass er sich gut in das vorhandene KIS integrieren lässt. Das trifft auch für den Einsatz digitaler Archive zu. Ein Archivierungssystem sollte vollständig in den rechnerunterstützten Teil eines KIS und insbesondere im Klinischen Arbeitsplatzsystem integriert sein [Häber 2005]. Nur durch eine hohe Integration ist es möglich, die elektronischen Dokumente in das digitale Archiv zu übernehmen und dort abzulegen. Da die Integration ein wesentlicher Aspekt bei der digitalen Archivierung ist, soll im folgenden Abschnitt näher auf die Integration eingegangen werden.

2.4 Integration

„Integration ist der Zusammenschluss von Teilen zu einem Ganzen, das gegenüber seinen Teilen eine neue Qualität aufweist. Ein integriertes KIS besteht nicht nur aus einer Menge unabhängiger Komponenten, sondern die Komponenten arbeiten auch eng zusammen“. [Winter et al. 2005, Seite 584]

In Anlehnung an [Winter et al. 2005] sollen in diesem Abschnitt die verschiedenen Arten der Integration erläutert werden.

Datenintegration

Datenintegration ist in einem KIS gewährleistet, wenn einmal erfasste Daten überall dort zur Verfügung stehen, wo sie benötigt werden. Damit soll vermieden werden, dass ein und dieselben Patientendaten mehrfach aufgezeichnet werden. Nach [Haux et al. 2004] ist die Datenintegration die Voraussetzung für die multiple Verwendbarkeit von Patientendaten, d.h. einmal aufgezeichnete Daten können für verschiedene Ziele, Fragen und Aufgaben verwendet werden [Leiner et al. 2006]. Ein Beispiel für eine fehlende Datenintegration ist, wenn eine Anamnese zu einem Patienten in einem Krankenhaus mehrfach erhoben und gespeichert wird.

Funktionsintegration

Funktionsintegration ist gegeben, wenn die von einem Anwendungsbaustein angebotenen Funktionen überall dort genutzt werden können, wo sie benötigt werden. Dabei können auf einem Arbeitsplatz Funktionen von verschiedenen Anwendungsbausteinen zur Verfügung stehen. Um die von einem Archivierungssystem angebotenen Funktionen z.B. im Klinischen Arbeitsplatzsystem nutzen zu können, muss die Funktionsintegration gewährleistet sein. Ist das gegeben, können Funktionen z.B. für die Recherche und Anzeige von archivierten Patientenunterlagen aufgerufen werden.

Präsentationsintegration

Präsentationsintegration bedeutet, dass unterschiedliche Anwendungsbausteine ihre Daten und Benutzeroberfläche in einer einheitlichen Weise präsentieren. So wird z.B. der Name des gerade bearbeiteten Patienten an nahezu derselben Stelle auf dem Bildschirm angezeigt, die Darstellung der Messwerte erfolgt in derselben Einheit und es werden die gleichen Symbole in den unterschiedlichen Anwendungsbausteinen verwendet. Durch die Präsentationsintegration wird gewährleistet, dass der Anwender innerhalb der verschiedenen Anwendungsbausteine in einer für ihn gewohnten und vertrauten Oberfläche arbeiten kann.

Kontextintegration

Durch die Funktions- und Präsentationsintegration auf dem Arbeitsplatzrechner wird bereits eine hohe Qualität der Integration erreicht. Um jedoch zu vermeiden, dass bei einem Wechsel des Anwendungsbausteins der Anwender sich erneut anmelden und den Kontext wiederherstellen muss, ist die Kontextintegration erforderlich. Durch die Kontextintegration wird erreicht, dass bei einem Wechsel des Anwendungsbausteins der einmal hergestellte Kontext in dem neuen Anwendungsbaustein weiter genutzt werden kann. Als Kontext können u.a. Informationen zum Benutzer, Fall, Patienten oder zum Dokument übergeben werden. Die übergebenen Kontextinformationen können z.B. in einem Archivierungssystem als Rechercheinformationen verwendet werden. Die Kontextintegration wird auch als visuelle Integration bezeichnet.

2.5 3LGM^2 – Eine Methode zur Beschreibung von Krankenhausinformationssystemen

Das 3LGM^2 ist ein Drei-Ebenen-Meta-Modell (Three Layer Graph Based Meta-Model). Es wurde entwickelt, um die Beschreibung, Bewertung und Planung von Informationssystemen im Gesundheitswesen zu unterstützen [3LGM^2]. Um Krankenhausinformationssysteme planen, steuern und überwachen zu können, ist eine Beschreibung der Architektur des Informationssystems erforderlich. Anhand dieser Beschreibung kann man erkennen, aus welchen klar abgrenzbaren Bausteinen das Krankenhausinformationssystem besteht bzw. wie es sich in diese Bausteine zerlegen lässt [Winter et al. 2005]. Mit Hilfe des 3LGM^2-Baukastens ist die Modellierung der Architektur eines Krankenhausinformationssystems möglich.

Wie der Name des Meta-Modells schon sagt, besteht das 3LGM^2 aus 3 Ebenen. Die nachfolgenden Erläuterungen für diese Ebenen im 3LGM^2 sind aus [Brigl et al. 2003], [Brigl et al. 2004] und [Winter et al. 2005] entnommen.

Fachliche Ebene

Die fachliche Ebene beschreibt die von einem KIS unterstützten Aufgaben eines Krankenhauses, die Objekttypen, die im Rahmen der Erledigung dieser Aufgaben jeweils bearbeitet bzw. interpretiert werden und die Organisationseinheiten, die diese Aufgaben erledigen. Abbildung 2-1 stellt die UML-Notation der fachlichen Ebene dar.

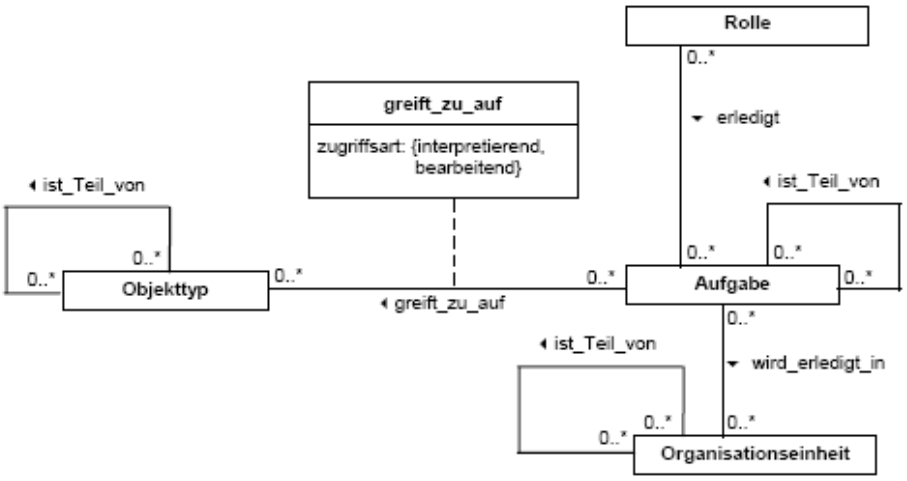


Abbildung 2-1: Das Meta-Modell der fachlichen Ebene

(entnommen aus [3LGM^2])

Logische Werkzeugebene

Auf der logischen Werkzeugebene werden Anwendungsbausteine (Synonym: Anwendungssystem) modelliert. Anwendungsbausteine bieten Unterstützung bei der Erledigung der auf der fachlichen Ebene dargestellten Aufgaben und verarbeiten, speichern und transportieren Daten. Es ist zwischen rechnerbasierten und konventionellen Anwendungsbausteinen zu unterscheiden:

- Rechnerbasierte Anwendungsbausteine basieren auf einem Softwareprodukt, das speziell an ein Krankenhaus angepasst bzw. parametriert werden muss. Die Daten werden in einem Datenbanksystem gespeichert.
- Konventionelle Anwendungsbausteine werden durch Organisationspläne gesteuert. Die Speicherung der Daten in Form von Dokumenten erfolgt in einer Dokumentensammlung.

Um den Zugriff auf entsprechende Informationen zu gewährleisten, ist eine Kommunikation zwischen den Anwendungsbausteinen erforderlich. Diese Kommunikation kann durch Schnittstellen zwischen den Anwendungsbausteinen (Bausteinschnittstelle) realisiert werden. Das UML-Klassendiagramm der logischen Werkzeugebene ist im Anhang dargestellt (vgl. Anhang Abbildung 9-1).

Physische Werkzeugebene

Auf der physischen Werkzeugebene werden die physischen Datenverarbeitungsbausteine modelliert, die zur Realisierung und für den Betrieb der Anwendungsbausteine erforderlich sind. Ein physischer Datenverarbeitungsbaustein kann entweder ein System von Personen und konventionellen Werkzeugen (z.B. Archivregale, papierbasierte Patientenakte, Formulare) oder ein Rechnersystem (z.B. PC, Server, Router, Drucker) sein. Durch die Kommunikation der physischen Datenverarbeitungsbausteine über Datenübertragungsverbindungen entsteht ein physisches Netzwerk. Innerhalb des Netzwerkes können die physischen Datenverarbeitungsbausteine verschiedenen Subnetzen zugeordnet sein. Die Subnetze sind von einem Netztyp und basieren auf Netzwerkprotokollen. In der Abbildung 2-2 ist das Klassendiagramm der physischen Werkzeugebene dargestellt.

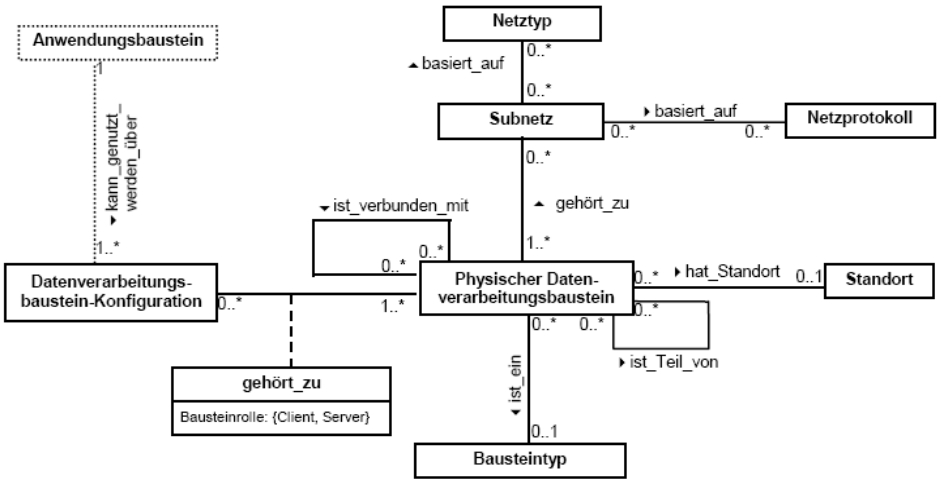


Abbildung 2-2: Das Meta-Modell der physischen Werkzeugebene (entnommen aus [3LGM²])

Eine Legende zur graphischen Darstellung der Elemente im 3LGM²-Baukasten befindet sich im Anhang in Abbildung 9-2.

Inter-Ebenen-Beziehungen

Zwischen den einzelnen Ebenen existieren Beziehungen, die so genannten Inter-Ebenen-Beziehungen, die im Meta-Modell durch gepunktete Linien und Symbole dargestellt werden.

Die Anwendungsbausteinkonfiguration repräsentiert die Beziehung zwischen den Aufgaben der fachlichen Ebene und den Anwendungsbausteinen der logischen Werkzeugebene. Dabei kann eine Aufgabe entweder durch mehrere Anwendungsbausteine gemeinsam, durch einen einzelnen Anwendungsbaustein oder durch eine Kombination dieser Anwendungsbausteine unterstützt werden. Die Anwendungsbausteinkonfiguration enthält somit alle Anwendungsbausteine, die notwendig sind, um gemeinsam eine Aufgabe zu erledigen. Es kann auch vorkommen, dass eine Aufgabe durch mehrere Anwendungsbausteinkonfigurationen unterstützt wird. Die Inter-Ebenen-Beziehung zwischen der fachlichen und der logischen Ebene beschreibt auch, in welchen Datenbanksystemen die Objekttypen gespeichert sind und wie diese repräsentiert werden.

Die Datenverarbeitungskonfiguration stellt die Inter-Ebenen-Beziehungen zwischen den Anwendungsbausteinen der logischen Werkzeugebene und den physischen Datenverarbeitungsbausteinen der physischen Werkzeugebene dar. Diese Beziehung beschreibt, ob der rechnerbasierte Anwendungsbaustein auf mehreren physischen Datenverarbeitungsbausteinen gemeinsam, auf einem einzelnen physischen Datenverarbeitungsbaustein oder auf einer Kombination davon installiert ist.

2.6 Referenzmodelle für Krankenhausinformationssysteme

Die folgenden Ausführungen sind [Winter et al. 1999a] entnommen.

Für ein erfolgreiches Management von Krankenhausinformationssystemen werden je nach Ausprägung von Planungshorizont, Aufgabe und Gegenstandsebene unterschiedliche Modelle benötigt. Um diese Modelle zu realisieren, können Referenzmodelle eingesetzt werden.

Ein Referenzmodell stellt für eine gewisse Klasse zu modellierender Sachverhalte Modellmuster bereit. Aus diesen Modellmustern können durch geeignet erscheinende Modifikationen, Einschränkungen oder Ergänzungen konkrete Modelle abgeleitet werden. Solche Muster können zum

Vergleich mit vorhandenen Modellen herangezogen werden, um z.B. die Vollständigkeit der Modelle zu bewerten.

Der Begriff des Referenzmodells wird wie folgt definiert:

> *„Sei eine Klasse S von Sachverhalten gegeben. Ein Modell R ist Referenz für S oder R ist ein Referenzmodell für die Klasse S, genau dann wenn R ein allgemeines Modell ist, das:*
>
> - *als Grundlage für die Konstruktion spezieller Modelle für Sachverhalte der Klasse S oder*
> - *als Vergleichsobjekt für Modelle von Sachverhalten der Klasse S*
>
> *dienen kann.“* [Winter 1999a, Seite 176]

Aus einem Referenzmodell können spezielle Modelle abgeleitet werden, die durch Konkretisierung bzw. durch die Festlegung diskriminierender Eigenschaften innerhalb eines Referenzmodells entstehen. Um spezielle Modelle zu entwickeln, sollte dem Referenzmodell ein Vorgehensmodell zugeordnet sein. Dieses Vorgehensmodell beschreibt, in welcher Weise sich spezielle Modelle auf der Grundlage des Referenzmodells konstruieren lassen bzw. wie das Referenzmodell als Vergleichsobjekt benutzt werden kann. So lassen sich z.B. spezielle Modelle, die aus demselben Referenzmodell abgeleitet wurden, bezüglich der Gemeinsamkeiten und Unterschiede gegenüber dem Referenzmodell vergleichen.

Je nachdem für welche Klasse der Sachverhalte ein Referenzmodell erstellt werden soll, werden die folgenden Typen von Referenzmodellen unterschieden:

- Organisations-Referenzmodelle: dienen zur Modellierung der (Produktions-) Abläufe, Daten- und Organisationsstrukturen einer Klasse von Organisationen. Spezielle Organisations-Referenzmodelle sind Informationssystem-Referenzmodelle. Bei Informationssystem-Referenzmodellen steht die Informationsverarbeitung einer Klasse von Organisationen im Vordergrund.
- Software-Referenzmodelle: dienen zur Modellierung verschiedener, durch Parametrierung erzeugbare Varianten eines (Standard-) Softwareprodukts.
- Vorgehens-Referenzmodelle: sind allgemeine Modelle für eine Klasse von Vorgehensweisen z.B. bei Projekten.

2.7 Elektronische Patientenakte

2.7.1 Begriffsdefinition

Die Elektronische Patientenakte ist laut [Haas 2005]

„die teilweise oder vollständig auf elektronischen (digitalen) Speichermedien und nach definierten Ordnungskriterien abgelegte Sammlung der medizinischen Informationen zu einem Patienten sowie eine zugehörige Interaktions- und Präsentationskomponente zum Navigieren in und Arbeiten mit der Akte.“ [Haas 2005, Seite 199]

Die in einer EPA abgelegten medizinischen Informationen zu einem Patienten stammen aus den verschiedenen rechnerbasierten Anwendungsbausteinen eines KIS. Eine Vielzahl der Dokumente (z.B. Arztbriefe) entsteht im KAS. Jedoch beinhaltet die EPA auch Patientendaten und -dokumente, die z.B. im Radiologieinformationssystem (RIS), Bildspeicher- und Kommunikationssystem (PACS), Laborinformationssystem (LIS) oder im Patientenverwaltungssystem (PVS) erzeugt wurden. Eine EPA enthält neben den Dokumenten auch Bilder (z.B. Röntgenbilder) und Signale (EKG, EEG, EMG). Der Zugriff auf die Daten und Dokumente der EPA sollte über das KAS erfolgen. Für die Speicherung der EPA in einem KIS existieren zwei Ansätze [Dujat 1996]:

1. Verteilter Ansatz: Beim verteilten Ansatz sind die Patientendaten physisch verteilt in den rechnerunterstützten Anwendungsbausteinen des KIS gespeichert. Die EPA besteht also lediglich aus Verweisen auf die originalen Daten und

Dokumente. Um die Konsistenz der Daten und die referentielle Integrität zu gewährleisten, ist eine Kommunikation und Synchronisation der Daten zwischen den einzelnen Anwendungsbausteinen erforderlich. Dabei können sich jedoch die unterschiedlichen Datenstrukturen in den Anwendungsbausteinen als problematisch erweisen.

2. Zentraler Ansatz: Beim zentralen Ansatz sind alle verfügbaren Daten und Dokumente zu einem Patienten in einer zentralen Patientendatenbank abgelegt. Die rechnerunterstützten Anwendungsbausteine des KIS stellen die Daten und Dokumente in elektronischer Form zur Verfügung, die anschließend über geeignete Kommunikationsschnittstellen und Datenübertragungsverbindungen in die EPA übernommen werden. Die EPA stellt aber auch Informationen an Teilsysteme des KIS zur Verfügung. Bei diesem Ansatz kann es zu einer redundanten Datenhaltung kommen, da die Daten und Dokumente im erzeugenden Anwendungsbaustein und in der zentralen Datenbank, der EPA, abgelegt sind. Der zentrale Ansatz ist insbesondere im amerikanischen Raum verbreitet [Dujat 1996].

Die EPA entsteht jedoch nicht allein durch das Einscannen von Papierdokumenten mit anschließender Ablage auf digitalen Datenträgern. In diesem Fall wäre sie nur eine Kopie der konventionellen Patientenakte, die vor allem der Platz sparenden Ablage und dem schnellen Wiederfinden von Dokumenten dient [Haas 2005]. Um die in einer EPA enthaltenen Informationen z.B. für Recherchen, Auswertungen oder für die Beantwortung von patientenübergreifenden Fragestellungen nutzen zu können, müssen die Dokumente mit Hilfe von Deskriptoren beschrieben werden.

Am Universitätsklinikum Leipzig wird die Elektronische Patientenakte durch das Softwareprodukt i.s.h.med[1] repräsentiert, das auf dem SAP R/3 Modul IS-H aufbaut. Das SAP R/3 Modul IS-H bietet Unterstützung bei der stationären Patientenverwaltung und der klinischen Basisdokumentation. In IS-H werden u.a. Daten, die bei der Aufnahme, Verlegung und Entlassung eines Patienten (ADT-Daten) aufgenommen wurden, aber auch Informationen, die zur Abrechnung von Leistungen benötigt werden (z.B. Diagnosen, Prozeduren), erfasst. Über Schnittstellen erfolgt die Übertragung dieser Informationen an einen zentralen Kommunikationsserver und weitere Subsysteme des Universitätsklinikums. Damit stehen diese Informationen auch im i.s.h.med zur Verfügung. I.s.h.med ist ein Zusatzmodul, das die die medizinische Dokumentation in einem Krankenhaus unterstützt. Die einzelnen Module von i.s.h.med stellen u.a. Funktionalitäten für

- die Befund- und Arztbriefschreibung,
- die Unterstützung der Dokumentation mit Diktat- und Spracherkennungsfunktion,
- die Leistungs- und Pflegedokumentation,
- den Medikationsprozess,
- das Erstellen und Verfolgen von Leistungsanforderungen,
- die patienten- und produktbezogenen Dokumentation von chargenpflichtigen Materialien (z.B. Medikamente, Blutprodukte),
- die Planung und Verfolgung von Terminen eines Patienten über Terminkalender und Plantafeln in den verschiedenen Einrichtungen sowie
- die Planung und Behandlung von Patienten in der Ambulanz

zur Verfügung [i.s.h.med].

[1] i.s.h.med ist ein gemeinsam entwickeltes Produkt der Firmen GSD und T-Systems Austria

Die Organisation und Präsentation der medizinischen Patientendaten erfolgt durch den Patientenorganizer, der eine Funktion von i.s.h.med ist. Der Patientenorganizer ermöglicht die Darstellung der Dokumente unabhängig von der Struktur, dem Format oder dem physischen Speicherort der Informationen [Dörge 2003]. Somit wird auch die Anzeige von Dokumenten aus anderen Anwendungsbausteinen unterstützt. Die Darstellung der Dokumente erfolgt in der EPA.

Das Softwareprodukt i.s.h.med wird vor allem in größeren Krankenhäusern eingesetzt.

2.7.2 Computer-based Patient Record System

Im angelsächsischen Sprachraum wird oftmals auch von einem „(computer-based) patient record system“ gesprochen. An dieser Stelle entsteht die Frage, was unter dem Begriff „System“ zu verstehen ist.

1991 hat das Institute of Medicine (IOM) ein „patient record system“[2] definiert als eine Menge von Komponenten, die Mechanismen für die Erstellung, Verwendung, Speicherung und das Wiederauffinden von Patientenakten bereitstellen [Himss 2003]. In dieser Definition wird weiterhin gesagt, dass das „patient record system“ Personen, Daten, Regeln, Vorschriften, Verarbeitungs- und Speichergeräte (z.B. Papier und Stift, Hard- und Software) sowie die Kommunikation und unterstützende Funktionen einschließt.

Laut [Pryor 1992] wurde das „ Computer-based Patient Record System“ (CPR-System) für die Verwaltung von Patientenakten entwickelt. Die in der Patientenakte enthaltenen Daten und Dokumente können dabei entweder physisch verteilt oder zentral in einer Datenbank liegen. Nach [Ball 1992] gehören zu den Aufgaben eines CPR-Systems, dass:

- die Vertraulichkeit der patientenbezogenen Daten geschützt wird,
- nur autorisierte Nutzer Zugriff auf die benötigten Informationen haben,
- die Darstellung der Patientendaten benutzerspezifisch erfolgt,
- Ärzte bei ihren Entscheidungen unterstützt werden, in dem Links zu Wissens- oder Literaturdatenbanken existieren.

Nach [Pryor 1992] muss das CPR-System weiterhin

- sicherstellen, dass die Konsistenz und Integrität der Daten in der Patientenakte gewährleistet sind,
- den Eintrag von redundanten Daten aus verschiedenen Quellen verhindern,
- den Zugriff auf die Patientenakte gewährleisten, unabhängig davon, in welchem Anwendungssystem die Daten erzeugt wurden.

Das CPR-System ist ein Baustein in einem medizinischen Informationssystem, in dem alle Daten und Dokumente zu einem Patienten aus den verschiedenen Anwendungsbausteinen integriert werden [Dick et al. 1992].

In der Literatur wird weiterhin der Begriff „electronic health record system“ (EHR-System) verwendet. Dazu ist zunächst der Unterschied zwischen einem „electronic health record“ (elektronische Gesundheitsakte) und einem „patient record“ (Patientenakte) zu erklären. Eine elektronische Gesundheitsakte ist institutionsübergreifend angelegt und enthält alle gesundheitsrelevanten Daten zu einer Person. Der Zugriff auf die elektronische Gesundheitsakte

[2] Die Definition wurde veröffentlicht in: Dick R.S., Steen E.B. (1991): The Computer-Based Patient Record: An Essential Technology for Health Care. National Acadamy Press: Washington DC. Die überarbeitete Version wurde 1997 veröffentlicht.

erfolgt in der Regel webbasiert [Blobel 2005]. Eine Patientenakte umfasst dagegen nur die medizinischen Informationen, die innerhalb einer Einrichtung erstellt wurden.

In Anlehnung an [Ruotsalainen P. 2004] soll der Unterschied zwischen einem EHR-System und einem Archiv erläutert werden.

Ein EHR-System ist ein Informationssystem, das die Aufzeichnung, das Wiederauffinden und die Veränderung von Informationen in einer elektronischen Gesundheitsakte unterstützt. Ein Archiv ist eine Organisation, die die Aufgabe hat, die Gesundheitsakten für den Zugriff und die Nutzung durch autorisierte Nutzer zu erhalten. EHR-Systeme und Archive können unterschiedlich miteinander kombiniert werden. Das EHR-System kann ein einzelnes Informationssystem sein, in das die Archivfunktionen integriert sind. Das Archiv und das EHR-System können aber auch kooperative oder förderative Informationssysteme sein. Beide haben gemeinsam, dass sie sich viele Sicherheitsdienste teilen. Zusätzlich benötigt die Archiv-Organisation dokumentierte Vorgehensweisen für die Aufbewahrung der Informationen, für den Zugriff und für die Verteilung von Informationen zwischen anderen Archiven.

Die EPA umfasst alle medizinischen Aufzeichnungen, die auf digitalen Datenträgern abgelegt sind. Der Zugriff, die Verfügbarkeit, die Präsentation, Verwaltung und das Wiederauffinden der abgelegten Informationen wird durch das CPR- bzw. EHR-System gewährleistet. Dieser Aspekt wird auch in der Definition der EPA von Haas berücksichtigt, die aussagt, dass zu einer EPA auch immer eine Interaktions- und Präsentationskomponente gehört.

2.7.3 Archivierte Elektronische Patientenakte

Nach Abschluss der Behandlung eines Patienten sind die Patientenunterlagen langfristig zu archivieren. Mit der Realisierung einer EPA und zur Umsetzung des Ziels, möglichst papierarm zu arbeiten, ist es natürlich nicht sinnvoll, die elektronisch erzeugten Patientenunterlagen auszudrucken, um sie im Anschluss daran in einer Papierakte zu archivieren. Es muss vielmehr eine Möglichkeit geben, die elektronisch erzeugten Dokumente zeitnah digital zu archivieren. Die Anzeige der archivierten Unterlagen wird dabei über die Archivierte Elektronische Patientenakte (APA) realisiert. Die APA ist eine virtuelle Akte, in der alle unveränderlichen Daten und Dokumente zu einem Patienten in einer übersichtlichen Aktenstruktur dargestellt werden. Laut [Häber et al. 2005] besteht die APA:

„aus Dokumenten, Bildern und sonstigen digitalen Objekten, die für die Langzeitaufbewahrung freigegeben und möglichst in geeigneten standardisierten Formaten unveränderbar abgelegt sind.“ [Häber et al. 2005, Seite 8]

Die APA enthält jedoch nur Verweise auf die entsprechenden archivierten Patientenunterlagen. Die Patientenunterlagen selbst werden in einem Ablagesystem aufbewahrt, das Bestandteil des digitalen Archivs ist. Die Aktenstruktur in einer APA wird an die Anforderungen des jeweiligen Krankenhauses angepasst und entspricht im Allgemeinen dem Aufbau einer Papierakte.

Die APA ist nach [Häber et al. 2005] ein Bestandteil der EPA. Der Benutzer kann in der Regel sowohl auf archivierte als auch auf in Bearbeitung befindliche Dokumente in der EPA zugreifen. Damit soll vermieden werden, dass zum einen eine Patientenakte für die archivierten und zum anderen eine Patientenakte für die in Bearbeitung befindlichen Dokumente existieren. Bei den archivierten Dokumenten muss jedoch sichergestellt sein, dass diese nicht mehr verändert werden können. Auf die archivierten Dokumente darf nur ein lesender Zugriff möglich sein. Die APA entsteht letztendlich durch Signierung und Transformation der Dokumente in der EPA.

2.8 Digitales Archiv

2.8.1 Entwicklung

Die Entwicklung von digitalen Archiven begann Mitte der 80er Jahre mit der Archivierung von gescannten Dokumenten (Imaging) [Weiß et al. 2005]. Hier stand vor allem die unveränderbare Ablage von Dokumenten auf Datenträgern im Vordergrund. Im Laufe der Jahre entstanden neue

Anforderungen bezüglich der Bearbeitung und Verteilung von Dokumenten, so dass die Entwicklung in Richtung Dokumentenmanagementsysteme ging. Heute sind die Dokumentenverwaltung und Dokumentenablage die Kernkomponenten von elektronischen Dokumentenmanagement- und Archivierungssystemen (DMAS). Dabei ist das elektronische Dokumentenmanagement für das Verwalten und Wiederauffinden von Dokumenten und anderen Objekten zuständig, während das Archivierungssystem die Aufbewahrung von Dokumenten über einen längeren Zeitraum unterstützt [Schmücker et al. 2006]. Das Archivierungssystem ist immer ein integraler Bestandteil von Dokumentenmanagementsystemen. Die Umkehrung muss aber nicht zwingend gelten [Klingelhöller 2001].

Nach [Schmücker 1996c] wurden die ersten elektronischen Dokumentenmanagement- und Archivierungssysteme für Patientenakten in deutschen Krankenhäusern vorwiegend ab 1994 installiert. Die ersten DMAS konnten nur teilweise mit anderen Anwendungssystemen kommunizieren und waren zum Teil noch nicht in das Netzwerk des Krankenhauses eingebunden. Die heutige Entwicklung geht dahin, das digitale Archiv vollständig in den rechnerunterstützten Teil des KIS zu integrieren.

2.8.2 Definition

Ein Archiv im ursprünglichen Sinn ist eine

„Einrichtung zur systemat. Erfassung, Ordnung, Verwahrung, Verwaltung, und Verwertung von Schriftgut, Bild- und/oder Tonträgern (Archivalien).“ [Brockhaus 2004, Seite 204]

In einem Archiv erfolgt die dauerhafte Aufbewahrung von Unterlagen. Patientenunterlagen sind jedoch gemäß gesetzlicher Aufbewahrungspflichten und Verjährungsbestimmungen nur für einen begrenzten Zeitraum (in der Regel 30 Jahre) aufzubewahren. Krankenhaus-Archive dienen also nicht zur dauerhaften, sondern zur Langzeitaufbewahrung von Patientenunterlagen. Der Begriff des Archivs wird an dieser Stelle für die Ablage der Dokumente auf Zeit verwendet. Nach [Häber et al. 2005] muss das digitale Archiv die ordnungsgemäße, revisionssichere und rechtlich anerkannte Aufbewahrung von Daten, Dokumenten, Bildern, Signalen etc. über einen Zeitraum von 30 Jahren und mehr sicherstellen.

Die Aufbewahrung der elektronischen Dokumente erfolgt auf geeigneten Datenträgern in einem Ablagesystem [Gulbins et al. 2002]. Für die Organisation der Ablage und Verwaltung der zu archivierenden Dokumente wird ein Archivierungssystem benötigt, welches die strukturierte Anzeige und Suche der archivierten Dokumente ermöglicht. Die Darstellung der Dokumente erfolgt in einer Aktenstruktur, die dem Aufbau einer Papierakte ähnelt. Das Ablagesystem wird auf der physischen Werkzeugebene des 3LGM^2-Modells dargestellt, während das Archivierungssystem ein rechnerbasierter Anwendungsbaustein auf der logischen Werkzeugebene ist. Zu einem digitalen gehören immer ein Ablage- und ein Archivierungssystem.

Die digitale Archivierung von Patientenunterlagen beinhaltet sowohl die

- Archivierung von medizinischen Bildern im Bereich der diagnostischen Radiologie als auch die
- Archivierung von Dokumenten jeglicher Art (sowohl patientenbezogene als auch administrative Dokumente).

In vielen Krankenhäusern erfolgt eine getrennte Archivierung von medizinischen Bildern und Dokumenten. Während im Bereich der diagnostischen Radiologie oftmals ein Bildspeicher- und Kommunikationssystem (PACS) eingesetzt wird, erfolgt die konventionelle Archivierung der Dokumente in Papierarchiven. Es ist jedoch sinnvoll, die Aufbewahrung von medizinischen Bildern und Dokumenten in einem zentralen digitalen Archiv zu integrieren [Häber et al. 2005].

Einen Schwerpunkt bei der digitalen Archivierung stellen unterschriftsrelevante Dokumente dar. Eine Vielzahl der Dokumente wird bereits elektronisch erzeugt (z.B. Arztbriefe, Befunde) und liegt in elektronischer Form vor. Da jedoch ca. 60 % der klinischen Dokumente unterschriftsrelevant sind, müssen die elektronischen Dokumente zurzeit noch zur Unterschrift ausgedruckt werden [Brandner

2005]. Damit entsteht ein Medienbruch. Durch die Gleichstellung der qualifizierten elektronischen Signatur[3] mit der eigenhändigen Unterschrift lässt sich dieses Problem in Zukunft vermeiden. Anstatt den Arztbrief auszudrucken und eigenhändig zu unterschreiben, kann der Arzt den Arztbrief elektronisch signieren und anschließend zur Aufbewahrung im Archivierungssystem freigeben.

2.8.3 Rechtliche Anforderungen

Es gibt eine Vielzahl von Gesetzen und Verordnungen, die sich mit der Aufbewahrung von Daten und Dokumenten befassen. Für die digitale Archivierung von Patientendaten sind dabei die nachfolgend genannten Gesetzestexte von besonderer Bedeutung:

- Handels- und Steuerrecht (HGB, AO)
- Zivil- und Strafrecht (ZPO, BGB, StGB, StPo)
- Archivgesetze (Bund, Länder)
- Signaturgesetz, Signaturverordnung
- Betriebsverfassungsgesetz
- Datenschutzgesetze (Bundesdatenschutzgesetz, Landesdatenschutz- und Landeskrankenhausgesetze)
- Musterberufsordnung für die deutschen Ärztinnen und Ärzte
- Röntgenverordnung, Strahlenschutzverordnung
- evt. Medizinproduktegesetz, Teledienst- und Telediensteda tenschutzgesetze (bei Telearchivierung)

An digitale Archive werden hohe Anforderungen gestellt. Zu den speziellen rechtlichen Anforderungen gehören die Ordnungsmäßigkeit, die Revisionssicherheit sowie die rechtliche Anerkennung der darin aufbewahrten Dokumente. Die Kernaussagen der rechtlichen Anforderung sind in [Häber et al. 2005] wiederzufinden.

Aufbewahrungspflicht und Verjährungsfrist

Die Dokumentationspflicht für die medizinische Behandlung von Patienten ist mit einer Aufbewahrungspflicht verbunden. Nach § 10 Musterberufordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä) Abs. 3 sind Patientenunterlagen für die Dauer von 10 Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Demzufolge sind z.B. Arztbriefe, Krankenhausberichte, Gutachten über Patienten, Röntgenaufnahmen, Laborbefunde, Sonographische Untersuchungen, Karteikarten und sonstige ärztliche Aufzeichnungen 10 Jahre lang aufzubewahren. Längere Aufbewahrungsfristen[4] bestehen nach § 28 Abs. 3 Röntgenverordnung (30 Jahre, z.B. für Aufzeichnungen und Berechnungen zu Röntgenbehandlungen), § 85 Abs. 2 Strahlenschutzverordnung (30 Jahre für Aufzeichnungen über die Behandlung), bei berufsgenossenschaftlichen Verletzungsgefahren (20 Jahre) und Durchgangsarztverfahren (15 Jahre).

Patientenunterlagen sind also mindestens 10 und in bestimmten Fällen sogar bis zu 30 Jahre lang aufzubewahren. Diese gesetzlichen Aufbewahrungsvorschriften bleiben unberührt von den Verjährungsfristen des BGB. Gemäß § 195 des BGB besteht eine allgemeine Verjährungsfrist von 30 Jahren. Patienten können also zivilrechtliche Ansprüche gegen ein Krankenhaus innerhalb von 30

[3] Auf die elektronische Signatur wird in einem späteren Kapitel ausführlich eingegangen.

[4] Merkblatt für die Aufbewahrungsfristen von der Kassenärztlichen Vereinigung Berlin, verfügbar unter: http://www.kvberlin.de/STFrameset165/index.html?/Homepage/service/formular/aufbewahrungsfristen.html

Jahren geltend machen. Daraus resultiert auch die 30-jährige Aufbewahrungsdauer von Patientenunterlagen. Werden Patientenunterlagen vor Ablauf der 30 Jahre vernichtet, stellt dies ein Prozessrisiko bei Schadens- und Haftpflichtprozessen für ein Krankenhaus dar.

Für Mord und Totschlag besteht nach § 78 Strafgesetzbuch keine Verjährungsfrist. Diese Dokumente müssten also dauerhaft aufbewahrt werden.

Zulässigkeit digitaler Archivierung

Die Aufbewahrung von Patientenunterlagen auf elektronischen Datenträgern ist gemäß Musterberufsordnung, Röntgenverordnung (§§ 28, 43) und Sozialgesetzbuch V (§§ 294 ff.) zulässig. Allerdings sind zusätzliche Sicherungs- und Schutzmaßnahmen zu treffen. So dürfen gemäß § 10 Abs. 5 MBO-Ä [MBO-Ä 2004] die Aufzeichnungen auch auf elektronischen Datenträgern oder anderen Speichermedien vorgenommen werden, wenn durch Sicherungs- und Schutzmaßnahmen eine Veränderung, Vernichtung oder unrechtmäßige Verwendung der Aufzeichnungen verhindert wird.

Nach § 28 Abs. 4 Röntgenverordnung (RöVo) können Röntgenbilder und Aufzeichnungen als Wiedergabe auf einem Bild- oder Datenträger aufbewahrt werden, wenn sichergestellt ist, dass die Wiedergaben oder die Daten

1. mit den Bildern oder Aufzeichnungen bildlich oder inhaltlich übereinstimmen, wenn sie lesbar gemacht werden und
2. während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Zeit lesbar gemacht werden können und
3. sichergestellt ist, dass während der Aufbewahrungsfrist keine Informationsänderungen oder -verluste eintreten können.

Werden auf den elektronischen Datenträgern personenbezogene Patientendaten (Familienname, Vornamen, Geburtsdatum, Geschlecht), Befunde, Röntgenbilder oder sonstige Aufzeichnungen aufbewahrt, dann ist nach § 28 Abs. 5 RöVo durch geeignete Maßnahmen sicherzustellen, dass

1. der Urheber, der Entstehungsort und –zeitpunkt eindeutig erkennbar sind,
2. das Basisbild mit den bei der Nachbearbeitung verwendeten Bildbearbeitungsparametern unverändert aufbewahrt wird; werden Serien von Einzelbildern angefertigt, muss erkennbar sein, wie viele Röntgenbilder insgesamt gefertigt wurden und ob alle bei der Untersuchung erzeugten Röntgenbilder oder nur eine Auswahl aufbewahrt wurden; wird nur eine Auswahl an Röntgenbildern aufbewahrt, müssen die laufenden Nummern der Röntgenbilder einer Serie mit aufbewahrt werden,
3. nachträgliche Änderungen oder Ergänzungen als solche erkennbar sind und mit Angaben zu Urheber und Zeitpunkt der nachträglichen Änderungen oder Ergänzungen aufbewahrt werden und
4. während der Dauer der Aufbewahrung die Verknüpfung der personenbezogenen Patientendaten mit dem erhobenen Befund, den Daten, die den Bilderzeugungsprozess beschreiben, den Bilddaten und den sonstigen Aufzeichnungen nach Absatz 1 Satz 2 jederzeit hergestellt werden kann.

Gemäß § 43 RöVo sind Aufzeichnungen auch in elektronischer Form zulässig, wenn das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist [RöVo 2002].

Auch im Steuer- und Handelsrecht ist die Aufbewahrung von Unterlagen auf elektronischen Datenträgern zulässig, wenn dabei die „Grundsätze ordnungsgemäßer Buchführung“ eingehalten werden. Als gesetzliche Grundlage dienen hier die Abgabenordnung (§ 147 Abs. 3 AO) und das Handelsgesetzbuch (§ 257 Abs. 3 HGB). Diese Gesetze gelten für die ordnungsgemäße Aufbewahrung von Unterlagen im Allgemeinen und sind somit für alle digitalen Archive verbindlich, unabhängig davon in welchen Bereichen sie eingesetzt werden. Hier steht vor allem die Unveränderbarkeit der

Dokumente im Vordergrund. Auf die ordnungsgemäße Aufbewahrung wird in einem weiteren Kapitel näher eingegangen.

Zivilprozessrecht

Entsprechend der Zivilprozessordnung (ZPO) gelten Urkunden als ein sicheres Beweismittel vor Gericht. Die Urkunde erbringt nach § 416 ZPO den vollen Beweis dafür, dass die in ihr enthaltenen Erklärungen auch tatsächlich vom Aussteller abgegeben wurden. Der in der ZPO verwendete Urkundenbegriff geht dabei von Papierdokumenten aus, die entweder eigenhändig vom Aussteller unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind. Nach § 371a ZPO besitzen private elektronische Dokumente einen Anschein der Echtheit, wenn sie mit einer qualifizierten elektronischen Signatur versehen sind. Der Anschein der Echtheit kann nur dann erschüttert werden, wenn Zweifel daran bestehen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben wurde. Wurde das elektronische Dokument mit der qualifizierten elektronischen Signatur von einer öffentlichen Behörde oder von einer mit öffentlichem Glauben versehenen Person erstellt, gilt gemäß § 437 die Vermutung der Echtheit [Zivilprozessordnung 2005]. Die Echtheitsvermutung kann nur widerlegt werden, wenn der Prozessgegner das Gegenteil beweist [Häber et al. 2005].

Datenschutzgesetze

Als Grundlage für den Datenschutz im Gesundheitswesen dienen das Bundesdatenschutzgesetz (BDSG) in Verbindung mit den Landesdatenschutzgesetzen (LDSGe) und Landeskrankenhausgesetzen (LKHGe). Entsprechend diesen Gesetzen dürfen Krankenhäuser nur die Patientendaten verarbeiten, die sie zur Erledigung ihrer Aufgaben benötigen und nur in dem zur Erledigung der Aufgaben benötigten Umfang [Haufe et al. 2000].

Im Bundesdatenschutzgesetz ist der Schutz von personenbezogenen Daten, die erhoben, verarbeitet und verwendet werden, geregelt. Nach §9 BDSG sind personenbezogene Daten durch technische und organisatorische Maßnahmen zu schützen. Zum Schutz personenbezogener Daten sind nach § 9 Satz 1 (Anlage) Maßnahmen zu treffen, die sicherstellen, dass

- nur autorisierte Nutzer Zutritt zu den Datenverarbeitungsanlagen besitzen (Zutrittskontrolle)
- nur autorisierte Nutzer die Datenverarbeitungsanlage nutzen (Zugangskontrolle)
- personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle)
- personenbezogene Daten bei der elektronischen Übertragung, während des Transports oder der Speicherung auf einen Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Weitergabekontrolle)
- jederzeit feststellbar ist, wer wann welche personenbezogenen Daten eingegeben, verändert oder entfernt hat (Eingabekontrolle)
- personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle)
- personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)
- zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden [BDSG].

Gemäß §20 und §35 BDSG hat ein Patient das Recht auf Berichtigung, Löschung und Sperrung der über ihn gespeicherten Patientendaten. Hier entsteht ein Widerspruch zum HGB und der AO, die eine Unveränderbarkeit der Daten fordern.

Für ein digitales Archiv entsteht die Anforderung, dass es sich merkt, welche Dokumente zu einem Patienten gehören und wann die Aufbewahrungspflicht für die einzelnen Dokumente abläuft. Nach Ablauf der Aufbewahrungsfrist sind die Daten und Dokumente zu löschen, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind. Die einem Patienten zugeordneten Dokumente besitzen in der Regel unterschiedliche Löschfristen und können durchaus auch verteilt in dem

digitalen Archiv abgelegt sein. Ist eine Löschung der Daten wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, kann nach § 35 Abs. 3 BDSG auch eine Sperrung der Daten vorgenommen werden. Allerdings ist es nicht ausreichend, den Zugriff auf die Daten zu sperren oder nur die Verweise auf die Dokumente zu löschen. Die Daten bleiben trotzdem lesbar, auch wenn der Zugriff durch das digitale Archiv nicht mehr unterstützt wird [Schmücker 1998b]. Auf alle Fälle sind Berichtigungen, Löschungen oder Sperrungen der patientenbezogenen Daten zu protokollieren. Daraus entsteht für ein digitales Archiv die Anforderung, eine Historie über die Änderungen von Daten und Dokumenten zu führen.

Schweigepflicht

Die ärztliche Schweigepflicht ist im § 203 des Strafgesetzbuches sowie in der Musterberufsordnung für deutsche Ärztinnen und Ärzte und in den Datenschutzgesetzen geregelt. Demnach dürfen Informationen, die ein Patient dem Arzt anvertraut oder die der Arzt während der Behandlung erlangt, nicht unbefugt an Dritte weitergegeben bzw. offenbart werden. Verstöße gegen die ärztliche Schweigepflicht werden strafrechtlich verfolgt und dem Arzt drohen berufsrechtliche Sanktionen durch die Ärztekammer. Da die Archivierung von Patientendaten auch von einem externen Dienstleister durchgeführt werden kann, ist zu beachten, dass auch hier die Schweigepflicht nicht verletzt werden darf. Das Oberlandesgericht Düsseldorf hat in einem Urteil[5] ([OLG], [Schell]) entschieden, dass die Weitergabe von nicht anonymisierten Patientenunterlagen durch ein externes Archivierungsunternehmen gegen die Grundsätze der ärztlichen Schweigepflicht verstößt. Bereits die Tatsache, dass ein Patient in Behandlung eines Arztes oder Krankenhauses war, stellt ein Geheimnis dar, das der ärztlichen Schweigepflicht unterliegt. Kann also ein Mitarbeiter des beauftragten Archivierungsunternehmens den Namen eines Patienten auf einer Patientenakte lesen, liegt eine Verletzung der ärztlichen Schweigepflicht vor. Eine externe Archivierung von Patientenunterlagen ist nur dann möglich, wenn der Patient schriftlich in die Archivierung seiner Patientenunterlagen durch einen externen Dienstleister einwilligt. Dies gilt auch für bereits im Krankenhaus archivierte Patientenakten, die an einen externen Dienstleister übergeben werden. Eine Weitergabe von Patientendaten und -dokumenten ist grundsätzlich nur mit der Einwilligung des Patienten oder durch gesetzliche Ermächtigungen erlaubt.

Bei der Archivierung von Patientenunterlagen muss sichergestellt sein, dass rollen- und einrichtungsbasierte Zugriffsrechte aus den Produktivsystemen in das digitale Archiv übernommen werden bzw. unter Umständen auch erst zu realisieren sind [Häber et al. 2005].

2.8.3.1. Ordnungsmäßigkeit digitaler Archive

Bei dem Begriff der Ordnungsmäßigkeit geht es vor allem um die Nachvollziehbarkeit von dokumentenorientierten Prozessen, die Gewährleistung der Integrität und Authentizität sowie die sichere Aufbewahrung von Dokumenten. Aufgrund gesetzlicher Regelungen gilt die ordnungsgemäße Aufbewahrung insbesondere für Dokumente, die:

- zur ordnungsgemäßen Buchführung benötigt werden
- einer gesetzlichen Aufbewahrungsfrist unterliegen oder
- als Beweismittel von rechtlich relevanten Sachverhalten herangezogen werden (vgl. [Götzer et al. 2004], [VOI 2005]).

Als rechtliche Grundlage für die Ordnungsmäßigkeit dienen das Handelsgesetzbuch (HGB), die Abgabenordnung (AO) sowie die Grundsätze ordnungsgemäßer Buchführung (GoB). Zu den wesentlichen Anforderungen aus dem HGB und den GoB gehören, dass die Aufzeichnungen

- vollständig, richtig, zeitgerecht und geordnet vorgenommen werden
- sicher gegen solche Veränderungen sind, dass der ursprüngliche Inhalt nicht mehr feststellbar oder der Zeitpunkt der Veränderung ungewiss ist

[5] Urteil vom 20. August 1996 – 20 U 139/95 vom Oberlandesgericht Düsseldorf

- nachvollziehbar für einen sachverständigen Dritten sind
- während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können
- bildlich und inhaltlich mit dem Original übereinstimmen.

Im Jahre 1977 wurde mit dem Einführungsgesetz zur Abgabenordnung die Grundlage für die Aufbewahrung von Unterlagen auf Bild- und Datenträgern geschaffen. Demnach können die Unterlagen auch auf Bild- und Datenträgern aufbewahrt werden, wenn die Aufbewahrung den „Grundsätzen ordnungsgemäßer Buchführung“ (GoB)[6] entspricht. Da die GoB von Unterlagen in Papierform ausgehen, wurden sie weiterentwickelt und im Hinblick auf den Einsatz von DV-gestützten Buchführungssystemen präzisiert. So entstanden die „Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme“ (GoBS), die von der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. erarbeitet und zusammen mit einem Schreiben vom Bundesfinanzministerium im Bundessteuergesetzblatt vom 14.12.1995 veröffentlicht wurden.

Die folgenden Informationen zu den GoBS lehnen sich an [Henstdorf et al. 1999] an.

Mit den GoBS wurden konkrete Vorgaben für die digitale Archivierung geschaffen. Um den ordnungsgemäßen Einsatz eines digitalen Archivs zu bestätigen, wird die Erstellung einer Verfahrensdokumentation gefordert. Die Erstellung der Verfahrensdokumentation liegt allein in der Verantwortung des Betreibers des digitalen Archivs. Dabei müssen der Inhalt, Aufbau und Ablauf des Verfahrens aus der Verfahrensdokumentation vollständig ersichtlich sein. Für die Beschreibung können bereits erstellte Dokumentationen wie z.B. das Pflichtenheft, Fachkonzepte und die Herstellerdokumentation herangezogen werden. Über den Umfang und Aufbau der Verfahrensdokumentation werden in den GoBS keine Aussagen gemacht. Jedoch sollte die Verfahrensdokumentation folgende Punkte beinhalten:

- eine Beschreibung der sachlogischen Lösung,
- eine Beschreibung der programmtechnischen Lösung
- eine Beschreibung, wie die Programmidentität gewährt wird,
- eine Beschreibung, wie die Integrität der Daten gewahrt wird,
- Arbeitsanweisungen für den Anwender.

In der Literatur existieren unterschiedliche Gliederungsstrukturen für den Aufbau einer Verfahrensdokumentation. Der Arbeitskreis „Regelwerk Verfahrensdokumentation“ des TÜViT und des VOI hat ein Regelwerk geschaffen, das die unterschiedlichen Gliederungsstrukturen in einem Regelwerk standardisiert. Die Gliederungsstruktur einer Verfahrensdokumentation kann in [Henstdorf et al. 1999] und [VOI 2004] nachgelesen und soll daher hier nicht weiter verfolgt werden.

Besonderer Wert wird in den GoBS auf die Dokumentation des Internen Kontrollsystems (IKS) gelegt. Das IKS beinhaltet alle aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen. Anhand des IKS muss ersichtlich sein, wer wann mit welchen Mitteln Änderungen vorgenommen hat. Zu der Beschreibung eines IKS gehören laut [Henstdorf 1999]:

- Zugangskontrollmechanismen
- Loginmechanismen
- Definition der Benutzerprofile
- Maschinelle Kontrollen

[6] Bei den GoB handelt es sich um einen unbestimmten Rechtsbegriff.

- Benutzerverwaltung mit Zuständigkeiten und Verantwortungsbereichen
- Beschreibung der archivierungsrelevanten Arbeitsabläufe
- Beschreibung der Protokollierung von Änderungen, logischem Löschen usw.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Maßnahmenkatalog erarbeitet, der im IT-Grundschutzhandbuch neu überarbeitet und im November 2005 veröffentlicht wurde. Entsprechend des Maßnahmekataloges M2.263 [BSI 2005] muss für eine ordnungsgemäße Archivierung sichergestellt sein, dass über den gesamten Archivierungszeitraum

- das benutzte Datenformat dem Stand der Technik entspricht und von den verwendeten Anwendungen verarbeitet werden kann
- die gespeicherten Daten lesbar sind und unter Beibehaltung der Semantik und der Nachweiskraft reproduziert werden können
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann
- die Speichermedien physikalisch lesbar sind
- die eingesetzten kryptographischen Verfahren zur Verschlüsselung und zur digitalen Signatur dem Stand der Technik entsprechen
- für alle Komponenten der Speichereinheit (Speichermedien, Laufwerke, Jukeboxen sowie die Steuersoftware) Ersatz- und Wartungsmöglichkeiten bestehen.

Die Erfüllung der Ordnungsmäßigkeit ist eine wichtige Voraussetzung für die rechtliche Anerkennung der archivierten Dokumente in einem digitalen Archiv. Es muss sichergestellt sein, dass die archivierten Dokumente weder gelöscht noch verändert oder verfälscht werden können. Der Zugriff unbefugter Dritter auf die personenbezogenen Patientendaten ist auszuschließen.

Ein weiteres wichtiges Kriterium, das ein digitales Archiv erfüllen muss, ist die Revisionssicherheit.

2.8.3.2. Revisionssicherheit digitaler Archive

Der Begriff der Revision kommt aus dem Lateinischen und bedeutet Überprüfung bzw. Nachprüfung. Ein digitales Archiv ist revisionssicher, wenn nachgeprüft werden kann, ob es die Anforderungen aus den GoBS erfüllt, ordnungsgemäß betrieben wird und die Dokumente unveränderbar und verfälschungssicher darin archiviert sind [Kampffmeyer et al. 1997]. Der Verband für Organisations- und Informationssysteme e.V. (VOI) hat den Begriff der revisionssicheren Archivierung in den 1996 veröffentlichten „Grundsätze elektronischer Archivierung“, dem „Code of Practice“, wie folgt definiert:

„Die Archivierung entsprechend den Vorgaben der GoB und den GoBS wird als revisionssichere Archivierung bezeichnet.“ [Kampffmeyer et al. 1997, Seite 10].

Der Nachweis der Revisionssicherheit kann nur durch eine Verfahrensdokumentation erbracht werden, die in den GoBS gefordert wird. Anhand dieser Verfahrensdokumentation muss es für eine unabhängige dritte Person möglich sein, sich einen Überblick über die in einem digitalen Archiv eingesetzten Verfahren und deren Funktionsweise zu verschaffen. Dazu gehört auch, dass jederzeit nachvollzogen werden kann, wer wann welche Daten in welcher Weise verarbeitet hat. Der Einsatz von nur einmal beschreibbaren Speichermedien führt allein also noch nicht zu einer revisionssicheren Archivierung. Es muss der gesamte Prozess von der Einführung über den Betrieb bis zur Ablösung oder Migration auf ein neues digitales Archiv sach- und fachgerecht im Rahmen der Verfahrensdokumentation begleitet und validiert werden [VOI 2005]. Dies erfordert die Umsetzung entsprechender organisatorischer und technischer Maßnahmen. Zu diesen Maßnahmen gehören, dass

- alle Zugriffe auf bzw. Veränderungen der archivierten Daten und Dokumente kontrolliert, protokolliert und ausgewertet werden

- eine unzulässige Veränderung oder Löschung der Daten verhindert wird
- Veränderungen während der Transformation ausgeschlossen werden
- eine Benutzerverwaltung sowie Zugangskontrollen und Zugriffsberechtigungen eingerichtet und
- Daten und Programme gesichert werden.

Werden diese Maßnahmen in einem digitalen Archiv nicht umgesetzt, ist die Ordnungsmäßigkeit des Archivierungsverfahrens nicht mehr gewährleistet. Dies kann zum Verlust der Beweiskraft der archivierten Dokumente führen.

2.8.3.3. Rechtliche Anerkennung der aufbewahrten Dokumente

Bei der Aufbewahrung von Patientenunterlagen in einem digitalen Archiv muss sichergestellt sein, dass der Beweiswert der elektronischen Dokumente innerhalb der Aufbewahrungszeit erhalten bleibt. Dies ist nur dann möglich, wenn die Integrität und Authentizität der elektronischen Dokumente gewährleistet ist. Die Integrität kann durch die Verwendung der qualifizierten elektronischen Signatur und die Authentizität durch elektronische Zertifikate nachgewiesen werden [Rossnagel 2006].

2.8.3.4. Die 10 Merksätze des VOI

Um die Ordnungsmäßigkeit, Revisionssicherheit und rechtliche Anerkennung eines digitalen Archivs zu gewährleisten, hat der Verband Organisations- und Kommunikationssysteme e.V. als Fachverband der Anbieter für Dokumenten-Management- und elektronische Archivierungssysteme 1996 10 Merksätze herausgegeben:

1. Jedes Dokument muss unveränderbar archiviert werden.
2. Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
3. Jedes Dokument muss mit geeigneten Retrievaltechniken wieder auffindbar sein.
4. Es muss genau das Dokument wieder gefunden werden, das gesucht worden ist.
5. Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
6. Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
7. Jedes Dokument muss zeitnah wieder gefunden werden können.
8. Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
9. Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.
10. Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HGB, AO etc.) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

Tabelle 2-1: Merksätze für eine ordnungsgemäße, revisionssichere und rechtlich anerkannte Archivierung

(entnommen aus [Kampffmeyer et al. 1997, Seite 20])

2.8.4 Probleme bei der Langzeitarchivierung

Die Informationen in diesem Abschnitt beruhen auf [Häber et al. 2005].

Zu den Problemen bei der Langzeitarchivierung von Patientenunterlagen gehören, dass die Lesbarkeit, der rechtliche Beweiswert sowie die Integrität und die Authentizität der elektronischen Dokumente innerhalb der Aufbewahrungsfrist erhalten bleiben. Die Lesbarkeit eines elektronischen Dokumentes wird jedoch durch zwei wesentliche Faktoren beeinflusst:

- durch die Software, mit der ein Dokument erstellt wurde
- durch die Hardware, insbesondere die eingesetzten Speichermedien und Laufwerke.

Wer aber weiß heute, welche Datenformate auch noch in 30 Jahren lesbar sind? Da die Lesbarkeit der Dokumente eine wesentliche Anforderung an das digitale Archiv ist, sind die Patientenunterlagen in standardisierten Formaten abzulegen. Weiterhin kann es erforderlich sein, die archivierten Dokumente rechtzeitig in aktuellere Formate umzuwandeln [Viebeg 2006]. Die Änderung des Dateiformates führt jedoch dazu, dass elektronisch signierte Dokumente ihre Beweiskraft verlieren.

Eine weitere Problematik sind die für die digitale Archivierung eingesetzten Speichermedien. Diese Speichermedien zeichnen sich durch hohe Speicherkapazitäten und schnelle Zugriffszeiten aus. Da jedoch die Menge der zu archivierenden Daten und Dokumente wächst, unterliegen auch die Speichermedien einer ständigen Weiterentwicklung. Auf dem Markt sind Innovationszyklen von 2 bis 3 Jahren zu beobachten, in denen entweder ein neues Speichermedium entwickelt oder eine neue Generation eines Mediums mit höherer Speicherdichte verfügbar ist. Um zu vermeiden, dass die Daten und Dokumente auf den Speichermedien zwar noch lesbar sind, es aber keine Laufwerke zum Einlesen der Medien gibt, sollte nach ca. 5 bis 8 Jahren eine Migration der Datenbestände vorgenommen werden. Als Speichermedien werden heute WORM-Medien, digital-optische Medien oder Festplattensysteme eingesetzt.

2.9 Elektronische Signatur

„Elektronische Signaturen sind an Dateneinheiten angehängte Daten oder kryptographische Transformationen, die es dem Empfänger ermöglichen, die Authentizität und die Integrität der Dateneinheit festzustellen und die Daten gegen Fälschung (z.B. durch den Empfänger) zu sichern.“ [Häber et al. 2005, Seite 8]

Im Jahre 2001 wurden mit dem „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ (Signaturgesetz), der „Verordnung zur elektronischen Signatur“ (Signaturverordnung) und dem „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäfteverkehr“ (Formanpassungsgesetz) die gesetzlichen Grundlagen für die Verwendung der elektronischen Signatur geschaffen. Durch das Formanpassungsgesetz wurde der §126 im BGB dahingehend geändert, dass die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden kann, wenn das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Gemeinsam mit dem Signaturgesetz[7] wird also die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgesetzt. Damit erfüllt das Signaturgesetz die Vorgaben der EU-Richtlinie, die eine rechtliche Anerkennung der elektronischen Signatur fordert. Eine Ergänzung zum Signaturgesetz stellt die Signaturverordnung dar. Sie beinhaltet die technisch-organisatorischen Anforderungen an die elektronische Signatur und die Public-Key-Infrastruktur.

Elektronische Signaturen werden vor allem dort eingesetzt, wo Daten sicher elektronisch übertragen, gespeichert oder verarbeitet werden [Von Seck 2003]. Mit Hilfe der elektronischen Signatur ist

[7] § 6 Abs. 2 Signaturgesetz

nachweisbar, dass das elektronische Dokument nicht verändert wurde und von wem das Dokument elektronisch signiert wurde [Hollerbach et al. 2003a].

Während im ersten Signaturgesetz nur der Begriff der „digitalen Signatur“ verwendet wurde, unterscheidet das neue Signaturgesetz zwischen vier Signaturen. Diese Signaturen sollen im Folgenden kurz dargestellt werden:

Stufe	Anforderungen	Rechtssicherheit
Elektronische Signatur	• dient zur Authentifizierung des Urhebers • keine Anforderungen bezüglich der Sicherheit oder Fälschungssicherheit • müssen nicht mit dem unterzeichneten Dokument verbunden sein	bietet geringe bzw. keine Rechtsicherheit Beispiel: eingescannte Unterschrift
Fortgeschrittene elektronische Signatur	• ist ausschließlich dem Signaturschlüssel-Inhaber zugeordnet • ermöglicht Identifizierung des Schlüssel-Inhabers • wird mit Mitteln erzeugt, die der Schlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann • nachträgliche Veränderung der Daten muss erkennbar sein	bietet etwas höhere Rechtssicherheit als die elektronische Signatur, trotzdem geringe Beweiskraft; Rechtssicherheit kann durch den Einsatz von Verfahrensbeschreibungen erhöht werden
Qualifizierte elektronische Signatur	• erfordert Zertifikatserstellung durch einen qualifizierten Zertifizierungsdiensteanbieter, • beruht auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat • ist mit einer sicheren Signaturerstellungseinheit erstellt	bietet hohe Rechtssicherheit gleichgestellt zur eigenhändigen Unterschrift
Qualifizierte elektronische Signatur mit Anbieterakkreditierung	• beruht auf qualifizierten Zertifikaten von akkreditierten Zertifizierungsdiensteanbietern	bietet die höchste Rechtssicherheit

Tabelle 2-2: Überblick über die im Signaturgesetz definierten elektronischen Signaturen

2.9.1 Grundprinzip Signaturverfahren

Das Grundprinzip des Signaturverfahrens soll in Anlehnung an [Brandner et al. 2002] erläutert werden.

Die elektronische Signatur basiert auf einer asymmetrischen Verschlüsselungsmethode (Public-Key-Verfahren). Bei der asymmetrischen Verschlüsselung wird ein Schlüsselpaar erzeugt, das aus einem Signatur- und einem Signaturprüfschlüssel besteht. Der Signaturschlüssel[8] ist nur dem Besitzer bekannt, während der Signaturprüfschlüssel[9] für jedermann frei zugänglich ist. Wird nun ein Dokument elektronisch signiert, dann wird mit Hilfe einer Hashfunktion eine eindeutige Checksumme für das elektronische Dokumente berechnet. Diese Checksumme wird anschließend mit dem Signaturschlüssel der signierenden Person verschlüsselt und als Signatur an das Dokument angehängt. Zur Entschlüsselung der Signatur benötigt der Empfänger den zum Signaturschlüssel gehörenden Signaturprüfschlüssel. Beim Empfänger wird mit Hilfe der Hashfunktion erneut die Checksumme aus dem Dokument berechnet. Unter Verwendung des Signaturprüfschlüssels entschlüsselt der Empfänger die elektronische Signatur. Als Ergebnis der Entschlüsselung entsteht wiederum eine Checksumme, die mit der zuvor berechneten Checksumme aus dem Dokument verglichen wird. Stimmen beide Checksummen überein, ist die Integrität des Dokumentes gewährleistet. Das Dokument wurde genauso erhalten wie es versandt wurde.

2.9.2 Zertifizierungsdiensteanbieter

Den zum Signaturschlüssel dazugehörigen Signaturprüfschlüssel bekommt der Empfänger entweder von der signierenden Person oder er kann den Signaturprüfschlüssel aus dem öffentlichen Verzeichnis eines Zertifizierungsdiensteanbieters (ZTD) entnehmen. Ein ZTD ist für die Erstellung des Schlüsselpaares sowie für die Ausstellung von qualifizierten Zertifikaten verantwortlich. Um den Signaturschlüssel gegen unberechtigte Nutzung[10] zu schützen, kann der ZTD den Signaturschlüssel auf einer Signaturkarte speichern [Brandner et al. 2002]. Die Signaturkarte ist zusätzlich durch ein Passwort geschützt. In einem qualifizierten Zertifikat bestätigt der ZTD, dass der Signaturprüfschlüssel zu dem im Zertifikat aufgeführten Inhaber des Signaturschlüssels gehört. Das Zertifikat wird durch den ZTD elektronisch signiert und enthält nach § 7 Signaturgesetz [SigG 2001]

1. den Namen des Signaturschlüssel-Inhabers
2. den zugeordneten Signaturprüfschlüssel
3. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann
4. die laufende Nummer des Zertifikates
5. Beginn und Ende der Gültigkeit des Zertifikates
6. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist
7. Angaben, ob die Nutzung des Signaturschlüssels beschränkt ist
8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt
9. nach Bedarf Attribute des Signaturschlüssel-Inhabers (z.B. Vertretungsmacht).

---

[8] Signaturschlüssel sind nach § 2 Abs. 4 Signaturgesetz einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer Signatur verwendet werden.

[9] Signaturprüfschlüssel sind nach § 2 Abs. 5 Signaturgesetz elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer Signatur verwendet werden.

[10] Diese Anforderung ergibt sich aus § 17 Abs. 1 Signaturgesetz.

Der ZTD veröffentlicht die Zertifikate in einem Verzeichnisdienst [Brandner et al.2002]. Über den Verzeichnisdienst ist eine Überprüfung der Zertifikate möglich (z.B. bzgl. ihrer Gültigkeit). Da oftmals auch der Zeitpunkt, an dem ein Dokument erstellt und signiert wurde, von Bedeutung ist, können über den ZTD Zeitstempel eingeholt werden. Mit einem Zeitstempel bestätigt der ZTD nach § 2 Abs. 14 Signaturgesetz das Vorliegen elektronischer Daten zu einem bestimmten Zeitpunkt. Für die Sperrung von Zertifikaten betreibt der ZTD einen Sperrdienst. Die Sperrung kann vom Signaturschlüssel- und damit Zertifikatsinhaber beantragt werden, wenn z.B. die Geheimhaltung des Signaturschlüssels nicht mehr gewährleistet ist. Die Sperrung kann aber auch durch den ZTD oder die Bundesnetzagentur erfolgen.

Die Lizenzierung und Kontrolle der ZTD erfolgt durch die Bundesnetzagentur (BNetzA)[11], die nach § 3 des Signaturgesetzes die zuständige Behörde ist. Die Bundesnetzagentur stellt eine Übersicht aller Zertifizierungsdiensteanbieter zur Verfügung, die für das Ausstellen von qualifizierten Zertifikaten oder von qualifizierten Zeitstempeln eine Akkreditierung nach dem Signaturgesetz erhalten haben.

2.9.3 Probleme bei der Langzeitarchivierung elektronisch signierter Dokumente

Die qualifizierte elektronische Signatur ermöglicht erstmals eine beweiskräftige, revisionssichere und rechtlich anerkannte Archivierung von Patientenunterlagen in einem digitalen Archiv [Häber et al. 2005]. Da Patientenunterlagen jedoch teilweise bis zu 30 Jahre lang beweiskräftig aufzubewahren sind, ergibt sich für Krankenhäuser ein Problem. Die elektronisch signierten Dokumente können ihre Beweiskraft mit der Zeit verlieren. Zu den Ursachen dafür gehören laut [Häber et al. 2005], dass

- die qualifizierten Signaturzertifikate nur zeitlich begrenzt verfügbar und prüfbar sind. Während das Zertifikat von einem akkreditierten Zertifizierungsdiensteanbieter nach Ablauf der Gültigkeit noch mindestens 30 Jahre online prüfbar ist, ist das Zertifikat von einem nicht-akkreditierten Zertifizierungsdiensteanbieter nur 5 Jahre prüfbar.
- die bei der Erzeugung der Signaturen verwendeten kryptographischen Algorithmen mit der Zeit ihre Sicherheitseignung durch „Alterung“ verlieren.
- die Informationen zu Sicherheitseignungen kryptograhischer Algorithmen den Betreibern von elektronischen Archivierungssystemen nicht in auswertbarer Form zu Verfügung stehen. Diese Informationen müssen dem Bundesanzeiger entnommen werden.
- durch die Transformation signierter Dokumente in andere Datenformate oder auf andere Datenträger der Beweiswert der ursprünglichen Signatur gemindert wird. Dazu gehören z.B. die Transformation von Papier auf elektronische Medien oder die Vorlage eines elektronisch signierten Dokumentes in Papierform.
- die verfügbaren Signaturstandards insbesondere bezüglich der Signaturerneuerung und Verifikationsdaten unzureichend sind.

In dem Projekt ArchiSig wurden Konzepte zur Lösung dieser Probleme erarbeitet und anschließend realisiert.

2.9.4 Das Projekt ArchiSig

Das Projekt „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ ist ein Verbundprojekt, das vom Bundesfinanzministerium für Wirtschaft und Arbeit im Rahmen des Vorhabens „VERNET – Sichere und verlässliche Transaktionen in offenen

[11] Das Gesetz zur Neuregelung des Energiewirtschaftsrechts wurde am 12.07.2005 im Bundesgesetzblatt (BGI 2005 Teil I Nr.42, Seite 1979 ff) verkündet und trat am 13.072005 in Kraft. Gemäß Artikel 2 des Gesetzes wurde der Name der „Regulierungsbehörde für Telekommunikation und Postwesen“ (Reg TP) in „Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen“ umbenannt. Die amtliche Kurzbezeichnung ist „Bundesnetzagentur“. [BNetzA 2005]

Kommunikationsnetzen“ gefördert wurde. Es wurde vom Juli 2001 bis Dezember 2003 durchgeführt. Die Ergebnisse dieses Forschungsprojektes sind im Buch „Beweiskräftige und sichere Langzeitarchivierung elektronisch signierter Dokumente“ zusammengefasst. Die folgenden Ausführungen zu diesem Projekt einschließlich Archivzeitstempel orientieren sich an [Brandner et al. 2006b] und an [ArchiSig].

In dem Projekt ArchiSig wurden Archivierungskonzepte erarbeitet, die eine sichere und beweiskräftige Langzeitarchivierung digital erzeugter und signierter Daten über 30 Jahre und mehr ermöglichen. Eine wesentliche Erkenntnis, die aus diesem Projekt gewonnen wurde, ist, dass der gesamte Lebenszyklus elektronischer Dokumente von der Erzeugung, Signaturerzeugung, Präsentation, Kommunikation bis hin zur Langzeitspeicherung in einem digitalen Archiv zu betrachten ist. Dabei wird sogar die dauerhafte Erhaltung von elektronischen Dokumenten berücksichtigt. Weiterhin wurde im Rahmen dieses Projektes ein Konzept erarbeitet, das die Neusignierung von elektronischen Dokumenten ermöglicht, wenn die Signaturen zu veralten drohen. Die Erneuerung der Signaturen sollte dabei vom digitalen Archiv übernommen werden. In einem KIS könnte die Umsetzung dieses Konzeptes wie folgt aussehen:

Die rechnergestützten Anwendungsbausteine des KIS übergeben die elektronisch erzeugten Dokumente, die elektronisch signiert und verifiziert sind, zur Langzeitarchivierung und Neusignierung an das Archivierungssystem. Das Archivierungssystem erzeugt zu diesen Dokumenten und Signaturen so genannte Archivzeitstempel und signiert diese immer wieder neu, bevor die Sicherheit der verwendeten kryptographischen Algorithmen nachlässt. Anhand des Archivzeitstempels kann verifiziert werden, ob das Dokument mit seinen Signaturen rechtzeitig neu signiert worden ist.

Im Oktober 2003 konnte anhand von simulierten Gerichtsprozessen nachgewiesen werden, dass durch die in dem Projekt realisierten Verfahren zur Langzeitarchivierung elektronisch signierter Dokumente der Beweiswert der aufbewahrten Dokumente erhalten bleibt. Wird das ArchiSig-Konzept in einem digitalen Archiv umgesetzt, besteht also eine verlässliche Rechtssicherheit in Bezug auf die aufbewahrten signierten Dokumente.

Als Ergebnis des Projektes ArchiSig entstanden die „Grundsätze für die Langzeitsicherung elektronisch signierter Dokumente“[12] .

Um zu vermeiden, dass die Signatur bei jedem Dokument einzeln erneuert werden muss, können so genannte Archivzeitstempel eingesetzt werden. Als Grundlage für die Archivzeitstempel dienen Hashbäume, die beliebig viele signierte Dokumente über einen Zeitstempel zusammenfassen. Die signierten Dokumente oder andere Datenobjekte werden in den Blättern des Hashbaumes dargestellt. Jedes Dokument wird über seinen Hashwert eindeutig repräsentiert. Die darüberliegenden Hashwerte werden über die Folge der Sohnknoten gebildet. Dazu werden die Sohnknoten konkateniert und dann erneut gehasht. Der Wurzel-Hashwert wird mit einem Zeitstempel von einem akkreditierten Zertifizierungsdiensteanbieter signiert. Damit ist die Integrität des gesamten Baumes einschließlich der damit gesicherten Dokumente gewährleistet.

[12] Die Grundsätze stellen eine Empfehlung dar und besitzen keinen rechtlichen Charakter. Sie sind verfügbar unter: http://www.archisig.de/grundsaetze.pdf

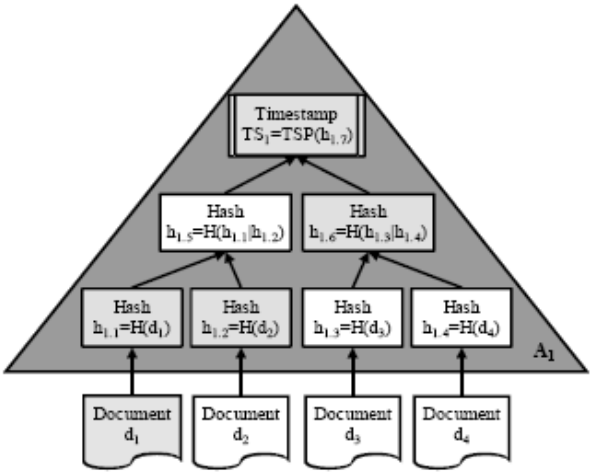


Abbildung 2-3: Darstellung des Aufbaus eines Archivzeitstempels

(entnommen aus [Farnbacher 2004])

In der Regel wird an das Archivsystem ein Dokument übergeben. Zu diesem Dokument wird ein Hashwert gebildet. Gemeinsam mit den Hashwerten weiterer Dokumente erfolgt der Aufbau eines Hashbaumes, der mit einem akkreditierten Zeitstempel versehen wird. Archivsysteme sollten also eine Neusignierung der Dokumente unterstützen. Daher sollte dies als Funktion von einem digitalen Archivsystem angeboten werden.

Die Zeitstempel müssen erneuert werden, bevor die verwendeten Hash- oder Public-Key-Algorithmen, die im Zeitstempel verwendet wurden, unsicher werden. Dazu wird der Zeitstempel des Archivzeitstempels gehasht und als Blatt in den Hashbaum des neu zu bildenden Archivzeitstempels eingefügt. Bei der Zeitstempelerneuerung muss nicht auf die archivierten Dokumente selbst, sondern nur auf den betroffenen Archivzeitstempel zugegriffen werden. Die Neusignierung eines Zeitstempels kann solange wiederholt werden, wie der im Hashbaum verwendetet Hashalgorithmus noch sicher ist. Erst wenn dieser unsicher wird, ist eine Neusignierung des Hashbaumes erforderlich. Dieses Verfahren ist aufwendiger, da hier neben den unsicher werdenden Archivzeitstempeln auch die durch sie referenzierten signierten Dokumente zu berücksichtigen sind. Für die betroffenen Archivzeitstempel werden die archivierten Dokumente und die zwischenzeitlich erzeugten reduzierten Archivzeitstempel mit einem neuen sicherheitsgeeigneten Hashalgorithmus gehasht. So wird erneut ein Archivzeitstempel gebildet.

2.9.5 Das Projekt TransiDoc

„TransiDoc - Rechtssichere Transformation signierter Dokumente“[13] ist ein vom Bundesministerium für Wirtschaft und Arbeit (BMWA) gefördertes Projekt und schließt sich an das ArchiSig- Projekt an. Die Laufzeit des Projektes geht bis März 2007. Als Ergebnis soll eine rechtssichere Transformation von elektronisch signierten Dokumenten möglich sein, bei dem das transformierte Dokument die gleiche Beweiskraft wie das Ursprungsdokument besitzt. Damit könnte zukünftig auf die Aufbewahrung des Ursprungsdokumentes verzichtet werden. Unter dem Begriff Transformation wird dabei die Umwandlung eines Ausgangsdokumentes in ein Zieldokument verstanden. Grundsätzlich werden in dem Projekt drei Transformationen unterschieden:

- die Transformation eines Papierdokumentes in ein elektronisches Dokument (P-to-E)
- die Transformation eines elektronischen Dokumentes in ein Papierdokument (E-to-P) und

[13] Siehe auch: http://www.transidoc.de.

- die Transformation eines elektronischen Dokumentes in ein anderes elektronisches Dokument (E-to-E).

Um zu verhindern, dass elektronisch signierte Dokumente nach einer Transformation ihre Beweiskraft verlieren, sieht das TransiDoc-Projekt die Einführung eines Transformationssiegels vor. Das Transformationssiegel ist ein Vermerk, der mit einer elektronischen Signatur beglaubigt ist. Mit Hilfe des Transformationssiegels kann nachvollzogen werden, was während einer Transformation mit dem Dokument geschah. Es sichert die transformierten Inhalte, bestätigt die Korrektheit der Transformation, garantiert die Vertrauenswürdigkeit[14] und ermöglicht eine nachträgliche Überprüfung des transformierten Dokumentes [Viebeg 2006]. Bei einer nachträglichen Überprüfung muss nach [Viebeg 2006] erkennbar sein

- dass es sich um ein transformiertes Dokument handelt
- wer das Ausgangsdokument signiert bzw. unterschrieben hat
- wer die Transformation durchgeführt hat und
- ob die entsprechende Person autorisiert war, diese Transformation durchzuführen.

[14] „Vertrauenswürdigkeit bedeutet, dass nachträglich verifizierbar ist, welche Transformation durchgeführt wurde, dass die Inhaltstreue überprüft wurde und dass das Prüfergebnis vermerkt wurde und zurechenbar ist.“ [TransiDoc]

3 Aufgaben und Funktionen eines digitalen Archivs

3.1 Funktionen

In diesem Abschnitt sollen Funktionen eines digitalen Archivs beschrieben werden. Die wesentlichen Kernaussagen lehnen sich an [Häber et al. 2005] an.

3.1.1 Übernahme der Daten und Dokumente

Für die Übernahme der zu archivierenden Patientenunterlagen gibt es verschiedene Möglichkeiten. Zunächst ist zu unterscheiden, ob die zu archivierenden Dokumente in elektronischer Form oder in Papierform vorliegen. Liegen die Dokumente in Papierform vor, müssen sie mit Hilfe eines Scanners digitalisiert werden. Bei einem handschriftlich unterschriebenen Papierdokument ist zu berücksichtigen, dass die Unterschrift sich auf das ursprüngliche Dokument (also das Papierdokument) bezieht. Da während der Transformation von Papier in die elektronische Form Veränderungen im Dokument entstehen können, verliert die Unterschrift durch die Transformation ihre Prüfbarkeit und wird rechtlich unwirksam. Das eingescannte Dokument würde damit nicht die gleiche Beweiskraft wie das originale Papierdokument besitzen. Um die Beweiskraft des digitalisierten Dokumentes zu erhalten, muss es mit einer qualifizierten elektronischen Signatur versehen sein. Durch diese Signatur wird von einer natürlichen Person bestätigt, dass die Transformation ordnungsgemäß durchgeführt wurde und eine Übereinstimmung des Papierdokumentes mit dem elektronischen Dokument nach der Transformation vorlag. Da oftmals auch der Zeitpunkt der Transformation von Bedeutung ist, ist das Anbringen eines amtlichen Zeitstempels erforderlich. Dazu wird nach dem Scanprozess ein Hashwert über die elektronische Version des Dokumentes gebildet und mit der qualifizierten elektronischen Signatur verknüpft. Bei der Erfassung großer Datenmengen (z.B. das rückwirkende Einscannen von archivierten papierbasierten Patientenakten) kann auch ein externer Scan-Dienstleister eingesetzt werden. Diese Dienstleister stellen die digitalisierten Dokumente einschließlich der dazu erfassten Indexdaten auf einem Datenträger oder online zur Verfügung. Im Anschluss an die Digitalisierung können die Dokumente in das digitale Archiv übernommen werden.

Liegen die zu archivierenden Dokumente in elektronischer Form vor, können sie über Schnittstellen oder über so genannte Austauschverzeichnisse in das digitale Archiv übernommen werden. Die Schnittstellen müssen dabei von den jeweiligen Subsystemen des KIS zur Verfügung gestellt werden und sollten standardisiert sein. Bei der Verwendung von Austauschverzeichnissen werden die zu archivierenden Unterlagen mit der dazugehörigen Indexdatei in einem bestimmten Verzeichnis im Filesystem abgelegt. Aus diesem Verzeichnis werden die abgelegten elektronischen Dokumente geholt und in das digitale Archiv übernommen. Um die Integrität und Authentizität der zu archivierenden elektronischen Dokumente sicherzustellen, müssen sie mit einer qualifizierten elektronischen Signatur versehen sein. Das Signieren des Dokumentes kann dabei direkt aus dem rechnerbasierten Anwendungsbaustein, in dem das Dokument erzeugt wurde, erfolgen. So wurde z.B. im Rahmen des ArchiSig-Projektes am Universitätsklinikum Heidelberg die Möglichkeit geschaffen, die mit i.s.h.med erstellten Arztbriefe elektronisch zu signieren [Brandner et al. 2006a]. Der Signaturvorgang ist auf alle Fälle in den Archivierungsprozess zu integrieren. Für die mit einer qualifizierten elektronischen Signatur versehenen archivierten Dokumente gilt vor Gericht die Echtheitsvermutung, d.h. der Richter geht von der Echtheit des Dokumentes aus. Bestehen Zweifel an der Echtheit eines Dokumentes, dann muss der Beweis durch die gegnerische Partei erbracht werden.

Weiterhin besteht die Möglichkeit, die auf einem Mikrofilm abgelegten Dokumente mit Hilfe eines Mikrofilmscanners zu digitalisieren.

3.1.2 Ablage und Langzeitspeicherung

Nach dem Import der zu archivierenden Patientenunterlagen in das Archivierungssystem müssen diese ordnungsgemäß und revisionssicher auf digitalen Speichermedien abgelegt und langfristig gespeichert werden. Da auf die Patientenunterlagen in den ersten Monaten nach der Entlassung eines Patienten noch relativ häufig zugegriffen wird, können die Unterlagen zunächst auf einem elektronischen

Kurzzeitspeicher abgelegt werden. Für diesen werden Speichermedien verwendet, die einen schnellen Zugriff auf die Unterlagen ermöglichen. Diese Speichermedien sind in der Regel in der Anschaffung sehr teuer. Aus diesem Grund werden ältere Daten und Dokumente nach einer bestimmten Zeit vom elektronischen Kurzzeitspeicher in einen elektronischen Langzeitspeicher ausgelagert. Da die Zugriffe auf die in dem digitalen Archiv abgelegten Unterlagen mit der Zeit sinken, können für die Langzeitspeicherung kostengünstigere Medien (z.B. WORM, UDO) eingesetzt werden. Diese Medien besitzen langsamere Zugriffszeiten. Die Langzeitspeicherung erfolgt auf einem Langzeitspeichermedium, dass die Unveränderbarkeit der Daten gewährleistet.

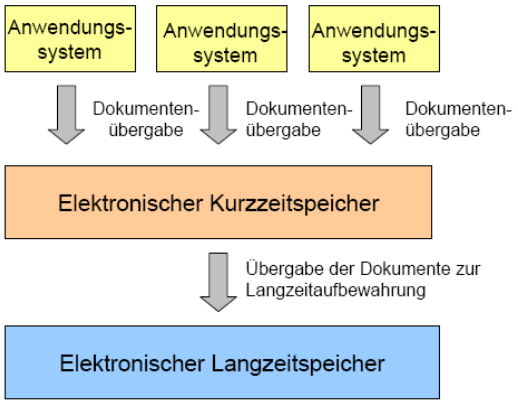


Abbildung 3-1: Archivstruktur

Die ordnungsgemäße Aufbewahrung setzt eine strukturierte Ablage der zu archivierenden Objekte voraus, denn nur so können diese auch wieder gefunden und eindeutig zugeordnet werden. Unterstützung bei der Verwaltung dieser Objekte bieten so genannte Dokumentenmanagement-Systeme. Die Objekte werden unveränderlich in dem digitalen Archiv abgelegt, d.h. eine Veränderung oder Löschung der archivierten Objekte ist auszuschließen. Hier entsteht ein Widerspruch zu den Datenschutzgesetzen. Gemäß Datenschutzgesetz sind die gespeicherten Patientendaten und -dokumente nach Ablauf der Aufbewahrungsfrist zu löschen bzw. zu sperren, wenn diese nicht mehr zur Aufgabenerfüllung benötigt werden. Weiterhin kann ein Patient jederzeit sein Recht auf Berichtigung, Sperrung oder Löschung der über ihn gespeicherten Daten in Anspruch nehmen. In der Praxis wird das Problem so gelöst, dass zum einen nur bestimmte Benutzer das Recht zum Löschen besitzen und zum anderen nicht das Dokument, sondern nur die Referenz und die Indexdaten zum Dokument gelöscht werden. Das Dokument ist somit zwar noch vorhanden, es ist aber nicht mehr auffindbar. Bei einer Migration auf ein neues Speichermedium werden diese Dokumente allerdings nicht mit übernommen.

Um eine langfristige Lesbarkeit der Patientendaten zu gewährleisten, muss die Ablage in standardisierten revisionssicheren und rechtlich anerkannten Datenformaten erfolgen. Dabei ist es schwierig, vorherzusehen, welche Datenformate auch noch nach 30 Jahren lesbar sind. Im Rahmen einer Diplomarbeit zum Thema „Datenformate und Transformation elektronisch signierter Dokumente“[15] an der Universität Heidelberg/Fachhochschule Heilbronn wurden Kriterien erarbeitet, die eine Bewertung der Datenformate bezüglich ihrer Eignung für die beweiskräftige und sichere Langzeitaufbewahrung von medizinischen Dokumenten ermöglicht [Hollerbach et al. 2003a]. Nach [Hollerbach et al. 2005b] sind für die Langzeitaufbewahrung von medizinischen Dokumenten die folgenden Dateiformate geeignet:

- PDF für Textdokumente,
- XML für Beschreibungssprachen,

[15] Hollerbach A. (2003): Datenformate und Transformation elektronisch signierter Dokumente. Diplomarbeit, Ruprecht-Karls-Universität Heidelberg/Fachhochschule Heilbronn. Abteilung Medizinische Informatik.

- TIFF für Bilder,
- DICOM für die radiologischen bildgebenden Verfahren und
- S/MIME[16] für die Archivierung von E-Mails.

Mit Microsoft Office erstelle Dokumente sind dagegen nicht für die Langzeitspeicherung geeignet, da dieses Datenformat häufigen Versionswechseln unterliegt und die Spezifikation dieses Datenformates nicht offen gelegt ist [Hollerbach et al. 2006].

Für die Langzeitspeicherung der zu archivierenden Objekte sind standardisierte Datenträger einzusetzen. Nur so ist gewährleistet, dass es auch noch nach mehreren Jahren (mindestens 5 Jahre) Laufwerke gibt, die ein Einlesen des Datenträgers ermöglichen.

Damit die in einem digitalen Archiv aufbewahrten Dokumente auch wiedergefunden werden, ist eine Beschreibung der Dokumente durch Deskriptoren notwendig. Die Deskriptoren werden zusammen mit den Dokumenten im digitalen Archiv aufbewahrt.

3.1.3 Indexierung

Jedes Dokument, welches in einem digitalen Archiv abgelegt wird, muss durch so genannte Deskriptoren eindeutig beschrieben werden. Anhand dieser Deskriptoren ist eine gezielte Suche nach Patienteninformationen möglich. Je mehr Deskriptoren zu einem Dokument erfasst werden, desto einfacher kann es später wieder aufgefunden werden. Welche Deskriptoren zu einem Dokument zu erfassen sind, hängt von der Art des Dokumentes ab. Aus diesem Grund werden die Dokumente in Dokumentenklassen (z.B. Arztbrief, Röntgenbefund, OP-Bericht) eingeteilt. Für jede Dokumentenklasse sind die zu erfassenden Deskriptoren zu definieren. Die Realisierung der Dokumentenklassen mit den Deskriptoren setzt ein umfangreiches Indexierungskonzept voraus. Laut [Häber et al. 2005] und [Schmücker 1998a] sollten jedoch mindestens die Fallidentifikationsnummer, die Dokumentenklasse (z.B. Arztbrief, Röntgenbefund), die Bewegung (z.B. Aufnahme, Entlassung) oder Maßnahme (z.B. Operation, radiodiagnostische Untersuchung), die erbringende und anfordernde Leistungsstelle sowie der Zeitpunkt der Leistungserstellung als Deskriptoren erfasst werden. Zu einer Dokumentenklasse kann auch die Lebensdauer hinterlegt sein. So ist eine fristgemäße Vernichtung der verschiedenen Dokumentenarten möglich. Die Deskriptoren, die zur Identifizierung eines Dokumentes dienen, werden auch als Indexdaten oder Metadaten bezeichnet.

Die Funktion zum Indexieren kann vom Archivierungssystem zur Verfügung gestellt werden, sie kann aber auch von den Subsystemen des KIS übernommen werden. So ist es z.B. möglich, dass die Subsysteme, in denen die Dokumente erzeugt werden, die zu archivierenden Dokumente einschließlich der zugehörigen Indexdaten an das digitale Archiv übergeben. Unabhängig von der Herkunft der Indexdaten werden diese zusammen mit einem Verweis auf das Dokument in einer Datenbank abgespeichert. Die Dokumente selbst werden in der Regel im Ablagesystem des digitalen Archivs aufbewahrt.

Es ist zwischen manueller und automatischer Indexierung zu unterscheiden. Bei der manuellen Indexierung werden die Indexdaten zu einem Dokument über Bildschirmmasken erfasst (z.B. bei der Erstellung oder nach dem Einscannen eines Dokumentes). Diese Art der Erfassung von Patienteninformationen ist zum einen sehr aufwändig und zum anderen können Fehler bei der Eingabe entstehen (z.B. Zahlendreher in der Patientenidentifikationsnummer). Weiterhin können die eingegebenen Indexdaten von unterschiedlicher Qualität sein, je nachdem, welcher Nutzer die Daten erfasst hat. Aus diesem Grund sollten in den Erfassungsmasken nach Möglichkeit keine Freitexte, sondern Auswahllisten verwendet werden. Bei der automatischen Indexierung werden die Indexdaten aus den Dokumenten ermittelt. Dafür gibt es gibt verschiedene Ansätze:

[16] S/Mime ist ein Datenformat, das zur sicheren E-Mail-Kommunikation eingesetzt wird.

1. Indexierung über Barcodeerkennung

   Die Papierdokumente werden mit einem Barcode versehen. Der Barcode setzt sich aus vorher fest definierten Informationen zusammen, z.B. kann der Barcode der Fallidentifikationsnummer eines Patienten entsprechen. Beim Einscannen des Dokumentes wird der Barcode mit Unterstützung von zusätzlichen Werkzeugen erkannt und dem Dokument als Indexwert zugeordnet.

2. Indexierung über das Texterkennungsverfahren OCR

   OCR steht für Optical Character Recognition und ist ein Verfahren, das das Auslesen von Text aus Dokumenten ermöglicht, die als Image vorliegen. Die in dem Image enthaltenen Informationen können vom Rechner nicht interpretiert werden und werden daher auch als nicht-kodierte Informationen (NCI = Non Coded Information) bezeichnet. Mit Hilfe der OCR-Texterkennung können einzelne Indexwerte oder der gesamte Inhalt eines NCI-Dokumentes ausgelesen werden. Die Erkennung einzelner Indizierungsattribute wird bei Formularen mit einem festen Aufbau angewandt. Die Indizierungsattribute befinden sich an definierten Bereichen innerhalb des Formulars. In diesen Bereichen wird eine Texterkennung durchgeführt und die erkannten Indizierungsattribute werden als Index zu dem Dokument gespeichert. Sollen dagegen alle in dem Dokument enthaltenen Informationen als Index abgespeichert werden (z.B. für Nutzung der Volltextsuche), dann muss der gesamte Text aus dem Dokument ausgelesen werden. Stopp- und Füllwörter werden dabei ausgeschlossen. Der Datenbestand der Indexdatenbank wird in diesem Fall sehr groß.

3. Indexierung von elektronisch hinterlegten und lesbaren Formularen

   Bei der Erfassung von Patientendaten über eine Bildschirmmaske oder bei der Erstellung eines Dokumentes sind bestimmte Felder als Index hinterlegt. Diese Felder müssen entweder vom Nutzer ausgefüllt werden (z.B. Erfassung der Stammdaten des Patienten) oder sie werden automatisch generiert (z.B. Patienten- und Fallidentifikationsnummer).

Da die manuelle Indexierung zeitaufwendig und nicht zuverlässig ist, sollte die Indexierung so weit wie möglich automatisiert durchgeführt werden. In der Regel erfolgt die Indexierung der Dokumente in den Anwendungsbausteinen, in denen die Dokumente erstellt werden. Das Archivierungssystem sollte aber auch eine nachträgliche Indexierung der Dokumente unterstützen.

Oftmals existieren auch Dokumente, die zusammengehören. So bilden z.B. das Röntgenbild und der Röntgenbefund eine Einheit. Diese Dokumente müssen als zusammengehörig gekennzeichnet (indexiert) und gemeinsam angesprochen werden können [Häber et al. 2005].

3.1.4 Recherche im digitalen Archiv

Im Wesentlichen werden die folgenden zwei Suchverfahren unterschieden:

- indizierte Suche
- Volltextsuche (inhaltliche Suche)

Bei der indizierten Suche werden die zu den Dokumenten hinterlegten Deskriptoren durchsucht. Durch die Deskriptoren wird ein Dokument beschrieben. Die Deskriptoren werden als Suchkriterien verwendet, um gezielt nach Daten und Dokumenten im digitalen Archiv zu suchen. Typische Deskriptoren sind u.a. Patientenname, Geburtsdatum, Patientenidentifikationsnummer, Diagnosen, Therapien, Dokumentendatum, Dokumentenklasse und Dokumentenart. Anhand der Deskriptoren muss jedes Dokument eindeutig wiederauffindbar sein.

Neben der indizierten Suche gibt es noch die Volltextsuche, bei der die Inhalte der archivierten Dokumente nach bestimmten Suchkriterien durchsucht werden. Voraussetzung für die Volltextsuche ist jedoch, dass die Dokumente in kodierter Form vorliegen (CI = Coded Information). Eingescannte Dokumente gehören zu den NCI-Dokumenten. Soll auch eine Volltextsuche in den gescannten Dokumenten möglich sein, so muss in den Dokumenten eine OCR-Erkennung durchgeführt werden. Die erkannten Informationen können (müssen aber nicht) als Indexinformationen zum

Originaldokument in einer Volltextdatenbank abgespeichert werden. Damit stehen diese Indexinformationen für weitere Recherchen und das Wiederauffinden von Dokumenten zur Verfügung. Die indizierte Suche und die Volltextsuche können miteinander kombiniert werden.

Die Suchfunktion sollte die Verwendung von Wildcards sowie die Kombination einzelner Suchkriterien (z.B. über logischer Operatoren) unterstützen.

Die Suche nach Daten und Dokumenten zu einem Patienten sollte von berechtigten Nutzern an jedem klinischen Arbeitsplatz zu jeder Zeit möglich sein. Die Recherche kann dabei entweder aus dem führenden Informationssystem, über eine webbasierte Oberfläche oder über einen Rechercheclient durchgeführt werden. Es sollte immer die Möglichkeit bestehen, die archivierten Patientenunterlagen unabhängig vom führenden Informationssystem zu betrachten. Die Ergebnisse der Suchanfrage können in Form einer Trefferliste zurückgegeben werden. Ein Abspeichern der Trefferliste kann dabei vom Archivierungssystem unterstützt werden. Bei normalen Suchanfragen sollte das digitale Archiv eine Antwortzeit von 2 Sekunden nicht überschreiten [Häber et al. 2005].

Der Anwender sollte zusätzlich die Möglichkeit haben, sich selbst benutzerorientierte Mappen anzulegen, z.B. um sich nur aktuelle Dokumente oder Dokumente aus einem bestimmten Bereich anzeigen zu lassen.

3.1.5 Anzeige, Präsentation und Reproduktion von Dokumenten

Die Anzeige der archivierten Dokumente kann entweder über das Archivierungssystem oder aus einem Anwendungsbaustein des KIS erfolgen. Für die Einsicht der Dokumente direkt über das Archivierungssystem werden von den Anbietern webbasierte Oberflächen zur Verfügung gestellt. Über diese Oberfläche muss der Benutzer sich am Archivierungssystem anmelden, um auf die archivierten Dokumente und Daten zugreifen zu können. Um ein erneutes Anmelden des Benutzers an einer zusätzlichen Oberfläche zu vermeiden, gibt es zwei weitere Möglichkeiten:

- Die Anzeige der archivierten Dokumente wird in ein Anwendungssystem integriert. Die Dokumente werden über einen Link geöffnet, der zu dem entsprechenden Dokument im Ablagesystem führt.
- Indexierter Aufruf der APA eines Patienten. In diesem Fall werden Kontextinformationen übergeben, die einen direkten Einsprung in die APA eines Patienten ermöglichen. Die entsprechende APA wird in einem Web-Browser geöffnet.

Die Dokumente werden entweder über die Anwendungsprogramme, mit denen sie erstellt wurden, oder über Viewer angezeigt. Die Anzeige der Dokumente über die Erstellungsprogramme setzt jedoch voraus, dass an jedem Arbeitsplatz, an dem die archivierten Dokumente angezeigt werden sollen, diese Programme installiert sind. Da die Daten und Dokumente bis zu 30 Jahre lang zu archivieren sind, unterliegen die Programme häufig Versionswechseln. Oftmals ist mit einer neuen Version auch eine Änderung des Dateiformates verbunden. Um eine langfristige Lesbarkeit der einzelnen Dateiformate zu gewährleisten, müsste jede Version des Anwendungsprogrammes, mit der die Dokumente erstellt wurden, an den Arbeitsplätzen installiert werden. Für ein Universitätsklinikum entsteht somit ein hoher Aufwand für die Wartung der einzelnen Arbeitsplatzrechner. Mit der Installation fallen häufig auch Lizenzkosten für die Nutzung der Programme an. Um diese Probleme zu umgehen, bietet sich der Einsatz von Viewern an. Viewer sind Programme, mit denen Dokumente eines bestimmten oder mehrerer Dateiformate (PDF, DICOM, ASCII, TIFF, JPEG) angezeigt werden können. Das erzeugende Programm wird zur Anzeige nicht benötigt. Da es verschiedene Dateiformate gibt, existieren auch unterschiedliche Viewer zur Anzeige der Dokumente. Aus diesem Grund sollten nur standardisierte Dateiformate eingesetzt werden, die von einem Standardviewer gelesen werden können. Viewer unterstützen die Bearbeitung von Dokumenten nicht. Somit ist eine Veränderung der Dokumente ausgeschlossen. Ein Viewer sollte jedoch bestimmte Funktionen zur Anzeige der Dokumente zur Verfügung stellen. Zu diesen Funktionen gehören u.a. die Anzeige des Dokumentes in Originalgröße, das Vergrößern oder Verkleinern von Dokumentenausschnitten mittels einer Zoom-Funktion, das Blättern in mehreren Seiten, das Drehen und Spiegeln des Dokumentes, Veränderung des Kontrastes und der Helligkeit beim Abtasten und Reproduzieren der Dokumente. Die Anbieter von

Archivierungssystemen stellen in der Regel einen eigenen Viewer zur Verfügung. Einige Anbieter unterstützen aber auch die Einbindung von externen Viewern.

Weiterhin sollte eine gleichzeitige Anzeige von verschiedenen Patientenunterlagen unterstützt werden. Dadurch können z.B. Röntgenbilder nebeneinander betrachtet und verglichen werden. So lassen sich Veränderungen im Krankheitsverlauf besser erkennen.

Für die Präsentation der Daten und Dokumente existieren unterschiedliche Konzepte [Häber et al. 2005]:

- listenförmige Darstellung der Dokumente in Form eines Inhaltsverzeichnisses
- tabellenförmige, quantitative Darstellung der Dokumente in Abhängigkeit von Behandlungsperioden und Dokumentenklassen oder Behandlungsperioden und Maßnahmen
- Verwendung von Metaphern wie Dokumentenstapel, Ringbücher, Hefte etc. für Dokumentensammlungen als Abbild der realen Welt bezüglich Erscheinungsbild und Funktionalität
- Verkleinerte Darstellung von Dokumenten, so genannte Thumbnails oder Stamps
- Darstellung durch LifeLines[17].

Manchmal kann es notwendig sein, Notizen zu einem Dokument zu hinterlegen. Bei Papierdokumenten kann dies in Form von Klebezetteln erfolgen. Auch in einem Archivierungssystem sollte es möglich sein, bestimmte Bereiche im Dokument zu markieren oder Notizen zu hinterlegen (z.B. für Pflegekräfte). Dabei kann es auch erforderlich sein, bestimmte Bereiche im Dokument für bestimmte Benutzergruppen auszublenden. Das Anbringen von Notizen oder die farbliche Markierung von Bereichen stellen keine Veränderung des elektronischen Dokumentes dar und sind somit ein zulässiges Hilfsmittel.

Neben der Ausgabe auf dem Bildschirm sollte natürlich auch ein Ausdruck des elektronischen Dokumentes auf dem Drucker oder eine Weiterleitung des Dokumentes (z.B. per E-Mail an den weiterbehandelnden Arzt) möglich sein. Die Funktion zur Reproduktion eines digitalen Dokumentes kann vom Archivierungssystem zur Verfügung gestellt werden. Diese Funktion kann aber auch von einem anderen Anwendungsbaustein des KIS übernommen werden. In diesem Fall greift der entsprechende Anwendungsbaustein über Schnittstellen auf die im Ablagesystem abgelegten Dokumente zu.

Der Zugriff auf die archivierten Patientenunterlagen sollte vom KAS möglich sein. Dabei ist sicherzustellen, dass nur befugte Benutzer die Berechtigung zur Anzeige und zum Ausdruck der Dokumente besitzen. Es sollte eine benutzerspezifische Sicht erfolgen, d.h. der Nutzer sieht nur die Dokumente und Funktionen, für die er auch die entsprechenden Berechtigungen besitzt.

3.1.6 Administration

Die Funktion Administration umfasst:

- die Benutzer- und Berechtigungsverwaltung
- die Erstellung der Aktenstruktur
- die Definition der Dokumentenklassen einschließlich der dazugehörigen Dokumentenattribute

[17] LifeLines ist eine Technik, die in Java implementiert wurde. Diese Technik wurde entwickelt, um eine übersichtliche Darstellung der Patientenhistorie zu ermöglichen. Die Darstellung der EPA erfolgt unter Verwendung von so genannten „Timelines“ (horizontalen Balken). Durch diese horizontalen Balken können Behandlungszeiträume mit den entsprechenden Diagnosen, Maßnahmen usw. übersichtlich dargestellt werden. Informationen zu LifeLines sind verfügbar unter: www.cs.umd.edu/hcil

- Überwachungsfunktionen
- die Erstellung von Protokollen
- das Management der Speichermedien
- das Ansteuern von Speicherlaufwerken
- die Datensicherung.

Patientendaten gehören zu den sensiblen Daten, die einer besonderen Geheimhaltung unterliegen. Gemäß des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze in Verbindung mit den Landeskrankenhausgesetzen dürfen Patientendaten nur dann verarbeitet werden, wenn sie zur Erledigung der Aufgaben benötigt werden. Eine Einsicht in die APA eines Patienten darf einer Person (z.B. behandelnder Arzt) also nur dann gewährt werden, wenn ein Behandlungszusammenhang besteht. Es gilt der folgende Grundsatz:

„Patientendaten dürfen nur im Rahmen der Zweckbestimmung des Behandlungsvertrages und den damit verbundenen gesetzlichen Regelungen erhoben und verarbeitet, nicht aber uneingeschränkt ausgetauscht und verwendet werden. Für wissenschaftliche Zwecke sollen in der Regel Daten nur anonymisiert, pseudonymisiert oder mit Einwilligung der Patienten verwendet werden.“ [Häber et al. 2005, Seite 23]

Gemäß § 33 Abs. 7 Sächsisches Krankenhausgesetz unterliegen die personenbezogenen Daten, die in automatisierten Verfahren gespeichert und direkt aufrufbar sind, nach Abschluss der Behandlung eines Patienten dem alleinigen Zugriff der jeweiligen Fachabteilung. Ein Zugriff auf diese Daten ist nur mit Zustimmung der Fachabteilung zulässig. Es ist die Aufgabe eines digitalen Archivs, die archivierten Daten und Dokumente gegen unbefugte Zugriffe zu schützen. Um sicherzustellen, dass nur autorisierte Nutzer auf die archivierten Patientendaten und -dokumente zugreifen können, muss ein Berechtigungskonzept erstellt werden, in dem festzulegen ist,

1. welcher Benutzer mit dem Archivierungssystem arbeiten darf und
2. „WER AUF WAS WANN WIE ZUGREIFEN DARF“ [Häber et al. 2005].

Dazu müssen einzelne Berechtigungsstufen und Rollen definiert werden können, die über die Patienten-ID, Fall-ID und Dokumentenarten bis zur Dokumentenebene einstellbar sind [Häber et al. 2005]. In einer Rolle werden Benutzer zu Gruppen zusammengefasst, z.B. entsprechend ihrer Aufgabenstellung oder Funktion (Arzt, Pflegepersonal usw.).

Für die Verwaltung der Benutzer und Berechtigungen kann ein Administrationstool bereitgestellt werden. Es besteht jedoch auch die Möglichkeit, Benutzer und Rollen aus einer bestehenden Benutzerverwaltung zu übernehmen, z.B. vom SAP, Active Directory oder LDAP. Die Authentifizierung des Benutzers erfolgt entweder in den administrativen/klinischen Anwendungsbausteinen oder am Archivierungssystem selbst. In Notfällen muss ein Zugriff auf die APA möglich sein. Weiterhin kann es erforderlich sein, dass ein Zugriff auf bestimmte Patientenunterlagen auch anderen Krankenhäusern, niedergelassenen Ärzten oder dem Medizinischen Dienst der Krankenkassen (MDK) für einen bestimmten Zeitraum zur Verfügung gestellt wird. Ein Zugriff kann z.B. im Rahmen der Integrierten Versorgung oder beim Einholen einer Zweitmeinung erforderlich sein. In all diesen Fällen müssen die Zugriffe auf die entsprechenden Patientenunterlagen lückenlos protokolliert werden. Dazu gehören auch Änderungen an den Zugriffsberechtigungen.

Entsprechend § 9a BDSG können Anbieter von digitalen Archiven[18] ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Ein Beispiel für das Ergebnis einer

[18] Genauer Wortlaut: „Anbieter von Datenverarbeitungssystemen und –programmen und datenverarbeitenden Stellen“

Begutachtung und Bewertung ist das Datenschutz-Gütesiegel[19], das vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) vergeben wird. Mit der Vergabe des Gütesiegels bestätigt das ULD, dass das IT-Produkt (z.B. das digitale Archiv) die Vorschriften über den Datenschutz und die Datensicherheit erfüllt. Die Prüfung erfolgt durch einen unabhängigen Sachverständigen, der das Produkt unter rechtlichen und technischen Aspekten begutachtet. Besonderer Wert wird dabei auf die Datenvermeidung, Datensparsamkeit (z.B. Verwendung von Löschfunktionen zum automatischen Löschen von archivierten Dateien nach Ablauf der Aufbewahrungsfrist), Datensicherheit, Revisionsfähigkeit und auf die Gewährleistung der Rechte der Betroffenen gelegt. Das Gütesiegel wird für Hard- und Software sowie für automatisierte Datenverarbeitungsverfahren erteilt, die zur Nutzung durch öffentliche Stellen geeignet sind [ULDa]. Im medizinischen Bereich wurden bisher 5 Produkte vom ULD zertifiziert [ULDb]. Darunter ist ein Produkt für die elektronische externe Archivierung von Röntgenbildern und ein Verfahren zur Kommunikation und revisionssicheren Langzeitarchivierung von digitalen medizinischen Bildern und Befundberichten. Es ist zu erwarten, dass Audits und Gütesiegel zur Überprüfung des Datenschutzes und der Datensicherheit auch in anderen Bundesländern zum Einsatz kommen.

Das digitale Archiv muss die Protokollierung aller Aktionen (z.B. das Löschen eines Dokumentes, Änderung der Ablagestruktur) und Zugriffe auf die archivierten Patientenunterlagen unterstützen. Nur so ist die Nachvollziehbarkeit gewährleistet. Anhand der Protokollierungen können statistische Auswertungen durchgeführt werden, z.B. Zugriffshäufigkeiten und Datenträgerbelegungen.

Öffnet ein Nutzer ein Dokument in einer APA, dann bleibt ihm in der Regel verborgen, von wo das Dokument geholt wird. Es ist die Aufgabe des digitalen Archivs, die Patientenunterlagen ordnungsgemäß und revisionssicher auf einem Speichermedium abzulegen. Die Verwaltung der Speichermedien sowie die Ansteuerung der Laufwerke erfolgt durch das digitale Archiv. Über das Administrationstool können die Dokumentenklassen, Dokumentenarten, Dokumentenattribute und die Verzeichnisstruktur der APA durch einen Administrator definiert werden. Manche Anbieter unterstützen sogar die Anzeige, was auf welchem Speichermedium abgelegt ist.

Um eine hohe Verfügbarkeit zu gewährleisten, ist regelmäßig eine Datensicherung durchzuführen. In der Datensicherung sollten die Indexdaten, die archivierten Daten und Dokumente sowie die Berechtigungsstrukturen enthalten sein. Für die Sicherung des digitalen Archivs ist ein Datensicherungskonzept zu erstellen.

3.1.7 Versionsmanagement

Die Veränderung eines archivierten Dokumentes ist nicht zulässig. Trotzdem kann es hilfreich sein, ein archiviertes Dokument für eine Weiterbearbeitung zur Verfügung zu stellen. In diesem Fall wird das Dokument unter einer neuen Version im digitalen Archiv abgespeichert. Das ursprüngliche Dokument bleibt unverändert erhalten. Die Verwaltung der Versionen stellt somit eine weitere Funktionalität dar. Um Suchanfragen zu unterstützen, sollte auch die Möglichkeit bestehen, standardisierte Kataloge und Hauskataloge für Diagnosen und Prozeduren mit den Versionen und Indexdaten zu speichern.

3.1.8 Historienverwaltung

Für die Verwaltung von digitalen Patientenakten muss laut [Häber et al. 2005] die Historie der zugehörigen Patienten- und Falldaten lückenlos zur Verfügung stehen. Die Historienverwaltung ermöglicht das Wiederauffinden von Patientenunterlagen auch bei nachträglichen Änderungen in den Daten wie z.B. bei einer Namensänderung durch Heirat. Dabei muss eine Suche sowohl nach den alten als auch nach den neuen Daten möglich sein.

[19] Weitere Informationen zum Datenschutz-Gütesiegel sind verfügbar unter: http://www.datenschutzzentrum.de/guetesiegel

Weiterhin kann eine Verlegungshistorie durch den Mitschnitt von HL7-Nachrichten geführt werden. Anhand der Verlegungshistorie wird geprüft, ob es einen Behandlungszusammenhang gibt. Nur wenn ein solcher besteht, wird Zugriff auf die APA eines Patienten gewährt.

3.1.9 Neusignierung

Elektronisch signierte Dokumente verlieren mit der Zeit an Beweiskraft. Die Ursache dafür ist, dass die elektronische Signatur auf kryptographischen Algorithmen beruht, die im Laufe der Zeit unsicher werden. Die Fälschungssicherheit des Dokumentes ist damit nicht mehr gewährleistet. Aus diesem Grund muss die elektronische Signatur erneuert werden, bevor die verwendeten Signaturalgorithmen ihre Sicherheit verlieren und somit eine Fälschung der Signatur möglich ist. Eine Erneuerung der Signatur wird auch in der Signaturverordnung gefordert. Gemäß § 17 SigV muss die elektronische Signatur mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen. Für die Erneuerung der Signatur von elektronischen Dokumenten ist die Umsetzung des ArchiSig-Konzeptes erforderlich. Die Erneuerung der Signatur stellt somit eine wichtige Funktion des digitalen Archivs dar. Die Anbieter von Archivierungssystemen arbeiten zurzeit an der Umsetzung des ArchiSig-Konzeptes. Dabei besteht die Möglichkeit, Softwareprodukte von Anbietern, die sich auf dieses Problem spezialisiert haben (z.B. ArchiSoft vom Fraunhofer-Institut SIT, digiSeal von der secrypt GmbH), in das digitale Archiv zu integrieren.

3.1.10 Löschfunktion

Grundsätzlich dürfen die in einem digitalen Archiv abgelegten Patientenunterlagen weder gelöscht noch verändert werden. Aus datenschutzrechtlicher Sicht ist jedoch ein Löschen der archivierten Dokumente in zwei Fällen notwendig:

1. die Aufbewahrungsfrist des Dokumentes ist abgelaufen oder
2. der Patient bittet um die Sperrung oder Löschung der über ihn gespeicherten Patientendaten.

Das Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist kann über automatische Löschfunktionen realisiert werden. Dazu wird die Aufbewahrungsdauer zu den einzelnen Dokumentenarten als Attribut hinterlegt sowie der Zeitpunkt, wann das Dokument in das digitale Archiv importiert wurde. Nach Ablauf der Aufbewahrungsfrist wird das Dokument automatisch gelöscht. Die Aufbewahrungsdauer wird jedoch immer vom letzten Aufenthalt bzw. der letzten Untersuchung eines Patienten gerechnet. Falls der Patient also innerhalb der Aufbewahrungsdauer der Dokumente erneut behandelt wird, muss die Aufbewahrungsdauer der Dokumente angepasst werden. Wie diese Anpassung der Aufbewahrungsdauer erfolgt, soll für die im Rahmen der Diplomarbeit bearbeiteten Anbieter erläutert werden.

Für den zweiten Fall muss das Archivierungssystem das manuelle Löschen von Dokumenten unterstützen. Das Löschen einzelner Dokumente darf dabei nur von einem autorisierten Nutzer durchgeführt werden. Das Löschrecht wird über die Benutzerverwaltung an ausgewählte Nutzer vergeben. Um sicherzustellen, dass das Dokument auch wirklich gelöscht werden soll, kann es erforderlich sein, dass zwei Nutzer die Löschung durch ihre Signatur bestätigen müssen.

Da in der Regel die Patientenunterlagen in einem digitalen Archiv auf WORM-Medien abgelegt werden, ist ein Löschen der Dokumente nicht möglich. In diesem Fall erfolgt eine Sperrung der Dokumente. Dabei werden die Verweise in der APA auf das Dokument und die dazugehörigen Indexdaten entfernt. Die Referenz und die Indexdaten zum Dokument werden in der Datenbank gelöscht. Damit ist das gesperrte Dokument zwar noch im digitalen Archiv vorhanden, eine Zuordnung des Dokumentes ist jedoch nicht mehr möglich. Das Dokument ist nicht mehr auffindbar. Bei einer späteren Migration werden die gesperrten Dokumente nicht übernommen. Die Sperrung und Löschung von Dokumenten ist grundsätzlich zu protokollieren.

3.1.11 Zusammenfassung

Zu den Grundfunktionen eines digitalen Archivs gehören also:

- die Übernahme der Daten und Dokumente in das digitale Archiv
- die revisionssichere, ordnungsgemäße Ablage und Langzeitspeicherung der Daten und Dokumente
- die Indexierung
- die Recherche
- die Anzeige, Präsentation und Reproduktion von Dokumenten
- die Administration
- das Versionsmanagement
- die Historienverwaltung
- die Neusignierung der Dokumente
- das Sperren /Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist bzw. auf Bitte des Patienten.

Optional können Funktionen für das Scannen, Erstellen der Signatur oder Programme zur Erstellung von Dokumenten (z.B. Arztbrief) angeboten werden.

3.2 Aufgaben

Aus diesen Funktionen lassen sich die folgenden Aufgaben ableiten:

1. Archivierte Patientenakte anlegen

   Eine APA kann manuell durch einen Benutzer oder automatisch angelegt werden. Die automatische Erstellung einer APA erfolgt entweder beim Import eines Dokumentes von einem unbekannten Patienten oder durch die administrative Aufnahme eines Patienten. Beim Import eines Dokumentes in das Archivierungssystem wird anhand bestimmter Attribute (z.B. Patienten- oder Fallidentifikationsnummer) geprüft, ob eine APA zu dem Patienten im Archivierungssystem existiert. Falls es noch keine APA zu dem Patienten gibt, wird automatisch eine angelegt.

2. Dokument importieren

   Wenn ein Dokument abgeschlossen und freigegeben ist, kann es zur Aufbewahrung an das Archivierungssystem übergeben werden. Beim Import bekommt jedes Dokument vom Archivierungssystem eine eindeutige Identifikationsnummer zugewiesen. Im Allgemeinen werden die Dokumente einschließlich der Indexinformationen importiert. Die Indexinformationen können aber auch aus dem Dokument ermittelt werden. Neben Dokumenten ist auch ein Import von Bildern, Befunden, Videos und Signalen direkt aus dem erzeugenden Quellsystem in das Archivierungssystem möglich. Falls die Dokumente beim Import noch nicht in einem langzeitstabilen Dateiformat vorliegen, müssen sie automatisch in ein Langzeitformat konvertiert werden. Nur so ist eine langfristige Lesbarkeit der Dokumente gewährleistet.

3. Dokument archivieren

   Nachdem die Patientenunterlagen importiert wurden, müssen sie im Ablagesystem ordnungsgemäß und revisionssicher gespeichert werden.

4. Dokument transformieren

   Um die langfristige Lesbarkeit von elektronischen Dokumenten zu erhalten, kann es laut [Viebeg 2006] notwendig sein, die gespeicherten Dokumente im Laufe ihrer Aufbewahrungszeit rechtzeitig in andere, aktuellere Formate umzuwandeln. Dabei muss sichergestellt sein, dass durch die Transformation der Beweiswert des signierten Dokumentes nicht verloren geht. Mit dieser Problematik beschäftigt sich das Projekt TransiDoc, das Verfahren und Konzepte für eine rechtssichere Transformation von elektronisch signierten Dokumenten erarbeitet [TransiDoc]. Das Projekt ist noch nicht abgeschlossen. Zukünftige Archivierungssysteme sollten die rechtssichere Transformation von elektronisch signierten Dokumenten unterstützen. Dazu sind jedoch die vollständigen Ergebnisse des TransiDoc-Projektes abzuwarten.

5. Dokument löschen und Vernichtung protokollieren

   Die Aufbewahrungsdauer beginnt mit dem Zeitpunkt, an dem ein Dokument in das Archivierungssystem importiert wurde. Nach Ablauf der Aufbewahrungsdauer sind die Dokumente zu löschen bzw. zu sperren. Das automatische Löschen von Dokumenten erfolgt anhand eines Attributes, in dem die Aufbewahrungsdauer zu einem Dokument hinterlegt ist. Eine Sperrung oder Löschung eines Dokumentes kann auch aufgrund der Bitte eines Patienten entsprechend Bundesdatenschutzgesetz erforderlich sein. Das manuelle Löschen von Dokumente darf nur durch autorisierte Nutzer erfolgen. Das gelöschte Dokument darf auch bei Recherchen nicht mehr angezeigt werden. Das Löschen bzw. Sperren von Dokumenten ist zu protokollieren.

6. Archivierte Patientenakte vernichten

   Nach Ablauf der Aufbewahrungsfrist ist die APA zu vernichten. Es muss sichergestellt sein, dass kein Zugriff mehr auf die APA möglich ist. Die in einer APA enthaltenen Informationen dürfen nach dem Löschen auch nicht mehr bei Recherchen angezeigt werden. Das Löschen einer APA ist zu protokollieren.

7. Dokument suchen

   Mit Hilfe der Deskriptoren kann gezielt nach Dokumenten in dem Archivierungssystem gesucht werden. Die Suche wird standardmäßig in den zu einem Dokument hinterlegten Indexdaten durchgeführt. Anhand der Deskriptoren ist auch eine gezielte Suche nach Informationen zu einem Patienten, Fall, Aufenthalt oder APA eines Patienten möglich.

8. Dokument signieren

   Spätestens bei der Übergabe eines elektronischen Dokumentes an das digitale Archiv müssen unterschriftsrelevante Dokumente mit einer qualifizierten elektronischen Signatur versehen sein. Dadurch wird die Integrität und Authentizität des Dokumentes sichergestellt. Nach [Fischer-Dieskau et al. 2006] bietet es sich an, auch nicht elektronisch signierte Dokumente durch einen initialen Archivzeitstempel abzusichern. Der Archivzeitstempel beinhaltet einen Zeitstempel mit einer qualifizierten elektronischen Signatur. Dadurch kann die Integrität des Dokumentes ab dem Zeitpunkt der Erstellung des initialen Archivzeitstempels nachgewiesen werden [Fischer-Dieskau et al. 2006].

   Bei der elektronischen Signierung von Dokumenten ist darauf zu achten, dass das Dokument erst in ein langzeitstabiles Dateiformat konvertiert wird. Das konvertierte Dokument muss zur inhaltlichen Kontrolle noch einmal angezeigt werden, bevor die elektronische Signatur erzeugt wird.

9. Dokument versenden

   Dokumente können per Fax oder per E-Mail verschickt werden. Für den Versand eines Dokumentes per E-Mail gibt es zwei Möglichkeiten:

- Es wird nur der Link auf das Dokument versandt. In diesem Fall kann der Empfänger nur das Dokument öffnen, wenn er einen Zugriff auf das Archivierungssystem und die Berechtigung zur Ansicht des Dokumentes besitzt.
- Das Dokument wird per E-Mail versandt. In diesem Fall wird das Berechtigungskonzept des Archivierungssystems umgangen. Jeder, der die E-Mail empfängt, kann das Dokument lesen. Beim Versand eines Dokumentes per E-Mail muss also durch den Absender genau geprüft werden, ob der Empfänger auch berechtigt ist, das Dokument zu lesen.

Der Versand von Dokumenten per Fax oder E-Mail kann über die Vergabe von Berechtigungen geregelt werden. Über die Berechtigungen kann z.B. festgelegt werden, welche Dokumentenklassen durch welchen Mitarbeiter versandt werden dürfen.

10. Archivierte Patientenakte versenden

    Neben dem Versand eines einzelnen Dokumentes kann es auch erforderlich sein, die komplette APA eines Patienten zu versenden. Auch hier besteht die Möglichkeit, entweder einen Link auf die APA oder die APA selbst zu versenden.

11. Signatur erneuern

    Die Signaturen müssen erneuert werden, bevor die verwendeten Signaturalgorithmen unsicher werden und die elektronisch signierten Dokumente ihre Beweiskraft verlieren. Entsprechende Archivierungskonzepte wurden im Projekt ArchiSig erarbeitet.

12. Berechtigung prüfen

    Es ist zu prüfen, ob der Benutzer die erforderlichen Rechte zur Einsichtnahme in die Daten und Dokumente eines Patienten besitzt. Bei Recherchen ist darauf zu achten, dass der Benutzer nur die Dokumente angezeigt bekommt, die er auch anschauen darf. Weiterhin muss sichergestellt sein, dass nur autorisierte Benutzer Dokumente löschen bzw. sperren dürfen.

13. Dokumente anzeigen

    Der Benutzer kann sich die Dokumente anschauen. Allein das Ansehen eines Dokumentes hat keinen Einfluss auf die Beweiskraft [Häber et al. 2005], da keine Veränderung des Dokumentes erfolgt. Für die Anzeige des elektronisch gespeicherten Dokumentes muss ein geeigneter Viewer zur Verfügung stehen. Bei der Anzeige von Patientenunterlagen werden folgende Prozesse durchlaufen:

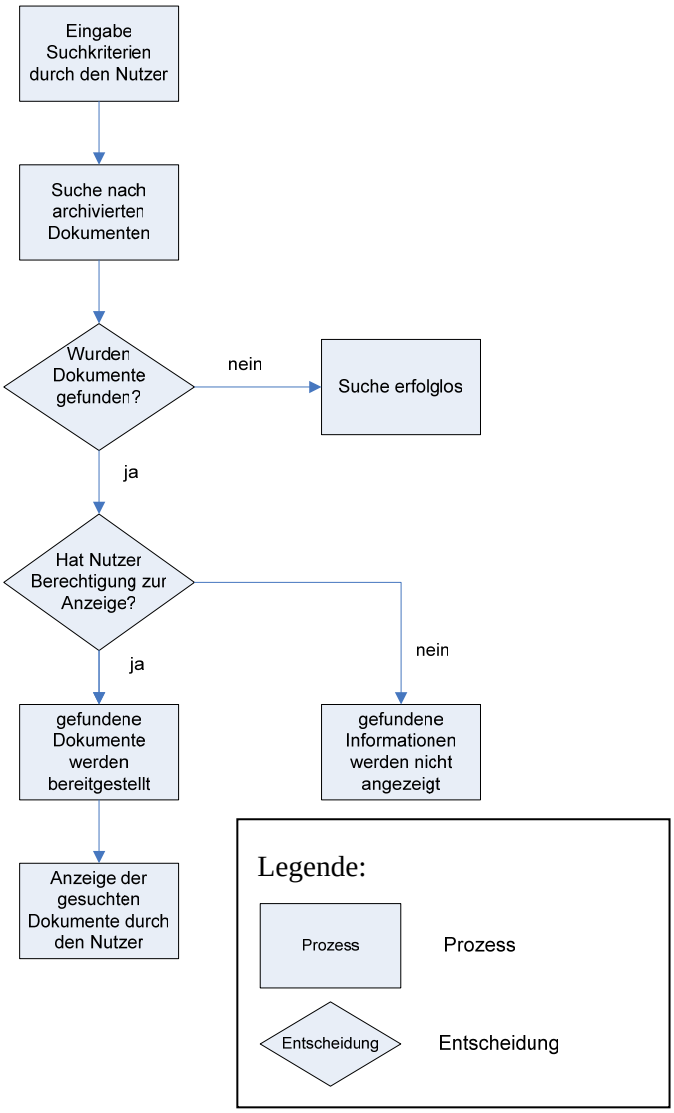


Abbildung 3-2: Prozesse von der Suche bis zur Anzeige von Patientenunterlagen

14. Dokumenteninhalt suchen

    Die archivierten Dokumente können nach beliebigen Begriffen durchsucht werden. Dazu müssen die Dokumente in kodierter Form vorliegen oder es wird eine OCR-Erkennung in den Dokumenten durchgeführt.

15. Zugriff protokollieren

    Alle Zugriffe auf die Daten und Dokumente in einem digitalen Archiv sind lückenlos zu protokollieren.

16. Dokument digitalisieren

    Wenn die zu archivierenden Dokumente in Papierform vorliegen, müssen die Papierdokumente zunächst mit Hilfe eines Scanners eingescannt und indexiert werden. Das eingescannte Dokument liegt anschließend in elektronischer Form in einem Langzeitformat vor. Das Digitalisieren eines Dokumentes kann z.B. erforderlich sein, wenn ein Patient bei der Aufnahme Dokumente von einem externen Arzt mitbringt.

    Die Aufgabe Dokument digitalisieren setzt sich aus den Teilaufgaben Dokument einscannen und Dokument indexieren zusammen.

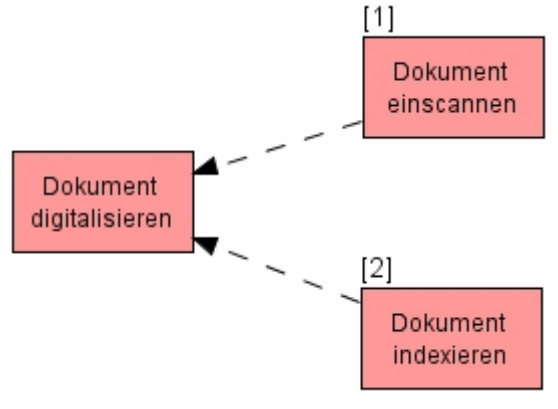


Abbildung 3-3: Aufgabe Dokument digitalisieren

17. Dokument drucken

    Das Archivierungssystem verfügt über eine Druckfunktion. Damit ist der Ausdruck von einzelnen Dokumenten möglich. Der Ausdruck von Dokumenten ist nur autorisierten Nutzern gestattet.

18. Aufbewahrungsdauer anpassen

    Die Aufbewahrungsdauer wird immer seit der letzten Behandlung oder dem letzten Aufenthalt eines Patienten gerechnet. Bei einer erneuten Behandlung oder einem erneuten Aufenthalt eines Patienten im Krankenhaus muss die Aufbewahrungsdauer der bis dahin erstellten Dokumente angepasst werden.

4 Referenzmodell für die digitale Archivierung

4.1 Fachliche Ebene

4.1.1 Aufgaben

Auf die Aufgaben eines digitalen Archivs wurde bereits im Abschnitt 3.2 eingegangen. Es gibt jedoch auch Aufgaben, die außerhalb des digitalen Archivs erledigt werden. Bei der Erledigung dieser Aufgaben entstehen Informationen, die das digitale Archiv benötigt.

1. Administrative Aufnahme

   Die Beschreibung der administrativen Aufnahme ist aus dem „Referenzmodell der fachlichen Ebene“, das an der privaten Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT) erstellt wurde, entnommen. Als Quelle diente [Hübner-Bloder 2005].

   Zur administrativen Aufnahme gehört z. B. das Festhalten des Kostenübernehmers, der Aufnahmeart, der Wahl- und Regelleistungen, der Angehörigen und des Einweisers. Plausibilitätsprüfungen und Aufzeichnungshilfen (Auswahllisten, automatische Belegung von Feldern) sichern die Qualität der Aufnahmedaten. Die Kostenübernahmeklärung mit dem Kostenträger wird initiiert. Der Patient wird außerdem einer Station und einem Bett zugeordnet. Die hier erhobenen verwaltungsrelevanten Daten des Patienten müssen für alle weiteren Aufgaben zur Verfügung stehen (z. B. in Form von Organisationsmitteln wie Etiketten). Die vom einweisenden Arzt ggf. übermittelten Informationen (z. B. bisherige Befunde und Bilder) werden an den zuständigen Arzt weitergeleitet. Die Aufnahme erfolgt ggf. auch direkt auf Station (z. B. bei Notfällen). Dazu gehört auch die Änderung bereits aufgezeichneter Aufnahmedaten. Nicht ansprechbare Notfallpatienten können vorläufig aufgenommen werden. Die während der Notfallbehandlung aufgezeichneten Daten können später übernommen werden. Neugeborene werden mit Bezug zum Behandlungsfall der Mutter aufgenommen. Begleitpersonen werden mit Bezug zum Patienten aufgenommen.

   Die Aufnahmeart (z.B. ambulant, stationär) kann gewechselt werden, ohne dass eine neue Fallnummer vergeben wird.

2. Dokumentenbeschreibung erzeugen (indexieren)

   Jedes Dokument wird mit Hilfe von Deskriptoren beschrieben. Die Deskriptoren dienen zum Wiederauffinden der Dokumente. Die Indexierung erfolgt in der Regel in dem Anwendungsbaustein, in welchem das Dokument erstellt wurde oder beim Import des Dokumentes.

4.1.2 Objekttypen

Im Referenzmodell werden die folgenden Objekttypen verwendet:

- **ADT-Information:** Dieser Objekttyp enthält Informationen über die Aufnahme, Verlegung und Entlassung eines Patienten.
- **APA:** Eine APA ist eine virtuelle Akte, in der Informationen zum Patienten, Fall sowie Dokumente, die nicht mehr verändert werden, in einer übersichtlichen Aktenstruktur dargestellt werden.
- **Dokument der APA:** In dem Objekttyp Dokument sind alle inhaltlichen Informationen des Dokumentes gespeichert.
- **Dokumentenbeschreibung:** In diesem Objekttyp werden die Informationen zu einem Patienten, Fall und Dokument zusammengefasst. Diese Informationen stellen die

beschreibenden Attribute (Deskriptoren) zu einem Dokument dar. Anhand der Deskriptoren kann ein Dokument einem Patienten, Fall und einer Dokumentenklasse zugeordnet werden. Die Deskriptoren können als Suchkriterien verwendet werden, um gezielt nach Patientenunterlagen im digitalen Archiv zu suchen.

- **elektronisches Dokument:** Dieser Objekttyp umfasst alle inhaltlichen Informationen eines elektronischen Dokumentes, das zu archivieren ist.
- **elektronisches Dokument im Langzeitformat**: Das elektronische Dokument liegt einschließlich der Indexinformationen in einem langzeitstabilen Dateiformat vor.
- **Fall:** Dieser Objekttyp umfasst alle Informationen, die einen Behandlungsfall beschreiben [Winter et al. 2005]. Zu diesen Informationen gehören z.B. eine Fallidentifikationssnummer, Behandlungsart, Aufnahmedatum, Station, Aufnahmediagnose, Verlegstation, Entlassungsdiagnose, Entlassungsdatum.
- **Nachricht über APA:** Dieser Objekttyp enthält die Information, dass eine APA versandt wurde.
- **Nachricht über Dokument:** Dieser Objekttyp enthält die Information, dass eine Dokument versandt wurde.
- **Papierdokument:** Der Objekttyp Papierdokument umfasst die in dem papierbasierten Dokument enthaltenen inhaltlichen Informationen.
- **Patient:** Der Objekttyp Patient enthält alle Informationen, die einen Patienten identifizieren und beschreiben. Zu diesen Informationen gehören z.B. die Patientenidentifikationsnummer, Name, Vorname, Geburtsdatum und die Adresse des Patienten.
- **Signiertes Dokument:** In dem signierten Dokument sind die Signatur einschließlich der Signaturinformationen (Name der signierenden Person, Datum und Zeitpunkt der Signaturerstellung) und Verifikationsdaten (z.B. Informationen über die Zertifikate und den verwendeten Signaturalgorithmus, Gültigkeitsdauer der Zertifikate, Zeitstempel zur Überprüfung der elektronischen Signatur) abgelegt [Hollerbach et al. 2005b].

4.1.3 Fachliche Ebene des Referenzmodells

In der folgenden Abbildung sind Aufgaben und Objekttypen auf der fachlichen Ebene des Referenzmodells dargestellt.

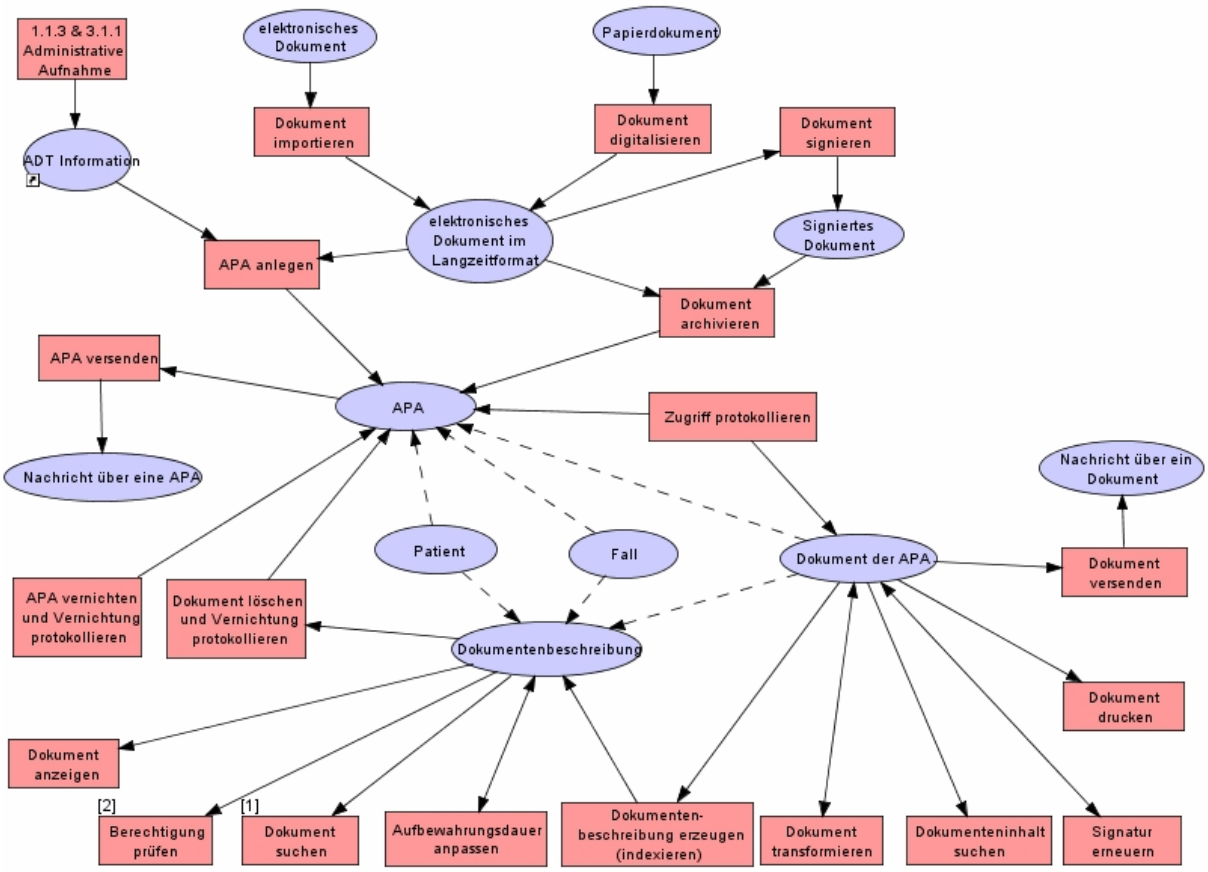


Abbildung 4-1: Fachliche Ebene des Referenzmodells

4.2 Logische Werkzeugebene

In diesem Kapitel sollen die Anwendungsbausteine vorgestellt werden, die zur Erledigung der Aufgaben benötigt werden. Die Anwendungsbausteine setzen sich zum einen aus den Teilkomponenten eines Archivierungssystems zusammen, zum anderen werden aber auch Anwendungsbausteine zur Kommunikation mit dem Archivierungssystem benötigt.

4.2.1 Anwendungsbausteine zur Kommunikation

Es ist sinnvoll, ein Archivierungssystem in das KIS zu integrieren. In diesem Abschnitt sollen typische Anwendungsbausteine erläutert werden, die mit dem Archivierungssystem kommunizieren und somit zur Erledigung der Aufgaben beitragen. Die Anwendungsbausteine werden in Anlehnung an [Winter et al. 2005] und [Haux et al. 2004] beschrieben.

Patientenverwaltungssystem

In einem Patientenverwaltungssystem (PVS) werden Daten zur Aufnahme, Verlegung und Entlassung von Patienten sowie abrechnungsrelevante Leistungen erfasst. Bei der Aufnahme eines Patienten werden seine Stammdaten erfasst. Anhand der Stammdaten muss überprüft werden, ob der Patient das erste Mal in Behandlung ist oder bereits früher einmal in Behandlung war. Handelt es sich um den ersten Aufenthalt, dann bekommt der Patient eine neue eindeutige Patientenidentifikationsnummer (PIN) zugewiesen. War der Patient schon einmal in Behandlung, muss er als Wiederkehrer identifiziert werden. In diesem Fall existiert bereits eine APA. Die darin abgelegten Patientenunterlagen sind dem behandelnden Personal zur Verfügung zu stellen ist. Pro Fall wird durch das PVS eine eindeutige Fallidentifikationsnummer vergeben.

Die Patientenstamm- und Falldaten werden zur Beschreibung von patientenbezogenen Dokumenten benötigt. Da die Patientenunterlagen in verschiedenen Subsystemen eines KIS erzeugt werden, müssen bestimmte Patientenstamm- und Falldaten als Indexdaten den anderen Subsystemen des KIS zur Verfügung gestellt werden. So können patienten- und fallbezogene Daten bereits bei der Aufnahme eines Patienten an das Archivierungssystem kommuniziert werden. Damit sind diese Patientendaten dem Archivierungssystem bekannt und neue Dokumente können eindeutig (z.B. anhand der Patienten- oder Fallidentifikationssnummer) dem Patienten oder Fall zugeordnet werden. Weiterhin sind bestimmte Parameter bei der Verlegung (z.B. Verlegungsdatum, Klinik, Station) und Entlassung eines Patienten (z.B. Entlassungsdatum, Klinik, Entlassungsdiagnose) automatisch an das Archivierungssystem zu kommunizieren.

In vielen größeren Krankenhäusern wird für die Patientenverwaltung das SAP R/3 Modul IS-H eingesetzt. Dieses Modul unterstützt die Patientenverwaltung, Abrechnung von Leistungen sowie die Verschlüsselung von Diagnosen und Prozeduren. Für die Kommunikation wird ein SAP eigenes Nachrichtenformat verwendet. Da in kleineren Krankenhäusern jedoch auch Produkte von anderen Anbietern für die Patientenverwaltung eingesetzt werden, soll im Modell die Patientenverwaltung durch den neutralen Anwendungsbaustein Patientenverwaltungssystem dargestellt werden.

Klinisches Dokumentations- und Managementsystem

Das Klinische Dokumentations- und Managementsystem (KDMS) wird für die klinische Dokumentation in einem Krankenhaus eingesetzt. Das KDMS ist in der Regel der führende Anwendungsbaustein in einem Krankenhaus. Um zu vermeiden, dass der Anwender für eine Anzeige und Recherche von archivierten Dokumenten das KDMS verlassen muss, ist der Aufruf des Archivierungssystems in das KDMS zu integrieren. Der Aufruf kann z.B. über einen Button „Archiv“ im KDMS erfolgen. Beim Aufruf des Archivierungssystems ist die Kontextintegration zu gewährleisten, d.h. bereits vorhandene Kontextinformationen wie z.B. Benutzerlogin, Benutzergruppe, Patienten- und Fallidentifikationsnummer werden vom KDMS an das Archivierungssystem übergeben. Damit sind eine erneute Anmeldung des Benutzers sowie eine erneute Suche (z.B. nach dem Patienten oder Fall) nicht erforderlich. Der einmal hergestellte Kontext im KDMS wird beim Aufruf des Archivierungssystems übernommen und kann dort weiter genutzt werden. Für die Anzeige der archivierten Dokumente wird ein Viewer vom Archivierungssystem bereitgestellt.

Modalitäten

Modalitäten sind medizinische Geräte (z.B. Röntgengerät, MRT, CT), mit denen Bilder erzeugt werden. Ein Archivierungssystem sollte sowohl die Aufbewahrung von Dokumenten als auch von medizinischen Bildern unterstützen. Es muss also eine Möglichkeit geben, die medizinischen Bilder direkt von den Modalitäten zu übernehmen und im digitalen Archiv abzulegen. Für den Austausch der Bilder müssen sowohl von der Modalität als auch von dem Archivierungssystem entsprechende Schnittstellen (z.B. DICOM) zur Verfügung gestellt werden.

Anwendungsbausteine zur Unterstützung von betriebswirtschaftlichen Prozessen

Im Verwaltungsbereich in einem Krankenhaus werden weiterhin Anwendungsbausteine für die betriebswirtschaftlichen Prozesse benötigt. Zu den typischen Anwendungsbausteinen, die diese Prozesse unterstützen, gehören u.a.:

- ein Finanzbuchhaltungssystem
- ein Materialwirtschaftssystem sowie
- ein Controllingsystem.

In vielen Krankenhäusern werden SAP R/3 Anwendungen für die betriebswirtschaftlichen Prozesse eingesetzt. SAP bietet z.B. für die Finanzbuchhaltung das Modul FI, für die Materialwirtschaft das Modul MM und für das Controlling das Modul CO an. Die Kommunikation zwischen der SAP R/3 Anwendung und dem Archivierungssystem wird über die SAP-Schnittstelle ArchiveLink realisiert. Ein Krankenhaus kann aber auch andere Produkte für die betriebswirtschaftlichen Prozesse verwenden.

Kommunikationsserver

Die Kommunikation mit dem Archivierungssystem kann auch über einen Kommunikationsserver erfolgen. Der Kommunikationsserver ermöglicht den Austausch von Nachrichten zwischen zwei Anwendungsbausteinen, insbesondere dann, wenn keine direkte Kommunikation zwischen diesen möglich ist. Der Anwendungsbaustein sendet eine Nachricht an den Kommunikationsserver, der diese Nachricht an den entsprechenden Empfänger weiterleitet. Liegt die Nachricht in einem Format vor, das der empfangende Anwendungsbaustein nicht kennt, übersetzt der Kommunikationsserver die Nachricht in ein für den empfangenden Anwendungsbaustein verständliches Format. Weiterhin können bestimmte Nachrichten (z.B. ADT-Nachrichten) an mehrere Anwendungsbausteine versandt werden. Zu den Aufgaben eines Kommunikationsservers gehört auch die Überwachung der einzelnen Kommunikationsbeziehungen. In vielen Krankenhäusern erfolgt die Kommunikation der verschiedenen Anwendungsbausteine über einen Kommunikationsserver.

Radiologieinformationssystem

Ein RIS ist ein Anwendungsbaustein, der für das Management in der diagnostischen Radiologie eingesetzt wird. Der Anwendungsbaustein bietet Unterstützung bei der

- Planung und Verwaltung von Untersuchungsterminen
- Organisation des Untersuchungsablaufs sowie bei der Bereitstellung des jeweils erforderlichen Personals
- Bereitstellung der Patientendaten und der geforderten Untersuchungsparameter an den Modalitäten
- Erstellung von Befunden [Haux et al. 2004].

Bildspeicher- und Kommunikationssystem

Für die Befundung und Speicherung der Bilder wird in vielen Krankenhäusern ein Bildspeicher- und Kommunikationssystem (PACS) eingesetzt. Das PACS ermöglicht gleichzeitig die langfristige Aufbewahrung der digitalen Bilder und Befunde. Weiterhin regelt es die Kommunikation mit den Modalitäten. Allerdings stellt das PACS nur ein Archivsystem für die diagnostische Radiologie dar. Die Dokumente, die in anderen Anwendungsbausteinen erstellt wurden, müssen in einem weiteren Archiv aufbewahrt werden. Damit erfolgt eine getrennte Aufbewahrung medizinischer Bilder und Dokumente. Zukünftig sollte über die Realisierung eines einzigen digitalen Archivs nachgedacht werden, das sowohl die langfristige Aufbewahrung von Dokumenten als auch von medizinischen Bildern unterstützt. Die Bilder und Befunde können dann vom RIS entweder direkt oder über den Kommunikationsserver an das Archivierungssystem übermittelt und archiviert werden.

Laborinformationssystem

Ein Laborinformationssystem (LIS) ist ein rechnergestützter Anwendungsbaustein, der ein Labor bei der Verwaltung von Analysen unterstützt. Zu den Aufgaben eines LIS gehören

- den Ablauf der Analyse einer Probe (z.B. Körperflüssigkeit, Gewebe) zu steuern,
- die Analyseautomaten mit den notwendigen Daten zum Untersuchungsauftrag zu versorgen,
- die Ergebnisse der Analyse entgegenzunehmen,
- Befunde zu erstellen,
- die Ergebnisse zu validieren und
- Qualitätssicherungsmaßnahmen durchzuführen [Winter et al. 2005].

Die Laborbefunde sind zur Langzeitarchivierung entweder direkt oder über den Kommunikationsserver an das Archivierungssystem zu übergeben.

Patientendatenmanagementsystem

Ein Patientendatenmanagementsystem (PDMS) ist ein Anwendungsbaustein, der die Aufgaben in der Intensivmedizin unterstützt. Dazu gehört u.a. die Überwachung von Messgeräten, die automatisch Vitalparameter eines Patienten (z.B. Blutdruck, Puls, Atemfrequenz) patientenbezogen aufzeichnen. Die aufgezeichneten Daten werden dem medizinischen Personal in einer übersichtlichen Form auf dem Bildschirm präsentiert. Liegt ein Wert eines Patienten im kritischen Bereich, wird das medizinische Personal sofort alarmiert. Um die Sicherheit eines Patienten auf der Intensivstation zu gewährleisten, muss das PDMS einschließlich der aufgezeichneten Daten ständig verfügbar sein. Wird der Patient von der Intensiv- auf die Normalstation verlegt, wird über das PDMS eine kurze Zusammenfassung der wichtigsten Dokumentationsinhalte für die Normalstation erstellt.

Ein PDMS dient somit der automatischen Aufzeichnung, Speicherung und Präsentation von patientenbezogenen klinischen Daten auf einer Intensivstation.

OP-Dokumentationssystem

Ein OP-Dokumentationssystem unterstützt die Erstellung von OP-Berichten. In einem OP-Bericht werden laut [Ingenerf et al. 2005] wichtige Daten wie z.B. das ärztliche Personal, die Operationszeiten, die durchgeführten Eingriffe, postoperative Diagnosen, intraoperative Komplikationen sowie Besonderheiten und Merkmale zur postoperativen Weiterbehandlung zusammengefasst. Weiterhin ersetzt das OP-Dokumentationssystem das OP-Buch, in dem alle Operationen aufgeführt sind.

Nachrichtenübermittlungssystem

Der Versand eines Dokumentes bis hin zu einer kompletten APA kann per E-Mail über ein Nachrichtenübermittlungssystem erfolgen. Als Nachrichtenübermittlungssystem kann z.B. Microsoft Outlook eingesetzt werden.

Signatursystem

Für die elektronische Signierung von Dokumenten ist ein Signatursystem erforderlich. Das Signatursystem setzt sich nach [Brandner et al. 2002] aus folgenden Komponenten zusammen:

- Kontrollkomponente: Die Kontrollkomponente empfängt Signaturanfragen von den rechnerbasierten Anwendungsbausteinen, analysiert diese und sendet sie an die anderen Komponenten.
- Signaturkomponente: Die Signaturkomponente dient zur sicheren Erzeugung von elektronischen Signaturen unter Verwendung der Signaturkarte. Bevor die Signatur erstellt wird, müssen die zu signierenden Daten zur Kontrolle auf dem Bildschirm angezeigt werden. Die Signaturkomponente sollte die Erzeugung mehrerer Signaturen unterstützen. Die Signaturen werden in standardisierten Formaten gespeichert.
- Verifikationskomponente: Die Verifikationskomponente dient zur Überprüfung der Integrität und Authentizität elektronisch signierter Dokumente. Bei der Verifikation wird die Gültigkeit der Zertifikate überprüft.
- Anzeigekomponente: Die Anzeigekomponente dient zur eindeutigen Darstellung des Dokumentes, das elektronisch signiert werden soll. Mit Hilfe der Anzeigekomponente kann überprüft werden, auf welchen Inhalt die Signaturen sich beziehen. Der Inhalt des Dokumentes kann über die Anzeigekomponente nicht geändert werden.
- Konvertierungskomponente: Die Konvertierungskomponente ermöglicht die Transformation von unterschriftsrelevanten Dokumenten in ein standardisiertes langzeitstabiles Dateiformat.
- Druckkomponente: Die Druckkomponente ermöglicht den Ausdruck von elektronisch signierten Dokumenten. Vor dem Ausdruck wird das elektronisch signierte Dokument über die Verifikationskomponente überprüft. Das Ergebnis der Verifikation muss auf dem Ausdruck des Dokumentes sichtbar sein.

- Erneuerungskomponente: Die Erneuerungskomponente dient zur Erneuerung der Signaturen, bevor die kryptographischen Algorithmen ihre Sicherheit verlieren.

Das Signatursystem kann in verschiedene Anwendungsbausteine integriert sein.

Weitere Anwendungsbausteine

Natürlich können in einem Krankenhaus noch weitere Anwendungsbausteine zum Einsatz kommen. Grundsätzlich ist beim Einsatz eines Anwendungsbaustein darauf zu achten, dass die zu archivierenden Daten und Dokumente vollständig zur Langzeitaufbewahrung an das Archivierungssystem übergeben werden. Nur so ist eine vollständige APA gewährleistet.

4.2.2 Bausteinschnittstellen

Damit die Anwendungsbausteine in einem KIS auch untereinander Daten und Dokumente austauschen können, sind Schnittstellen, so genannte Bausteinschnittstellen, erforderlich. Dabei ist unbedingt darauf zu achten, dass für die Kommunikation standardisierte Bausteinschnittstellen eingesetzt werden. Der Austausch von Patientendaten kann durch die Verwendung eines Kommunikationsstandards unterstützt werden. Ein Kommunikationsstandard ermöglicht den Empfang und Versand von Nachrichten eines bestimmten Ereignistyps. Für die Kommunikation innerhalb eines Krankenhauses werden die Kommunikationsstandards HL7, DICOM sowie die SAP-Standards HCM und ArchiveLink verwendet.

Health Level Seven (HL7)

HL7[20] ist ein speziell für das Gesundheitswesen entwickelter Kommunikationsstandard, der die Übermittlung von patienten- und fallbezogenen Nachrichten ermöglicht. Die Kommunikation zwischen zwei Anwendungsbausteinen soll in Anlehnung an [Winter et al. 2005] beschrieben werden:

Ein Anwendungsbaustein A sendet aufgrund des Eintretens eines Ereignisses eine Nachricht an einen anderen Anwendungsbaustein B. Der für die Nachricht verwendete Nachrichtentyp hängt dabei vom Typ des eingetretenen Ereignisses ab. Jedem Ereignistyp ist ein Nachrichtentyp zugeordnet. In HL7 werden die Ereignistypen durch ein dreistelliges Kürzel beschrieben, z.B. A01 (Aufnahme eines Patienten), A02 (Verlegung eines Patienten) oder A03 (Entlassung eines Patienten). Durch den Nachrichtentyp wird der Aufbau der versendeten Nachricht beschrieben und die Bedeutung der einzelnen Teile der Nachricht festgelegt. Wenn der Anwendungsbaustein B die Nachricht erhalten hat, sendet dieser eine Bestätigung über den Empfang der Nachricht an den Anwendungsbaustein A zurück.

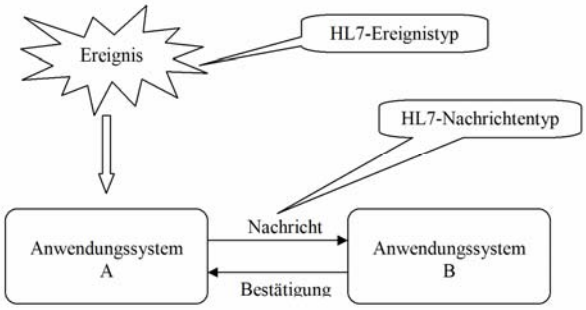


Abbildung 4-2: Ereignisgesteuerte Kommunikation bei HL7

(entnommen aus [Winter et al. 2005, Seite 592])

[20] weitere Informationen zum Kommunikationsstandard HL7 sind verfügbar unter: http://www.hl7.de/standard/standards.php

Eine Nachricht setzt sich aus verschiedenen Segmenten zusammen, die sich wiederum in einzelne Datenfelder gliedern lassen. Am Anfang jeder HL7-Nachricht steht das „message header segment“ (MSH). In diesem Segment kann z.B. der sendende (MSH-3) und empfangende Anwendungsbaustein (MSH-5) angegeben werden. Ein weiteres Segment ist das „patient identification segment“ (PID), welches zur Übermittlung patientenbezogener Daten wie z.B. Patientenidentifikationsnummer, Name und Geburtsdatum dient. Dieses Segment wird z.B. für Nachrichten verwendet, die zur Übermittlung von administrativen Patientendaten (ADT) dienen.

Digital Imaging and Communications in Medicine (DICOM)

DICOM[21] ist ein von der US-amerikanischen National Electrical Manufacturers Association (NEMA) entwickelter Kommunikationsstandard, der für die Übermittlung von medizinischen Bildern eingesetzt wird. Als Grundlage diente der ACR-NEMA-Standard, der ab 1983 in einer gemeinsamen Arbeitsgruppe des American College of Radiology (ACR) und der NEMA mit dem Ziel entwickelt wurde, erstmals einen Standard für den Austausch von medizinischen Bildern zu schaffen. Neben medizinischen Bildern werden auch bildbegleitende Informationen über:

- den Patienten (z.B. Name, Geburtsdatum, Identifikationsnummer)
- die Modalität und Aufnahme (z.B. Gerätetyp, Aufnahmeparameter)
- die Organisation (z.B. Untersuchung, Studie)

kommuniziert [Lehmann 2005]. Mit Hilfe des Kommunikationsstandards DICOM können also Bilder zwischen den Modalitäten, dem RIS, dem Bildbetrachtungs- und dem Archivierungssystem ausgetauscht werden.

Für den Austausch von medizinischen Daten sind Dienste erforderlich, die die Übertragung regeln. Im Teil 4 des DICOM-Standards werden Dienstklassen (service class) spezifiziert, die zur Kommunikation von medizinischen Daten dienen. Von einer Dienstklasse werden bestimmte Dienstleistungen zur Verfügung gestellt. Es werden u.a. die folgenden Dienstklassen definiert:

- Storage Service Class: ermöglicht die Übertragung von medizinischen Daten (z.B. Bilder, Berichte)
- Query/Retrieve Service Class: dient zur Abfrage von Informationen
- Print Management Service Class: ermöglicht den Ausdruck von bildbezogenen Daten.

Die jeweiligen Dienstklassen müssen vom jeweiligen Anwendungsbaustein unterstützt werden. Die Übertragung von medizinischen Daten erfolgt immer zwischen einem „Service Class User“[22] (SCU) und einem „Service Class Provider“[23](SCP). Der SCU ruft Dienste auf, die vom SCP bereitgestellt werden.

Hospital Communication Module (HCM)

Der SAP-Standard HCM wird von SAP für den Austausch von ADT-Nachrichten zur Verfügung gestellt. Beim Eintreten eines bestimmten Ereignisses (z.B. Aufnahme eines Patienten) wird eine zu dem Ereignis gehörende Nachricht erzeugt. Die Nachrichten werden in einem SAP-eigenen Nachrichtenformat (HCM-Format) erstellt und kommuniziert. HCM ist Bestandteil des SAP-Moduls IS-H. Da nicht alle Subsysteme eines KIS HCM-Nachrichten verarbeiten können, wird häufig ein

[21] weitere Informationen über den DICOM-Standard sind verfügbar unter: http://medical.nema.org

[22] Service Class User: the role played by a DICOM Aplication Entity (DIMSE-Service-User) which performs operation and invokes notifications on a specific Association [NEMA 2006].

[23] Service Class Provider: the role played by a DICOM Application Entity (DIMSE-Service-User) which performs operations and invokes notifications on a specific Association [NEMA 2006].

Kommunikationsserver (z.B. e*Gate) eingesetzt, der die HCM-Nachrichten in HL7-Nachrichten übersetzt [MI-Lexikon].

SAP ArchiveLink

Für die Kommunikation mit SAP R/3 Anwendungen muss der SAP-Standard ArchiveLink unterstützt werden. Dafür wird von SAP eine spezielle Schnittstelle bereitgestellt, die in das SAP R/3 System integriert ist. Um Dokumente direkt aus SAP R/3 Anwendungen archivieren zu können, müssen die Anbieter von Archivierungssystemen eine Schnittstelle zur Verfügung zu stellen, die von SAP zertifiziert wurde

Zu SAP ArchiveLink gehören die folgenden Schnittstellen:

- Benutzerschnittstelle
- Schnittstelle zu den SAP R/3 Anwendungen, die so genannte Anwendungsschnittstelle
- Schnittstelle zu externen Komponenten (z.B. zum Ablagesystem), die so genannte Archivschnittstelle [SAP 2001].

Über die Anwendungsschnittstelle können aus der SAP R/3 Anwendung Funktionen im Archivierungssystem angesprochen werden wie z.B. Dokument ablegen, Dokument bereitstellen und Dokument anzeigen. Die Archivschnittstelle definiert Funktionen, die Anbieter von digitalen Archiven realisieren müssen, um ihr Archivierungssystem und Ablagesystem an SAP R/3 anbinden zu können. Zu ArchiveLink gehört weiterhin ein Viewer, der die Anzeige von archivierten SAP-Dokumenten unterstützt [Gulbins et al. 2002].

Weitere Bausteinschnittstellen

Für die Übernahme der Daten und Dokumente aus den verschiedenen Anwendungsbausteinen stellt das Archivierungssystem eine eigene Schnittstelle zur Verfügung. Diese Schnittstelle wird oftmals als COLD-Schnittstelle bezeichnet und dient vor allem zur Massenübernahme von Dokumenten. Weiterhin stellt das Archivierungssystem Schnittstellen für:

- die Anbindung von Ablagesystemen
- den Zugriff auf eine bestehende Benutzer- und Berechtigungsverwaltung
- die Anbindung von Volltextsuchsystemen und
- die Integration von Signatursystemen

bereit.

Zusammenfassung

Dokumente aus SAP R/3-Anwendungen können über den SAP-Standard ArchiveLink in das Archivierungssystem übernommen werden. Für den Empfang von ADT-Nachrichten muss das Archivierungssystem die Kommunikationsstandards HL7 bzw. HCM unterstützen. Der Import von medizinischen Bildern und bildbegleitenden Informationen von den Modalitäten oder einem RIS erfolgt über den Kommunikationsstandard DICOM. Bausteinschnittstellen, die diese Standards verwenden, werden nachfolgend als HL7-, HCM-, DICOM- und ArchiveLink-Schnittstelle bezeichnet.

Neben der internen Kommunikation in einem Krankenhaus kann es natürlich auch notwendig sein, elektronische Dokumente mit anderen medizinischen Einrichtungen auszutauschen (z.B. mit einer Arztpraxis). Für die Kommunikation mit anderen medizinischen Einrichtungen kommen Verfahren

wie z.B. der VDAP[24] Communication Standard (VCS) oder PaDoK[25] zum Einsatz. Auf diese Verfahren soll in der Arbeit jedoch nicht weiter eingegangen werden.

Die Massenerfassung von Dokumenten erfolgt in der Regel über die COLD-Schnittstelle. Weiterhin werden Schnittstellen für die Anbindung von Ablage- und Volltextsuchsystemen, für die Integration von Signatursystemen sowie für den Zugriff auf eine bestehende Benutzer- und Berechtigungsverwaltung zur Verfügung gestellt.

4.2.3 Darstellung der Kommunikation auf der logischen Werkzeugebene im 3LGM²-Modell

In diesem Abschnitt wird die Kommunikation der Anwendungsbausteine mit dem Archivierungssystem auf der logischen Werkzeugebene im 3LGM²-Modell dargestellt. Die Kommunikation der einzelnen Anwendungsbausteine kann entweder über einen Kommunikationsserver oder direkt mit dem Archivierungssystem erfolgen.

In vielen Krankenhäusern kommunizieren die einzelnen Anwendungsbausteine über einen Kommunikationsserver. Für die Archivierung der medizinischen Bilder in der diagnostischen Radiologie kommt oftmals ein PACS zum Einsatz. In Zukunft ist über die Realisierung eines einheitlichen digitalen Archivs nachzudenken. Die folgende Abbildung stellt die Kommunikation der einzelnen Anwendungsbausteine mit dem Archivierungssystem über den Kommunikationsserver dar.

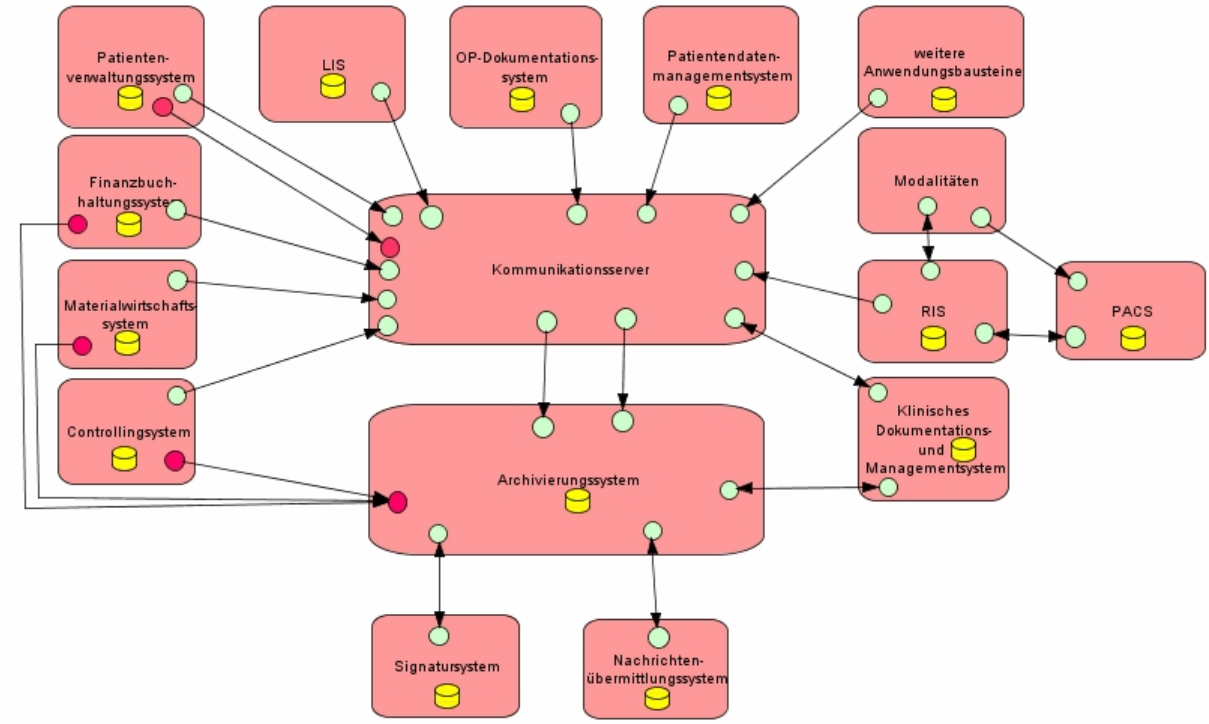


Abbildung 4-3: Kommunikation auf der logischen Werkzeugebene

[24] VCS wurde vom Verband deutscher Arztinformationshersteller und Provider (VDAP) e.V. zum sicheren Austausch von Patientendaten zwischen niedergelassenen Ärzten, Krankenhäusern sowie weiteren Institutionen des Gesundheitswesen entwickelt.

[25] PaDok (patientenbegleitende Dokumentation) ist ein vom Fraunhofer Institut für Biomedizinische Technik entwickeltes Verfahren zur sicheren Kommunikation.

4.2.4 Anwendungsbausteine eines Archivierungssystems

Ein Archivierungssystem setzt sich aus mehreren Komponenten zusammen, die in diesem Abschnitt vorgestellt werden sollen.

Administrationssystem

Bei der Administration eines digitalen Archivs ist grundsätzlich zu unterscheiden zwischen der Administration des Archivierungssystems und der Systemadministration des Ablagesystems. Das Administrationssystem wird vom Archivierungssystem bereitgestellt. In dem Administrationssystem erfolgt die Verwaltung der Benutzer, Kennwörter und Benutzerberechtigungen. Die Vergabe der Benutzerberechtigungen kann über die Zuweisung von Benutzergruppen und Rollen erfolgen. In der Benutzerverwaltung kann für jeden Benutzer definiert werden, welche Funktionen er ausführen darf. Zu diesen Funktionen gehören z.B. der Ausdruck, das Lesen, der Export oder der Versand von Dokumenten. Für die Benutzer können Benutzerprofile angelegt werden. Weiterhin dient das Administrationssystem zur

- Definition der Aktenarten (z.B. Fall-, Patientenakte) und Aktenstruktur
- Definition der Dokumentenklassen einschließlich der dazugehörigen Indexdaten
- Definition der Ablagestruktur.

Das Administrationssystem muss die Übernahme und einen Abgleich mit einer bereits existierenden Benutzer- und Berechtigungsverwaltung unterstützen.

Das Ablagesystem stellt in der Regel ein Werkzeug für die Systemadministration zur Verfügung. Über die Systemadministration erfolgt u.a.:

- die Konfiguration des Ablagesystems
- die Verwaltung der Speichermedien
- die Überwachung und Protokollierung von Aktionen sowie
- die Anzeige der verfügbaren Speicherkapazitäten.

Visualisierungssystem

Die Anzeige der Dokumente in einem Archivierungssystem erfolgt durch das Visualisierungssystem, das auch als Viewer bezeichnet werden kann. Anbieter von Archivierungssystemen stellen im Allgemeinen einen eigenen Viewer zur Ansicht der Dokumente bereit. Der Viewer sollte mindestens die Anzeige von Dokumenten in den Dateiformaten PDF, TIFF und JPEG unterstützen. Einige Archivierungssysteme verfügen auch über einen integrierten DICOM-Viewer. Für spezielle Dateiformate sollte jedoch auch die Möglichkeit bestehen, Viewer von einem Fremdanbieter in das Archivierungssystem zu integrieren.

Das Visualisierungssystem bietet u.a. Funktionen für das Vergrößern und Verkleinern von Dokumentausschnitten, für das Drehen von Dokumenten, das Hinzufügen von Notizen und farblichen Markierungen, für das Blättern innerhalb eines mehrseitigen Dokumentes, das Verändern des Kontrastes und für das Ausdrucken von Dokumenten.

Scansystem für Einzelerfassung

Für die Erfassung und Digitalisierung von papierbasierten Dokumenten sind Scansysteme erforderlich. Die Scansysteme werden vor allem an Arbeitsplätzen eingesetzt, an denen papierbasierte Dokumente eintreffen. In Abhängigkeit von der Anzahl der einzuscannenden Dokumente werden Scansysteme für die Einzelerfassung und Scansysteme für die Massenerfassung unterschieden.

Scansysteme für die Einzelerfassung kommen dort zum Einsatz, wo nur einzelne Dokumente erfasst werden müssen. Dazu gehört z.B. der Arbeitplatzrechner in der ambulanten oder stationären Patientenaufnahme in einem Krankenhaus. Mit Hilfe dieses Scansystems können Dokumente, die ein Patient von seinem niedergelassenen Arzt mitbringt, sofort eingescannt und elektronisch für den

weiterbehandelnden Arzt zur Verfügung gestellt werden. Auch auf einer Station fallen Papierdokumente an. So muss z.B. der Patient schriftlich in die Durchführung einer Operation einwilligen. Dazu unterschreibt er in der Regel einen Aufklärungsbogen, der dem Arzt als Nachweis dient, dass der Patient über die Risiken der Operation informiert wurde.

Das eingescannte Dokument wird über ein Anzeigemodul auf dem Bildschirm des Bearbeiters dargestellt. Damit kann der Bearbeiter die Übereinstimmung zwischen dem Originaldokument und dem eingescannten Dokument überprüfen. Mit dem Scansystem wird in der Regel auch ein Indexiermodul bereitgestellt. Der Bearbeiter kann somit manuell Attribute für das Dokument erfassen. Die Attribute dienen später zum Wiederauffinden des Dokumentes. Das eingescannte Dokument wird nach der Indexierung in ein langzeitstabiles Dateiformat (TIFF) transformiert. Durch das Anbringen der qualifizierten elektronischen Signatur bestätigt der Bearbeiter die ordnungsgemäße Umwandlung des Dokumentes [Häber et al. 2005]. Die Beweiskraft des transformierten Dokumentes bleibt somit erhalten.

Scansystem für die Massenerfassung

Sollen größere Mengen an Papierdokumenten digitalisiert werden, ist der Einsatz von Scansystemen erforderlich, die die Massenerfassung von Dokumenten unterstützen. Diese Scansysteme können z.B. für das Einscannen von Papierakten verwendet werden. Das Scansystem für die Massenerfassung dient zur Erledigung der Aufgabe „Dokument digitalisieren“.

Für die Massenerfassung von Papierdokumenten ist die manuelle Indexierung ungeeignet. Aus diesem Grund bieten diese Scansysteme Indexiermodule an, die eine automatische Indexierung der Dokumente vornehmen. Die automatische Indexierung erfolgt mittels Barcode- und OCR-Texterkennung. Da bei der automatischen Indexierung Fehler auftreten können (z.B. Barcode wurde nicht erkannt) und auch die Texterkennung nicht immer fehlerfrei ist, müssen die erkannten Informationen überprüft werden. Dafür wird in der Regel ein Validierungssystem vom Scansystem bereitgestellt, das dem Bearbeiter die erkannten Indexdaten zur inhaltlichen Kontrolle am Bildschirm anzeigt. Die Validierung der Daten kann mit Hilfe von Plausibilitätsprüfungen erfolgen.

Scansysteme stellen für die Massenerfassung von Dokumenten oftmals auch ein Klassifizierungssystem zur Verfügung. Ein Klassifizierungssystem ist eine Lernsoftware, die den Inhalt eines Dokumentes nach bestimmten Merkmalen durchsucht. Anhand dieser Merkmale kann das Klassifizierungssystem das Dokument einer Dokumentenklasse zuordnen. Wenn die Dokumentenklasse bekannt ist, können die erforderlichen Indexdaten über OCR, ICR oder OMR ermittelt werden. Klassifizierungssysteme werden sowohl für die Klassifikation von Formularen als auch für die Klassifikation von unstrukturierten Dokumenten eingesetzt. Die Indexierung und Zuordnung der Dokumente erfolgt in einem Klassifikationssystem automatisch.

Nachdem die papierbasierten Dokumente eingescannt, indexiert und validiert wurden, können sie an das digitale Archiv übergeben werden. Die Indexdaten und die Referenz zum Dokument werden in der Datenbank abgelegt. Das eingescannte Dokument wird im Ablagesystem gespeichert.

In der folgenden Abbildung sind mögliche Module eines Scansystems dargestellt, das zur Massenerfassung von Dokumenten dient.

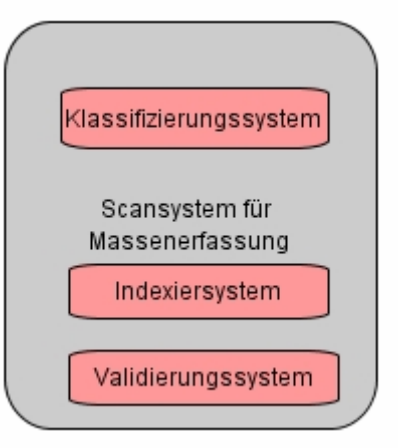


Abbildung 4-4: Darstellung möglicher Module eines Scansystems für die Massenerfassung

Recherchesystem

Das Recherchesystem ermöglicht die Suche nach Dokumenten unabhängig vom führenden Informationssystem. In dem Recherchesystem kann der Benutzer nach Dokumenten zu einem Patienten, Fall oder Aufenthalt suchen. Es ist auch eine gezielte Suche nach einer APA oder Fallakte zu einem Patienten möglich. Über eine Suchmaske erfolgt die Eingabe der Suchkriterien. Es können mehrere Suchkriterien miteinander kombiniert werden. Weiterhin muss das Recherchesystem patienten- und fallübergreifende Recherchen unterstützen. Der Arzt hat so die Möglichkeit, fachbezogene Recherchen durchzuführen. Die Ergebnisse der Recherche werden z.B. in Form einer Trefferliste angezeigt. Für die Recherche ist es unerheblich, wo die Dokumente gespeichert sind. Die Abfrage wird standardmäßig in den Indexdaten durchgeführt, die in der Datenbank des Archivierungssystems abgelegt sind. In der Datenbank ist auch die Referenz zum Dokument gespeichert. Die Recherche kann entweder über einen Rechercheclient oder über eine webbasierte Oberfläche erfolgen. Der Rechercheclient wird vom Anbieter des Archivierungssystems bereitgestellt und ist auf jedem Arbeitsplatzrechner zu installieren, von dem die Recherche durchgeführt werden soll. Die Recherche über eine webbasierte Oberfläche setzt dagegen nur die Installation eines Webbrowser voraus (z.B. Internet Explorer, Netscape). Anbieter von Archivierungssystemen bieten oftmals für die Recherche sowohl einen Rechercheclient als auch eine webbasierte Oberfläche an. In beiden Fällen ist eine Anmeldung des Benutzers am Archivierungssystem erforderlich. Im Referenzmodell werden diese beiden Recherchesysteme durch zwei getrennte Anwendungsbausteine dargestellt, die jedoch beide Teilmodule des Archivierungssystems sind.

Das Recherchesystem sollte die Erstellung von benutzerspezifischen Akten ermöglichen. Damit kann der Benutzer die für ihn relevanten Dokumente in einer eigenen Akte zusammenstellen. Für die Abfrage der dazustellenden Dokumente in der Akte können auch Filter eingesetzt werden. Dies ermöglicht z.B. die Anzeige von Dokumenten, die an einem Tag in einer bestimmten Abteilung erstellt wurden.

Zugriffskontrollsystem

Das Zugriffskontrollsystem muss sicherstellen, dass nur autorisierte Benutzer auf die archivierten Dokumente zugreifen können. Die einzelnen Anfragen, die an das Archivierungssystem gestellt werden, sind bzgl. der Berechtigung zu kontrollieren und zu protokollieren. Unbefugten Benutzern ist der Zugriff auf die Dokumente zu verwehren. Bei einer Recherche muss sichergestellt sein, dass dem Benutzer nur die Dokumente angezeigt werden, auf die er Zugriff hat.

Importsystem

Das Importsystem ermöglicht die automatische Übernahme von strukturierten Dokumenten aus den Anwendungsbausteinen eines KIS. In dem Importsystem wird für jede Dokumentenklasse der Aufbau sowie das Ablageformat definiert. Weiterhin können Regeln festgelegt werden, nach denen die Indexdaten aus dem Dokument ermittelt werden können. Die Dokumente werden vom Importsystem

automatisch oder im Dialog aus den Anwendungsbausteinen übernommen, entsprechend den hinterlegten Definitionen aufbereitet und zur Archivierung an das digitale Archiv übergeben. Über das Importsystem kann auch die Zuweisung von Layouts erfolgen. Weiterhin können Regeln festgelegt werden, nach denen die Indexdaten aus dem Dokument ermittelt werden können. Es ist zu unterscheiden zwischen dem Import von einzelnen Dokumenten und der Massenerfassung von Dokumenten. Für die Massenerfassung von Dokumenten werden so genannte COLD[26]-Verfahren eingesetzt. COLD-Verfahren ermöglichen die automatische Abarbeitung und Archivierung von fest definierten Jobs zu definierten Zeiten. Die Verfahrensweise beim Import der Dokumente ist jedoch gleich. Der Import von einzelnen Dokumenten kann aus dem führenden Anwendungsbaustein erfolgen. Der Massenimport von strukturierten Dokumenten erfolgt über eine COLD-Schnittstelle.

Volltextsuchsystem

Der Einsatz eines Volltextsuchsystems ist erforderlich, wenn eine Recherche in den Dokumentinhalten möglich sein soll. Dies kann z.B. notwendig sein, wenn nach Begriffen gesucht werden soll, die nicht als Index zu einem Dokument erfasst wurden. Volltextsuchsysteme verwenden in der Regel eine eigene Datenbank, in der die Inhalte der Dokumente mit Ausnahme von Stopp- und Füllwörtern gespeichert sind. Ein Volltextsuchsystem kann z.B. die phonetische Suche unterstützen. Bei der phonetischen Suche wird nach Wörtern gesucht, die ähnlich ausgesprochen, aber unterschiedlich geschrieben werden. Wird z.B. als Suchbegriff der Patientenname Meier eingegeben, dann werden auch die Patienten mit dem Namen Meyer, Maier usw. gefunden. Die phonetische Suche kann auch eingesetzt werden, um Wörter mit Rechtschreibfehlern oder unterschiedlichen Schreibweisen zu erkennen. Als weitere Funktionen kann ein Volltextsuchsystem Unterstützung bieten bei der

- Suche nach Synonymen,
- Suche nach Begriffskombinationen unter Verwendung logischer Operatoren (z.B. AND, OR, NOT) ,
- Suche nach inhaltlich verwandten Wörtern.

Workflowsystem

Mit Hilfe eines Workflowsystems können standardisierte und sich häufig wiederholende Geschäfts- und Teilprozesse auf die Organisationsstruktur eines Unternehmens (z.B. Krankenhaus) abgebildet werden. Die Prozesse können entsprechend dieses Workflows rechnergesteuert abgearbeitet werden. Workflows unterstützen vor allem die Weiterleitung von elektronischen Dokumenten. Die Weiterleitung kann z.B. erforderlich sein, wenn ein Dokument von mehreren Personen inhaltlich kontrolliert und elektronisch signiert werden muss. Weiterhin kann mit Hilfe eines Workflows z.B. festgelegt werden, wann welche Dokumente wie ins digitale Archiv übernommen werden sollen. Workflows bieten den Vorteil, dass der Status des Dokumentes jederzeit nachvollziehbar ist und überprüft werden kann, von wem das Dokument bearbeitet wurde. Für die graphische Darstellung der Geschäftsprozesse wird in der Regel ein Workflowdesigner zur Verfügung gestellt.

Eine Kernfrage ist allerdings, von wem die Workflowfunktionalitäten bereitgestellt werden sollen: vom Archivierungssystem oder vom führenden Anwendungsbaustein [Häber et al. 2006]. Dazu existieren unterschiedliche Meinungen bei den Anbietern von Softwareprodukten für die digitale Archivierung.

4.2.5 Datenbanksystem

Für die Verwaltung und das Wiederauffinden der archivierten Patientenunterlagen werden in der Regel Datenbanken mit relationalen Datenbankmanagementsystemen (z.B. Oracle oder MS SQL Server) eingesetzt. In der Datenbank sind nur Verweise auf die Dokumente sowie die dazugehörigen

[26] COLD steht für Computer Output to Laser Disk, d.h. elektronische Dokumente werden auf ein optisches Speichermedium ausgegegen [Gulbins et al. 2002].

Indexdaten gespeichert. Das Dokument selbst wird auf einem Ablagesystem archiviert. Die Verbindung zwischen Datenbank und Ablagesystem erfolgt über die Identifikationsnummer des Dokumentes (Dokumenten-ID). Beim Import des Dokumentes bekommt jedes Dokument eine Dokumenten-ID vom Archivierungssystem zugewiesen, die als Index in der Datenbank abgelegt wird. Um eine eindeutige Zuordnung des Dokumentes zu gewährleisten, wird es unter dieser ID im Ablagesystem archiviert. Wird die Dokumenten-ID aus der Datenbank gelöscht, ist das Dokument zwar noch vorhanden, es ist jedoch nicht mehr auffindbar. Weiterhin können die Signaturinformationen zu einem Dokument in der Datenbank abgelegt sein.

Zur Unterstützung der Volltextsuche kann optional eine Volltextdatenbank eingesetzt werden. Während in einer Indexdatenbank nur die zu einem Dokument hinterlegten Deskriptoren abgelegt sind, wird in einer Volltextdatenbank der gesamte Inhalt eines Dokumentes (mit Ausnahme von Stopp- und Füllwörtern) als Indexinformation zum Dokument abgespeichert. Eine Volltextdatenbank stellt eine Ergänzung zur Indexdatenbank dar.

4.2.6 Logische Werkzeugebene des Referenzmodells

In der folgenden Abbildung sind die einzelnen Komponenten eines Archivierungssystems sowie die Kommunikation mit typischen Anwendungsbausteinen in einem Krankenhaus auf der logischen Werkzeugebene im 3LGM^2-Modell dargestellt. Die Anwendungsbausteine kommunizieren über den Kommunikationsserver mit dem Archivierungssystem. Im Allgemeinen wird auch ein direkter Aufruf von archivierten Dokumenten aus dem Klinischen Dokumentations- und Managementsystem unterstützt. Falls das Archivierungssystem die ArchiveLink-Schnittstelle unterstützt, können die Dokumente auch über eine SAP-basierte Anwendung (z.B. Finanzbuchhaltungssystem FI, Materialwirtschaftssystem MM, Controllingsystem CO) eingesehen werden.

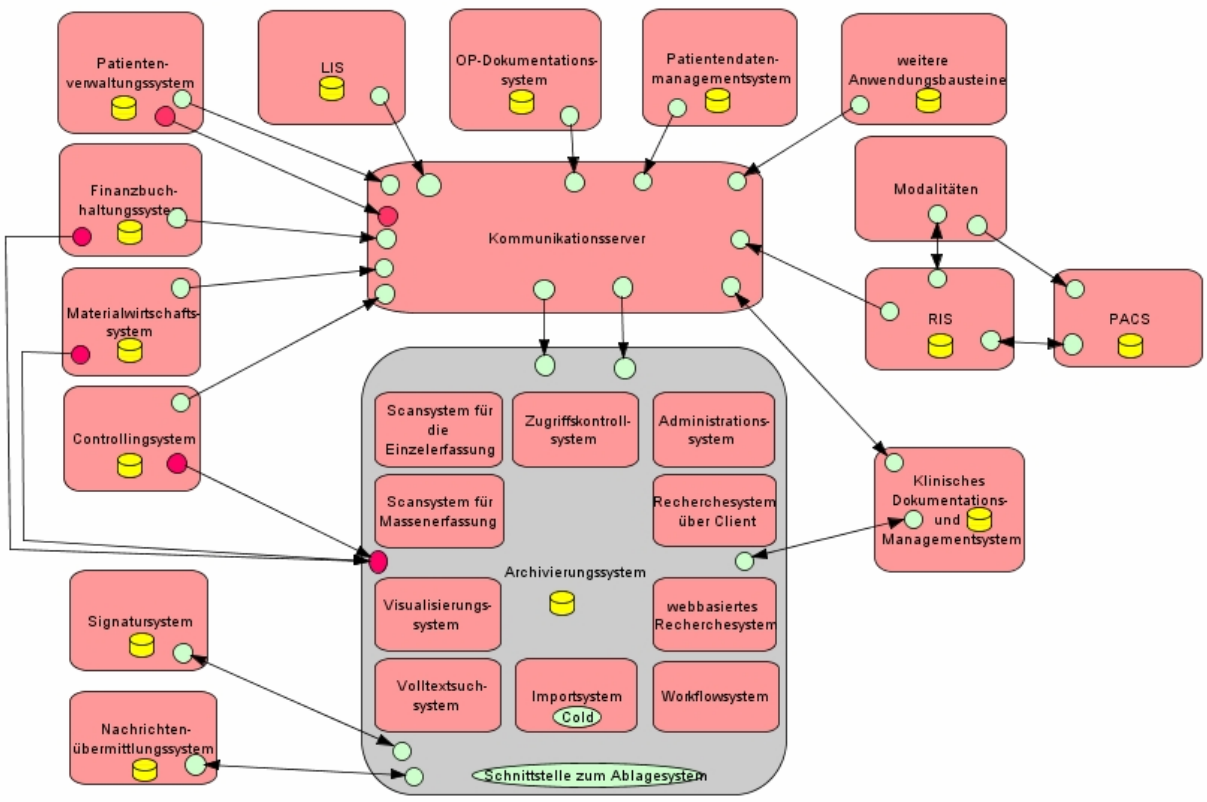


Abbildung 4-5: Logische Ebene des Referenzmodells

4.3 Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene

Im Anhang in Abbildung 9-3 ist in einer Matrix dargestellt, welche Aufgaben von welchen Anwendungsbausteinen erledigt werden. Die Aufgaben „Dokument transformieren“ und „Aufbewahrungsdauer anpassen“ wurden dem Archivierungssystem zugeordnet, da nicht bekannt ist, von welchem Teilmodul die Aufgaben erledigt werden. Daher ist in der Matrix bei den Aufgaben eine Verbindung zu allen Teilmodulen des Archivierungssystems dargestellt. Die Aufgabe „Dokument archivieren“ ist keinem Anwendungsbaustein zugeordnet. Die archivierten Dokumente werden auf einem Ablagesystem gespeichert, dass jedoch kein Bestandteil der logischen Werkzeugebene ist. Für das Löschen einer APA oder eines einzelnen Dokumentes mit einer anschließenden Protokollierung werden verschiedene Anwendungsbausteine benötigt. Das Löschen wird in den Recherchesystemen durchgeführt. Die Protokollierung erfolgt jedoch durch das Zugriffskontrollsystem, das auch die Benutzerberechtigungen überprüft. Die Aufgabe „Dokumentenbeschreibung erzeugen (indexieren)“ kann entweder in den Anwendungsbausteinen der Funktionsbereiche oder vom Importsystem des Archivierungssystems erledigt werden. Mit Hilfe des Visualisierungssystems werden die Aufgaben „Dokument anzeigen“ und „Dokument drucken“ durchgeführt. Die Scansysteme werden zur Erledigung der Aufgabe „Dokument digitalisieren“ eingesetzt. Diese Aufgabe beinhaltet sowohl das Einscannen als auch das Indexieren von Dokumenten. Um ein Dokument nach bestimmten Begriffen zu durchsuchen, die nicht als Index zu einem Dokument abgelegt wurden, wird das Volltextsuchsystem benötigt. Die Suche eines Dokumentes kann aus dem führenden Anwendungsbaustein in einem KIS oder über eines der beiden Recherchesysteme erfolgen. In den Recherchesystemen werden oftmals auch die Aufgaben „Dokument versenden“ und „APA versenden“ durchgeführt. Den Modalitäten und dem Kommunikationsserver sind im Rahmen der digitalen Archivierung keine Aufgaben zugeordnet. Diese beiden Anwendungsbausteine müssen jedoch mit betrachtet werden, da über den Kommunikationsserver die ADT-Nachrichten und die zu archivierenden Dokumente mit den Indexdaten an das Archivierungssystem kommuniziert werden. Mit Hilfe der Modalitäten werden medizinische Bilder erzeugt, die natürlich auch zu archivieren sind. Für die Aufgabe „Dokument importieren“ wird ein Importsystem benötigt, das die Dokumente in einem langzeitstabilen Dateiformat zur Archivierung übergibt. Die Aufgabe „Dokument signieren“ wird von dem Anwendungsbaustein Signatursystem unterstützt.

4.4 Physische Werkzeugebene

Die physische Werkzeugebene setzt sich aus verschiedenen Hardwarekomponenten zusammen. Eine zentrale Bedeutung hat das Ablage- bzw. Speichersystem. Die Installation der einzelnen Softwaremodule des Archivierungssystems erfolgt zum einen auf Servern, zum anderen ist aber auch eine Installation auf den Arbeitsplatzrechnern in einem Klinikum erforderlich. Zur Unterstützung können an den Arbeitsplatzrechnern verschiedene rechnerbasierte physische Datenverarbeitungsbausteine wie z.B. Drucker, Scanner, Barcodeleser und Kartenlesegeräte angeschlossen sein.

4.4.1 Ablagesystem

An das Ablagesystem in einem Krankenhaus werden hohe Anforderungen gestellt. Zum einen zeichnet es sich durch hohe Speicherkapazitäten aus. Aufgrund der langen Aufbewahrungszeiten und dem jährlich wachsenden Datenvolumen müssen die Speicherkapazitäten in einem Ablagesystem erweiterbar sein. Die Erweiterung der Speicherkapazität sollte dabei ohne größeren Aufwand realisiert werden können und sich auf die Investition in zusätzliche Speichermedien beschränken. Zu den weiteren Anforderungen, die ein Ablagesystem erfüllen muss, gehören schnelle Zugriffszeiten sowie eine hohe Verfügbarkeit (24 Stunden x 7 Tage). In Abhängigkeit von der Anzahl der Zugriffe und den Zugriffszeiten werden nach [Gulbins et al. 2002] drei Arten von Ablagesystemen unterschieden:

- Online-Ablagesystem: Diese Ablagesysteme zeichnen sich durch einen direkten und schnellen Zugriff auf die Daten aus. Als Online-Ablagesystem werden vor allem Plattensysteme eingesetzt. Da die Kosten im Vergleich zu den nachfolgend genannten Ablagesystemen hoch

sind, werden diese Ablagesysteme insbesondere für Daten verwendet, auf die häufig zugegriffen wird.

- Nearline-Ablagesystem: In einem Nearline-Ablagesystem befinden sich die Daten nicht im direkten Zugriff. Für den Zugriff auf die Daten muss das entsprechende Speichermedium rechnergesteuert zunächst in einem Laufwerk bereitgestellt werden. Die Zugriffszeiten sind etwas langsamer als bei den Online-Ablagesystemen. Nearline-Ablagesysteme verfügen jedoch über eine höhere Speicherkapazität und sind zudem eine günstige Alternative zu den teuren Online-Ablagesystemen. Da die Zugriffe auf die Daten im Laufe der Zeit abnehmen, werden die Daten oftmals nach einiger Zeit von einem Online- auf ein Nearline-Ablagesystem ausgelagert. Zu den Nearline-Ablagesystemen gehören z.B. optische Speichermedien in Jukeboxen.
- Offline-Ablagesysteme: Diese Ablagesysteme verfügen über eine hohe Speicherkapazität. Die Daten sind auf einem Speichermedium abgelegt, das sich nicht mehr im direkten Zugriff des Ablagesystems befindet. Ein Beispiel dafür ist die Aufbewahrung von Magnetbändern oder Magnetkassetten in einem Ablageschrank an einem entfernten Standort. Um die Daten wieder zur Verfügung zu stellen, muss das entsprechende Speichermedium manuell/personell geholt und in das Laufwerk des Ablagesystems eingelegt werden. Offline-Ablagesysteme dienen zur Aufbewahrung von Daten, auf die nicht mehr oder selten zugegriffen wird, die aber gemäß gesetzlichen Vorschriften aufzubewahren sind. Der Unterschied zwischen einem Nearline- und Offline-Ablagesystem besteht also nur darin, wo sich die entsprechenden Speichermedien des Ablagesystems befinden. Falls sich das Speichermedium direkt im Ablagesystem befindet (z.B. das WORM-Medium in der Jukebox, das Magnetband in der Tape Library) handelt es sich um ein Nearline-Ablagesystem. Sobald das Speichermedium jedoch außerhalb des Ablagesystems gelagert wird (z.B. Aufbewahrung des WORM-Mediums oder des Magnetbandes in einem Schrank), ist es ein Offline-Ablagesystem.

Da in einem Krankenhaus der Zugriff auf Patientenunterlagen in den ersten Monaten noch sehr häufig ist, werden die Dokumente zunächst auf einem Online-Ablagesystem aufbewahrt, das als elektronischer Kurzzeitspeicher dient. Für die Aufbewahrung der Daten kommen in der Regel Festplattensysteme zum Einsatz, die eine redundante Datenhaltung ermöglichen. Nach einigen Monaten (ca. 3 bis 6 Monaten) werden die Daten in der Regel von dem Online- auf ein Nearline-Ablagesystem ausgelagert. Damit ist der Zugriff auf die Daten weiterhin gewährleistet. Nearline-Ablagesysteme übernehmen somit die Aufgabe eines Langzeitspeichers.

Die Ablage von Patientenunterlagen in einem Offline-Ablagesystem ist sicherlich weniger für Krankenhäuser geeignet. Für eine optimale Patientenversorgung müssen die Informationen zu einem Patienten schnell und zeitnah zur Verfügung stehen. Dabei kann es auch notwendig sein, auf bereits archivierte Daten zuzugreifen (z.B. zur Beobachtung des Krankheitsverlaufs). Wurde bei einem Patienten bei einem früheren Aufenthalt z.B. eine Unverträglichkeit bei bestimmten Medikamenten festgestellt, kann diese Information einen entscheidenden Einfluss auf die Behandlung haben. Offline-Ablagesysteme werden vor allem zur Datensicherung eingesetzt.

Im Folgenden sollen drei Ablagesysteme vorgestellt werden, die häufig für die Speicherung der Daten in Krankenhäusern verwendet werden.

Festplattensubsystem

Ein Festplattensubsystem besteht aus mehreren Festplatten, die in einem RAID-Verbund zusammenarbeiten können. Die Festplatten werden über einen RAID-Array-Controller zu einem logischen Speicherbereich verbunden. Der Begriff RAID steht für „Redundant Array of Inexpensive Disks“ (RAID) und beschreibt die physische Anordnung von Datenträgern (z.B. Festplatten). SCSI-Festplatten sind über eine eindeutige „Logical Unit Number“ (LUN) identifizierbar. Um eine hohe Verfügbarkeit zu gewährleisten, werden die Daten redundant auf den einzelnen Festplatten abgelegt. Fällt also z.B. eine einzelne Festplatte aus, können die Daten anhand der redundant gespeicherten

Daten auf den anderen Festplatten wiederhergestellt werden und sind somit weiterhin verfügbar. In Abhängigkeit davon, wie die Daten in einem RAID-Verbund gespeichert werden sollen, existieren verschiedene RAID-Level[27]. Das Festplattensubsystem in einem RAID-Verbund gehört zu den Online-Ablagesystemen, die in Abhängigkeit vom RAID-Level eine redundante Datenhaltung ermöglichen.

Jukebox

Für die langfristige Aufbewahrung von Daten werden in Krankenhäusern in der Regel optische Speichermedien [Gulbins et al. 2002] wie z.B. WORMs und UDOs eingesetzt. Diese Speichermedien haben die Eigenschaft, dass sie nur einmal beschrieben werden können. Das Löschen, Überschreiben oder Ändern von darauf abgelegten Daten ist ausgeschlossen. Die Speichermedien WORM und UDO erfüllen somit die Anforderung nach einer unveränderlichen Aufbewahrung der Daten. CDs und DVDs sind dagegen nicht als Speichermedium für die langfristige Aufbewahrung von Daten geeignet. Ein kleiner Kratzer reicht aus, um die Lesbarkeit der CD oder DVD zu zerstören.

Die Aufbewahrung der optischen Speichermedien kann in einer Jukebox erfolgen. Eine Jukebox besteht aus mehreren Ablagefächern und Laufwerken. Ein Roboter stellt die Speichermedien für den Zugriff bereit. Dazu nimmt er das entsprechende Medium aus einem Ablagefach und legt es in ein Laufwerk ein. Die zu speichernden Daten werden in einer Jukebox sequentiell auf die optischen Speichermedien geschrieben. Die Daten liegen zwar somit in einer zeitlichen Reihenfolge vor. Es kann jedoch vorkommen, dass logisch zusammengehörige Dokumente auf mehreren Speichermedien verteilt liegen. Die Kapazität einer Jukebox hängt von der Anzahl der Ablagefächer sowie der Speicherkapazität der eingesetzten Speichermedien ab. In einem digitalen Archiv können mehrere Jukeboxen als Ablagesysteme eingesetzt werden. Da Jukeboxen aus mechanischen Elementen bestehen, die einem natürlichen Verschleiß unterliegen, müssen sie regelmäßig gewartet werden [Gulbins et al. 2002]. Der Ausfall einer Jukebox führt dazu, dass ein Zugriff auf die darin abgelegten Dokumente nicht mehr möglich ist. Aus diesem Grund empfiehlt es sich, die Daten redundant vorzuhalten. Die optischen Speichermedien in einer Jukebox werden auch als Nearline-Ablagesystem bezeichnet.

Tape Library

In vielen Krankenhäusern erfolgt die Datensicherung auf Magnetbändern. Um die Daten zu sichern, müssen die Bänder manuell in einer Tape Library eingelegt werden. Die Tape Library besteht aus einem oder mehreren Bandlaufwerken[28] und aus einzelnen Slots, in denen sich die Bänder zur Datensicherung befinden. Die Verwaltung der einzelnen Bänder sowie die Datensicherung und Wiederherstellung von Daten wird mit Hilfe einer Backup-Software durchgeführt. Mit der Backup-Software wird festgelegt, wann welche Daten gesichert werden. Die Daten werden sequentiell auf die Bänder geschrieben und gelesen. Das zu lesende oder zu beschreibende Band wird dabei voll automatisch aus dem Slot entnommen und über einen Wechselmechanismus in das Bandlaufwerk eingelegt. Da die Anzahl der Slots in einer Tape Library begrenzt ist, müssen die Bänder nach der Datensicherung manuell gegen neue Magnetbänder ausgetauscht werden. Ansonsten besteht die Gefahr, dass die auf dem Band gesicherten Daten bei der nächsten Datensicherung überschrieben werden. In der Backup-Software kann ein Überschreibschutz für die einzelnen Magnetbänder definiert werden. Bei der Aufbewahrung der Magnetbänder ist darauf zu achten, dass sie geschützt gegen Feuchtigkeit, Staub oder magnetische Einflüsse an einem sicheren Ort gelagert werden. Magnetbänder eignen sich insbesondere für die Aufbewahrung von großen Datenmengen, auf die jedoch selten zugriffen wird. Die Daten werden komprimiert auf den Magnetbändern abgelegt. Die Speicherkapazität ist dabei von dem eingesetzten Bandformat abhängig. Auf SDLT S4-Bändern[29]

[27] Die RAID-Level gehen von 0 bis 7.

[28] Große Libraries arbeiten mit mehr als 20 Bandlaufwerken und mehreren 100 Slots. Kleine Libraries (Autoloader) besitzen in der Regel maximal zwei Bandlaufwerke und nicht mehr als 16 Slots.

[29] SDLT S4-Bänder sind seit diesem Jahr auf dem Markt verfügbar.

können beispielsweise unkomprimiert bis zu 800 GB pro Band (mit Komprimierung 1,6 TB pro Band) gespeichert werden. Das Datenvolumen bei einem LTO-3-Band liegt unkomprimiert bei ca. 400 GB (mit Komprimierung bei ca. 800 GB).

Eine Tape Library wird über die SCSI- oder Fibre Channel-Schnittstelle an einen Server angeschlossen. Die Tape Library kann aber auch in einem Storage Area Network als Speichersubsystem zur Verfügung gestellt werden. Nachfolgend sollen zwei Möglichkeiten vorgestellt werden, wie ein Speichersystem in ein Netzwerk eingebunden werden kann. Diese zwei Speicherarchitekturen werden verstärkt für die Langzeitspeicherung eingesetzt.

Storage Area Network

Der Begriff „Storage Area Network“ (SAN) beschreibt eine Topologie, in der die Server und Speichersysteme über Fibre Channel[30] miteinander kommunizieren. Der Vorteil eines SAN besteht darin, dass alle Server in einem Netzwerk über das SAN auf alle Speichersysteme zugreifen können. Ein Speichersystem kann dabei von mehreren Servern zur Datenablage verwendet werden. Als Kommunikationsprotokoll wird das SCSI-Protokoll verwendet. Die Übertragung der Daten erfolgt blockbasiert, d.h. es werden einzelne Datenblöcke zwischen den eingesetzten Speichersystemen und Servern ausgetauscht. Die Bandbreite in einem SAN liegt im Bereich von 2 und 4 GBit/s. Damit sind theoretisch Übertragungsraten von bis zu 400 MB/s möglich. Für das Management der einzelnen Speichersysteme in einem SAN muss eine spezielle Software eingesetzt werden. Diese Software unterstützt u.a.

- die synchrone und asynchrone Spiegelung der Daten auf ein entferntes Speichersystem
- die Fehlererkennung innerhalb eines SANs [Hein et al. 2002] sowie
- die Erstellung und Verwaltung der Storage Volumes im SAN.

In der folgenden Abbildung ist der Aufbau eines SAN dargestellt. Die einzelnen Arbeitsplatzrechner kommunizieren über das LAN mit den Servern. In den Servern sind so genannte Hostbus-Adapterkarten eingebaut, die über ein Glasfaserkabel mit einem Fibre Channel Switch verbunden werden. Der Fibre Channel Switch übernimmt das Routing sowie Aliasing in dem SAN. An dem Fibre Channel Switch sind die einzelnen Speichersysteme angeschlossen.

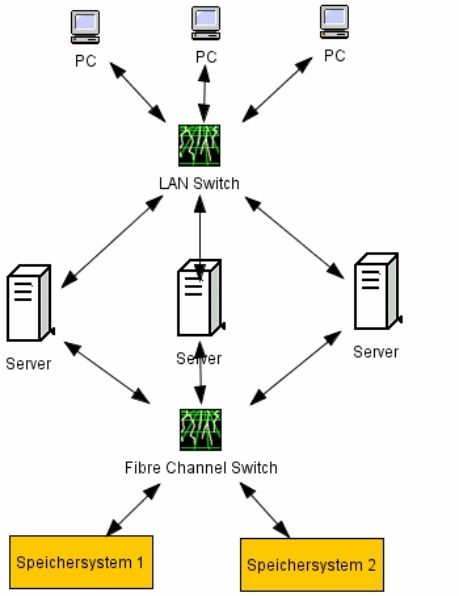


Abbildung 4-6: Storage Area Network

[30] Fibre Channel ist seit 1994 ein ANSI-Standard.

In einem SAN können die einzelnen Komponenten wie z.B. Fibre Channel Switch und das Speichersystem redundant an verschiedenen Standorten vorgehalten werden. Damit wird gewährleistet, dass die Daten auch im Katastrophenfall weiterhin verfügbar sind.

Network Attached Storage

Bei einem Network Attached Storage, kurz NAS genannt, handelt es sich um einen Fileserver, der Speicher für die Ablage von Dateien über das Netzwerk zur Verfügung stellt. An dem Fileserver ist ein Speichersystem angeschlossen. Die gespeicherten Dateien werden vom Fileserver für den Zugriff bereitgestellt. Der Zugriff auf die Dateien erfolgt normalerweise von einzelnen Arbeitsplatzrechnern, die über ein Ethernet-Netzwerk mit dem Fileserver verbunden sind. Ein NAS ist plattformunabhängig, d.h. die gespeicherten Dateien können von Rechnern mit unterschiedlichen Betriebssystemen (z.B. Windows, Linux, Unix, Novell) genutzt werden. Für den Zugriff verwendet das NAS Netzwerkprotokolle[31]. Falls eine Erweiterung der Speicherkapazitäten erforderlich ist, kann ein weiteres NAS in das bestehende Netzwerk integriert werden [Hein et al. 2002]. Die folgende Abbildung zeigt das klassische NAS.

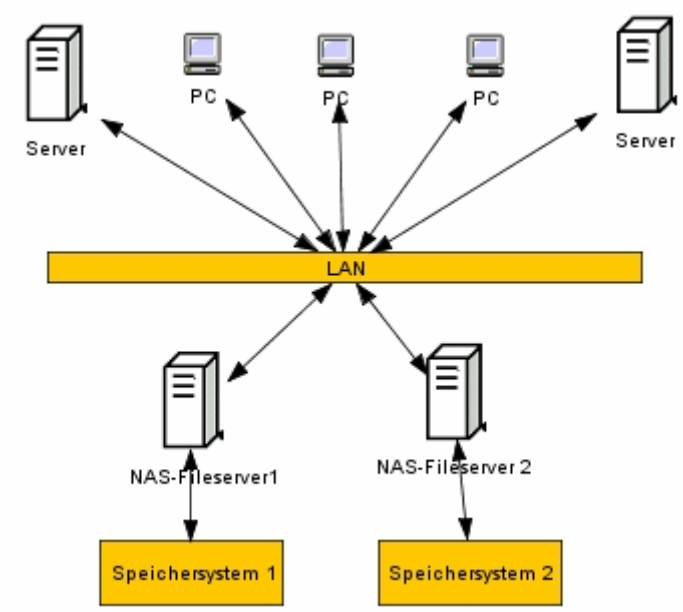


Abbildung 4-7: Klassisches Network Attached Storage

Das NAS hat sich im Laufe der Jahre weiterentwickelt und nähert sich heute immer mehr der Architektur in einem SAN. Ähnlich wie bei einem SAN ist der Aufbau eines direkten Speichernetzwerkes möglich. Durch die Nutzung von iSCSI[32] als Übertragungsprotokoll kann Speicher zentral mehreren Servern zur Verfügung gestellt werden [Robbe 2004].

Im Unterschied zum SAN erfolgt jedoch die Kommunikation in einem NAS über ein Netzwerkprotokoll (z.B. TCP/IP) und anstelle des Fibre Channel Switch wird ein Ethernet Switch eingesetzt. Der Vorteil eines NAS gegenüber einem SAN besteht darin, dass es einfacher und preisgünstiger bei fast identischer Performance in einfachen Umgebungen aufzubauen ist.

[31] Beim Betriebssystem Windows wird z.B. das „Common Internet File System“ (CIFS)-Protokoll verwendet, während Unix das „Network Files System“ (NFS)-Protokoll einsetzt.

[32] iSCSI steht für IP-basierendes SCSI. Bei iSCSI werden SCSI-Datenpakete und SCSI-Kommandos so moduliert, dass diese über ein IP-Netz (z.B. Ethernet) zum Speichersystem übertragen werden können [Robbe 2004].

4.4.2 Server

Für die Einrichtung des Archivierungssystems werden grundsätzlich benötigt:

- ein Datenbankserver, auf dem die Datenbank zur Verwaltung der Indexdaten und Referenzen zu den Dokumenten liegt, und
- ein Applikationsserver, auf dem die Serversoftware für das Archivierungssystem installiert ist.

Über den Applikationsserver wird der Zugriff auf die archivierten Dokumente in dem Ablagesystem geregelt. Die Übertragungsgeschwindigkeit zwischen dem Ablagesystem und dem Applikationsserver sollte nach [Häber et al. 2005] im Gigabit-Bereich liegen. Der Applikationsserver ist in das Netzwerk eines Krankenhauses zu integrieren und gegen unbefugte Zugriffe von außen durch geeignete Sicherheitsmaßnahmen zu schützen. In Abhängigkeit von der Anzahl der zu importierenden Daten und Dokumente kann es sinnvoll sein, die Importprozesse auf einem eigenen Server zu implementieren, damit Routineprozesse nicht beeinträchtigt werden [Häber et al. 2005]. Für die Massenübernahme von Dokumenten wäre also ein weiterer Server erforderlich. Die Installation von webbasierten Softwarekomponenten erfolgt oftmals auch auf einem separaten Server, dem so genannten Web-Server. Natürlich wäre es auch denkbar, mehrere Softwarekomponenten des Archivierungssystems auf einem Server zu installieren. Dies wird jedoch aus Performancegründen von den Anbietern nicht empfohlen bzw. ist im Einzelfall zu prüfen.

Weiterhin befinden sich auf der physischen Werkzeugebene die Server für die Anwendungsbausteine, die mit dem Archivierungssystem kommunizieren.

4.4.3 Arbeitsplatzrechner

Zur Unterstützung der jeweiligen Aufgaben in den unterschiedlichen Organisationseinheiten in einem Krankenhaus werden Arbeitsplatzrechner benötigt. Auf Station, in der Ambulanz und in der Patientenverwaltung erfolgt die Erledigung der Aufgaben über klinische Arbeitsplatzsysteme. Die in der Radiologie, im Labor, auf der Intensivstation, in der Krankenhausverwaltung usw. eingesetzten Rechner werden im Referenzmodell als Arbeitsplatzrechner bezeichnet.

4.4.4 Unterstützende Datenverarbeitungsbausteine am Arbeitsplatzrechner

Je nachdem, wo sich der Arbeitsplatzrechner in einem Klinikum befindet, ist der Einsatz von weiteren rechnerbasierten physischen Datenverarbeitungsbausteinen notwendig. Zur Erfassung von papierbasierten Dokumenten werden Scanner benötigt. Scanner müssen an den Arbeitsplätzen verfügbar sein, wo Papierdokumente eintreffen. Dazu gehört z.B. die Patientenaufnahme. In der Patientenaufnahme können somit Dokumente, die ein Patient mitbringt, eingescannt und manuell oder automatisch indexiert werden. Damit stehen die eingescannten Informationen elektronisch für den weiterbehandelnden Arzt zur Verfügung. Scanner können aber auch auf den Stationen oder in der Ambulanz für die Erfassung von Papierdokumenten oder Formularen zum Einsatz kommen. In Abhängigkeit von der täglich zu erfassenden Anzahl der Dokumente können die Scanner eine unterschiedliche Leistungsfähigkeit und Performance besitzen. Für die Massenerfassung von Dokumenten (z.B. beim Einscannen von Papierakten) müssen die Arbeitsplätze mit Hochleistungsscannern ausgestattet sein. Weiterhin muss ein Scanner die

- Erfassung von Dokumenten unterschiedlicher Formate (z.B. A3, A4, A5) sowie
- das gleichzeitige Einscannen der Vorder- und Rückseite

unterstützen.

Der Bearbeiter muss das eingescannte Dokument auf die inhaltliche und bildliche Übereinstimmung mit dem Originaldokument überprüfen. Um die ordnungsgemäße Umwandlung und Übereinstimmung zu bestätigen, wird das Anbringen der qualifizierten Signatur verlangt [Häber et al. 2005]. Für die elektronische Signierung von Dokumenten sind Kartenlesegeräte an den Arbeitsplatzrechnern

erforderlich. Mit Hilfe eines Kartenlesegerätes ist das Einlesen der Signaturkarte möglich. Jeder Mitarbeiter verfügt über eine eigene Signaturkarte, auf der sein persönlicher Signaturschlüssel gespeichert ist. Die Signaturkarte ist zusätzlich durch eine PIN geschützt. Die signierende Person muss sich also zunächst durch die Eingabe der richtigen PIN am Kartenlesegerät identifizieren. Die Signaturkarte kann z.B. der elektronische Mitarbeiterausweis sein. Die Kartenlesegeräte müssen überall an den Arbeitsplatzrechnern verfügbar sein, wo Dokumente elektronisch signiert werden müssen.

Die Indexierung von Papierdokumenten kann mit Hilfe eines Barcodes erfolgen. Das Papierdokument wird mit einem Barcode versehen, der sich aus bestimmten Informationen zusammensetzt. Der Barcode wird über einen Barcodeleser ausgelesen.

Für den Ausdruck von archivierten Dokumenten werden Drucker auf den Stationen, in der Ambulanz und in der Krankenhausverwaltung benötigt. Der Ausdruck von archivierten Dokumenten widerspricht allerdings dem Ziel, in einem Krankenhaus möglichst papierlos zu arbeiten. Wenn in einem digitalen Archiv die langfristige Verfügbarkeit und Lesbarkeit der archivierten Dokumente innerhalb der Aufbewahrungsdauer gewährleistet ist, müssen die Dokumente nicht noch einmal zur Aufbewahrung in einer Patientenakte ausgedruckt werden. Nur in Ausnahmefällen ist der Ausdruck von Dokumenten notwendig, z.B. wenn ein Dokument dem niedergelassenen Arzt nicht elektronisch zugestellt werden kann. Es wird sich in den nächsten Jahren zeigen, ob der Umgang mit elektronischen Dokumenten von den Anwendern in einem Krankenhaus akzeptiert wird.

Zu den unterstützenden rechnerbasierten physischen Datenverarbeitungsbausteinen an einem Arbeitsplatzrechner gehören also:

- Scanner
- Kartenlesegeräte
- Drucker
- Barcodeleser.

4.4.5 Physische Werkzeugebene des Referenzmodells

In der folgenden Abbildung ist die physische Werkzeugebene im 3LGM^2-Modell dargestellt. Sollen die Ablagesysteme in einem SAN eingesetzt werden, müssen in den einzelnen Applikationsservern Hostbusadapterkarten eingebaut sein. In einem SAN kommunizieren die Server mit dem Ablagesystem über Fibre Channel. In einem NAS erfolgt die Kommunikation über Ethernet.

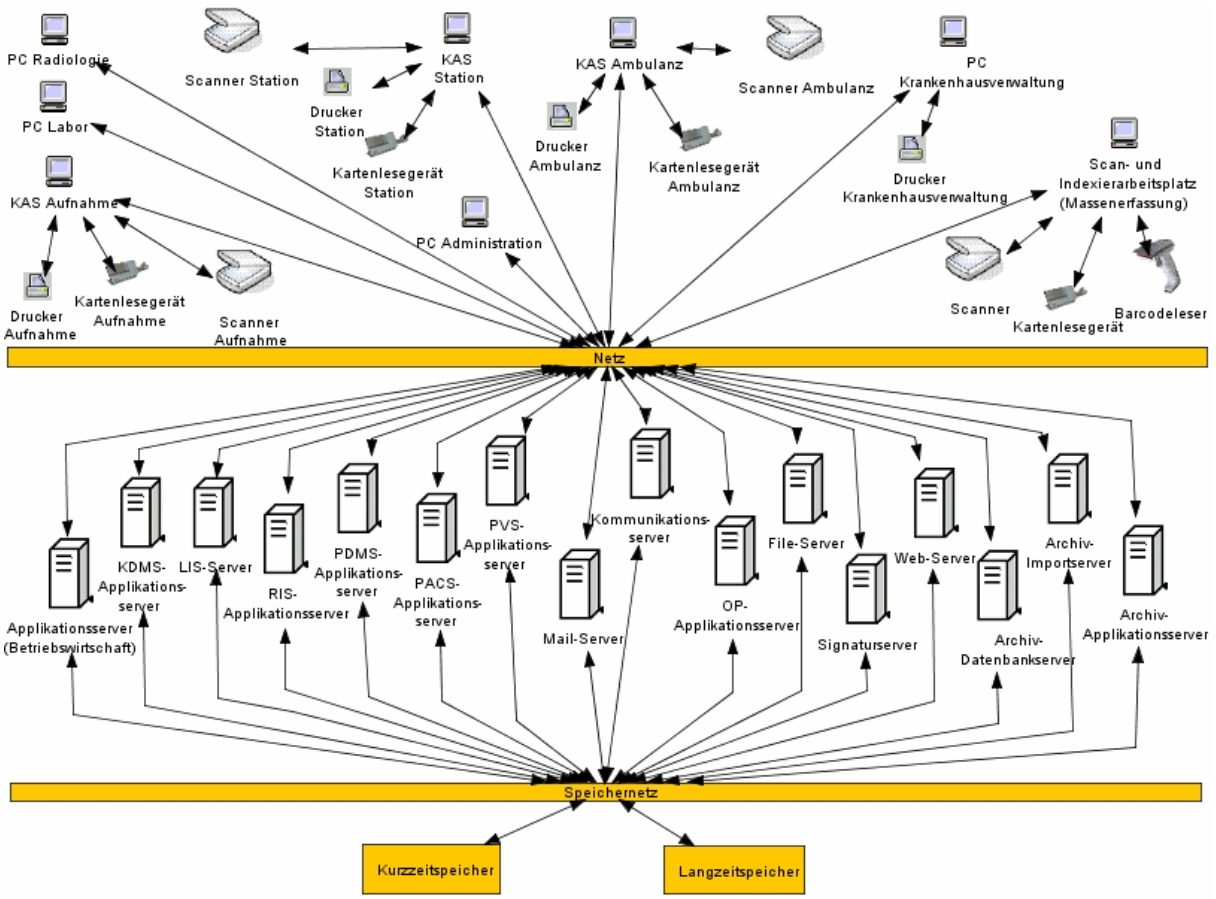


Abbildung 4-8: Physische Werkzeugebene des Referenzmodells

4.5 Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene

Die Zuordnung der einzelnen Anwendungsbausteine zu den physischen Datenverarbeitungsbausteinen ist im Anhang in Abbildung 9-4 in einer Matrix dargestellt. Die physischen Datenverarbeitungsbausteine Barcodeleser, Drucker, Kartenlesegeräte und Scanner werden nicht für den Betrieb von Anwendungsbausteinen benötigt. Aus diesem Grund sind ihnen auch keine Anwendungsbausteine zugeordnet. Diese physischen Werkzeuge unterstützen die automatische Indexierung von Papierdokumenten, den Ausdruck von Dokumenten, die elektronische Signierung von Dokumenten sowie die Erfassung von papierbasierten Dokumenten. Damit müssen sie auch auf der physischen Werkzeugebene dargestellt werden. Mit Hilfe der Matrix ist zu erkennen, dass Applikationsserver für die Anwendungsbausteine der Funktionsbereiche (z.B. Labor, Radiologie, Intensivmedizin) und Krankenhausverwaltung zum Einsatz kommen. Die Installation der einzelnen Module des Archivierungssystems erfolgt sowohl auf Servern (Applikations-, Web-, Importserver) als auch auf bestimmten Arbeitsplatzrechnern. Die Datenbank zur Verwaltung der Indexdaten und Referenzen zu den archivierten Dokumenten liegt auf dem Datenbankserver. Dies ist jedoch nicht anhand der Inter-Ebenen-Beziehungen erkennbar. Das Signatursystem ist eine Client-Server-Anwendung.

Die 3 Ebenen des 3LGM^2-basierten Referenzmodells für die digitale Archivierung von Patientenunterlagen sind einschließlich der Inter-Ebenen-Beziehungen im Anhang in Abbildung 9-5 dargestellt.

5 Modellierung der angebotenen Hard- und Softwareprodukte ausgewählter Anbieter

In diesem Kapitel sollen die für die digitale Archivierung angebotenen Hard- und Softwareprodukte von vier Anbietern aus dem Referenzmodell abgeleitet werden. Die Informationen zu den nachfolgenden Produkten sind aus Informationsmaterialien entnommen bzw. in Gesprächen mit den einzelnen Firmen entstanden. Die Reihenfolge der Anbieter ist zufällig gewählt.

5.1 d.velop AG

Mit dem Produkt d.3 wird von der d.velop AG ein Softwareprodukt angeboten, das sowohl die digitale Archivierung als auch das Dokumenten- und Workflowmanagement unterstützt. D.3 ist ein branchenneutrales Produkt und wird branchenübergreifend von der Firma d.velop consulting & solutions GmbH betreut. Die Firma d.velop consulting & solutions GmbH ist ein Tochterunternehmen der d.velop AG. Die d.velop AG betreut den Bereich Gesundheitswesen.

5.1.1 Begriffsdefinition

Im d.3-System wird der Begriff der APA verwendet. Die APA stellt gemäß der Definition einen Teil der EPA dar. Damit werden im d.3-System alle Dokumente dargestellt, die entweder archiviert oder in Bearbeitung sind. Die APA beinhaltet jedoch nur die archivierten Dokumente.

5.1.2 Fachliche Ebene

1. Archivierte Patientenakte anlegen

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

2. Dokument importieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

   Es können einzelne Dokumente, die mit einer Windows-Anwendung (z.B. Office- und PDF-Dokumente) erstellt wurden, im Dialog importiert werden. Office-Dokumente werden beim Import automatisch in die Dateiformate PDF bzw. TIFF konvertiert. Es wird aber auch der Massenimport von Dokumenten aus den verschiedenen Anwendungsbausteinen unterstützt.

3. Dokument archivieren

   D.3 ist ein reines Softwareprodukt, das die Dokumente über eine Schnittstelle zur Aufbewahrung an das Ablagesystem übergibt. Die Archivierung des Dokumentes übernimmt jedoch das Ablagesystem, das kein Bestandteil von d.3 ist.

4. Dokument transformieren

   Da das TransiDoc-Projekt noch nicht abgeschlossen wurde, kann diese Aufgabe noch nicht unterstützt werden.

5. Dokument löschen und Vernichtung protokollieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

6. Archivierte Patientenakte vernichten und Vernichtung protokollieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

7. Dokument suchen

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

8. Dokument signieren

   Innerhalb des d.3-Systems können nur Dokumente elektronisch signiert werden, die in einem revisionssicheren Dateiformat (z.B. TIFF) vorliegen. Für alle anderen Dateiformate erfolgt die Signaturerstellung und –prüfung durch die erzeugende Anwendung (z.B. Microsoft Office, Adobe Acrobat Reader).

9. Dokument versenden

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

10. Archivierte Patientenakte versenden

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

11. Signatur erneuern

    Die Erneuerung der Signatur gemäß ArchiSig-Projekt ist in Vorbereitung und wahrscheinlich mit dem nächsten Release verfügbar.

12. Berechtigung prüfen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

13. Dokumente anzeigen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

    Es wird die Anzeige von TIFF-, JPEG, PCX-, BMP und ASCII-Dateien unterstützt.

14. Dokumenteninhalt suchen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

    Mittels einer Online-OCR-Erkennung kann gezielt nach bestimmten Wörtern in einem mehrseitigen Dokument oder in einer APA gesucht werden.

15. Zugriff protokollieren

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

16. Dokument digitalisieren

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

17. Dokument drucken

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

18. Aufbewahrungsdauer anpassen

    Die Aufbewahrungsdauer zu einem Dokument kann manuell verändert werden, z.B. über eine Hookfunktion. Die Hookfunktion ermöglicht die Ausführung von Programmcode in definierten Punkten im Archivierungssystem. Mit dieser Funktion kann somit das Sterbe-Datum eines Dokumentes in der Datenbank geändert werden. Die Änderung des Aufbewahrungsdatums ist für den normalen Anwender nicht möglich.

Die folgende Abbildung zeigt die fachliche Ebene des Produktes d.3. Die Aufgabe „Signatur erneuern“ ist in der Abbildung grau dargestellt. Damit soll ausgedrückt werden, dass die Aufgabe zurzeit noch nicht unterstützt wird. Diese Aufgabe soll jedoch mit dem nächsten Release vom Archivierungssystem erledigt werden. Die Aufgabe „Dokument archivieren“ kann nur durch das Ablagesystem erfolgen, das natürlich vorhanden ist, aber nicht zum d.3-System gehört. Aus diesem Grund ist diese Aufgabe gelb markiert.

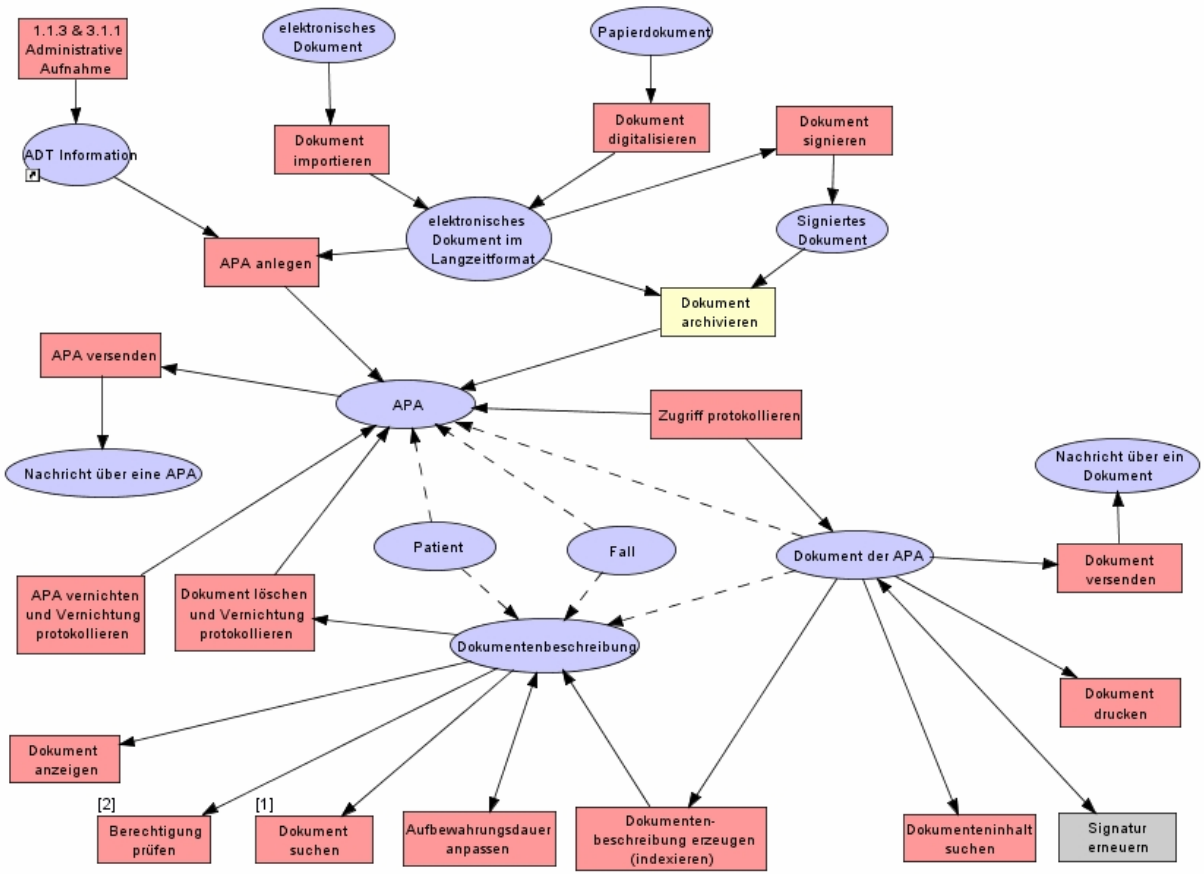


Abbildung 5-1: Fachliche Ebene von d.3

5.1.3 Logische Werkzeugebene

5.1.3.1. Anwendungsbausteine

Administrationssystem d.admin

Das Administrationssystem dient zur Verwaltung von

- Benutzern, Benutzergruppen und Benutzerprofilen
- Repositoryfeldern und Wertemengen
- Dokumentarten (z.B. medizinisches Dokument)
- Aktenarten (z.B. Fall-, Patienten-, Gesundheitsakte)
- Aktenplänen[33]
- Dokumentverzeichnissen
- Rollen und
- Dokumentklassen (z.B. Arztbrief, Anamnese, Röntgenbefund).

[33] Mit Hilfe eines Aktenplanes wird der Aufbau der einzelnen Aktenarten definiert.

Es besteht die Möglichkeit, eine bereits existierende Benutzer- und Berechtigungsverwaltung (z.B. im Microsoft Active Directory, LDAP-Directory oder SAP IS-H) zu nutzen, um die Benutzer und Gruppen in das Administrationssystem zu übernehmen und zu synchronisieren. Der Zugriff auf ein LDAP- oder Microsoft Active Directory erfolgt durch einen LDAP-Konnektor. Über eine Benutzer/Kennwort-Synchronisation ist eine Single-Sign-On-Umgebung realisierbar, d.h. der Benutzer muss sich nur einmal anmelden. Weiterhin kann über das Administrationssystem festgelegt werden, welche Dokumentenklassen durch welche Personen (z.B. per Fax, Mail) versandt werden dürfen.

Zugriffskontrollsystem d.3 server

Über diesen Anwendungsbaustein wird sichergestellt, dass nur autorisierte Benutzer auf die archivierten Dokumente im d.3-System zugreifen können. In einem Audit-Log werden alle administrativen Tätigkeiten wie z.B. das Anlegen oder Ändern von Benutzern und Dokumentarten sowie die Zugriffe auf die Dokumente in einer Datenbanktabelle protokolliert. Der d.3 Server setzt sich aus mehreren Serverkomponenten zusammen.

Recherchesystem

Das Recherchesystem ermöglicht die Suche nach Dokumenten, die in einem oder in mehreren verteilten Archivsystemen abgelegt sein können. Standardmäßig erfolgt die Suche in den Dokumentattributen. Wurde beim Import der Dokumente jedoch eine OCR-Erkennung durchgeführt, dann ist auch eine Suche in den erkannten Informationen möglich. Einzelne Suchkriterien können miteinander kombiniert werden. Weiterhin ist die Verwendung von Wildcards (Platzhaltern) bei der Eingabe von Suchkriterien möglich.

Für die Recherche werden unterschiedliche Komponenten zur Verfügung gestellt:

- d.3 explorer: Der d.3 explorer ist der Standard-Rechercheclient und muss an jedem Arbeitsplatz installiert sein, an dem die Recherche durchgeführt werden soll. Der d.3 explorer unterstützt die benutzerspezifische Gestaltung der Bildschirmdarstellung (z.B. durch das Ein-/Ausblenden der Detailansicht, Übersichtsfenster, Attributfenster, Katalogansicht). Weiterhin können per Drag & Drop Dokumente aus anderen Anwendungen (z.B. Windows Explorer) eingefügt werden.
- d.3 web explorer: Die Suche und Anzeige von Dokumenten erfolgt über einen webbasierten Browser. Eine Autorisierung des Benutzers ist erforderlich. Dieser webbasierte Explorer deckt den kompletten Funktionsumfang des Standard-Recherchecliens ab.
- d.3 web publisher: Mit dem web publisher können Dokumente im Internet/Intranet eingesehen werden, die veröffentlicht wurden und somit für jedermann zur Ansicht zur Verfügung stehen (z.B. Verfahrensdokumentationen). Der Aufruf der Dokumente erfolgt über einen webbasierten Browser. Eine Autorisierung des Benutzers ist nicht erforderlich. Es wird immer die aktuelle Version eines Dokumentes angezeigt.

Es wird auch die Recherche aus einem führenden Informationssystem unterstützt, d.h. der Benutzer kann sich die archivierten Patientenunterlagen aus dem führenden Informationssystem heraus anzeigen lassen. Der Aufruf des Archivierungssystems wurde bisher in Cymed und i.s.h.med realisiert.

Visualisierungssystem d.3 view

Für die Anzeige der Dokumente auf dem Bildschirm wird ein eigener Viewer zur Verfügung gestellt, der die Anzeige von TIFF-, JPEG, PCX-, BMP und ASCII-Dateien unterstützt. Der Viewer bietet folgende Funktionalitäten:

- Vergrößern und Verkleinern von Dokumentausschnitten mittels einer Zoomfunktion
- automatische Ausrichtung einer Seite in Leserichtung
- Zusammenfassung verschiedener Dateien zu einer einzigen TIFF-Datei, die aus mehreren Seiten besteht

- Bereitstellung von skalierten Bildausschnitten für andere Anwendungen
- Veränderung des Kontrastes
- Hinzufügen von Notizen bzw. Anmerkungen[34] (z.B. Einfügen von Pfeilen, Linien, Text, Haftnotizen, Verknüpfungen, Textmarkierungen). Zusätzlich können die Anmerkungen mit Rechten geschützt werden.
- Ausdruck von Dokumenten oder Dokumentausschnitten
- Versenden von Dokumenten (z.B. per Mail, Fax).

Es besteht weiterhin die Möglichkeit, die Dokumente mittels einer Online-OCR-Erkennung nach bestimmten Schlagwörtern zu durchsuchen. Die Online-OCR-Erkennung kann z.B. bei der Suche nach einem bestimmten Begriff in einem mehrseitigen Dokument oder bei der Suche in einer eingescannten Altakte verwendet werden. Die bei der Online-OCR-Erkennung erkannten Informationen werden nicht gespeichert.

Scansystem

Für die Erfassung und Archivierung von papierbasierten Dokumenten werden zwei Scansysteme angeboten. Das Scansystem d.3 capture batch dient zur stapelorientierten Erfassung von papierbasierten Dokumenten. Es stellt Module für

- die Administration (Anlegen von Stapelklassen),
- die Barcoderkennung mit der Erstellung von Barcodeblättern zur Dokumententrennung,
- manuelle Indexierung,
- Datenvalidierung,
- Export der eingescannten Dokumente und Indexdaten,
- OCR-Erkennung,
- Signierung von Dokumenten und
- das Einscannen von Dokumenten

zur Verfügung.

Die Dokumente werden stapelorientiert in einer vorher festgelegten Reihenfolge durch die einzelnen Module der Scansoftware d.3 capture batch abgearbeitet. Die Definition der Bearbeitungsreihenfolge erfolgt grafisch in dem Administrationsmodul in so genannten Stapelklassen. In einer Stapelklasse werden weiterhin die Dokumentenklassen festgelegt. Eine Dokumentenklasse enthält die Dokumentenart mit den dazugehörigen Indexdaten. Die Dokumente werden zunächst über das Scanmodul erfasst. Zu den Aufgaben des Scanmoduls gehören u.a. die Ansteuerung der einzelnen Scanner, das automatische Ausrichten des Dokumentes in Leserichtung und das Entfernen von leeren Seiten. Die Indexierung kann manuell über das Indexiermodul oder automatisch durch das Barcodeerkennungsmodul erfolgen. Treten bei der Bearbeitung eines Stapels in einem Modul Fehler auf (z.B. Barcode wurde nicht erkannt), ist eine manuelle Nachbearbeitung durch eine Person erforderlich. Der Export der eingescannten Dokumente und Indexdaten wird nur bei einer erfolgreichen Abarbeitung des Stapels durchgeführt.

Das zweite Scansystem d.3 capture dialog dient zur interaktiven Erfassung von einzelnen Dokumenten. Es bietet folgende Funktionalitäten:

[34] Das Anbringen von Notizen bei elektronischen Dokumenten ist als Hilfsmittel zulässig, da keine Veränderung des Originaldokumentes erfolgt.

- manuelle Seitenbearbeitung (z.B. Drehen des Dokumentes, Umsortierung von Seiten)
- Texterkennung durch OCR,
- Barcodeerkennung,
- manuelle und automatische Indexierung sowie
- Bereitstellung des Dokumentes als TIFF-, JPEG oder BMP-Datei.

Klassifizierungssystem

Das Klassifizierungssystem d.classify unterstützt die automatische Klassifikation von gescannten Papierdokumenten und wird zusammen mit dem Scansystem eingesetzt. Die Dokumentenklasse wird unter Verwendung von semantischen und statistischen Verfahren aus dem Dokumenteninhalt ermittelt. Neben der Dokumentenklasse werden auch Deskriptoren wie z.B. Patientenname und Patientenidentifikationsnummer bestimmt.

Importsystem

Mit einer Windows-Anwendung erstellte Dokumente können nach der Fertigstellung über das Importmodul des d.3 explorers im Dialog importiert werden. Die Dokumente werden automatisch in langzeitstabile Dateiformate überführt. Die Umwandlung der Office-Dokumente erfolgt über den Konvertierungsdienst d.3 rendition service. Der Konvertierungsdienst unterstützt die Umwandlung von Office-Dokumenten in die Dateiformate TIFF und PDF. Der Benutzer kann entscheiden, ob zusätzlich zu dem konvertierten Dokument das originale Dokument mit abgespeichert werden soll.

Der Massenimport von Dokumenten aus den verschiedenen Anwendungsbausteinen erfolgt über die Schnittstellen des Importsystems d.cold. Die Software d.cold stellt verschiedene Schnittstellen für den Import der Dokumente zur Verfügung. Die Dokumente werden zunächst nach bestimmten Regeln aufbereitet und anschließend in das d.3-System importiert. Aus diesem Grund müssen die zu importierenden Dokumente einen festen Aufbau besitzen. Wie die einzelnen Dokumente aufbereitet werden, wird in dem Softwaremodul d.cold definiert. In dem Modul können auch Interpretationsvorschriften festgelegt werden. Anhand der Interpretationsvorschriften werden die Indexdaten automatisch aus dem Dokument ermittelt. Nach dem Import werden die Dokumente gemäß dem Aktenplan in die Aktenstruktur des Patienten eingefügt. Das Importsystem d.cold bietet u.a. Schnittstellen zur Übernahme von eingescannten Dokumenten, SAP-Daten oder List- und Spooldateien an.

Workflowsystem d.3 flow

Das Workflowsystem ermöglicht die automatische Abarbeitung von standardisierten und sich häufig wiederholenden Geschäftsprozessen. Ein archiviertes Dokument kann entweder automatisch oder manuell in einen Leitweg gestellt werden. Andererseits kann ein Dokument jederzeit aus dem Workflow herausgenommen werden. Es ist jederzeit nachvollziehbar, wo und in welchem Status sich das Dokument sich auf dem Leitweg befindet. Der Workflow wird als XML-Datei zu der jeweiligen Dokumentenklasse im Archivierungssystem abgelegt.

Für die graphische Darstellung der Geschäftsprozesse wird ein Workflowdesigner zur Verfügung gestellt.

Offline-Archivsystem d.3 local engine

Dieses Softwaremodul ermöglicht die Erstellung eines Offline-Archivs. Die Dokumente können individuell vom Nutzer zusammengestellt und als Kopie in einem Offline-Archiv abgelegt werden, das auf eine CD oder DVD gebrannt und externen Personen zur Verfügung gestellt werden kann. Die Erstellung eines Offline-Archivs auf CD oder DVD erfolgt über einen Assistenten, der Bestandteil der d.3 local engine ist. Die Dokumente werden auf dem Speichermedium verschlüsselt abgelegt. Der Zugriff auf das Speichermedium ist nur passwortgeschützt möglich. Damit sind die Dokumente gegen unautorisierte Zugriffe geschützt. Bei der Erstellung eines Offline-Archivs auf einer CD/DVD werden zusätzlich der d.3 Client und die d.3 local engine abgelegt. Der d.3 Client stellt die Softwaremodule d.3 explorer und d.3 view bereit. Diese Softwaremodule ermöglichen die Anzeige und Recherche im

Offline-Archiv unabhängig vom d.3-System. Das Offline-Archiv steht dem Empfänger der CD/DVD nach erfolgreicher Passworteingabe für die Recherche und Anzeige zur Verfügung. Eine zusätzliche Installation von d.3-Softwarkomponenten ist nicht erforderlich. Das Offline-Archiv kann somit auf Remote-Arbeitsplatzrechnern eingesetzt werden, die nicht mit dem d.3-System kommunizieren. Es besteht jedoch auch die Möglichkeit, ein Offline-Archiv lokal auf einem Notebook einzurichten. Der Nutzer muss dazu die entsprechenden archivierten Patientenakten und Dokumente im d.3 explorer auswählen und über eine Funktion offline bereitstellen. Wird die d.3 local engine über ein Kontextmenü offline gesetzt, werden alle ausgewählten Dokumente in das Offline-Archiv kopiert. Das Offline-Archiv ist in einem lokalen Verzeichnis auf dem Notebook abgelegt. Sobald der Nutzer mit dem Notebook wieder online am d.3-System angemeldet ist, wird das Offline-Archiv mit dem Online-Archiv synchronisiert. Neue oder geänderte Dokumente werden automatisch in das Offline-Archiv übertragen. Falls Dokumente im Offline-Archiv geändert wurden, erfolgt ebenfalls eine Synchronisation mit dem Online-Archiv.

Mit der d.3 local engine können einzelne Dokumente oder ausgewählte archivierte Patientenakten offline zur Verfügung gestellt werden. Dabei besteht die Möglichkeit, die Dokumente verschlüsselt auf einer CD/DVD abzulegen. So können z.B. bestimmte Patientenunterlagen per CD/DVD für einen niedergelassenen Arzt bereitgestellt werden. Die Funktionen des d.3 explorers sind im Offline-Archiv jedoch nur eingeschränkt gegenüber dem Online-Archiv nutzbar.

Content Service System d.3 content service

Dieses Softwaremodul ermöglicht die Ablage von Dokumenten in einer Ordnerstruktur (wie sie z.B. der Anwender vom Windows Explorer kennt) aus einer gängigen Anwendung. Die Ordner einschließlich der Unterordner werden im Administrationssystem d.admin einschließlich der Attribute definiert. Der d.3 content service stellt die Ordner zur Ablage der Dokumente bereit. Über die Standardprotokolle WebDAV, IMAP und FTP können die Dokumente ausgetauscht werden. Das IMAP-Protokoll ermöglicht den Zugriff auf die definierte Verzeichnisstruktur von einem E-Mail Client (z.B. Microsoft Outlook, Lotus Notes). So können neu eingegangene E-Mails manuell oder automatisch durch Verwendung eines Regelassistenten in die Ordner kopiert werden. Die E-Mails werden in den Ordnern im EML[35]-Dateiformat abgelegt. Die Indexierung erfolgt automatisch anhand der zu jedem Ordner im Administrationssystem definierten Attribute. Die E-Mail ist anschließend im d.3-System sichtbar. Das WebDAV-Protokoll dient zur Bereitstellung von Web-Ordnern, während das FTP-Protokoll den Datenaustausch zwischen einzelnen Verzeichnissen unterstützt. Mit Hilfe des d.3 content service werden die einzelnen Akten als Ordner abgebildet.

Volltextsuchsystem

Es werden zwei Volltextsuchsysteme zur Verfügung gestellt. Das Softwaremodul d.3 search engine unterstützt:

- phonetische Suche
- Dokumentenranking nach Relevanz
- semantische/assoziative Suche, d.h. die Suche nach inhaltlich verwandten Wörtern
- Freitextsuche.

Als weiteres Modul steht das Volltextsuchsystem d.3 search pro zur Verfügung, das zusätzlich die Suche mit booleschen Operatoren, die Suche über Phrasen oder Fuzzy-Begriffe ermöglicht. Weiterhin können Zusammenfassungen von Dokumenten gebildet werden, um somit die Treffermenge besser einschätzen zu können.

[35] E-Mails in MIME-Kodierung

5.1.3.2. Schnittstellen

Zertifizierte SAP-Schnittstelle d.link for SAP R/3

Diese Schnittstelle ist von SAP zertifiziert und dient zur Kommunikation zwischen dem Archivierungssystem und SAP R/3.

COLD-Schnittstelle d.cold

Es werden COLD-Schnittstellen für die automatische Übernahme von eingescannten Dokumenten, SAP R/3 Dokumenten, List- und Spooldateien bereitgestellt. Über diese Schnittstellen erfolgt auch die Aufbereitung der Dokumente. Anhand von vorher definierten Interpretationsvorschriften können die Indexdaten automatisch aus dem Dokument ermittelt und gemeinsam mit dem Dokument archiviert werden.

Schnittstelle zur Anbindung von Volltextsuchmaschinen d.search

Über diese Schnittstelle können verschiedene Volltextsuchmaschinen (auch Fremprodukte) an das Archivierungssystem angebunden werden.

Schnittstelle zur Anbindung von Ablagesystemen d.3 storage manager

Der d.3 storage manager stellt eine Schnittstelle zwischen dem Archivierungssystem d.3 und dem Ablagesystem dar. Über diese Schnittstelle werden die zu archivierenden Dokumente an das jeweilige Ablagesystem übergeben. Es ist der Einsatz von mehreren Ablagesystemen möglich. Die Dokumente können gleichzeitig auf verschiedene Ablagesysteme verteilt werden. Die Schnittstelle unterstützt die Anbindung von optischen Speichersystemen und Content Adressed Speichersystemen wie z.B. die Centera von EMC^2.

Schnittstelle für die Integration von Signaturverfahren d.3 sign

D.3 verfügt über keine eigene Public Key Infrastruktur. Über die Schnittstelle d.sign können jedoch die unterschiedlichen Signaturverfahren in das d.3-System integriert werden. Die Signaturinformationen werden geschützt in der Datenbank auf dem d.3 Applikationsserver abgelegt. Archivierte Dokumente, die elektronisch signiert sind, werden für den Benutzer sichtbar dargestellt. Ein Dokument kann von mehreren Personen signiert sein.

Schnittstelle für die Archivierung von E-Mails d. link for microsoft exchange/d.link for lotus notes

Über diese Schnittstelle können E-Mails einschließlich der darin enthaltenen Anlagen im Archivierungssystem abgelegt werden. Die Informationen werden als TIFF-Datei abgelegt und automatisch indexiert. Als Indexdaten für die E-Mail werden der Empfänger, Senderinformationen, Datum und Betreffzeile verwendet. Die Archivierung der E-Mails kann entweder manuell (z.B. per Knopfdruck in Microsoft Outlook) oder automatisch erfolgen. Die Ansicht archivierter E-Mails ist aus der gewohnten Anwendung möglich.

Schnittstelle zur Anbindung von Office-Dokumenten d.link for office

Mit Hilfe dieser Schnittstelle können beliebige Dokumentenattribute automatisch aus dem Archivierungssystem in ein Officedokument übernommen werden. Somit können bereits vorhandene Informationen aus dem Archivierungssystem genutzt werden, z.B. für die Übernahme der Stammdaten eines Patienten zur Erstellung eines Arztbriefes. Bei der Archivierung von Dokumenten, die auf einer Vorlage beruhen, erfolgt eine automatische Indexierung anhand der Formularfelder.

HL7-Schnittstelle

Prinzipiell werden alle ADT Nachrichten der HL7-Schnittstelle unterstützt. Da aber jede Nachricht im Archivierungssystem entsprechend konfiguriert werden muss, werden in der Praxis nur die vom Kunden gewünschten ADT-Nachrichten eingerichtet.

DICOM-Schnittstelle

Es werden zurzeit die beiden Dienstklassen „Storage Service Class“ und die „Query/Retrieve Service Class“ als „Service Class Provider“ in d.3 implementiert. Damit sind der Empfang sowie der Abruf von medizinischen Daten in dem Softwareprodukt d.3 möglich. Auf Kundenwunsch können weitere Dienstklassen implementiert werden.

LDAP-Konnektor

Der LDAP-Konnektor ermöglicht den Zugriff auf LDAP-Directories wie z.B. das Microsoft Active Directory oder das Domino Directory.

5.1.3.3. Datenbanksystem

In der Datenbank werden die Indexdaten sowie die Referenzen zu den einzelnen Dokumenten abgelegt. Als Datenbanken werden Oracle, Microsoft SQL, PervasiveSQL, DB/2 und Informix unterstützt.

5.1.3.4. Darstellung der logischen Werkzeugebene von d.3

Die folgende Abbildung zeigt die logische Werkzeugebene von d.3.

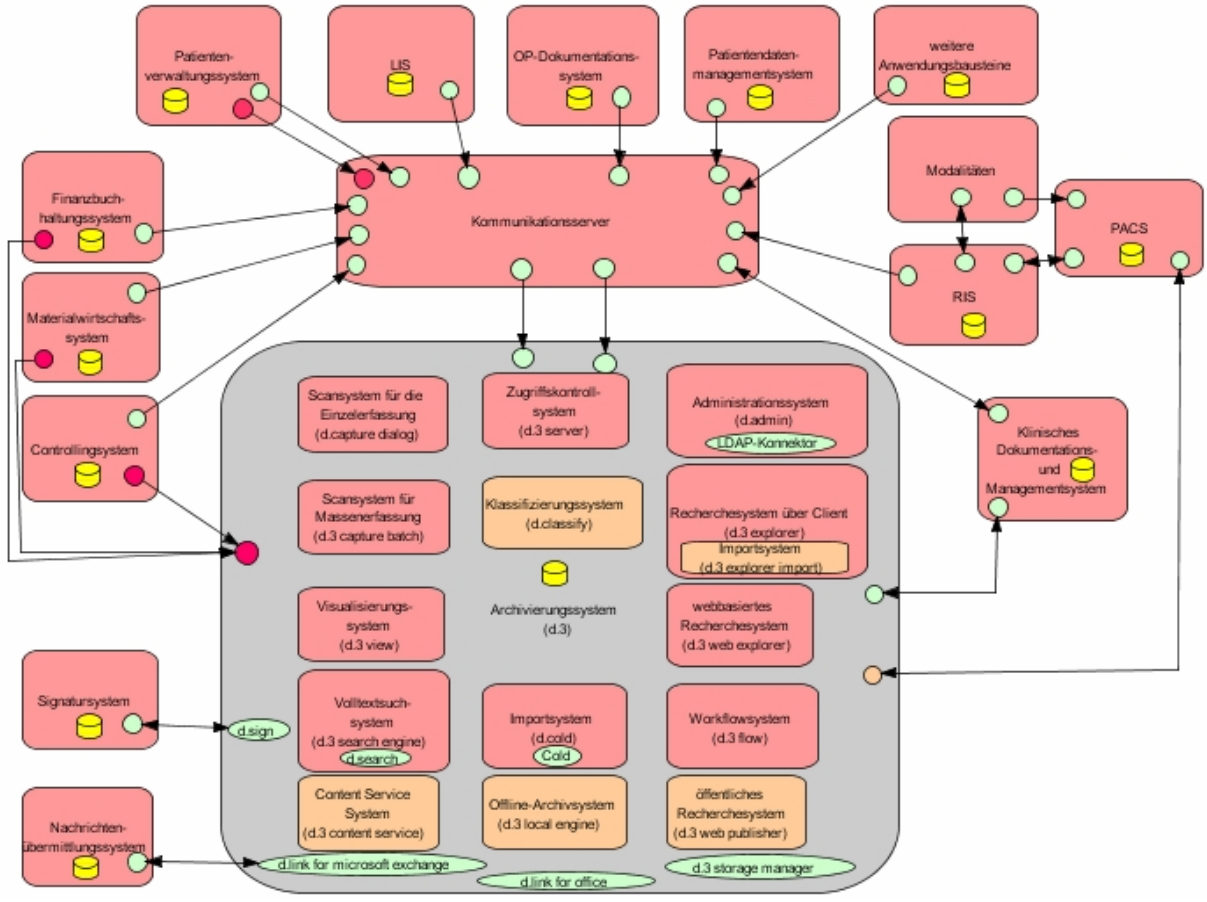


Abbildung 5-2: Logische Werkzeugebene von d.3

5.1.4 Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene

Im Anhang in Abbildung 9-6 sind die Inter-Ebenen-Beziehungen zwischen der fachlichen Ebene und der logischen Werkzeugebene dargestellt. Anhand der Abbildung ist zu erkennen, dass die Aufgaben „Dokument archivieren“ und „Signatur erneuern“ von keinem Anwendungsbaustein erledigt wird. Die

Aufgabe „Aufbewahrungsdauer anpassen“ wird vom Archivierungssystem erledigt. Eine genaue Zuordnung der Aufgabe zu einem bestimmten Anwendungsbaustein im Archivierungssystem ist nicht möglich. Weiterhin ist erkennbar, dass es zwei Anwendungsbausteine für den Dokumentenimport gibt.

5.1.5 Physische Werkzeugebene

Das Produkt d.3 ist ein reines Softwareprodukt und beinhaltet keine Hardwarekomponenten (z.B. Ablagesystem, Server). Die entsprechende Hardware kann vom Kunden selbst oder über einen Vertriebspartner von der d.velop AG beschafft werden. D.3 ist hardwareunabhängig. Aus diesem Grund ist eine Integration des Archivierungssystems in eine bereits bestehende IT-Landschaft möglich. Im Folgenden soll erläutert werden, welche Hardware für die Installation des d.3-Systems erforderlich ist.

Für die Installation der einzelnen Komponenten werden u.a. die folgenden Server benötigt:

- d. 3 Applikationsserver (mind. 1 Prozessor 3 Ghz Xeon; 1 GB RAM; 80 GB RAID 1 HDD)[36]

  Als Betriebssystem können u.a. Microsoft Windows 2000 Server, Microsoft Windows 2003 Server, SuSE Linux ab V7.0 oder RedHat ab V7.0 eingesetzt werden.

- Datenbankserver (mind. 1 Prozessor 3 Ghz Xeon; 2 GB RAM; 120 GB RAID 5 HDD)

  Auf diesem Server ist die Datenbank zur Verwaltung der Dokumente und Indexdaten abgelegt. Die Signaturinformationen werden als Datei auf dem Server gespeichert.

- Importserver d.3 Cold (1 Prozessor 3 Ghz Pentium; 512 MB RAM; mind. 120 GB HDD)

  Dieser Server wird für den Massenimport von Daten und Dokumenten eingesetzt.

- d.3 Fileserver (mind. 1 Prozessor 3 Ghz Xeon; 1 GB RAM; min. 250 GB RAID 5 HDD)

- Web-Server[37].

Die Komponenten können auch auf einem einzelnen Server installiert sein. Dies wird jedoch aus Performancegründen nicht von der d.velop AG empfohlen.

Für die Aufbewahrung der Dokumente wird ein Ablagesystem benötigt, in dem die zu archivierenden Dokumente einschließlich der dazugehörigen Signaturdateien (*.pk7) abgelegt werden. Notizen, die zu einem Dokument erstellt wurden, werden ebenfalls im Ablagesystem gespeichert. Es wird die Archivierung der Dokumente auf einem File-Server, in einem NAS und in einem SAN unterstützt.

Das Volltextsuchsystem wird in der Regel auf dem d.3 Applikationsserver installiert. Die erkannten Informationen werden als Indexdaten zu einem Dokument abgelegt. Jede Suchmaschine benutzt zur Ablage ein eigenes Verfahren. Die Standardsuchmaschine d.3 search engine legt z.B. die erkannten Indexdaten in Form von Hash-Bäumen im Dateisystem ab.

Die Anzeige und Recherche der Dokumente erfolgt über die Arbeitsplatzrechner. Soll die Anzeige und Recherche über den Standard-Recherchecliient von d.3 erfolgen, ist auf allen Arbeitplatzrechnern das Modul d.explorer zu installieren. Erfolgt die Recherche webbasiert, müssen die Arbeitplatzrechner nur über einen Webbrowser verfügen. Als Webbrowser werden der Internet Explorer, Netscape oder auch Mozilla unterstützt. Für die Anzeige der Dokumente muss auf allen Rechnern der Viewer d.3 view installiert sein.

Für die Erfassung von papierbasierten Dokumenten müssen die entsprechenden Arbeitsplätze mit Scannern ausgestattet sein. Die Software d.capture dialog ist auf einem Arbeitsplatzrechner installiert, der zur Erfassung von einzelnen Dokumenten dient (z.B. Arbeitsplatzrechner in der

[36] In der Klammer sind die Hardwareanforderungen für den jeweiligen Server angegeben.

[37] Die Anforderungen bzgl. der Hardware sind nicht bekannt.

Patientenaufnahme). Die Software d.capture batch muss auf Arbeitsplatzrechnern installiert sein, die zur Massenerfassung von papierbasierten Dokumenten dienen.

In der folgenden Abbildung ist die physische Werkzeugebene des Produktes d.3 dargestellt.

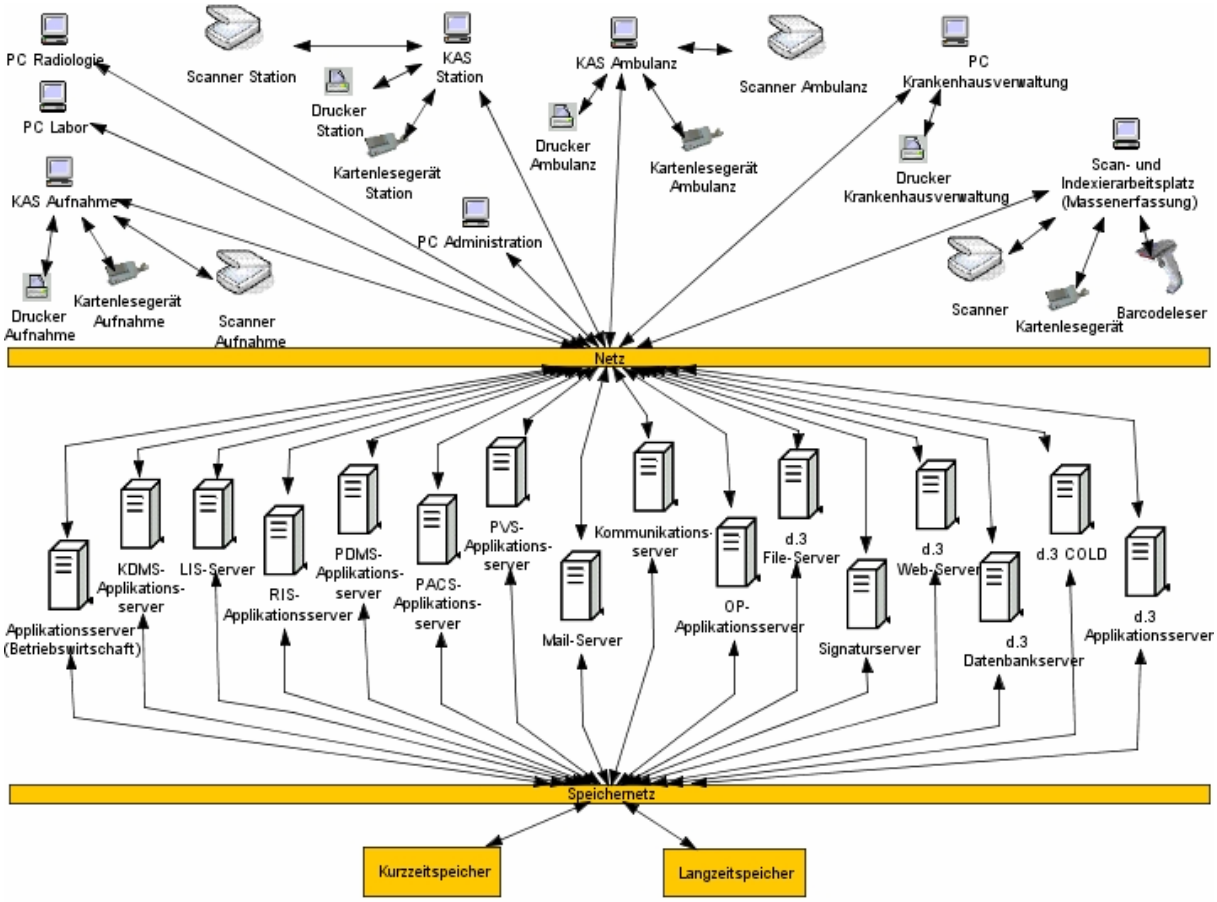


Abbildung 5-3: Physische Werkzeugebene von d.3

5.1.6 Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene

Im Anhang in Abbildung 9-7 sind die Inter-Ebenen-Beziehungen zwischen der logischen und physischen Werkzeugebene in einer Matrix dargestellt.

5.2 Heydt-Verlags-GmbH

Die Heydt-Verlags-GmbH wurde 1967 gegründet und bietet Dienstleistungen im Bereich optisch-analoger und optisch-digitaler Speichermedien im deutschsprachigen Raum an. Für die digitale Archivierung wird das Softwareprodukt HYDMedia angeboten, das in der Basisfunktionalität ein Archiv- und Dokumentenmanagementsystem darstellt. HYDMedia wird hauptsächlich im Gesundheitswesen (ca. 99 %) eingesetzt.

5.2.1 Begriffsdefinition

In dem Produkt HYDMedia wird generell von einer APA gesprochen. In der APA werden alle archivierten Dokumente eingestellt. Dokumente können in der APA über einen neuen Revisionsstand ergänzt, aber nicht mehr verändert werden.

5.2.2 Fachliche Ebene

1. Archivierte Patientenakte anlegen

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

2. Dokument importieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

3. Dokument archivieren

   HYDMedia ist ein reines Softwareprodukt, das die Dokumente über eine Schnittstelle zur Aufbewahrung an das Ablagesystem übergibt. Die Archivierung des Dokumentes übernimmt jedoch das Ablagesystem, das kein Bestandteil von HYDMedia ist.

4. Dokument transformieren

   Da das TransiDoc-Projekt noch nicht abgeschlossen wurde, kann diese Aufgabe noch nicht unterstützt werden.

5. Dokument löschen und Vernichtung protokollieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

6. Archivierte Patientenakte vernichten und Vernichtung protokollieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

7. Dokument suchen

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

8. Dokument signieren

   Es wird die elektronische Signierung von unterschriftsrelevanten Dokumenten unterstützt.

9. Dokument versenden

   Der Versand von Dokumenten wird in HYDMedia nicht unterstützt. Aus datenschutzrechtlichen Gründen ist lediglich ein Export der Dokumente möglich. Um Dokumente exportieren zu können, muss der Benutzer eine entsprechende Berechtigung besitzen. Falls der Benutzer diese Berechtigung hat, kann er die Dokumente exportieren und anschließend versenden.

10. APA versenden

    Diese Aufgabe wird von HYDMedia nicht unterstützt.

11. Signatur erneuern

    Die Umsetzung des ArchiSig-Projektes wird gerade für das Universitätsklinikum Heidelberg und das Städtische Klinikum Braunschweig realisiert.

12. Berechtigung prüfen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

13. Dokument anzeigen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

14. Dokumenteninhalt suchen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt. Die Volltextsuche erfolgt über die OCR-Erkennung.

15. Zugriff protokollieren

Diese Aufgabe wird gemäß Referenzmodell unterstützt.

16. Dokument digitalisieren

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

17. Dokument drucken

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

18. Aufbewahrungsdauer anpassen

    Ein erneuter Aufenthalt eines Patienten wird über eine HL7-Nachricht dem Archivierungssystem mitgeteilt. Der automatische Löschmechanismus der bisher erstellten Dokumente wird automatisch verlängert. Es erfolgt eine automatische Anpassung der Aufbewahrungsdauer, wenn der Patient einen weiteren Aufenthalt oder eine weitere Untersuchung im Krankenhaus hat.

In der folgenden Abbildung ist die fachliche Ebene des Produktes HYDMedia dargestellt. Der Versand eines einzelnen Dokumentes oder einer APA wird nicht unterstützt. Es besteht jedoch die Möglichkeit, Dokumente zu exportieren. Da dies eine zusätzliche Aufgabe im Vergleich mit dem Referenzmodell darstellt, ist die Aufgabe „Dokument exportieren“ durch eine andere Farbe gekennzeichnet.

Abbildung 5-4: Fachliche Ebene von HYDMedia

5.2.3 Logische Werkzeugebene

5.2.3.1. Anwendungsbausteine

Das Softwareprodukt HYDMedia setzt sich aus verschiedenen Softwarebausteinen zusammen. Zu den Basisbausteinen von HYDMedia gehören:

- das Datenschutz- und Zugriffskontrollsystem HYDDisp
- Administrationssystem HYDKonf
- Importsystem für den strukturierten Import aller möglichen Objektklassen HYDldxSv
- webbasierter Viewer HYDIntranet, der in jeden marktgängigen Anwendungsbaustein integriert werden kann
- ein Archivkontrollarbeitsplatz zum protokollierten Umhängen und Korrigieren falsch eingescannter Akten HYDView.

Administrationssystem HYDKonf

Die Administration des Archivierungssystems erfolgt über den Softwarebaustein HYDKonf. Das Administrationssystem dient zur Verwaltung von:

- Benutzern, Gruppen, Rollen und Benutzerberechtigungen in Form von Regeln. Einem Benutzer oder eine Gruppe können n-Regeln[38] zugewiesen werden.
- FTP-Einstellungen
- Funktionsprüfungen (z.B. Prüfung, ob eine Regel funktioniert)
- Archivmedien (z.B. CD-ROM, DVD-R, WORM).

Die Benutzerrechte können individuell für jeden Benutzer für eine Dokumentenart festgelegt werden. Dadurch wird genau definiert, wer z.B. ein Dokument drucken, exportieren oder die Indexierung eines Dokumentes ändern darf. Es besteht jedoch auch die Möglichkeit, die Zugriffsberechtigungen aus dem führenden Informationssystem (z.B. SAP IS-H) oder aus einer bereits existierenden Benutzerverwaltung (z.B. ActiveDirectory, LDAP) in das Administrationssystem zu übernehmen.

Zugriffssystem

Diese Software kontrolliert die einzelnen Anfragen, die an das Archivierungssystem gestellt werden, sowie die Zugriffsberechtigungen. Damit wird sichergestellt, dass nur autorisierte Nutzer auf die archivierten Patientenunterlagen zugreifen können. Für die Kontrolle der Archivanfragen und der Zugriffsberechtigungen gibt es zwei Ansätze:

- Die Software HYDDisp ist auf einem Server installiert, der die Anfragen und Berechtigungen überprüft. Erst bei einer erfolgreichen Überprüfung wird die Anfrage an das Archivierungssystem weitergeleitet. Dieser Ansatz wird bei Datenbankzugriffen gewählt, die über die Viewer HYDView3 und HYDOLEView erfolgen.
- Wenn die Zugriffe webbasiert erfolgen (z.B. über HYDIntranet, HYDIntranet Professional), dann erfolgt die Überprüfung und Kontrolle der Zugriffsberechtigung durch den HYDIntranetServer, auf dem das Dispatchermodul HYDDisp installiert ist.

In beiden Ansätzen wird jedoch auf ein und dieselbe Datenbank des Archivierungssystems zugegriffen.

---

[38] Beispiel für eine Regel: Ein externer Arzt darf auf die Arztbriefe der von ihm eingewiesenen Patienten zugreifen.

Recherchesystem

Für die Recherche nach archivierten Patientenunterlagen gibt es verschiedene Möglichkeiten:

- Die Recherche erfolgt über eine eigenständige Recherchesoftware. Dazu muss die Software HYDView3 auf jedem Arbeitsplatzrechner installiert sein, an dem eine Recherche durchgeführt werden soll. Mit dieser Recherchesoftware können archivierte Patientenunterlagen unabhängig von der Verfügbarkeit des führenden Informationssystems eingesehen werden.
- Die Suche und Anzeige von archivierten Patientenunterlagen erfolgt über einen webbasierten Browser. Dazu wird die browserorientierte Rechercheoberfläche HYDIntranet zur Verfügung gestellt, die man sich z.B. mit den Internetbrowsern von Netscape und Microsoft anschauen kann.

Die Suche erfolgt in den Indexdaten, die zu den einzelnen Dokumenten hinterlegt sind.

Visualisierungssystem

Für die Anzeige der archivierten Patientenunterlagen auf dem Bildschirm werden vier verschiedene Viewer angeboten, je nachdem, auf welche Weise die Recherche durchgeführt wird. Die Recherchesysteme HYDView3 und HYDIntranet stellen einen eigenen Viewer zur Ansicht der Dokumente bereit. HYDIntranet verfügt über einen integrierten Java-Viewer, während die Dokumente in HYDView3 über einen Stand-alone-Viewer angezeigt werden.

Es werden weiterhin zwei Viewer zur Verfügung gestellt, die über die COM-Schnittstelle HYDCnect in jede beliebige Benutzeroberfläche eines Anwendungsbaustein eingebunden werden können. Diese beiden Viewer sind nicht eigenständig aufrufbar. Sie benötigen immer einen Anwendungsbaustein, an den sie sich mit der Anzeigefunktionalität anhängen können. In diesem Anwendungsbaustein wird auch die Recherche durchgeführt. Für das Betriebssystem Windows wird der Viewer HYDOLEView angeboten. Dieser Viewer wird über einen Button in der Benutzeroberfläche aufgerufen. Die abgefragten Daten werden in Form einer Auswahlliste angezeigt. Über einen Doppelklick kann das entsprechende Dokument geöffnet werden. Bei der Verwendung von unterschiedlichen Betriebssystemen in den rechnergestützten Anwendungsbausteinen wird der Java Viewer HYDIntranet Professional benötigt.

Alle vier Viewer bieten die folgenden Funktionalitäten:

- Vergrößern und Verkleinern von Dokumentausschnitten mittels einer Zoomfunktion
- Drehen von Dokumenten
- Ausdruck von Dokumenten
- Export von Einzelbildern oder ganzer Bildserien
- Export der Bilddaten zum E-Mail-Versand
- benutzerspezifische Gestaltung der Bilschirmdarstellung (z.B. durch das Einblenden/Ausblenden von Thumbnails, Anzeige einer/mehrerer Seiten).

Scansystem

Für die Erfassung einer großen Anzahl von papierbasierten Dokumenten wird das Scansystem HYDScan angeboten. Dieses Softwaremodul dient zur reinen Erfassung der papierbasierten Dokumente. Das Scansystem bietet die folgenden Funktionalitäten:

- Ausrichtung der Seiten
- Auswahl des zu scannenden Bereiches (Cropping)
- Deskew
- Deshade

- Schmutzentfernung aus dem Hintergrund
- Barcode- und Patchcodelesung.

Nach dem Einscannen stehen die eingescannten Papierdokumente zur Indexierung bereit. Die Indexierung erfolgt über das Indexiersystem HYDIndP, das die automatische Indexierung von 1500 bis 3500 Dokumenten pro Stunde ermöglicht. Die Stammdaten zu einem Patienten können dabei aus dem Barcode ermittelt werden. Weitere Indexdaten werden über die OCR-Technik aus dem Dokument ausgelesen.

Für die Erfassung einzelner Dokumentenseiten direkt am Arbeitsplatz wird das Scansystem HYDImag zur Verfügung gestellt. Dieses Scansystem unterstützt das Anbringen von Notizen, farblichen Textmarkierungen und die Stempelfunktion. Die manuelle Indexierung der erfassten Dokumente erfolgt über das Indexiersystem HYDIndX, das zusammen mit dem Scansystem HYDScan eingesetzt wird. Das Indexiersystem HYDIndX wird vor allem dann genutzt, wenn wenige Attribute zu einem Dokument zu erfassen sind.

Importsystem HYDIdxSv

HYDIdxSv ist die zentrale Softwarekomponente für die strukturierte Übernahme der zu archivierenden Patientenunterlagen in das Archivierungssystem. Voraussetzung für die Erfassung und den Import der Daten ist, dass das Datenschutzsystem HYDDisp aktiviert ist. Weiterhin können über dieses Softwaremodul bestimmte Dokumente priorisiert werden. Das hat zur Folge, dass z.B. Dokumente mit einer hohen Priorität sofort nach ihrer Erstellung in HYDMedia sichtbar gemacht werden.

Für den Import der Patientenunterlagen werden verschiedene Module zur Verfügung gestellt. Diese Module haben die Aufgabe, die jeweiligen Dokumente und Bilder in archivtauglichen Dateiformaten an das zentrale Importsystem HYDldxSv zu übergeben. Dazu werden in den einzelnen Modulen der Aufbau der jeweiligen Dokumentenart sowie das entsprechende Ablageformat definiert. Das Modul HYDIdxSv führt dann den Datenimport durch. Die Indexdaten werden dabei in der Datenbank und die Dokumente auf dem Ablagesystem revisionssicher abgelegt und archiviert.

Folgende Importmodule werden angeboten:

(1) HYDCold

Dieses Modul dient zur automatischen Übernahme von Dokumenten, die einen festen Aufbau besitzen. Der Aufbau der jeweiligen Dokumentenart wird in einem Administrationssystem definiert, das Bestandteil des von HYDCold ist. Damit können beim Import des jeweiligen Dokumentes die Indexdaten automatisch aus dem Dokument ermittelt werden. Die vollautomatische Übernahme der Indexdaten und der Dokumente erfolgt über die COLD-Schnittstelle, die diese an das Importssystem HYDIdxSv zur revisionssicheren Archivierung übergibt. Das Modul HYDCold wird hauptsächlich für Dokumente eingesetzt, die von einem Laborinformations- oder Postsystem bereitgestellt werden.

(2) HYDImpCD

Mit diesem Modul können standardisierte Dokumente, die von externen Personen (z.B. niedergelassener Arzt) in elektronischer Form bereitgestellt werden, übernommen werden. Dabei erfolgt eine Anpassung der Dokumente an die Struktur von HYDMedia. Das Modul übergibt die Dokumente zur revisionssicheren Archivierung an das Importsystem HYDIdxSv.

(3) HYDOffice

Dieses Modul dient zur automatischen Übernahme von Dokumenten aus einer Office-Anwendung. Da die mit Office erstellten Dokumente weder revisionssicher sind noch eine langfristige Lesbarkeit gewährleistet ist, müssen diese Dokumente in archivtaugliche Dateiformate umgewandelt werden. In diesem Modul wird für jede Dokumentenart definiert, in welchen Dateiformaten die Dokumente abgelegt werden sollen. HYDOffice wandelt die Dokumente in das definierte Ablageformat um und hält zusätzlich den

Revisionsstand des Dokumentes fest. Der Ersteller sowie eventuelle Änderungen im Dokument werden in einem Log-File protokolliert. Über ein Customizing kann festgelegt werden, ob nur die transformierte Datei oder auch zusätzlich die Originaldatei archiviert werden soll. HYDOffice unterstützt die Archivierung von E-Mails einschließlich der darin enthaltenen Anhänge.

Über diese Importmodule erfolgt auch die Indexierung der Dokumente.

Workflowsystem

Das Workflowsystem und die Archivierung werden logisch getrennt voneinander betrachtet. Die Heydt-Verlags-GmbH verzichtet auf die Bereitstellung eines Workflowsystems im Archivierungssystem, da die Workflowfunktionalitäten in der Regel von anderen Anwendungsbausteinen bereitgestellt werden. Zur Unterstützung von Workflows wird der Anwendungsbaustein HYDBusiness Server angeboten, der jedoch kein Modul von HYDMedia darstellt.

Remotesystem

Das Remotesystem dient zur Freigabe von Dokumenten, auf die externe Personen (z.B. MDK, niedergelassene Ärzte) zugreifen sollen. Der Zugriff auf die freigegebenen Dokumente erfolgt über eine gesicherte VPN-Verbindung. Das Remotesystem wird auf dem Arbeitsplatzrechner des Medizincontrollers installiert, der für die Freigabe der Dokumente verantwortlich ist. Eine Autorisierung des Benutzers ist erforderlich. Externe Personen können sich nur die vom Medizincontroller freigegebenen Dokumente anschauen.

5.2.3.2. Schnittstellen

Das Archivierungssystem stellt folgende Schnittstellen zur Verfügung:

Zertifizierte SAP-Schnittstelle ArchiveLink

Diese Schnittstelle ist von SAP zertifiziert und dient zur Kommunikation zwischen dem Archivierungssystem und SAP R/3.

HL7-Schnittstelle

Die Kommunikation mit dem Kommunikationsserver oder den anderen Anwendungsbausteinen des KIS ist über die HL7-Schnittstelle möglich.

COLD-Schnittstelle HYDCold

Diese Schnittstelle dient zur automatischen Übernahme von List- und Spooldateien. Sie wird insbesondere für die Übernahme von Labordaten oder Daten aus einem Postsystem eingesetzt.

Schnittstelle zur Übernahme von Office-Dokumenten HYDOffice

Diese Schnittstelle dient zur automatischen Übernahme von Office Dokumenten.

Schnittstelle zur Übernahme von Bildern und Befunden HYDRAD

Diese Schnittstelle dient zur automatischen Übernahme von medizinischen Bildern im DICOM-Format.

5.2.3.3. Datenbanksystem

In der Datenbank werden die Referenzen zu den digitalen Dokumenten sowie die dazugehörigen Indexdaten und die Stammdaten zu einem Patienten gespeichert. Zusätzlich können auch Referenzen zum Mikrofilm in der Datenbank verwaltet werden. Der Dokumenteninhalt für die Volltextsuche wird in gesonderten Tabellen in der Datenbank abgelegt. Damit wird die Suchgeschwindigkeit bei einer Suche über die Deskriptoren nicht beeinträchtigt. Als Datenbankverwaltungssysteme werden Oracle, ADABAS D und Microsoft SQL-Server unterstützt.

5.2.3.4. Darstellung der logischen Werkzeugebene von HYDMedia

Die folgende Abbildung zeigt die logische Werkzeugebene von HYDMedia.

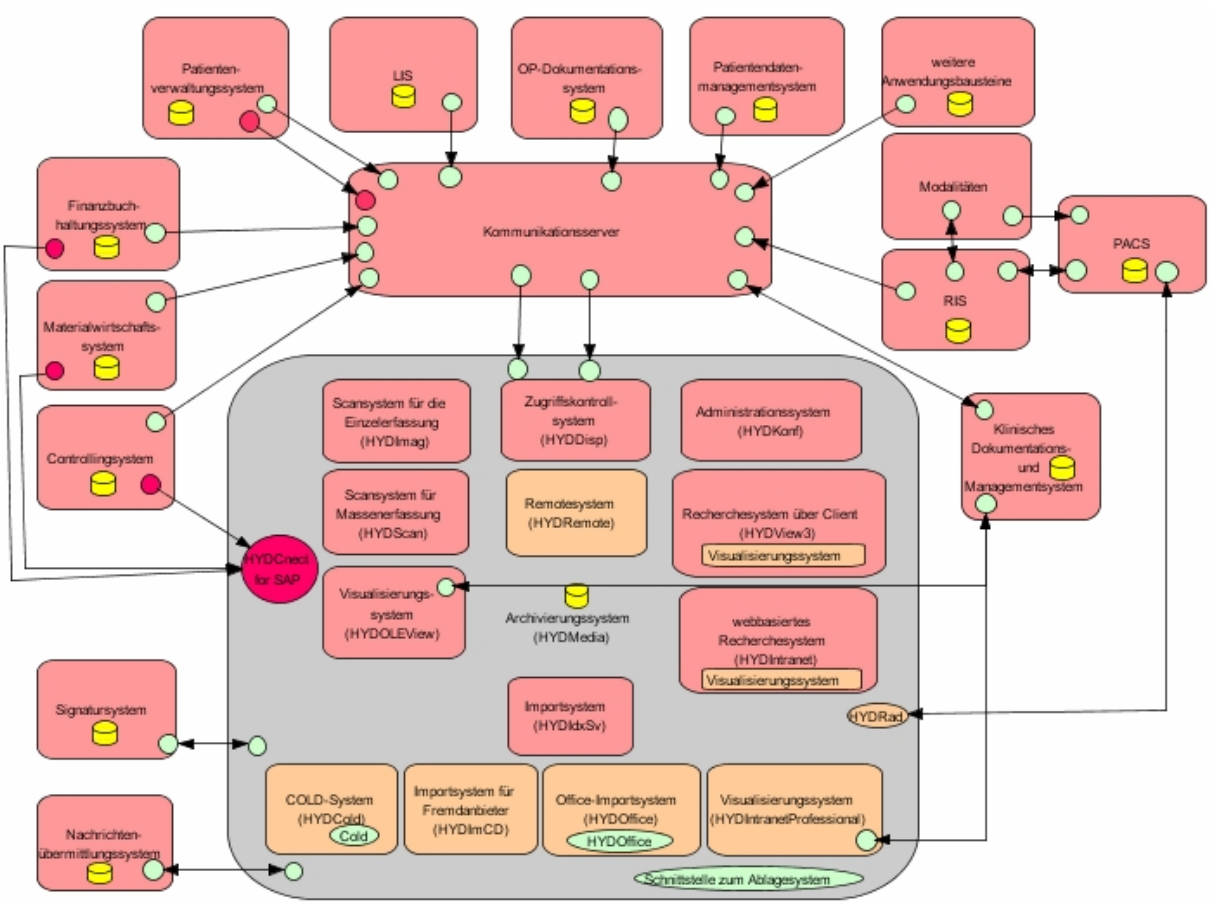


Abbildung 5-5: Logische Werkzeugebene von HYDMedia

5.2.4 Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene

Die Inter-Ebenen-Beziehungen zwischen der fachlichen Ebene und der logischen Werkzeugebene sind im Anhang in Abbildung 9-8 dargestellt. Anhand dieser Matrix ist erkennbar, dass für die Anzeige der Dokumente insgesamt vier Visualisierungssysteme angeboten werden. Die Aufgabe „Dokument archivieren“ wird nicht vom Archivierungssystem unterstützt. Für den Dokumentenimport werden verschiedene Module vom Archivierungssystem bereitgestellt.

5.2.5 Physische Werkzeugebene

HYDMedia ist ein reines Softwareprodukt. Der Kunde kann entscheiden, welches Ablagesystem er für die Archivierung einsetzen möchte. Es werden u.a.:

- die Ablage in einem SAN, NAS
- das Ablagesystem Centera von EMC^2 (die Heydt-Verlags-GmbH besitzt eine Zertifizierung für die Centera)
- die Ablage auf optischen Speichermedien (CDs, DVDs, WORMs) in einer Jukebox

unterstützt.

Für die Installation von HYDMedia wird

- immer ein Applikationsserver als zentrale Hardwareplattform
- ein Web-Server
- ein Datenbankserver und
- ein Importserver

benötigt.

Auf dem Applikationsserver sind standardmäßig die Module HYDDisp und HYDIdxSV installiert. Es können jedoch weitere Module hinzugefügt werden.

Zu den Basisbausteinen gehört das Modul HYDIntranet, dass auf einem Web-Server installiert ist. Die Kommunikation zwischen den einzelnen Arbeitsplatzrechnern und diesem Server wird über das http-Protokoll realisiert. Um auf die Web-Applikation zugreifen zu können, müssen die Arbeitsplatzrechner über einen javafähigen Browser (z.B. Internet Explorer) verfügen. Weiterhin sollten die Rechner mit folgender Hardware ausgestattet sein (Stand 10/2005):

- Pentium II-/III- oder AMD-Prozessor mit mindestens 350 MHz
- Arbeitsspeicher ab 64 MB RAM.

Am Arbeitsplatz wird eine Bildschirmgröße ab 19 Zoll empfohlen.

Die Administration von HYDMedia erfolgt über das Administrationssystem, das in der Regel auf maximal zwei Arbeitsplatzrechnern installiert ist. Die Freigabe der Dokumente wird ebenfalls an einem administrativen Arbeitsplatzrechner durchgeführt. Dazu muss das Remotesystem HYDRemote installiert sein. Soll für die Recherche der Standard-Rechercheclient HYDView3 genutzt werden, ist dieser auf dem jeweiligen Arbeitsplatzrechner einzurichten.

Für die Erfassung und Indexierung von papierbasierten Dokumenten müssen bestimmte Arbeitsplatzrechner mit Scannern ausgestattet sein. In Abhängigkeit vom einzuscannenden Datenvolumen, besitzen die Scanner eine unterschiedliche Leistungsfähigkeit.

In der folgenden Abbildung ist die physische Werkzeugebene von HYDMedia dargestellt.

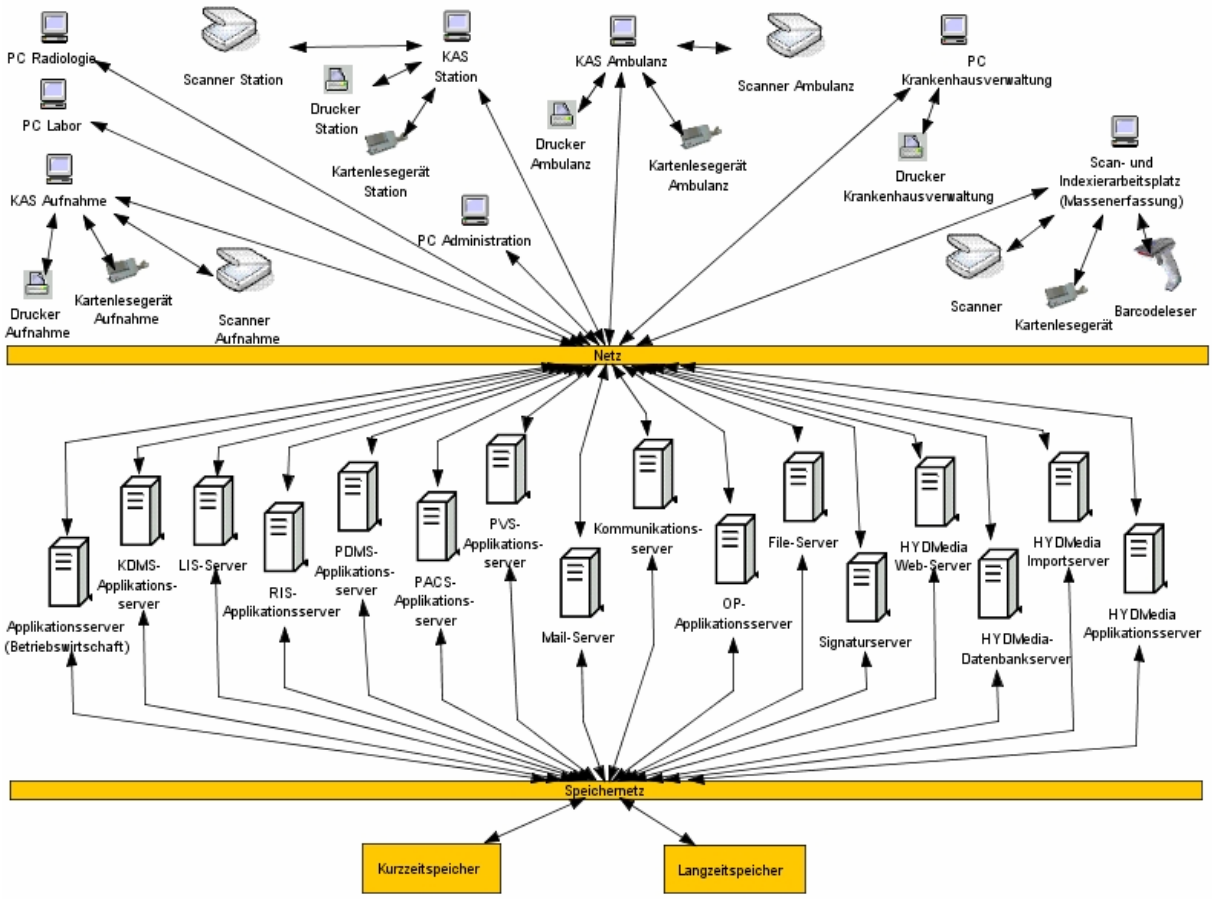


Abbildung 5-6: Physische Werkzeugebene von HYDMedia

5.2.6 Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene

Die Inter-Ebenen-Beziehungen zwischen der logischen und physischen Werkzeugebene sind zur Veranschaulichung in einer Matrix im Anhang in Abbildung 9-9 dargestellt.

5.2.7 Besonderheiten

Die Darstellung der Dokumente in HYDMedia wird über Kumulationen geregelt. Der Inhalt einer APA wird in einzelne Register unterteilt. Mit Hilfe der Register erfolgt eine inhaltliche Trennung der Dokumente. Die Definition, welche Dokumente voneinander unterschieden und wie die einzelnen Register platziert werden, definiert der Anwender selbst. Die Sortierung und Darstellung der APA einschließlich der Register kann per Knopfdruck geändert werden, ohne dass sich der Inhalt der Gesamtakte ändert. In einer Kumulation wird also festgelegt, was wie dargestellt wird. Diese Technik wird bisher nur von der Heydt-Verlags-GmbH eingesetzt.

5.3 forcont business technology GmbH

Die forcont business technology GmbH wurde 1990 als ein Tochterunternehmen der Firma IXOS Software AG in Leipzig gegründet. Für die Verwaltung der Daten und Dokumente wird das Softwareprodukt forcont factory angeboten. Die forcont factory ist ein browserbasiertes Dokumentenmanagement- und Workflowsystem, das die Daten und Dokumente aus unterschiedlichen Informationssystemen in eine gemeinsame und übersichtliche Aktenstruktur integriert. Das Produkt setzt sich aus mehreren Funktionsbausteinen zusammen. Zu diesen Funktionsbausteinen gehören:

- die System-Integration
- das Dokumentenmanagement
- die Workflow- und Business-Logik sowie
- die Archivierung.

Die forcont factory ist also kein Softwareprodukt, das ausschließlich für die Archivierung von Daten und Dokumenten eingesetzt wird. Die Archivierung stellt nur ein Backendsystem von vielen in der forcont factory dar. Das Softwareprodukt kann branchenneutral eingesetzt werden.

5.3.1 Begriffsdefinition

In der forcont factory gibt es keine Unterscheidung zwischen archivierten und lebenden Dokumenten. Es wird der gesamte Lebenszyklus eines Dokumentes abgebildet. Aus diesem Grund wird der Begriff der Patientenakte verwendet.

5.3.2 Fachliche Ebene

1. Patientenakte anlegen

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

2. Dokument importieren

   Der Import der Patientenunterlagen erfolgt über Konnektoren. Über Konnektoren können die Daten und Dokumente von den integrierten Informationssystemen entgegengenommen und im Archivierungssystem abgelegt werden. Es gibt jedoch auch die Möglichkeit einzelne Dokumente per Drag & Drop von einem beliebigen Filesystem in die forcont factory einzustellen. Das Dokument bleibt im Filesystem bestehen, eine Kopie wird im Archivierungssystem abgelegt. Dokumente, die mit Microsoft Office unter Verwendung von Templates erstellt wurden, können automatisch zur Aufbewahrung an das Archivierungssystem übergeben werden. Der Import von eingescannten Dokumenten erfolgt über eine Scan-Pipeline. Basis dieser Scan-Pipeline ist eine definierte Übergabeschnittstelle im Dateisystem. Die Dokumente werden in einem definierten Format einschließlich der Indexdaten in dem Importverzeichnis abgelegt. Externe Personen können über eine Web-Schnittstelle Dokumente importieren.

3. Dokument archivieren

   Für jeden Dokumententyp wird in der forcont factory der Aufbewahrungsort definiert. Als Aufbewahrungsort ist ein Ablagesystem zu wählen, dass die unveränderliche Aufbewahrung der Dokumente unterstützt. Die forcont factory ist ein Softwareprodukt. Damit stellt das Ablagesystem keine Komponente der forcont factory dar.

4. Dokument transformieren

   Da das TransiDoc-Projekt noch nicht abgeschlossen wurde, kann diese Aufgabe noch nicht unterstützt werden.

5. Dokument löschen und Vernichtung protokollieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

6. Patientenakte löschen und Vernichtung protokollieren

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

7. Dokument suchen

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

8. Dokument signieren

   Das Signieren und Verifizieren von elektronischen Dokumenten erfolgt durch ein Signatursystem. Die forcont factory kann die Erledigung dieser Aufgabe organisieren und die Ergebnisse entsprechend verwalten.

9. Dokument versenden

   Diese Aufgabe wird gemäß Referenzmodell unterstützt.

10. Patientenakte versenden

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

    Es gibt die Möglichkeit, einen Snapshot von der Akte anzufertigen. Bei einem Snapshot wird eine Kopie der Patientenakte erstellt und in einem zip-File abgelegt. Das zip-File enthält neben den Dokumenten der Patientenakte auch die Aktenstruktur in Form einer statischen HTML-Seite. Der Snapshot stellt immer eine Momentaufnahme dar. Das zip-File kann per E-Mail versandt werden. Der Anwender hat weiterhin die Möglichkeit, die Dokumente, die er versenden möchte, nach bestimmten Selektionskriterien zusammenzustellen.

11. Signatur erneuern

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

12. Berechtigung prüfen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

13. Dokument anzeigen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

14. Dokumenteninhalt suchen

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

15. Zugriff protokollieren

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

16. Dokument digitalisieren

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

17. Dokument drucken

    Diese Aufgabe wird gemäß Referenzmodell unterstützt.

18. Aufbewahrungsdauer anpassen

    Eine nachträgliche Anpassung der Aufbewahrungsdauer ist nicht vorgesehen und auch technisch kaum realisierbar. Die Aufbewahrungsdauer wird zum Zeitpunkt der Archivierung oder kurz danach als einmaliges Ereignis übermittelt und am Dokument verankert. Die Aufbewahrungsdauer ist danach genauso unveränderlich wie das Dokument selbst.

Die folgende Abbildung zeigt die fachliche Ebene des Produktes forcont factory.

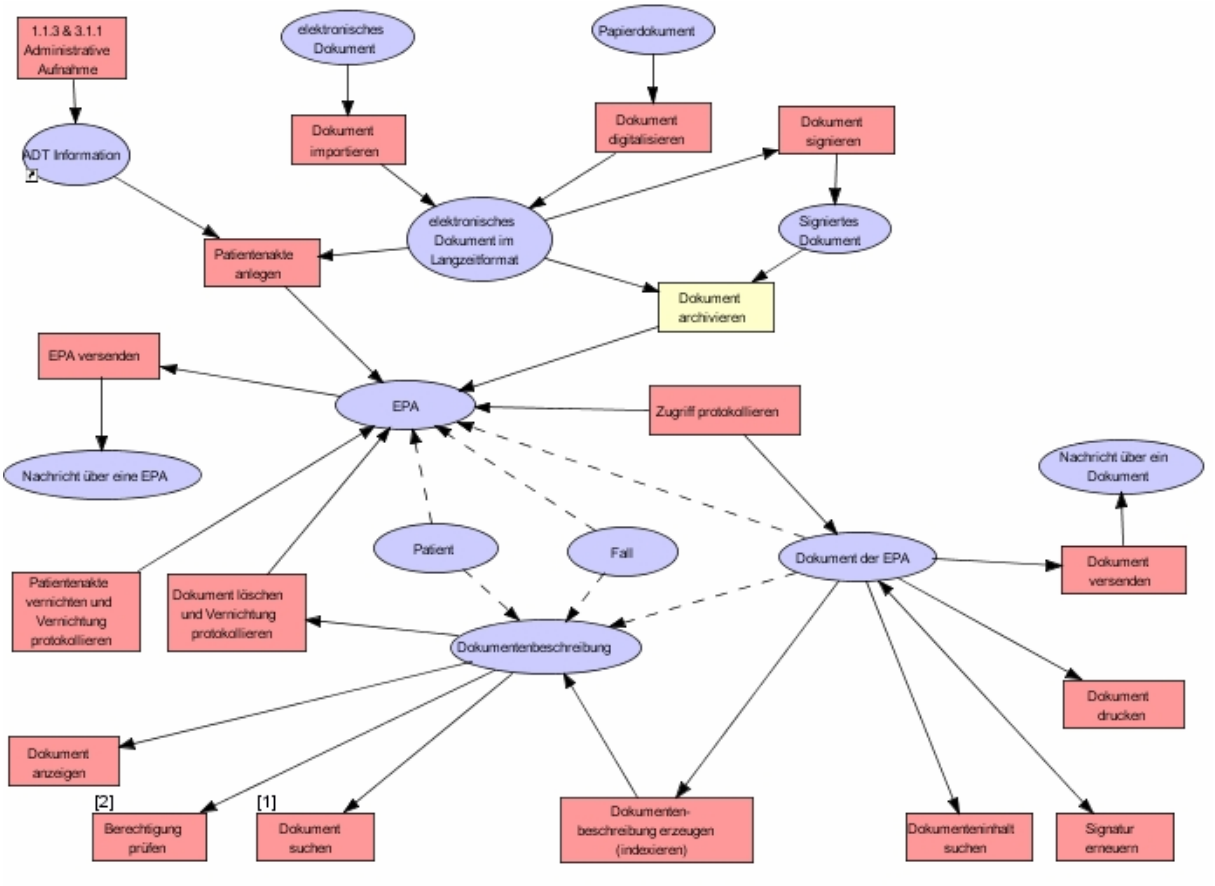


Abbildung 5-7: Fachliche Ebene der forcont factory

5.3.3 Logische Werkzeugebene

5.3.3.1. Anwendungsbausteine

Das Softwareprodukt forcont factory setzt sich aus den folgenden drei Basisbausteinen zusammen:

- Serverkomponente: Zu den Aufgaben der Serverkomponente gehören die Dokumenten- und Nutzerverwaltung sowie die Integration der Daten und Dokumente aus anderen Informationssystemen. Für die Integration der verschiedenen Informationssysteme wird eine Integrationskomponente zur Verfügung gestellt, die vier Schnittstellen anbietet:

  ⇒ Schnittstelle für den Zugriff auf die datenliefernden Informationssysteme (datasource interface), d.h. von Informationssystemen, die datensatzorientiert arbeiten (z.B. relationale Datenbanksysteme, SAP R/3-Anwendungen).

  ⇒ Schnittstelle für den Zugriff auf Informationssysteme, die Dokumente bereitstellen (doc-provider-interface). Dazu gehören z.B. Ablagesysteme wie die Centera oder Filesysteme.

  ⇒ Schnittstelle, die Funktionen für die Benutzerverwaltung bereitstellt. Zu diesen Funktionen gehören z.B. die Prüfung von Zugriffsberechtigungen, die Pflege von Benutzern und Rollen (User-Service-Interface).

  ⇒ Schnittstelle für die Anbindung eines Volltextsuchsystems (Volltext-Provider-Interface). Über diese Schnittstelle erfolgen die Übergabe der Dokumente zur Volltextindexierung, die Übergabe des Suchkriteriums und die Entgegennahme der Ergebnismenge.

- Präsentationskomponente: Die Präsentationskomponente übernimmt die Darstellung der Informationen und stellt zusammen mit dem Webbrowser eine Schnittstelle zum Anwender dar.
- AdminClient: Über den AdminClient erfolgt die Konfiguration der forcont factory. Der AdminClient stellt Funktionen für die Administration, das Customizing und das Monitoring bereit.

Administrationssystem

Die Administration erfolgt über die Oberfläche eines AdminClient, der die folgenden Aufgaben übernimmt:

- Integration der verschiedenen Anwendungsbausteine in die forcont factory (Festlegung der Daten- und Dokumentenprovider, Einbindung von Konnektoren)
- Definition der Dokumentenarten einschließlich der Indexdaten
- Festlegung der Aktenstruktur
- Konfiguration der jeweiligen Anwendersicht (Die Aktenstruktur einschließlich der darin dargestellten Dokumente sowie die für den Anwender ausführbaren Aktionen können individuell konfiguriert werden.)
- Verwaltung von Benutzern, Benutzergruppen und Rollen
- Barcodeverwaltung
- Administration der Scan-Pipeline sowie
- das Monitoring.

Für die Verwaltung der Benutzer und ihre Berechtigungen kann ein Abgleich mit einer bereits existierenden Benutzer- und Berechtigungsverwaltung (z.B. ActiveDirectory, LDAP, SAP R/3) vorgenommen werden. Jedoch ist eine weitergehende Vergabe von Berechtigungen im Administrationssystem der forcont factory erforderlich. Die Berechtigungen können auf verschiedenen Ebenen (Sichten, Ordner, Dokumentenattribute, Aktionen) von einem Administrator vergeben werden.

Zugriffskontrollsystem (factory servlet)

Alle Zugriffe in der forcont factory erfolgen ausschließlich über das factory servlet. Über das factory servlet wird sichergestellt, dass nur autorisierte Nutzer auf die Daten und Dokumente zugreifen können. Ein Servlet ist ein spezielles Java-Programm, das die Anforderung eines Web-Browsers verarbeitet und eine Antwort an den Browser zurückschickt.

Recherchesystem (forcont Präsentationskomponente)

Die Recherche erfolgt ausschließlich über einen Webbrowser. Damit entfällt die Client-Installation an den einzelnen Arbeitsplätzen. Der Anwender kann dabei zwischen verschiedenen Darstellungsmöglichkeiten wählen:

- Aktenlayout: Die Patientenunterlagen werden in einer Baumstruktur dargestellt. Der Anwender kann in der Baumstruktur bis zu dem gewünschten Dokument navigieren.
- Explorerlayout: Die Patientenunterlagen werden in einer dem Windows Explorer vergleichbaren Struktur dargestellt. Bilder können als Thumbnails dargestellt werden.
- listenförmige Darstellung: Die Dokumente werden in einer Liste angezeigt. Die listenförmige Darstellung kann z.B. bei Trefferlisten verwendet werden.

Es wird die indizierte Suche, die Volltextsuche sowie eine Kombination der beiden Suchmöglichkeiten unterstützt. Für die Suche können Wildcards verwendet werden. Die Ergebnisse der Recherche werden in einer Trefferliste ausgegeben.

Der Aufruf der forcont factory aus anderen Informationssystemen wird unterstützt und wurde z.B. in i.s.h.med realisiert. Auf der anderen Seite können in der forcont factory auch Dokumente von anderen Anwendungsbausteinen (z.B. SAP R/3) geöffnet werden. Beim Aufruf von Dokumenten aus anderen Anwendungsbausteinen erfolgt eine Benutzer/Kennwort Synchronisation. Damit ist ein erneutes Anmelden des Benutzers nicht erforderlich. Der Zugriff auf die Dokumente erfolgt unter Berücksichtigung des Berechtigungskonzeptes.

Visualisierungssystem

Für die Anzeige der Dokumente wird kein eigener Viewer zur Verfügung gestellt. Grundsätzlich werden die Dokumente über den Viewer angezeigt, der vom Betriebssystem des jeweiligen Arbeitsplatzrechners bereitgestellt wird. Falls dieser Viewer nicht ausreicht, sind auf den entsprechenden Arbeitplatzrechnern weitere Viewer zu installieren.

Scansystem

Prinzipiell wird erst einmal versucht, bereits vorhandene Scansysteme zu nutzen und in die forcont factory zu integrieren. Falls noch kein Scansystem im Einsatz ist, wird das Softwareprodukt KOFAX Ascent Capture angeboten. Diese Software unterstützt laut [KOFAX]

- die stapelorientierte Erfassung von Massenbelegen
- die Erstellung von mehrseitigen TIFF-Dateien
- die Trennung der einzelnen Dokumente durch Trennblätter
- die Formularverarbeitung
- die Imagebereinigung
- die Klassifizierung von Dokumenten
- die Erkennung von gedruckten Zeichen (OCR), handgeschriebenen Zeichen (ICR) und markierungssensiblen Bereichen wie z.B. Kreuze und Häkchen (OMR)
- die Barcodeerkennung
- die Indexierung
- die Datenvalidierung sowie
- die Ablage der Dokumente in vorher festgelegten Austauschverzeichnissen.

Aus den Austauschverzeichnissen werden die eingescannten Dokumente über eine Scan-Pipeline entgegengenommen, die die Dokumente in der entsprechenden Patientenakte hinterlegt und anschließend an ein Ablagesystem übergibt. Die Scan-Pipeline ist Bestandteil der forcont factory. In der Scan-Pipeline werden einzelne Verarbeitungsschritte zusammengefasst, die flexibel erweiter- bzw. austauschbar sind. Die Administration und Überwachung der Scan-Pipeline erfolgt im AdminClient.

Die Indexierung der gescannten Dokumente kann anhand eines Barcodes erfolgen, der z.B. die Patienten- oder Fallidentifikationssnummer enthält. Es gibt jedoch auch die Möglichkeit, die Dokumente beim Einscannen manuell zu indexieren.

Importsystem

Der Import von eingescannten oder strukturierten Dokumenten erfolgt über die forcont factory Pipeline. Die Pipeline holt die Dokumente aus einem Übergabeverzeichnis, bereitet sie nach vorher fest definierten Regeln auf und stellt sie in der forcont factory ein. Die Aufbereitung der Dokumente kann z.B. die Konvertierung von Dokumenten, die Erstellung von PDF-Dokumenten oder die Ermittlung von Indexdaten umfassen. Fehlerhafte Dokumente werden von der Pipeline aussortiert und später einer Fehlerbehandlung unterzogen. Über die Pipeline wird der Massenimport von Dokumenten unterstützt.

Workflowsystem (forcont factory workflow)

Das Workflowsystem wird als ein zusätzliches Modul zur Verfügung gestellt und bietet die folgenden Funktionalitäten:

- Abbildung paralleler und linearer Prozesse
- Zuweisung einer Aufgabe an konkrete User oder Rollen
- Wiedervorlage einer Aufgabe zu einem späteren Zeitpunkt
- Vertreterregelungen
- Eskalation bei Terminüberschreitungen
- Protokollierung und Historie des gesamten Vorgangs
- E-Mail-Anbindung
- Posteingangskorb
- Scan-Eingangskorb.

Bei der Ausführung eines Workflows kann genau nachvollzogen werden, WER WAS WANN gemacht hat sowie in welchem Status sich das jeweilige Dokument befindet. Die graphische Darstellung von Workflows wird unterstützt. Im Rahmen eines Workflows kann auch das elektronische Signieren von Dokumenten realisiert werden.

Volltextsuchsystem (forcont factory fulltex service)

Die Volltextsuche wird unterstützt. Damit ist auch eine Recherche in den Dokumentinhalten und unabhängig von den Indexdaten möglich. Für die Volltextsuche müssen die Dokumente als CI vorliegen. Die forcont factory nutzt das Volltextsuchsystem Inter:gator der Firma interface GmbH. Auf Anfrage können jedoch auch andere Volltextsuchsysteme unter Verwendung einer Treiber-Schnittstelle eingebunden werden.

Die Attribut- und Volltextsuche können miteinander kombiniert werden. Dadurch müssen nicht mehr alle Dokumente durchsucht werden, so dass der Suchaufwand sich reduziert. Bei der kombinierten Suche kann z.B. gezielt in einem Dokumententyp (z.B. Arztbrief) nach einem bestimmten Deskriptor gesucht werden.

5.3.3.2. Schnittstellen

Für die Integration der Daten und Dokumente aus bereits vorhandenen Informationssystemen in die Patientenakte werden verschiedene Konnektoren zur Verfügung gestellt. Die forcont factory bietet u.a. Konnektoren zu

- SAP R/3
- relationalen Datenbanken (Oracle, MS SQL)
- Filesystemen
- ADS/LDAP
- MS Office Produkten
- Ablagesystemen (z.B. Livelink Enterprise Archive Server, EMC, NetApp, Network).

Falls ein Konnektor zu einem bestimmten Anwendungsbaustein noch nicht vorhanden ist, gibt es die Möglichkeit, diesen zu programmieren und nachträglich einzufügen.

COLD-Schnittstelle

Diese Schnittstelle dient zur Übernahme von ASCII-Dateien aus anderen Anwendungsbausteinen. Bei den zu importierenden Dokumenten kann es sich z.B. um List- und Spooldateien oder auch um die eingescannten Dokumente von einem Scan-Dienstleister handeln. Über die Definition von Regeln können die Indexdaten automatisch aus dem jeweiligen Dokument ermittelt und zum Dokument abgelegt werden. Bei der Übernahme eingescannter Dokumente von einem Scan-Dienstleister werden im Allgemeinen die Indexdaten zu den Dokumenten mit bereitgestellt.

Schnittstelle zur Übernahme von Office-Dokumenten

Über diese Schnittstelle können Office-Dokumente automatisch zur Aufbewahrung an die forcont factory übergeben werden. Die Indexierung der Dokumente kann entweder manuell oder automatisch anhand von Formularfeldern erfolgen.

Es gibt jedoch auch die Möglichkeit, Dokumente direkt in der forcont factory zu erstellen. Ist zu dem Dokument ein Template hinterlegt, können bereits bekannte Indexdaten automatisch in das Office-Dokument eingefügt werden.

Schnittstelle für den Import für Daten/Dokumente (Datasource- und DOC-Provider-Interface)

Der Import der Daten und Dokumente erfolgt über das Datasource- und Doc-Provider-Interface. Die Dokumente müssen dabei in ein für die Langzeitarchivierung geeignetes Format transformiert werden. Dabei kann entweder nur das transformierte Dokument oder das transformierte Dokument einschließlich des Originaldokumentes zur Aufbewahrung übergeben werden.

Weiterhin unterstützt die forcont factory die Kommunikation von bestimmten HL7-Nachrichten. Die Kommunikation von DICOM-Nachrichten ist dagegen nur über den Kommunikationsserver möglich.

Die forcont factory verfügt über keine ArchiveLink-Schnittstelle. Die Kommunikation von SAP-Daten und Dokumenten erfolgt über den SAP Content Server.

5.3.3.3. Datenbanksystem

In der Datenbank der forcont factory werden standardmäßig nur die Benutzerberechtigungen, Übersetzungstabellen und die Customizing-Einstellungen (Daten- und Dokumentenprovider, die Aktenstruktur) abgelegt. Als Datenbanken werden Oracle, MySQL und MS SQL unterstützt. Die Indexdaten, Dokumenten-ID sowie die Referenz auf die Dokumente sind in der Regel in den Datenbanken der führenden Informationssysteme gespeichert, sie können aber auch in die Datenbank der forcont factory integriert werden.

5.3.3.4. Darstellung der logische Werkzeugebene der forcont factory

In der folgenden Abbildung ist die logische Werkzeugebene der forcont factory dargestellt. Anwendungsbausteine, die von einer anderen Firma in die forcont factory integriert werden, sind gelb gekennzeichnet.

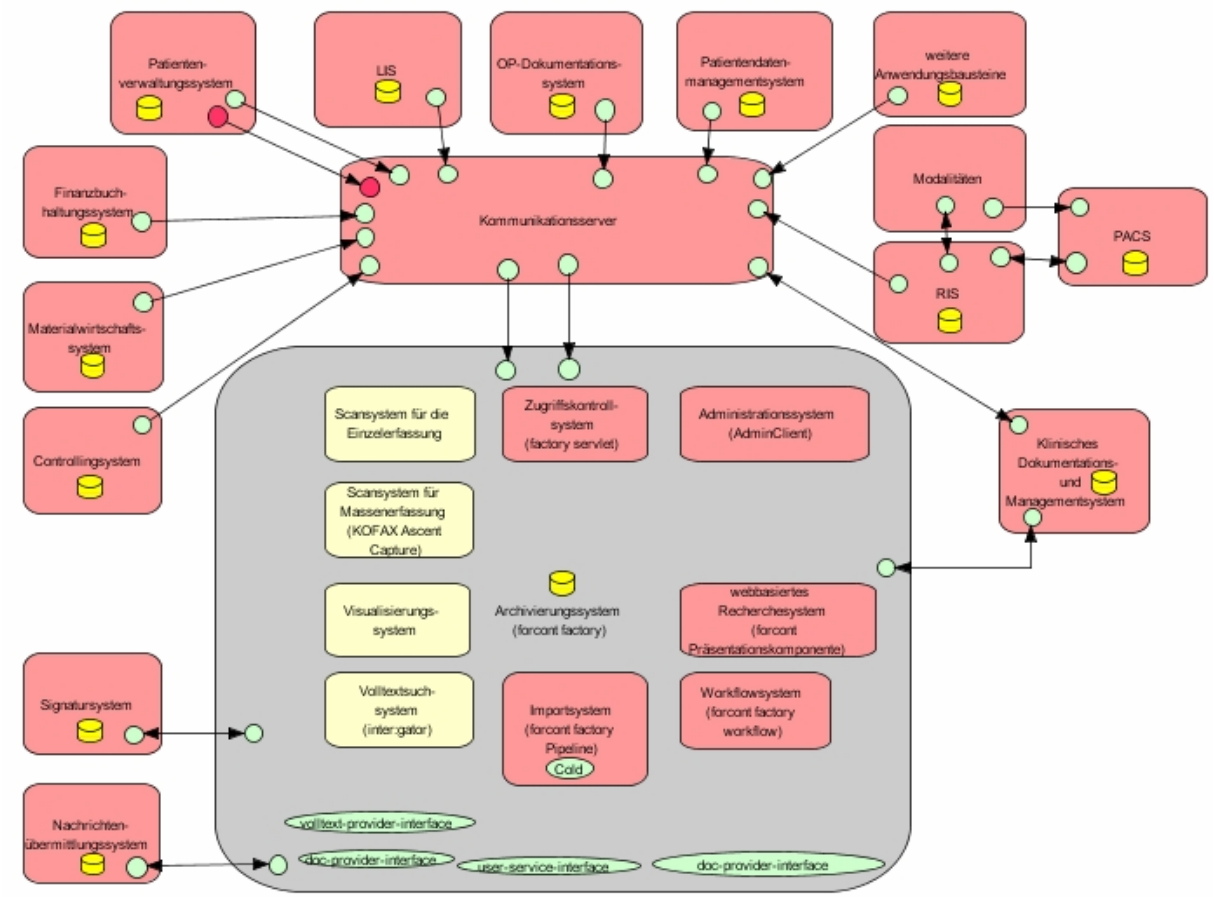


Abbildung 5-8: Logische Werkzeugebene der forcont factory

5.3.4 Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene

Die Abbildung 9-10 im Anhang enthält eine Matrix, in der die Inter-Ebenen-Beziehungen der forcont factory dargestellt sind. Die Aufgabe „Dokument archivieren“ wird nicht vom Archivierungssystem erledigt.

5.3.5 Physische Werkzeugebene

Die forcont factory unterstützt verschiedene Ablagesysteme, je nachdem ob die Dokumente weiterbearbeitet oder archiviert werden sollen. Für die Aufbewahrung von Patientenunterlagen sind Ablagesysteme zu wählen, die sicherstellen, dass die Dokumente unveränderbar abgelegt werden. Folgende Ablagesysteme, die dies gewährleisten, werden von der forcont factory unterstützt:

- Centera von EMC[2]
- Storage System von Network Appliance
- IXOS-OEM
- IXOS-Archivserver (Livelink Enterprise ArchiveServer).

Die Installation der forcont factory kann auf zwei Servern, dem Applikations- und Webserver, erfolgen. Die Server sollten mit mindestens 1 GB Hauptspeicher und einer ca. 40 GB großen Festplatte ausgestattet sein. Es ist davon auszugehen, dass beim Massenimport von Dokumenten ein weiterer Server eingesetzt wird. Die Installation der forcont factory ist betriebssystemunabhängig.

Die Installation des Scansystems ist an allen Arbeitsplatzrechnern notwendig, die mit einem Scanner ausgestattet sind. Ansonsten müssen keine Client-Installationen durchgeführt werden. Der Installationsaufwand ist somit gering.

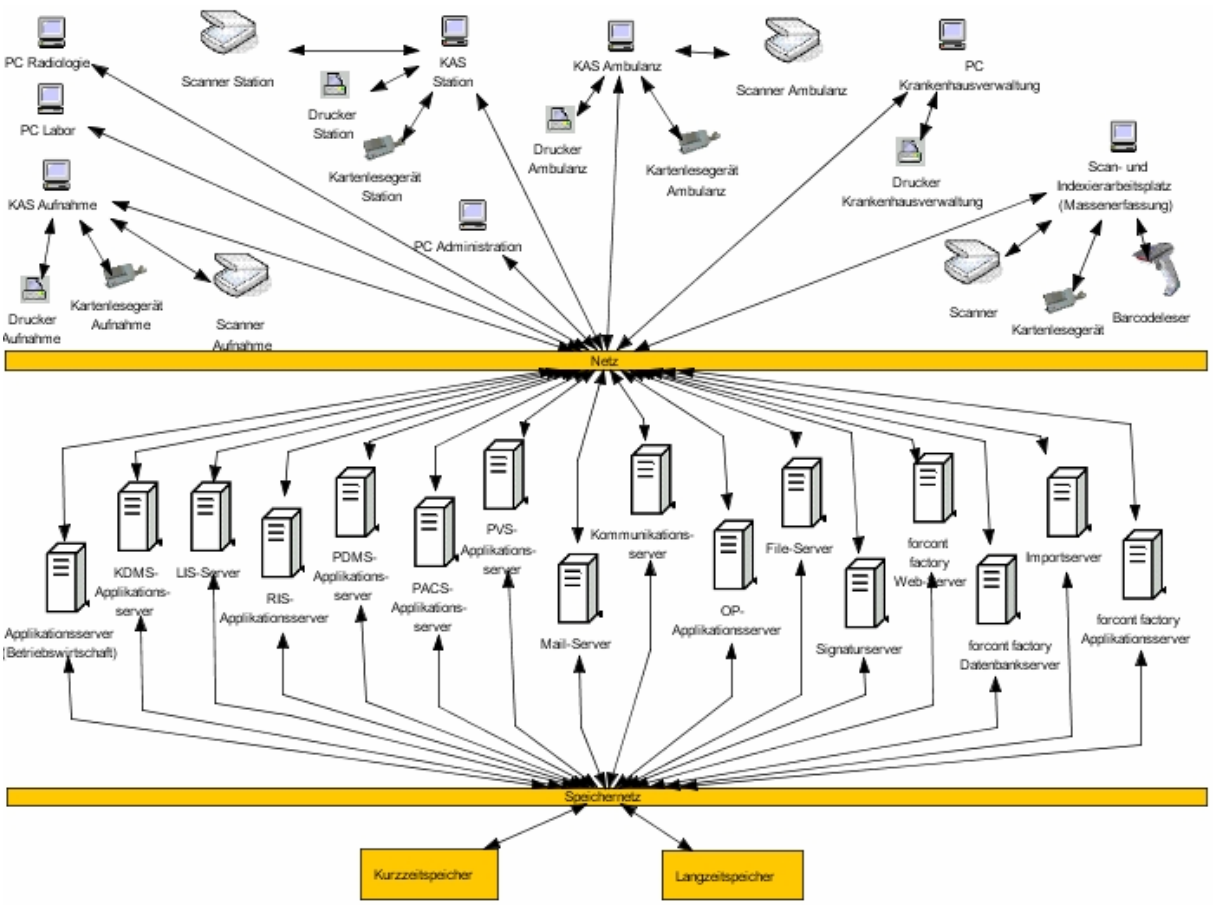


Abbildung 5-9: Physische Werkzeugebene der forcont factory

5.3.6 Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene

Die Inter-Ebenen-Beziehungen zwischen der logischen und physischen Werkzeugebene sind in einer Matrix in Abbildung 9-11 im Anhang dargestellt.

5.4 EMC²

Die Firma EMC² wurde 1979 gegründet und gehört zu den weltweit führenden Anbietern von Produkten, die die Speicherung und das Management von Informationen unterstützen. Der Hauptsitz der Firma liegt in Hopkinton in den USA. Für die Archivierung von Daten bietet EMC² das Produkt EMC Centera mit der Betriebssystemsoftware CentraStar an. Die EMC Centera ist ein IP-basiertes Speichersystem, das die unveränderliche Aufbewahrung von Daten über einen langen Zeitraum ermöglicht. Die Daten werden dabei auf einem Festplattensystem gespeichert. Der Zugriff auf die Daten erfolgt online. Damit sind die archivierten Daten innerhalb kürzester Zeit verfügbar. Die Betriebssystemsoftware CentraStar schützt die Daten gegen unbefugtes Löschen, Überschreiben oder Verändern. Das Speichersystem besitzt somit die Eigenschaft eines WORM-Mediums. Die Daten werden über eine Content Adresse im Speichersystem adressiert. Die Content Adressierung ist eine Technologie, die von der Firma EMC² speziell für die Langzeitsicherung von unveränderlichen Daten entwickelt wurde. Aufgrund der eingesetzten Technologie wird die EMC Centera auch als „Content Adressed Storage“ (CAS)-Speichersystem bezeichnet. Die EMC Centera ist das weltweit erste CAS-Speichersystem.

Die EMC Centera ist ein branchenneutrales Produkt und kann in verschiedenen Bereichen für die langfristige Aufbewahrung von Daten als Online-Speichersystem eingesetzt werden. In Deutschland stammen ca. 5% der EMC Centera-Kunden aus dem Bereich Gesundheitswesen. Auf dem amerikanischen Markt kommen ca. 15% der EMC-Centera Kunden aus dem Gesundheitswesen. Das Produkt lässt sich in den USA besser vermarkten, da die Kliniken im Allgemeinen größer sind als in Deutschland und damit größere Datenmengen produziert werden. In Deutschland kommen nur große Universitätskliniken oder Verbände wie Helios, Rhön-Kliniken, Asklepios an ein vergleichbares Datenvolumen heran. EMC[2] bietet mit der EMC Centera ein Produkt an, das die langfristige Archivierung von Daten bis in den Petabyte-Bereich ermöglicht.

5.4.1 Funktionsweise

Für das weitere Verständnis soll zunächst die Funktionsweise der EMC Centera beim Abspeichern eines Dokumentes erläutert werden.

Ein Anwendungsbaustein übergibt das zu archivierende Dokument über die API an die EMC Centera. Die EMC Centera berechnet aus dem Inhalt des Dokumentes und unter Verwendung eines Hash-Algorithmus (unter anderem nach dem MD5-Verfahren) einen 256-Bit langen Hashwert. Dieser Hashwert stellt die Content Adresse (CA) zum Dokument dar. Die Content Adresse ist vergleichbar mit einem eindeutigen Fingerabdruck zum Dokument. Anschließend wird das Dokument auf der EMC Centera als BLOB abgelegt und aus Sicherheitsgründen gespiegelt. Dabei wird ein Content Mirroring durchgeführt. Die CA wird zusammen mit den Metadaten des Dokumentes in einer XML-Datei gespeichert. Die XML-Datei wird auch als C-Clip-Deskriptor File (CDF) bezeichnet und auf der Applikationsseite generiert. Die Metadaten umfassen zum einen Attribute, die von der EMC Centera automatisch erzeugt werden, z.B. Dateiname, Dateigröße, Datum und Uhrzeit. Es können aber auch Metadaten, die von einem Anwendungsbaustein erzeugt wurden, in dem CDF gespeichert werden. Aus dem CDF wird erneut eine CA berechnet. Das CDF wird auf der EMC Centera gespeichert und ebenfalls gespiegelt. Die EMC Centera übergibt die CA des CDF dem Anwendungsbaustein (in diesem Fall dem Archivierungssystem), das die CA als Referenz auf das Dokument in einer Datenbank ablegt. Für die Bereitstellung des Dokumentes an einen Anwendungsbaustein muss grundsätzlich diese CA an die API der Centera übergeben werden. Da in der EMC Centera kein zentrales Verzeichnis, Pfadnamen oder URLs verwendet werden, ist die CA die einzige Referenz, durch die das Dokument wiederauffindbar ist. Der physische Speicherort des Dokumentes bleibt dem Anwendungsbaustein verborgen.

Die EMC Centera überwacht permanent die Datenintegrität. Wird der Inhalt eines Dokumentes verändert, generiert auf der einen Seite die EMC Centera beim Abspeichern eine neue CA und auf der anderen Seite der Anwendungsbaustein ein neues CDF. Das Originaldokument bleibt unverändert und ist über die ursprüngliche CA des CDF erreichbar. Das geänderte Dokument wird wie ein neues Dokument in der EMC Centera abgelegt, gespiegelt und ist über die aus dem CDF neu generierte CA verfügbar. Damit unterstützt die EMC Centera zum einen die Versionskontrolle, zum anderen sind die Daten gegen Verfälschungen geschützt.

Wird ein Dokument zur Archivierung an die EMC Centera übergeben, das mit einem bereits gespeicherten Dokument identisch ist, erkennt die EMC Centera die Übereinstimmung der Dokumente anhand der CA zum Dokument. In diesem Fall wird das Dokument nicht noch einmal abgespeichert. Es wird jedoch ein neues CDF erstellt, da die Dokumente zwar eine identische CA besitzen, sich aber in den Metadaten unterscheiden. Anschließend wird wieder die CA über dem CDF berechnet und an den Anwendungsbaustein zurückgegeben. Durch diese Funktionsweise wird verhindert, dass Dokumente mit identischem Inhalt unter verschiedenen Dateinamen auf der EMC Centera abgelegt werden.

5.4.2 Fachliche Ebene

Für das EMC Centera-System ergeben sich die folgenden Aufgaben:

1. Dokument archivieren

   Die Betriebssystemsoftware CentraStar legt das Dokument unveränderlich, ordnungsgemäß und revisionssicher auf dem Festplattensystem der EMC Centera ab. Für jedes Dokument wird eine eindeutige Adresse berechnet, die an das Archivierungssystem zur Aufbewahrung übergeben wird.

2. Dokument löschen und Vernichtung protokollieren

   Im Betriebssystem der EMC Centera können verschiedene Modi konfiguriert werden. Standardmäßig ist der Compliance-Modus eingestellt. In diesem Modus können die Dokumente erst nach Ablauf der Aufbewahrungszeit gelöscht werden. Die Aufbewahrungszeit wird als Attribut im CDF pro Dokument über die API der EMC Centera vom Anwendungsbaustein übergeben. Die EMC Centera übernimmt kein selbstständiges Löschen. Der Löschvorgang muss immer von einem Anwendungsbaustein initiiert werden. Wenn die EMC Centera eine Anforderung zur Löschung eines Dokumentes erhält, wird zunächst das Attribut für die Aufbewahrungszeit überprüft. Ein Löschen innerhalb der Aufbewahrungsfrist ist in diesem Modus nicht möglich. Mit jedem Löschvorgang eines Dokumentes wird eine Reflection-XML-Datei generiert, die auf dem EMC Centera-System abgelegt wird. Die Reflection-XML-Datei enthält die Protokollierung des Löschvorgangs. Der Compliance-Modus ist von der KPMG gemäß PS 880 (CE Plus) zertifiziert. Aus dem BDSG ergibt sich jedoch die Forderung, dass Patientendaten aufgrund der Bitte eines Patienten gelöscht werden müssen. Für diesen Zweck bietet EMC^2 den Governance-Modus an. Dieser Modus verfügt über eine „Priviledged Delete“-Funktion. Damit können Dokumente vor Ablauf der Aufbewahrungsfrist gelöscht werden.

3. Berechtigung prüfen

   Der Systemadministrator kann für jeden Anwendungsbaustein, der auf die EMC Centera zugreift, ein Login, Passwort und einzelne Berechtigungen vergeben. Damit muss sich jeder Anwendungsbaustein zunächst erfolgreich anmelden, um auf die Daten in der EMC Centera zugreifen zu können. Zusätzlich kann der Systemadministrator die ausführbaren Funktionen (z.B. Dokument speichern, löschen, abrufen) für jeden Anwendungsbaustein definieren.

Die EMC Centera ist ein reines Ablagesystem, das die unveränderliche Aufbewahrung von Dokumenten gewährleistet. Für die Anzeige, Suche oder den Versand der Dokumente sind zusätzliche Anwendungsbausteine erforderlich. Die Erneuerung der Signatur stellt für die EMC Centera selbst kein Problem dar. Die Signatur ist Bestandteil des Dokumentes. Die EMC Centera übergibt das Dokument an einen Anwendungsbaustein, der die Signatur erneuert und anschließend wieder an die EMC Centera zur Aufbewahrung übergibt. Da der Inhalt des Dokumentes verändert wurde, bekommt das Dokument eine neue Content Adresse zugewiesen. Das Dokument wird in der EMC Centera gespeichert. Damit ist sowohl das Dokument mit der alten als auch mit der neuen Signatur in der EMC Centera über die jeweilige Content Adresse verfügbar. Die EMC Centera speichert die Dokumente in dem Dateiformat ab, wie sie vom jeweiligen Anwendungsbaustein übergeben werden. Damit ist es die Aufgabe der einzelnen Anwendungsbausteine, die Dokumente in einem zur Langzeitaufbewahrung geeigneten Dateiformat zu übergeben.

Die folgende Abbildung zeigt die fachliche Ebene der EMC Centera. Es werden nur die Aufgaben „Dokument archivieren“, „Dokument löschen und Vernichtung protokollieren“ und „Berechtigung überprüfen“ erledigt. Während im Referenzmodell bei der Aufgabe „Berechtigung prüfen“ die Benutzerberechtigungen überprüft werden, kontrolliert die EMC Centera die Zugriffsberechtigungen der Anwendungsbausteine. Für die gelb markierten Aufgaben sind zusätzliche Anwendungsbausteine (z.B. ein Archivierungssystem) erforderlich.

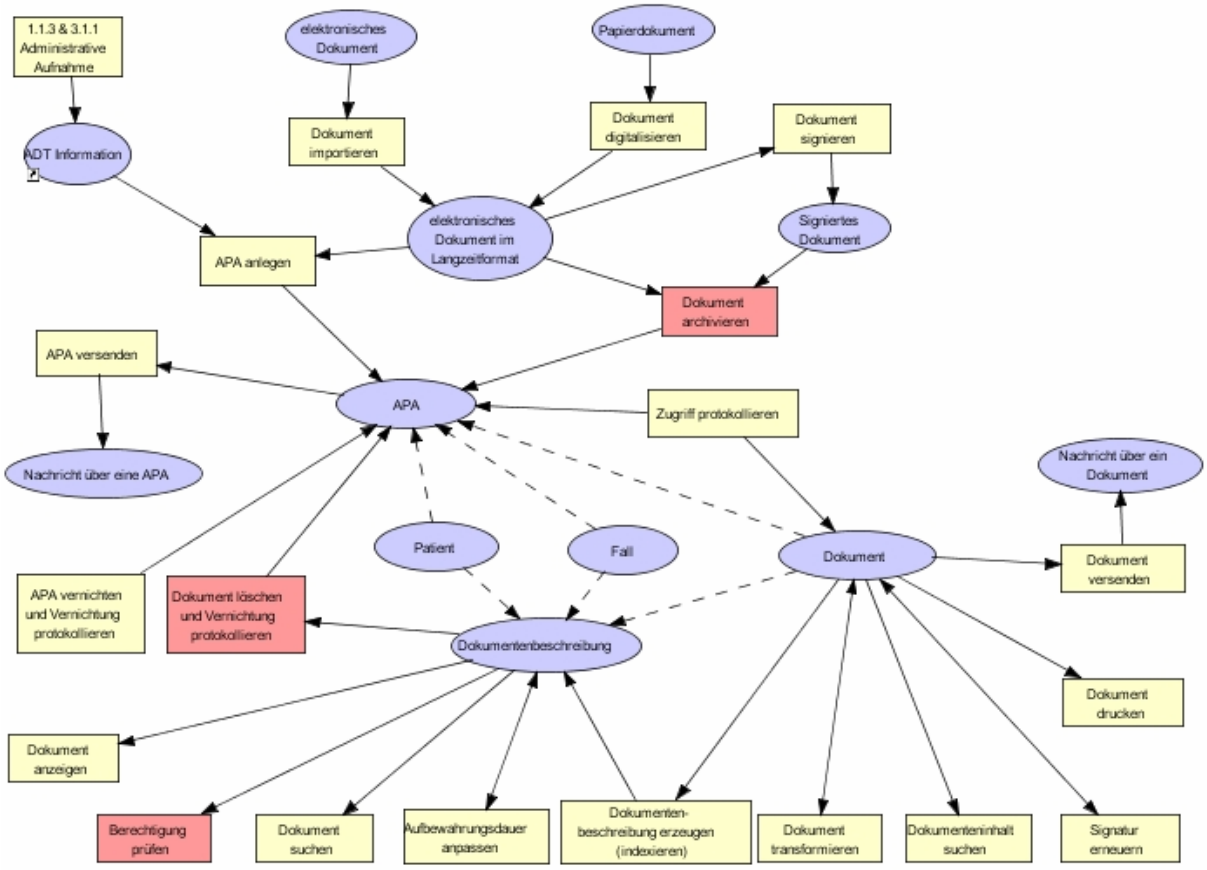


Abbildung 5-10: Fachliche Ebene der EMC Centera

5.4.3 Logische Werkzeugebene

5.4.3.1. Anwendungsbausteine

Für das Management der EMC Centera wird die auf Linux basierende Betriebssoftware CentraStar eingesetzt. Zu den Aufgaben der Software gehören

- die Ablage und das Wiederauffinden von Dokumenten sowie
- die Berechnung und Zuordnung einer eindeutigen Adresse (CA) für jedes Dokument.

Um eine hohe Verfügbarkeit der archivierten Daten zu gewährleisten, stellt die Software CentraStar Funktionen bereit, die eine

- selbstständige Fehlerbehebung
- automatische Konfiguration
- unterbrechungsfreie Wartung und Upgrades und
- die Selbstverwaltung

durch die EMC Centera ermöglichen. Weiterhin wird jedes Dokument in der EMC Centera gespiegelt. Ist ein Dokument aufgrund eines Hardwarefehlers nicht verfügbar, kann auf die gespiegelte Kopie des Dokumentes zugriffen werden. Falls ein Dokument nicht wiederhergestellt werden kann, wird eine erneute Spiegelkopie erzeugt und in der EMC Centera gespeichert. Jedes Dokument wird also immer redundant vorgehalten. Diese Funktionen werden selbstständig von der Software durchgeführt und bleiben dem Anwender weitgehend verborgen.

Für die Überwachung der EMC Centera wird ein EMC Centera Viewer bereitgestellt. Der EMC Centera Viewer ist ein eigenständiges Softwaremodul, das auf jedem Windows PC installiert sein kann, der über das LAN mit den Zugriffsnodes von der Centera verbunden ist. Der Aufruf des EMC Centera Viewers erfolgt über das Login und Passwort des Administrators. Über den Viewer kann der Systemadministrator sich z.B. die verfügbare Kapazität, die Anzahl der gespeicherten Dokumente oder das Logprotokoll anzeigen lassen. In dem Logprotokoll werden alle Vorgänge, die in der EMC Centera durchgeführt wurden, aufgezeichnet. Ist das Simple Network Management Protocol (SNMP) in der EMC Centera aktiviert, können Fehler, die während einer Operation auftreten, an ein Enterprise Netzwerkmanagement System gesandt werden. Damit ist der Status der EMC Centera jederzeit überprüfbar.

Über ein CLI-Menü im EMC Centera Viewer können Zugriffsberechtigungen für alle Anwendungsbausteine, die auf die EMC Centera zugreifen möchten, definiert werden. Es ist die

- die Vergabe eines Logins und Passworts sowie
- die Definition der Berechtigungen (z.B. Dokument speichern, anzeigen, löschen) für den zugreifenden Anwendungsbaustein möglich.

Die Verwaltung und Kontrolle der einzelnen Benutzerberechtigungen erfolgt durch die Anwendungsbausteine.

5.4.3.2. Schnittstellen

Der Zugriff auf die archivierten Dokumente erfolgt über eine API, die mit dem Ablagesystem EMC Centera von EMC[2] zur Verfügung gestellt wird. Anbieter von Softwareprodukten für die digitale Archivierung müssen diese API in ihr Produkt implementieren, wenn sie die EMC Centera als Ablagesystem einsetzen möchten. Die Dokumentationen zur API[39] sind über das Internet verfügbar. Zu den Aufgaben der API gehören:

- das Speichern von Dokumenten in der EMC Centera
- die Bereitstellung von archivierten Dokumenten an einen Anwendungsbaustein (z.B. Archivierungssystem)
- die Prüfung, ob ein Dokument mit identischem Inhalt bereits auf der EMC Centera abgelegt wurde. Falls ein identisches Dokument existiert, ist eine erneute Übertragung des Dokumentes an die EMC Centera nicht notwendig.
- das Löschen von Dokumenten (z.B. nach Ablauf der Aufbewahrungsfrist)
- die Unterstützung bei Abfragen von einem Anwendungsbaustein (z.B. Welche Dokumente wurden in einem bestimmten Zeitraum in der EMC Centera abgelegt?).

Die folgende Abbildung enthält die logische Werkzeugebene der EMC Centera. Abgebildet ist die Software CentraStar, die zum Management der EMC Centera dient. Für die Überwachung der EMC Centera wird ein Viewer zur Verfügung gestellt, der eine eigenständige Softwarekomponente ist. Der Zugriff auf die archivierten Daten von einem Anwendungsbaustein (z.B. Archivierungssystem) erfolgt über die API der EMC Centera. Diese API muss der Anwendungsbaustein implementiert haben.

5.4.3.3. Darstellung der logischen Werkzeugebene der EMC Centera

Die folgende Abbildung zeigt, wie die EMC Centera auf der logischen Werkzeugebene eingebunden wird.

---

[39] Nach einer Registrierung unter http://lighthouse.emc.com ist eine Einsicht in die Dokumentation zur API möglich.

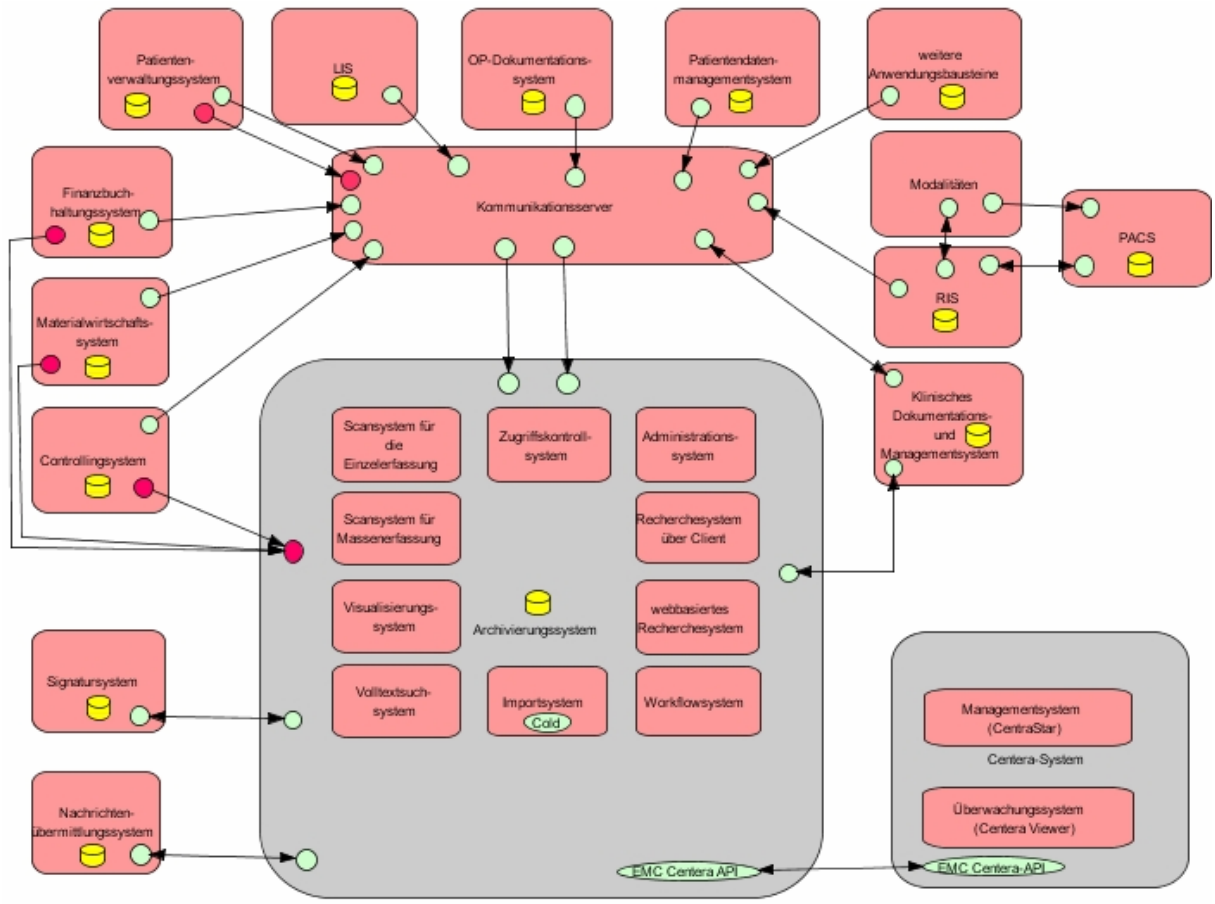


Abbildung 5-11: Logische Werkzeugebene der EMC Centera

5.4.4 Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene

In der Abbildung 9-12 im Anhang sind die Inter-Ebenen-Beziehungen zwischen der fachlichen Ebene und der logischen Werkzeugebene in einer Matrix dargestellt. Die EMC Centera erledigt die Aufgaben „Dokument archivieren“, „Dokument löschen und Vernichtung protokollieren“ und „Berechtigung prüfen“. Alle anderen Aufgaben müssen von einem anderen Anwendungsbaustein erledigt werden. Dies kann ein Archivierungssystem sein, muss aber nicht. Aus diesem Grund sind die anderen Aufgaben auch nicht dem Archivierungssystem zugeordnet.

5.4.5 Physische Werkzeugebene

Die EMC Centera basiert auf einer „Redundant Array of Independent Nodes“ (RAIN)-Technologie. Ein Knoten (Node) ist ein eigenständiger Rechner, der aus den folgenden Komponenten besteht:

- Intel Pentium 4 Prozessor mit 1 GHz RAM
- 4 Festplatten mit je 320 oder 500 GB
- 3 x 1 GB BaseT-Netzwerkkarten (zur Kommunikation mit einem Applikationsserver).

Jeder Knoten ist aus Sicherheitsgründen redundant ausgelegt. Es wird zwischen Zugriffs- und Speicherknoten unterschieden. Die Speicherknoten speichern und schützen die Daten. Die Kapazität eines Speicherknotens beträgt 900 GB netto. Die Zugriffsknoten stellen die Verbindung zwischen einem Applikationsserver und den Speicherknoten über die API der EMC Centera her. Dabei ist jeder Zugriffsknoten durch ein Ethernet-Kabel mit einem Netzwerk-Switch verbunden. Die Anzahl der Zugriffsknoten ist abhängig von der Zahl der eingesetzten Applikationsserver, die eine direkte

Kommunikation mit der EMC Centera aufbauen. Ein Zugriffsknoten kann gleichzeitig auch als Speicherknoten dienen.

Die Knoten werden in einem 19-Zoll-Schrank eingebaut. Dieser 19-Zoll-Schrank kann insgesamt bis zu 32 Knoten enthalten. Die Anzahl der Speicher- und Zugriffsknoten ist frei konfigurierbar. Erfolgt die Übergabe der zu archivierenden Daten ausschließlich über einen Kommunikationsserver, wird nur ein Zugriffsknoten benötigt. Damit können bis zu 32 Speicherknoten eingesetzt werden. Das ergibt eine maximale Speicherkapazität von ca. 64 TByte (bei Festplatten mit je 500 GB). Dabei ist zu beachten, dass alle Dokumente in der EMC Centera gespiegelt werden. Das tatsächliche zu speichernde Datenvolumen beträgt somit ca. 28 TByte pro 19-Zoll-Schrank.

Für die Speicher-Erweiterung der EMC Centera bieten sich zwei Möglichkeiten:

1. Falls in dem 19-Zoll-Schrank noch Platz ist, können weitere Speicherknoten (jeweils vier Stück pro Knoten) in den 19-Zoll-Schrank eingebaut werden. Eine Unterbrechung des Betriebes ist nicht erforderlich.
2. Ist der 19-Zoll-Schrank vollständig belegt, kann ein weiterer 19-Zoll-Schrank über ein zwei Gigabit-Ethernet-Kabel angeschlossen und mit weiteren Speicherknoten belegt werden. Über einen zusätzlichen GB-Switch können bis zu vier 19-Zoll-Schränke zu einem Cluster zusammengefügt werden.

Die zusätzlichen Speicherknoten werden automatisch erkannt. Der erweiterte Speicher ist sofort nutzbar.

Die replizierten Daten können zur Sicherheit an einem anderen Standort aufbewahrt werden als die originalen Daten. Falls es an einem Standort zu einer Katastrophe kommt (z.B. Ausfall mehrerer Speicherknoten, Zerstörung des Speichersystems durch Feuer oder Wasser), sind die Daten über das Local Area Network (LAN) oder Wide Area Network (WAN) in dem zweiten Standort weiterhin verfügbar. Somit entstehen keine Ausfallzeiten. Nach einer Reparatur der defekten Speicherknoten oder Austausch des gesamten Speichersystems können die Daten über die EMC Centera Restore Funktion aus dem entfernten Speichersystem wiederhergestellt werden. Die Wiederherstellung der Daten kann im laufenden Betrieb erfolgen.

Die folgende Abbildung enthält die physische Werkzeugebene der EMC Centera. Dargestellt sind die einzelnen 19-Zoll-Schränke (Racks), in denen die einzelnen Zugriffs- und Speicherknoten eingebaut sind. Maximal vier 19-Zoll-Schränke mit jeweils 32 Knoten können zu einem Cluster zusammengefasst werden. Die 19-Zoll-Schränke sind über einen Switch mit den einzelnen Applikationsservern verbunden.

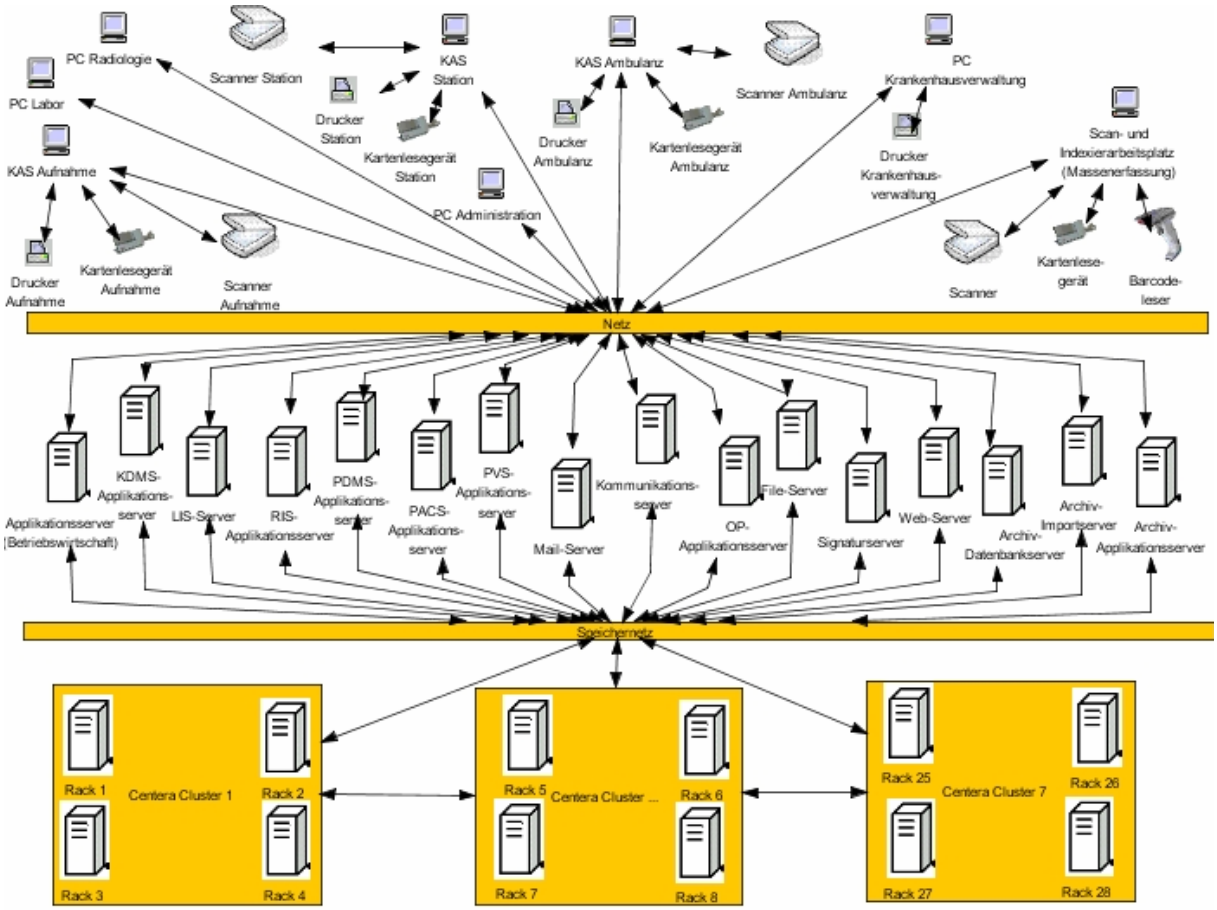


Abbildung 5-12: Physische Werkzeugebene der EMC Centera

5.4.6 Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene

Die EMC Centera verfügt nur über zwei Anwendungsbausteine. Der Anwendungsbaustein CentraStar ist auf jedem einzelnen Knoten installiert. An dem Arbeitsplatzrechner des Administrators muss der Anwendungsbaustein Centera Viewer verfügbar sein. Auf die Darstellung der Inter-Ebenen-Beziehungen in einer Matrix soll an dieser Stelle verzichtet werden.

5.4.7 Vorteile der Centera

Der Einsatz der EMC Centera bietet folgende Vorteile:

- Jedes Dokument wird nur einmal (mit Ausnahme der Spiegelkopie) in der EMC Centera abgelegt. Die Mehrfachablage von identischen Dokumenten wird vermieden.
- Die Daten werden unveränderbar unter Einhaltung der Aufbewahrungsfristen in der EMC Centera gespeichert. Sobald der Inhalt eines Dokumentes geändert wird, erzeugt die EMC Centera ein neues CDF mit einer neuen CA. Das geänderte Dokument wird wie ein neues Objekt in der EMC Centera behandelt. Das Originaldokument bleibt unveränderbar. Damit wird die Integrität der Daten gewährleistet und die Versionskontrolle unterstützt.
- Nach Ablauf der Aufbewahrungsfrist können die Dokumente gelöscht werden. Die Aufforderung, ein Dokument zu löschen, muss stets durch einen Anwendungsbaustein erfolgen. Der freie Speicherplatz wird wieder zur Verfügung gestellt.
- Die Shredding-Funktion ermöglicht die eindeutige und unwiederbringliche Löschung von Daten nach Ablauf der Aufbewahrungsfrist. Die Daten werden dabei mehrfach überschrieben.

- Aufgrund der Selbstverwaltung und automatischen Konfiguration der EMC Centera entfallen aufwendige Administrationstätigkeiten. Ein manuelles Backup der EMC Centera ist aufgrund der redundanten Datenhaltung nicht notwendig. Die Speicherverwaltung erfolgt selbstständig durch die EMC Centera. Upgrades werden ohne Unterbrechung des Betriebes durchgeführt.
- Das EMC Centera-System überwacht permanent die Datenintegrität, um Fehler zu erkennen und automatisch zu beheben. Falls bei der Überwachung ein fehlerhaftes Datenobjekt erkannt wird, erzeugt die EMC Centera automatisch eine erneute Kopie von dem redundanten Datenobjekt, das fehlerfrei ist. Damit wird sichergestellt, dass zu jeder Zeit das originale Datenobjekt und eine Spiegelkopie verfügbar sind. Die Aktionen werden in einem Log-File protokolliert.
- Durch die Replikation der Daten wird eine hohe Verfügbarkeit gewährleistet. Die Daten können dabei auf bis zu drei EMC Centera Systemen redundant vorgehalten werden.
- Der Speicher der EMC Centera ist zukünftig bis in den PetaByte Bereich erweiterbar. Die EMC Centera erkennt und konfiguriert den zusätzlichen Speicher automatisch.
- Ein gleichzeitiger Zugriff auf die archivierten Daten von verschiedenen Anwendungsbausteinen ist möglich.

Die EMC Centera ist als Ersatz für die optischen Speichermedien zu betrachten. Ein wesentlicher Vorteil ist die Online-Verfügbarkeit der Daten. Im Vergleich zu den optischen Speichermedien bietet die EMC Centera wesentlich schnellere Zugriffszeiten. Während die Zugriffszeiten bei optischen Speichermedien zwischen 10 und 30 Sekunden liegen, sind die Daten laut Aussage von EMC^2 in ca. 0,5 bis 1 Sekunde verfügbar.

Die Anschaffungskosten für die EMC Centera sind im Vergleich zu optischen Speichermedien jedoch nicht ganz unerheblich. Ab ca. 3 Jahren rechnet sich der Einsatz der EMC Centera in einem Unternehmen (z.B. Krankenhaus).

5.4.8 Internationaler Einsatz der EMC Centera im Gesundheitswesen

Die langfristige Aufbewahrung von Patientenunterlagen hat auch in anderen Ländern eine zentrale Bedeutung. In diesem Abschnitt soll der Einsatz der EMC Centera in den USA am Beispiel des Memorial Herman Healthcare Systems, welches ein Referenzkunde von EMC^2 ist, vorgestellt werden.

Das Memorial Hermann ist ein Gesundheitsversorger mit insgesamt 12 Krankenhäusern und verschiedenen spezialisierten Facheineinrichtungen. Für die Aufbewahrung der Daten wurde zunächst ein optisches Speichersystem eingesetzt. Aufgrund der ständig wachsenden Datenmengen stießen die optischen Speichermedien jedoch schnell an ihre Kapazitätsgrenzen. Die Zugriffszeiten auf die archivierten Daten stiegen mit dem Datenvolumen an und betrugen teilweise bis zu einer Minute. Ein weiterer Nachteil bestand darin, dass bei Problemen das optische Speichersystem Offline gesetzt werden musste, um die Fehler zu beheben. In dieser Zeit war ein Zugriff auf die archivierten Daten nicht möglich.

Im Jahr 2004 wurde das optische Speichersystem durch die EMC Centera von EMC^2 abgelöst. Die Centera wird im Memorial Hermann zur Ablage von Dokumenten und medizinischen Bildern eingesetzt. Die medizinischen Bilder werden in einem PACS und in einem kardiovaskulären Bildsystem erzeugt und anschließend zur langfristigen Aufbewahrung an die EMC Centera übergeben. Die EMC Centera wurde zunächst mit einem anfänglichen Speichervolumen von insgesamt 32 TByte ausgestattet. Bei der Planung des Speichersystems wurde davon ausgegangen, dass jährlich ca. 40 Millionen Bilder neu erzeugt werden. Die Bilder haben dabei eine Größe zwischen 30 KB und einem MB pro Seite. Die Zugriffszeiten betragen bei ca. 4500 Nutzern eine Sekunde und sind somit im Vergleich zu dem optischen Speichersystem wesentlich schneller. Bei der Aufbewahrung wird besonderer Wert auf die Einhaltung der gesetzlicher Anforderungen, die sich aus dem „Health Insurance Portability Act“ und der „Joint Commision on Accreditation of Healthcare Organizations“ ergeben, gelegt.

6 Vergleich der Modelle

Im Kapitel 5 wurde gezeigt, dass aus dem Referenzmodell durch geeignete Modifikationen, Einschränkungen oder Ergänzungen konkrete Modelle abgeleitet werden können. Da die Modelle aus demselben Referenzmodell abgeleitet wurden, ist ein Vergleich der einzelnen Produkte möglich. Bereits bei der Modellierung konnte festgestellt werden, dass sich das Produkt EMC Centera deutlich von den anderen Produkten unterscheidet. Die EMC Centera ist ein Ablagesystem, während die anderen drei Produkte zu den Archivierungssystemen gehören. Archivierungssysteme werden auf der logischen Werkzeugebene dargestellt. Das Ablagesystem ist auf der physischen Werkzeugebene zu finden. Beide Komponenten sind jedoch Bestandteil des digitalen Archivs, die sich bei der Erledigung der Aufgaben ergänzen.

6.1 Vergleich der fachlichen Ebene

Im Anhang in Abbildung 9-13 sind die fachlichen Ebenen von den Produkten der einzelnen Anbieter gegenübergestellt. Das sich das Ablage- und Archivierungssystem in den Aufgaben ergänzen, wird durch die gelb dargestellten Aufgaben verdeutlicht. Die Aufgabe „Dokument archivieren“ wird nur von der EMC Centera erledigt. Dagegen werden Aufgaben wie z.B. „Dokument anzeigen“, „Dokument suchen“, „Dokument drucken“, „Signatur erneuern“ und „Dokument versenden“ von einem Archivierungssystem erledigt. Die Aufgabe „Dokument löschen und Vernichtung protokollieren“ ist nur in Zusammenarbeit mit dem Archivierungssystem möglich. Die EMC Centera übernimmt kein selbstständiges Löschen. Der Löschvorgang muss immer von einem Anwendungsbaustein, in diesem Fall das Archivierungssystem, initiiert werden. Auch bei der Erledigung der Aufgabe „Berechtigung prüfen“ gibt es Unterschiede. Während das Archivierungssystem die Benutzerberechtigung überprüft, kontrolliert die EMC Centera die Berechtigung des zugreifenden Anwendungsbausteins. Ein Vergleich der einzelnen Produkte mit der EMC Centera ist an dieser Stelle nicht sinnvoll. Die EMC Centera ist als Ergänzung zu den anderen drei Produkten zu betrachten. Aus diesem Grund werden nur die Produkte d.3, HYDMedia und forcont factory mit dem Referenzmodell verglichen.

Die drei genannten Produkte erledigen im Wesentlichen die gleichen Aufgaben. Ein Unterschied besteht bei der Erledigung der Aufgabe „Aufbewahrungsdauer anpassen“. Eine Anpassung der Aufbewahrungsdauer ist nur im d.3-System und in HYDMedia möglich. In dem Produkt forcont factory ist eine nachträgliche Anpassung der Aufbewahrungsdauer nicht vorgesehen. Die Aufbewahrungsdauer wird zum Zeitpunkt der Archivierung als ein einmaliges Ereignis übermittelt und am Dokument verankert. Damit ist die Aufbewahrungsdauer genauso unveränderlich wie das Dokument selbst. Aus diesem Grund ist diese Aufgabe auch nicht in der fachlichen Ebene des Produktes forcont factory dargestellt. In HYDMedia erfolgt eine automatische Anpassung der Aufbewahrungsdauer mit dem letzten Patientenkontakt. Im d.3-System kann die Aufbewahrungsdauer zu einem Dokument manuell verändert werden, z.B. durch das Ausführen einer speziellen Funktion.

In HYDMedia fehlen auf der fachlichen Ebene die Aufgaben „Dokument versenden“ und „APA versenden“. Diese Aufgaben werden nicht unterstützt. Aus datenschutzrechtlichen Gründen ist lediglich ein Export der Dokumente möglich.

Die Erneuerung der Signatur gemäß dem ArchiSig-Konzept wurde bereits in den Produkten HYDMedia und forcont factory umgesetzt. Im d.3-System wird an der Realisierung dieser Aufgabe gearbeitet. Es ist geplant, dass diese Aufgabe mit dem nächsten Releasewechsel vom d.3-System erledigt wird. Aus diesem Grund ist die Aufgabe in der fachlichen Ebene von d.3 grau dargestellt.

Da das TransiDoc-Projekt noch nicht abgeschlossen ist, kann die Aufgabe „Dokument transformieren“ zurzeit von keinem Anbieter erfüllt werden.

In der forcont factory gibt es keine Unterscheidung zwischen archivierten und lebenden Dokumenten. Es wird generell von einer EPA gesprochen. Dagegen werden Dokumente, die nicht mehr verändert

werden, in HYDMedia und im d.3-System in einer APA dargestellt. Auf der fachlichen Ebene wird dies durch die Objekttypen EPA bzw. APA unterschieden.

6.2 Vergleich der logischen Werkzeugebene

Wesentliche Unterschiede zwischen den einzelnen Produkten ergeben sich auf der logischen Werkzeugebene. Im Vergleich mit dem Referenzmodell ist zu erkennen, welche Anwendungsbausteine zusätzlich sind bzw. welche fehlen. Die logischen Werkzeugebenen sind im Anhang in Abbildung 9-14 gegenübergestellt. Die Unterschiede und Gemeinsamkeiten der einzelnen Produkte gegenüber dem Referenzmodell sollen im Folgenden erläutert werden.

Das d.3-System verfügt über die gleichen Teilmodule wie das Archivierungssystem im Referenzmodell. Zusätzlich werden die folgenden Module angeboten:

- ein öffentliches Recherchesystem
- ein Offline-Archivsystem
- ein Content Service System.

Weiterhin wird ein Klassifizierungssystem zur Verfügung gestellt, dass zusammen mit dem Scansystem eingesetzt wird, aber ein eigenständiges Softwaremodul ist. Für den dialogbasierten Import von Dokumenten, die mit einer Windows-Anwendung erstellt wurden, wird ein weiteres Importmodul als Teil des Standard-Rechercheclients d.explorer bereitgestellt. Das d.3-System unterstützt den Empfang von ADT-Nachrichten im HL7-Nachrichtenformat. Dabei werden jedoch nur die HL7-Nachrichten im Archivierungssystem konfiguriert, die in dem jeweiligen Krankenhaus zur Kommunikation verwendet werden. Weiterhin wird gerade an der Implementierung der DICOM-Dienstklassen „Query/Retrieve Service Class“ und „Storage Service Class“ gearbeitet. Damit sind der Empfang und der Abruf von medizinischen Bildern aus einem PACS möglich.

Das Produkt HYDMedia besitzt kein eigenes Modul zur Unterstützung von Workflowfunktionalitäten, da diese in der Regel von anderen Anwendungsbausteinen bereitgestellt werden. Ob HYDMedia über ein Volltextsuchsystem verfügt, ist nicht bekannt. Für den Import der Dokumente gibt es ein zentrales Importsystem. Um die Daten und Dokumente jedoch in einem standardisierten Dateiformat an das zentrale Importsystem zu übergeben, werden weitere Importmodule bereitgestellt. Zu diesen gehören:

- ein Office-Importsystem
- ein COLD-System und
- ein Importsystem, dass die Übernahme von elektronischen Dokumenten, die von externen Personen bereitgestellt werden, ermöglicht.

Ein weiteres Zusatzmodul ist das Remotesystem, an dem Dokumente für den externen Zugriff freigegeben werden können. Für die Ansicht der Dokumente werden insgesamt vier Visualisierungssysteme angeboten, von denen zwei unabhängig von einem anderen Anwendungsbaustein aufgerufen werden können. Die anderen zwei Visualisierungssysteme können über die COM-Schnittstelle in die Benutzeroberfläche eines beliebigen Anwendungsbausteins integriert werden. In der Abbildung 9-14 ist die Integration der Visualisierungssysteme in das KDMS dargestellt. Mit der Schnittstelle HYDRad sind der Empfang und die Abfrage von medizinischen Bildern im DICOM-Format möglich. Es wird der Empfang von HL7-Nachrichten (ADT-Nachrichten) über den Kommunikationsserver unterstützt.

In dem Produkt forcont factory wird davon ausgegangen, dass bestimmte Anwendungsbausteine in einem Unternehmen schon existieren und diese somit in die forcont factory integriert werden können. Auf der logischen Werkzeugebene sind diese Anwendungsbausteine gelb dargestellt. Damit soll ausgedrückt werden, dass Anwendungsbausteine von Drittanbietern genutzt werden. Es gibt keine eigenen Module, die das Digitalisieren und die Anzeige der Dokumente unterstützen. Die Anzeige der Dokumente erfolgt über das Visualisierungssystem, das vom jeweiligen Betriebssystem des Arbeitsplatzrechners bereitgestellt wird. Für das Digitalisieren von Dokumenten wird auf Scansysteme zurückgegriffen, die im Unternehmen eingesetzt werden. Falls noch kein Scansystem im Einsatz ist,

wird das Scansystem KOFAX Ascent Capture empfohlen. Zur Unterstützung der Volltextsuche wird das Volltextsuchsystem Inter:gator der Firma interface GmbH angeboten. Es können jedoch auch Volltextsuchsysteme von anderen Anbietern eingesetzt werden. Weiterhin ist eine Recherche in der forcont factory nur über das webbasierte Recherchesystem oder aus dem führenden Informationssystem möglich. Ein eigener Rechercheclient wird nicht zur Verfügung gestellt. Die forcont factory besitzt keine zertifizierte SAP ArchiveLink-Schnittstelle. Der Empfang von medizinischen Bildern im DICOM-Format ist nur über den Kommunikationsserver möglich. ADT-Nachrichten können im HL7-Format direkt an das Archivierungssystem kommuniziert werden.

Allerdings gibt es auch Gemeinsamkeiten zwischen dem Referenzmodell und dem speziellen Modell der forcont factory. Zu den Gemeinsamkeiten gehört die Bereitstellung

- eines Zugriffskontrollsystems
- eines Administrationssystems
- eines Importsystems
- eines Workflowsystems sowie
- eines webbasierten Recherchesystems.

Die EMC Centera ist über eine API mit dem Archivierungssystem verbunden und stellt ein Management- und Überwachungssystem als Anwendungsbausteine bereit. Um mit der EMC Centera zu kommunizieren, muss das Archivierungssystem die API der EMC Centera implementiert haben. Die Archivierungssysteme d.3, HYDMedia und forcont factory stellen grundsätzlich eine Schnittstelle für die Einbindung eines Ablagesystems bereit. Alle drei Produkte unterstützen die Einbindung der EMC Centera als Ablagesystem. Über die API der EMC Centera übergibt das Archivierungssystem die Dokumente zur Aufbewahrung. Die Archivierung des Dokumentes erfolgt durch die EMC Centera. Wird ein Dokument benötigt, muss dies vom Archivierungssystem angefordert werden.

6.3 Vergleich der physischen Werkzeugebene

In der Abbildung 9-15 im Anhang sind die physischen Werkzeugebenen der einzelnen Produkte gegenübergestellt. Anhand dieser Abbildung ist zu erkennen, wie sich das Ablagesystem der EMC Centera auf der physischen Werkzeugebene einfügt. Die EMC Centera ist ein Online-Ablagesystem, das gleichzeitig die langfristige Aufbewahrung von unveränderlichen Daten unterstützt. Damit übernimmt sie die Aufgabe eines elektronischen Kurz- und Langzeitspeichers.

Die Hardware ist kein Bestandteil der Softwareprodukte d.3, HYDMedia und forcont factory. Trotzdem werden für die Installation entsprechende Hardwarekomponenten benötigt. Alle drei Produkte sind unabhängig vom jeweiligen Betriebssystem einsetzbar. Grundsätzlich werden ein Applikations- und ein Datenbankserver benötigt. In Abhängigkeit von der Anzahl der gleichzeitigen Zugriffe und der Auslastung des Servers durch Prozesse können die Serverapplikationen und die Datenbank auf einem Server installiert sein. Dies ist jedoch für jedes einzelne Krankenhaus zu prüfen. Da alle drei Produkte webbasierte Komponenten anbieten, ist ein Web-Server erforderlich. Der Massenimport von Dokumenten kann über einen Importserver erfolgen. Welches Ablagesystem eingesetzt wird, liegt bei allen drei Produkten in der Entscheidung des Kunden. Die Inter-Ebenen-Beziehungen des Produktes forcont factory zeigen (vgl. Abbildung 9-11), dass die Teilmodule mit Ausnahme der Scansysteme nur auf Servern installiert sind. Damit sind zunächst keine zusätzlichen Installationen an den Arbeitsplatzrechnern notwendig. Bei den Produkten d.3 oder HYDMedia kann die Recherche über einen Rechercheclient oder auch wie in der forcont factory webbasiert erfolgen. Entscheidet sich ein Krankenhaus für den Einsatz des Rechercheclients, ist eine Installation an den entsprechenden Arbeitsplatzrechnern erforderlich.

7 Archivierung im internationalen Raum

Bereits in [Ameh et al. 2002] wird beschrieben, wie wichtig die Aufbewahrung und der Abruf von medizinischen Informationen ist. Die Autoren berichten in diesem Artikel über ihre Erfahrungen, die sie mit der Aufbewahrung und dem wieder auffinden von chirurgischen Akten in Entwicklungsländern gesammelt haben. In diesen Ländern sind die wenigsten Krankenhäuser mit Computern ausgestattet. Die Suche nach medizinischen Dokumenten ist schwierig. Die Vollständigkeit der Akten ist nicht immer gegeben. Aus diesem Grund empfehlen die Autoren den Einsatz von Computern zumindest in größeren Krankenhäusern, um die elektronische Speicherung und das Wiederauffinden der medizinischen Informationen zu unterstützen. Die Aufbewahrung von medizinischen Akten hat laut [Ameh et al. 2002] einen entscheidenden Einfluss auf die Patientenversorgung, Audits sowie Lehre und Forschung. Nachstehend einige Betrachtungen zu Herangehensweisen in Belgien, Österreich und den USA.

7.1 Belgien

In Belgien hat die Archiv-Arbeitsgruppe der Belgischen Telematik-Kommission „Norms for Telematics in the healthcare sector“ untersucht, wie die langfristige Aufbewahrung von Patientenakten im Krankenhausbereich erfolgen kann. Bei der Aufbewahrung wird nicht zwischen elektronischen, fotographischen oder papierbasierten Patientenakten unterschieden. Die Belgische Telematik-Kommission hat eine Empfehlung für die Langzeitaufbewahrung von Patientenakten in einem Krankenhaus erarbeitet, die in Anlehnung an [Belgian Telematics Commission 2004] vorgestellt werden soll:

1. Die Dokumente in einer Patientenakte sollten das Datum sowie den Autoren enthalten.
2. Bei der Speicherung der Dokumente sollten Techniken verwendet werden, die eine Veränderung der Daten ausschließen.
3. Es wird empfohlen, die gesamte Patientenakte gemäß dem Civil Code (Artikel 2262 § 2 des Civil Code) mindestens 20 Jahre seit dem letzten Kontakt mit dem Patienten in der Einrichtung aufzubewahren. Der letzte Patientenkontakt ist definiert als das Entlassungsdatum des Patienten aus dem Krankenhaus oder das Datum des letzen Besuches in einer Ambulanz.
4. In den Patientenakten sollten mindestens der Entlassungsbrief des stationären Patienten, die Besuchsberichte von ambulanten Patienten, Pathologie- und Operationsberichte aufbewahrt werden. Weiterhin werden die Aufbewahrung der letzten Problemliste eines Patienten sowie die Aufbewahrung von spezifischen Auswertungen von Diagnosen empfohlen.
5. Für die Aufbewahrung der Patientenakten in einem Krankenhaus ist der Chefarzt verantwortlich. Bei der Aufbewahrung muss die Sicherheit, Zulässigkeit, Vertraulichkeit und die Verfügbarkeit gewährleistet sein. Die Patientenakten können dabei auch außerhalb des Krankenhauses aufbewahrt werden.
6. Die Dokumente einer Patientenakte können elektronisch (EPA), fotographisch (Bilder, Mikrofilme) oder papierbasiert sein. Bei der Konvertierung von Dokumenten (z.B. die Umwandlung eines Papierdokumentes in die elektronische Form) müssen Techniken eingesetzt werden, die die Integrität des Dokumentes und die Authentizität des Konvertierungsergebnisses gewährleisten. Für die Langzeitaufbewahrung von Dokumenten wird der Einsatz von nur einmal beschreibbaren Speichermedien empfohlen (z.B. CD, Mikrofilm).
7. Es sollten Möglichkeiten für die Aufbewahrung der Patientenakten in allgemeinen Archiven des Königreiches Belgien untersucht werden.

7.2 Österreich

Die folgenden Informationen stammen aus einem eigens entwickelten Fragebogen, der von den nachfolgend aufgeführten Krankenhäusern beantwortet wurde. Weiterhin standen diese Krankenhäuser für Fragen zur Verfügung. Anhand dieser Krankenhäuser soll ein Einblick in mögliche Archivierungsformen in Österreich gegeben werden. Die Reihenfolge der Krankenhäuser ist zufällig gewählt.

In Österreich liegen die Aufbewahrungsfristen von medizinischen Dokumenten zwischen 10 (ambulante Patientenakten) und 30 Jahren (stationäre Patientenakten). Die archivierten Patientenunterlagen müssen innerhalb dieser Aufbewahrungsdauer lesbar zur Verfügung gestellt werden. Bei der Archivierung von Patientenunterlagen sind vor allem das Bundesgesetz über die Kranken- und Kuranstalten, die Landesgesetze für Krankenanstalten sowie das Datenschutzgesetz zu beachten. Elektronische Dokumente sind in Österreich rechtlich anerkannt und als Beweismittel vor Gericht akzeptiert. Damit können die Papierdokumente nach dem Einscannen vernichtet werden. In Österreich werden die Patientenunterlagen sowohl auf die konventionelle Art als auch in elektronischer Form aufbewahrt.

An den Universitätskliniken des Allgemeinen Krankenhauses Wien (AKH) erfolgt die Archivierung der Patientenunterlagen über die Abteilung Medizinisches Dokumentationszentrum (ADZ). Das Medizinische Dokumentationszentrum hat die Aufgabe, die Patientendokumentationen mittels physischer und digitaler Archivierung an den Kliniken und Instituten des AKH sowie für die Wissenschaft und Forschung bereitzustellen [AKH]. Die digitale Archivierung kommt seit 1994 im AKH zum Einsatz. Gemäß § 17 Abs. 2 Wiener Krankenanstaltengesetz sind die Krankengeschichten nach ihrem Abschluss in Form von Mikrofilmen oder in gleichwertiger Weise in doppelter Ausfertigung aufzubewahren. Von den insgesamt 27 Universitätskliniken nutzen derzeit 21 die digitale Archivierung. Die an die digitale Archivierung angebundenen Kliniken lagern die aktuellen papierbasierten Krankengeschichten nach durchschnittlich 6 bis 12 Monaten aus. Das Medizinische Dokumentationszentrum bereitet die Papierdokumente zum Scannen vor (Entfernung der Klammern), scannt die Dokumente ein und führt anschließend eine Qualitätskontrolle durch. Bei der Qualitätskontrolle werden die eingescannten Dokumente auf Lesbarkeit und Vollständigkeit überprüft. Falls die Lesbarkeit und Vollständigkeit nicht erfüllt ist, werden die Dokumente noch einmal mit einer anderen Einstellung gescannt. Die eingescannten Dokumente werden in einem zentralen Ablagesystem archiviert. Nach der Qualitätskontrolle erfolgt die Freigabe der eingescannten Dokumente. Die Originalakten werden im Anschluss datenschutzgerecht entsorgt. Die eingescannten Dokumente entsprechen dem Original und sind vor Gericht als Beweismittel zulässig. Im Jahr 2005 wurden insgesamt 13 Millionen Seiten erfasst. Die elektronischen Dokumente können an den jeweiligen Kliniken über den Arbeitsplatzrechner abgefragt werden. Jede Klinik hat einen Zugriff auf die eigenen elektronischen Dokumente. Die eingescannten Dokumente werden sowohl in einer Jukebox als auch in einer Tape Library gespeichert. Die Verwaltung und Aufbewahrung der papierbasierten Patientenakten erfolgt ebenfalls durch das Medizinische Dokumentationszentrum. Zurzeit werden ca. 7 Millionen Patientendokumentationen durch das Medizinische Dokumentationszentrum verwaltet. Altakten werden weiterhin in physischer Form aufbewahrt. Mit der Einführung der digitalen Archivierung hat sich die Anzahl der physischen Krankengeschichten im AKH reduziert. Bei der digitalen Archivierung der Patientenunterlagen wird die elektronische Signatur nicht verwendet.

Im Landeskrankenhaus Bad Ischl erfolgt die langfristige Archivierung von Patientenunterlagen in elektronischer Form. Als elektronischer Kurzzeitspeicher kommt ein RAID-System zum Einsatz. Für die elektronische Langzeitspeicherung wird eine robotergesteuerte Tape Library verwendet. Pro Jahr werden ca. 100000 Dokumenten erzeugt, die zu archivieren sind. Dabei werden ca. 70 % der Dokumente elektronisch erzeugt. Elektronische Dokumente werden mittels einer Befundfreigabe vom verantwortlichen Arzt elektronisch signiert und somit freigegeben. Papierdokumente werden eingescannt und anschließend elektronisch zur Verfügung gestellt. Die Originaldokumente werden nach erfolgter Qualitätskontrolle vernichtet. Bei der Qualitätskontrolle werden pro Charge Stichproben kopiert und verglichen. Für die Verwaltung der Dokumente wird ein elektronisches Retrieval-System eingesetzt.

Im Donauspital in Wien werden die Patientenakten sowohl in Papierakten als auch in elektronischer Form aufbewahrt. Das jährlich zu archivierende Datenvolumen liegt bei ca. 3 Millionen Dokumenten. Die langfristige Archivierung der elektronischen Dokumente erfolgt auf einem festplattenbasierten System sowie auf einer Jukebox.

In den Salzburger Landeskliniken werden jährlich ca. 5 Millionen archivierungspflichtige Dokumente erzeugt. Die Dokumentation erfolgt zu 97% papierbasiert. Die während eines Aufenthaltes erstellten Befunde und Patientenunterlagen werden zunächst ausgedruckt und in einer Krankenakte gesammelt. Nach der Entlassung eines Patienten muss die Krankenakte vom Arzt als abgeschlossen gekennzeichnet werden. Erst dann ist die papierbasierte Krankenakte zur Archivierung freigegeben. Bei der Archivierung werden alle vorliegenden Dokumente der Krankenakte mit Unterschrift und sonstigen handschriftlichen Ergänzungen von einer eigenen Abteilung eingescannt und elektronisch abgelegt. Das Salzburger Krankenanstaltengesetz schreibt vor, dass die Krankengeschichten nach ihrem Abschluss mindestens 30 Jahre, allenfalls in Form von Mikrofilm in doppelter Ausfertigung, oder auf anderen gleichwertigen Informationsdatenträgern, deren Lesbarkeit für den Aufbewahrungszeitraum gesichert sein muss, aufzubewahren sind. Gleichwertige Informationsdatenträger sind elektronische Datenträger, die eine Unveränderbarkeit der Daten wie der Mikrofilm gewährleisten. In den Salzburger Landeskliniken werden die Krankenakten seit 1995 auf CD archiviert. Die digitalisierte Krankenakte wird in doppelter Ausfertigung auf CD gebrannt und für den elektronischen Zugriff auf ein Plattensystem kopiert. Das Plattensystem wird noch einmal auf Band gesichert. Damit existiert nach dem Einscannen jede Akte viermal. Falls Dokumente nachträglich zu der digitalisierten Krankenakte hinzuzufügen sind, werden diese Dokumente als eigene Akte unter der gleichen Aufnahmezahl und dem gleichen Aufnahmedatum im digitalen Archiv mit einem administrativen Merkmal gespeichert. Jede archivierte Krankenakte wird mit einem Schlussdokument versehen, das die Vorgehensweise bei der Archivierung der Krankenakte dokumentiert. Die eingescannten Dokumente gelten als Original. Die papierbasierte Krankenakte wird nach dem Scannen vernichtet. Vor Gericht gab es bisher keinen Einwand bzgl. der Anerkennung der elektronischen Dokumente. Im Jahre 2005 wurden die ersten CDs aus Sicherheitsgründen auf neue Datenträger kopiert. Die Verwaltung der archivierten Dokumente erfolgt mit Hilfe einer SQL-Datenbank. Die elektronische Signatur wird in den SLK noch nicht eingesetzt.

Im Bezirkskrankenhaus Schwaz werden die Patientenunterlagen in Papierakten langfristig aufbewahrt. Das jährlich zu archivierende Datenvolumen liegt bei ca. 200000 Dokumenten.

7.3 USA

In den USA gibt es eine Vielzahl von Gesetzen die sich mit der Erstellung, Speicherung, dem Zugriff, der Verwaltung und der Aufbewahrung von Aufzeichnungen über längere Zeiträume befassen [Archivas 2004]. Für die Aufbewahrung von Aufzeichnungen im Gesundheitswesen ist insbesondere auf die Einhaltung des „Health Insurance Portability and Accountability Act" (HIPAA) zu achten. Von diesem Gesetz sind alle Einrichtungen betroffen, die Gesundheitsinformationen erzeugen (z.B. Krankenhäuser, Apotheken, Pflegeeinrichtungen) oder empfangen (z.B. Krankenkassen, öffentliche Gesundheitsbehörden). Dieses Gesetz wurde 1996 vom Kongress erlassen. Mit dem zunehmenden Einsatz von webbasierten Anwendungen, die den Zugriff auf elektronische Gesundheitsinformationen ermöglichen, bestand die Notwendigkeit, allgemein anerkannte Richtlinien zum Schutz von Gesundheitsinformationen zu entwickeln [CMS 2004]. Um die Vertraulichkeit, Integrität und Verfügbarkeit von Patientendaten in elektronischer Form zu gewährleisten, wurden im Rahmen des „Health Insurance Portability and Accountability Act" (HIPAA) nationale Standards zum Schutz der Sicherheit und Vertraulichkeit von Patientendaten erarbeitet. Bei der Aufbewahrung von Patientenunterlagen ist besonders auf die Einhaltung der Sicherheits- und Privatsphärenstandards zu achten, die zwei wesentliche Regeln des HIPAA-Gesetzes im Abschnitt zwei „Administrative Simplification" darstellen. Die Bestimmungen zum Schutz der Privatsphäre regeln, wer auf die Gesundheitsinformationen zugreifen darf. Nach [U.S. Department of Health and Human Services] sind

- Informationen, die von Ärzten, Krankenschwestern und anderen Dienstleistern im Gesundheitswesen in der medizinischen Akte abgelegt wurden

- Konsultationen und Gespräche eines Arztes über die Behandlung seines Patienten mit anderen Ärzten oder Krankenschwestern
- Informationen über den Patienten, die im Computer gespeichert sind sowie
- Rechnungsinformationen zu einem Klinikaufenthalt

zu schützen. Die Richtlinie zum Schutz der Privatsphäre gilt für alle Patienteninformationen. Dabei spielt es keine Rolle, ob die Patienteninformationen in elektronischer Form oder auf Papier vorliegen. Auch für mündliche Patienteninformationen sind die Bestimmungen einzuhalten. Die Sicherheitsrichtlinie bezieht sich dagegen nur auf Patienteninformationen, die in elektronischer Form vorliegen. Dazu gehören die Erstellung, der Empfang, die Verwaltung und die Übertragung von Patienteninformationen. Die Sicherheitsrichtlinie enthält administrative, physische und technische Maßnahmen, die zum Schutz der Gesundheitsinformationen zu treffen sind. Die Maßnahmen sollen im Folgenden in Anlehnung an [Federal Register 2003] vorgestellt werden.

Die physischen Maßnahmen dienen zum Schutz von elektronischen Informationssystemen. Sie beinhalten u.a.

- die Einrichtung von Zugangskontrollen
- Maßnahmen zum Schutz des Arbeitsplatzrechners (z.B. Ausloggen am Arbeitsplatzrechner)
- physischer Schutz des Arbeitsplatzrechners vor unbefugten Zugriffen
- Verfahren zur Handhabung von elektronischen Datenträgern (z.B. Entsorgung, Wiederverwendung, Datenwiederherstellung, Datenspeicherung).

Die technischen Maßnahmen enthalten Bestimmungen für:

- Zugriffskontrollen: Die Zugriffskontrolle fordert eine eindeutige Benutzeridentifizierung sowie Zugriffsverfahren im Notfall.
- Auditkontrollen: Auditkontrollen dienen zur Aufzeichnung und Untersuchung von Aktivitäten in einem elektronischen Informationssystem.
- Integrität: Unter diesen Begriff werden Mechanismen verstanden, die die Integrität der Daten gewährleisten.
- Personenidentifizierung: Die Personenidentifizierung erfolgt mit Hilfe von Mechanismen, die gewährleisten, dass die Person auch wirklich diejenige ist, als die sie sich ausgibt.
- Übertragungssicherheit: Sicherheitsmaßnahmen, die die elektronischen Informationen bei der Übertragung in einem Netzwerk gegen unbefugte Zugriffe schützen.

Mit Hilfe der administrativen Maßnahmen erfolgt die Umsetzung der Sicherheitsstandard. Zu den administrativen Maßnahmen gehört, dass ein Sicherheitsbeauftragter festgelegt wird und regelmäßig Schulungen zur Stärkung des Sicherheitsbewusstseins der Mitarbeiter durchgeführt werden.

Digitale Archive müssen die Bestimmungen dieser beiden Richtlinien umsetzen. Die Patienteninformationen sind zum einen gegen unbefugte Zugriffe zu schützen, zum anderen muss aber auch eine sichere Aufbewahrung und Archivierung für mindestens 7 Jahre gewährleistet sein.

In den USA hat der Begriff „Compliance“ eine zentrale Bedeutung, d.h. es wird darauf geachtet, dass die gesetzlichen Vorgaben eingehalten werden. Laut [Project Consult] ist die Compliance eine der wichtigsten Marktreiber für den Einsatz von Dokumenten-Technologien.

8 Diskussion

8.1 Zielerfüllung

In diesem Kapitel werden die eingangs gestellten Fragen beantwortet, um zu prüfen, ob die im Kapitel 1.3 gestellten Ziele erreicht wurden.

Zu Ziel 1:

Ziel dieser Arbeit ist: ein 3LGM2-basiertes Referenzmodell für die digitale Archivierung von Patientenunterlagen zu erstellen.

F.1: Wie lässt sich mit Hilfe des 3LGM²-Baukastens ein Referenzmodell erstellen?

Um das Referenzmodell erstellen zu können, wurden im Kapitel 3.1 zunächst die Funktionalitäten erarbeitet, die ein digitales Archiv unterstützen sollte. Aus diesen Funktionalitäten wurden die Aufgaben abgeleitet. Anschließend wurde geprüft, welche Objekttypen auf der fachlichen Ebene darzustellen sind. Im nächsten Schritt wurde untersucht, welche Anwendungsbausteine zur Erledigung der Aufgaben benötigt werden. Zum Abschluss wurden die physischen Datenverarbeitungsbausteine der physischen Werkzeugebene ermittelt einschließlich der Inter-Ebenen-Beziehungen.

Die Erstellung eines Referenzmodells für die digitale Archivierung von Patientenunterlagen mit Hilfe des 3LGM²-Baukastens ist somit möglich.

F1.1: Welche Aufgaben und Funktionalitäten sollte ein digitales Archiv unterstützen?

Um das Referenzmodell erstellen zu können, wurden im Kapitel 3.1 zunächst die Funktionalitäten erarbeitet, die ein digitales Archiv unterstützen sollte. Zu den Grundfunktionalitäten gehören:

- die Übernahme der Daten und Dokumente aus den verschiedenen rechnerbasierten Anwendungsbausteinen eines KIS
- die ordnungsgemäße, revisionssichere Ablage und Langzeitspeicherung der Daten und Dokumente
- die Indexierung
- die Recherche nach Daten und Dokumenten
- die Anzeige, Präsentation und Reproduktion von Dokumenten
- die Administration
- das Versionsmanagement
- die Historienverwaltung
- die Erneuerung der Signatur von elektronischen Dokumenten gemäß ArchiSig-Projekt
- das Sperren bzw. Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist oder auf Bitte des Patienten.

Optional können Funktionen für das Scannen, die Erstellung der Signatur oder Programme zur Erstellung von Dokumenten angeboten werden.

Aus den Funktionalitäten können die Aufgaben abgeleitet werden. Folgende Aufgaben sollten dabei von einem digitalen Archiv unterstützt werden:

1. Archivierte Patientenakte anlegen

2. Dokument importieren
3. Dokument archivieren
4. Dokument transformieren
5. Dokument löschen und Vernichtung protokollieren
6. APA vernichten und Vernichtung protokollieren
7. Dokument suchen
8. Dokument signieren
9. Dokument versenden
10. APA versenden
11. Signatur erneuern
12. Berechtigung prüfen
13. Dokument anzeigen
14. Dokumenteninhalt suchen
15. Zugriff protokollieren
16. Dokument digitalisieren
17. Dokument drucken
18. Aufbewahrungsdauer anpassen.

Eine ausführliche Beschreibung der Aufgaben befindet sich im Kapitel 3.2.

F1.2: Welche Verfahren und Methoden zur digitalen Archivierung von Patientenunterlagen werden zurzeit in Krankenhäusern eingesetzt?

Im Zusammenhang mit den Funktionalitäten (Kapitel 3.1) und der Beschreibung der Anwendungsbausteine in einem Archivierungssystem (Kapitel 4.2.4) wurden verschiedene Verfahren und Methoden vorgestellt, die zurzeit zur digitalen Archivierung von Patientenunterlagen in Krankenhäusern zum Einsatz kommen.

Um Papierdokumente in elektronischer Form zur Verfügung zu stellen, müssen sie digitalisiert werden. Zur Digitalisierung von papierbasierten Dokumenten werden Scan- und Indexierverfahren eingesetzt. In Abhängigkeit von der Anzahl der zu scannenden Dokumente ist dabei zwischen der Einzel- und Massenerfassung von Dokumenten zu unterscheiden. Die Erfassung von einzelnen Seiten ist z.B. in der Patientenaufnahme erforderlich. Damit können Dokumente, die ein Patient mitbringt, eingescannt und dem weiterbehandelnden Arzt in elektronischer Form zur Verfügung gestellt werden. Um das Dokument auch für Recherchen zur Verfügung zu stellen, erfolgt eine manuelle Indexierung durch den Bearbeiter. Bei der Massenerfassung von papierbasierten Dokumenten werden Verfahren eingesetzt, die eine automatische Indexierung der Dokumente ermöglichen. Dazu gehören z.B. das OCR-Verfahren, die Barcodeerkennung sowie Verfahren zur automatischen Klassifikation von Dokumenten. Die Massenerfassung von papierbasierten Dokumenten wird vor allem für das rückwirkende Digitalisieren von Altakten verwendet.

Krankenhäuser, die noch nicht mit der elektronischen Signatur arbeiten, müssen unterschriftsrelevante Dokumente ausdrucken. Nachdem die Dokumente unterschrieben wurden, werden sie eingescannt und digital archiviert. Wurde das ausgedruckte Dokument mit einem Barcode versehen, kann es beim Einscannen automatisch dem Patienten oder Fall zugeordnet werden. Am Universitätsklinikum Heidelberg wurde im Rahmen des ArchiSig-Projektes die Möglichkeit geschaffen, die mit i.s.h.med erstellten Arztbriefe elektronisch zu signieren.

Für den Massenimport von List- und Spooldateien kommt das COLD-Verfahren zum Einsatz. Die Dateien werden importiert, anhand vorher definierter Regeln aufbereitet und anschließend zur Archivierung an das Ablagesystem übergeben. Zur Aufbereitung gehört die automatische Ermittlung der Indexinformationen aus dem Dokument.

Da auf die archivierten Dokumente in den ersten Monaten nach der Entlassung eines Patienten noch relativ häufig zugegriffen werden, bewahren die meisten Krankenhäuser die Dokumente zunächst auf einem elektronischen Kurzzeitspeicher auf. Der elektronische Kurzzeitspeicher gewährleistet einen schnellen Zugriff. Nach einigen Monaten (ca. 3 bis 6) werden diese Dokumente auf einen elektronischen Langzeitspeicher ausgelagert.

F1.3: Welche Aufgaben und Objekttypen sind auf der Fachlichen Ebene des 3LGM²-Modells zu modellieren?

Die Aufgaben, die ein digitales Archiv erledigt, wurden bereits beschrieben. Um aber eine Archivierte Patientenakte anzulegen, benötigt das Archivierungssystem Informationen zum Patienten. Diese Informationen werden bei der administrativen Aufnahme des Patienten erzeugt. Mit der administrativen Aufnahme eines Patienten wird automatisch eine APA angelegt. Aus diesem Grund gibt es im Referenzmodell die Aufgabe „Administrative Aufnahme“. Damit die Dokumente auch wiedergefunden werden, müssen sie mit Hilfe von Deskriptoren beschrieben werden. Die Indexierung erfolgt in der Regel in den Anwendungsbausteinen, in denen die Dokumente erzeugt wurden. Im Referenzmodell erfolgt die Indexierung über die Aufgabe „Dokumentenbeschreibung erzeugen (indexieren)“.

Um die fachliche Ebene des Referenzmodells zu modellieren, sind Objekttypen erforderlich, die im Rahmen einer Aufgabe bearbeitet oder interpretiert werden. Zur Modellierung werden die folgenden Objekttypen benötigt:

- ADT-Information
- APA
- Dokument der APA
- Dokumentenbeschreibung
- Elektronisches Dokument
- Elektronisches Dokument im Langzeitformat
- Fall
- Nachricht über APA
- Nachricht über ein Dokument
- Papierdokument
- Patient
- Signiertes Dokument.

Die fachliche Ebene des Referenzmodells einschließlich der Beschreibung der Objekttypen und der weiteren Aufgaben befindet sich im Kapitel 4.1.

F1.4: Welche Werkzeuge unterstützen die Erledigung dieser Aufgaben auf der Logischen Werkzeugebene?

Die Aufgaben werden durch rechnerbasierte Anwendungsbausteine erledigt, die vom Archivierungs- und Ablagesystem bereitgestellt werden. Dazu gehören:

- ein Administrationssystem

- ein Zugriffskontrollsystem
- ein Recherchesystem (entweder über einen Standard-Rechercheclient oder ein webbasiertes Recherchesystem)
- ein Scansystem für die Einzel- und Massenerfassung von Dokumenten
- ein Visualisierungssystem
- ein Volltextsuchsystem
- ein Importsystem und
- ein Workflowsystem.

Da die Daten und Dokumente nicht im Archivierungssystem, sondern in den anderen rechnerbasierten Anwendungsbausteinen eines KIS erzeugt werden, ist eine Kommunikation dieser Informationen über Bausteinschnittstellen erforderlich. Die zu kommunizierenden Daten und Dokumente werden u.a. in den folgenden Anwendungsbausteinen erstellt:

- Patientenverwaltungssystem
- Klinisches Dokumentations- und Managementsystem
- Modalitäten
- Kommunikationsserver
- Radiologieinformationssystem
- Bildspeicher- und Kommunikationssystem
- Laborinformationssystem
- Patientendatenmanagementsystem
- OP-Dokumentationssystem
- Finanzbuchhaltungs-, Materialwirtschafts- und Controllingsystem.

Für den Versand eines Dokumentes bis hin zu einer kompletten APA ist ein Nachrichtenübermittlungssystem erforderlich. Weiterhin wird ein Signatursystem benötigt, dass die Aufgabe „Dokument signieren“ unterstützt. Eine Beschreibung der logischen Werkzeugebene befindet sich im Kapitel 4.2.

F1.5: Wie sieht die physische Werkzeugebene aus?

Die Installation der rechnerbasierten Anwendungsbausteine erfolgt zum einen auf den Arbeitplatzrechnern und zum anderen auf Applikationsservern. Die physische Werkzeugebene enthält Applikationsserver für

- das Patientenverwaltungssystem
- das Klinische Dokumentations- und Managementsystem
- das Radiologieinformationssystem
- das Bildspeicher- und Kommunikationssystem
- das Laborinformationssystem
- das Patientendatenmanagementsystem
- das OP-Dokumentationssystem und
- die betriebswirtschaftlichen Prozesse (z.B. die Finanzbuchhaltung, das Controlling, die Materialwirtschaft).

Weiterhin wird ein Kommunikations-, Mail- und File-Server benötigt.

Die Implementierung des Archivierungssystem erfolgt in der Regel auf

- einem Datenbankserver, auf dem die Datenbank zur Verwaltung der Indexdaten und Referenzen zu den Dokumente liegt
- einem Applikationsserver, auf dem die Serverkomponenten des Archivierungssystem installiert sind
- einem Web-Server zur Installation von webbasierten Softwarekomponenten und
- einem Importserver.

Für die Aufbewahrung der Dokumente wird ein Ablagesystem benötigt. Die Einbindung des Ablagesystems kann in einem SAN oder NAS erfolgen. In der Regel werden die Dokumente zunächst auf einem elektronischen Kurzzeitspeicher abgelegt, der einen schnellen Zugriff auf die archivierten Dokumente ermöglicht. Wird auf die Dokumente nur noch selten zugegriffen, erfolgt eine Auslagerung auf einem elektronischen Langzeitspeicher.

Zusätzlich sollten bestimmte Arbeitsplatzrechner in einem Krankenhaus mit Druckern, Scannern, Kartenlesegeräten und Barcodelesern ausgestattet sein. Die Beschreibung und Darstellung der physischen Werkzeugebene befindet sich im Kapitel 4.4.

F1.6: Inwieweit ist es notwendig, zusätzlich zum 3LGM²-Modell noch andere Modellierungsmethoden und -werkzeuge einzusetzen, um die erforderlichen Aussagen in einem Referenzmodell machen zu können?

Die Darstellung von Prozessen für die digitale Archivierung wäre hilfreich gewesen. Die Modellierung von Prozessen wird jedoch nicht vom 3LGM²-Baukasten unterstützt. Aus diesem Grund wurde auf eine Darstellung der Prozesse in der Arbeit verzichtet.

F1.7: Welche Notwendigkeiten ergeben sich, das 3LGM²-Modell zu erweitern?

Um eine Aufgabe einem Anwendungsbaustein zuordnen zu können, muss für jede Aufgabe definiert werden, in welcher Organisationseinheit sie erledigt wird. Bei der digitalen Archivierung von Patientenunterlagen gibt es jedoch auch Aufgaben, die automatisch erledigt werden und somit keiner speziellen Organisationseinheit zugeordnet werden können. Die Zugriffe auf ein archiviertes Dokument oder eine APA müssen protokolliert werden. Die Protokollierung erfolgt durch das digitale Archiv und nicht durch eine bestimmte Personengruppe in einem Bereich. Die Aufgaben

- Archivierte Patientenakte anlegen
- Dokument importieren
- Dokument löschen und Vernichtung protokollieren
- APA löschen und Vernichtung protokollieren
- Berechtigung prüfen
- Signatur erneuern
- Aufbewahrungsdauer anpassen und
- Signatur erneuern

können in einer Organisationseinheit oder vom digitalen Archiv erledigt werden. Es müsste also auf der fachlichen Ebene eine Organisationseinheit für Aufgaben geben, die automatisch erledigt werden.

Im Referenzmodell wurden diese Aufgaben zunächst dem Bereich Informationsmanagement zugeordnet, da die Erledigung in der Regel von diesem Bereich überwacht und ausgewertet wird.

Als problematisch hat sich auch die Zuordnung der Aufgabe „Dokument archivieren“ zu einem Anwendungsbaustein herausgestellt. Die Archivierung eines Dokumentes erfolgt auf einem Ablagesystem, das Bestandteil der physischen Werkzeugebene ist.

Zu Ziel 2:

Ziel dieser Arbeit ist: ein Vergleich ausgewählter Hard- und Softwareprodukte für die digitale Archivierung von 4 Anbietern mit diesem Referenzmodell.

F2: Wie lassen sich aus dem 3LGM²-basierten Referenzmodell spezielle Modelle von vier ausgewählten Anbietern ableiten?

Im Kapitel 5 wurde gezeigt, das sich aus dem 3LGM²-basierten Referenzmodell durch Konkretisierung spezielle Modelle ableiten lassen. Dabei wurden die folgenden Produkte betrachtet:

- d.3 von der Firma d.velop AG
- HYDMedia von der Firma Heydt-Verlags-GmbH
- forcont factory von der Firma forcont business technology GmbH und
- EMC Centera von der Firma EMC².

Da die speziellen Modelle aus demselben Referenzmodell abgeleitet wurden, ist ein direkter Vergleich der einzelnen Produkte möglich. Ein ausführlicher Vergleich der einzelnen Modelle wird im Kapitel 6 durchgeführt.

A2.1: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma d.velop AG mit Hilfe des 3LGM²-Baukasten

Die Modellierung der einzelnen Ebenen ist im Kapitel 5.1 ausführlich dargestellt. Das vollständige Modell befindet sich auf der als Anlage beigefügten CD-ROM.

A2.2: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma Heydt-Verlags-GmbH mit Hilfe des 3LGM²-Baukasten

Die Modellierung der einzelnen Ebenen ist im Kapitel 5.2 ausführlich dargestellt. Das vollständige Modell befindet sich auf der als Anlage beigefügten CD-ROM.

A2.3: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma forcont business technology GmbH mit Hilfe des 3LGM²-Baukasten

Die Modellierung der einzelnen Ebenen ist im Kapitel 5.3 ausführlich dargestellt. Das vollständige Modell befindet sich auf der als Anlage beigefügten CD-ROM.

A2.4: Modellierung der angebotenen Hard- und Softwareprodukte für ein digitales Archiv der Firma EMC² mit Hilfe des 3LGM²-Baukasten

Die Modellierung der einzelnen Ebenen ist im Kapitel 5.4 ausführlich dargestellt. Das vollständige Modell befindet sich auf der als Anlage beigefügten CD-ROM.

F2.5: Was bieten diese Firmen an zusätzlichen Funktionalitäten an?

Die Firmen unterstützen den Austausch von Dokumenten mit externen Personen. In HYDMedia können die Dokumente über das Remotesystem freigegeben werden. Der Zugriff auf die Dokumente erfolgt über eine gesicherte VPN-Verbindung. Im d.3-System ist die Erstellung eines Offline-Archivs möglich, das in Form einer CD/DVD an eine externe Person übergeben werden kann. Sowohl im d.3-System als auch in der forcont factory ist die Einrichtung eines Web-Zugangs für externe Personen möglich. Über eine Web-Schnittstelle können Dokumente in das Archivierungssystem importiert werden.

Im d.3-System können veröffentlichte Dokumente über das öffentliche Recherchesystem von allen Personen eingesehen werden.

Die Darstellung der Dokumente in HYDMedia wird über Kumulationen geregelt. Dies ist eine spezielle Technik, die bisher nur von der Heydt-Verlags-GmbH verwendet wird.

Ein Besonderheit im Produkt forcont factory ist die Snapshot-Funktion, die eine Momentaufnahme der Patientenakte ermöglicht.

8.2 Diskussion der Ergebnisse und Ausblick

Das im Rahmen dieser Diplomarbeit entwickelte Referenzmodell soll den Informationsmanager zukünftig bei der Einführung eines digitalen Archivs unterstützen. Unter Bezugnahme auf das Referenzmodell sind ein Vergleich und eine Bewertung der unterschiedlichen Produkte, die auf dem Markt zur digitalen Archivierung angeboten werden, möglich. Weiterhin kann der Informationsmanager feststellen, wie sich ein bestimmtes Produkt in das vorhandene Informationssystem des Krankenhauses einfügt.

Bei einer Präsentation der zur digitalen Archivierung angebotenen Produkte ist erkennbar, dass es kaum Unterschiede bzgl. der angebotenen Funktionalitäten gibt. Es hat sich jedoch im Laufe der Arbeit gezeigt, wie schwierig es ist, aus dem Referenzmodell ein spezielles Modell abzuleiten. Anhand der Produktbeschreibungen ist oftmals nicht ersichtlich, um welche Komponenten es sich handelt. Die Bezeichnung einer Softwarekomponente als Server ist auf den ersten Blick verwirrend. Die Funktionalitäten eines digitalen Archivs werden in der Regel ausführlich beschrieben. Für die Zuordnung der Aufgaben zu den Anwendungsbausteinen sind jedoch weitere Informationen erforderlich. Die Erstellung der $3LGM^2$-Modelle wäre ohne zusätzliche Informationen von den einzelnen Firmen nicht möglich gewesen.

Mit der Aufbewahrung von Dokumenten über 30 Jahre und mehr gibt es auch bei den Anbietern von digitalen Archiven noch keine Erfahrung. Im Moment wird davon ausgegangen, dass sich die Dateiformate PDF, TIFF, DICOM, JPEG, PDF-A und in Zukunft auch XML als Langzeitformate durchsetzen werden. Um jedoch eine langfristige Lesbarkeit von elektronisch signierten Dokumenten zu gewährleisten, sind die Ergebnisse des Projektes TransiDoc abzuwarten. Das Referenzmodell ist dementsprechend zu erweitern.

Die digitale Archivierung wird sich in den nächsten Jahren auch in anderen Branchen, vor allem im Verwaltungsbereich, ausweiten.

9 Anhang

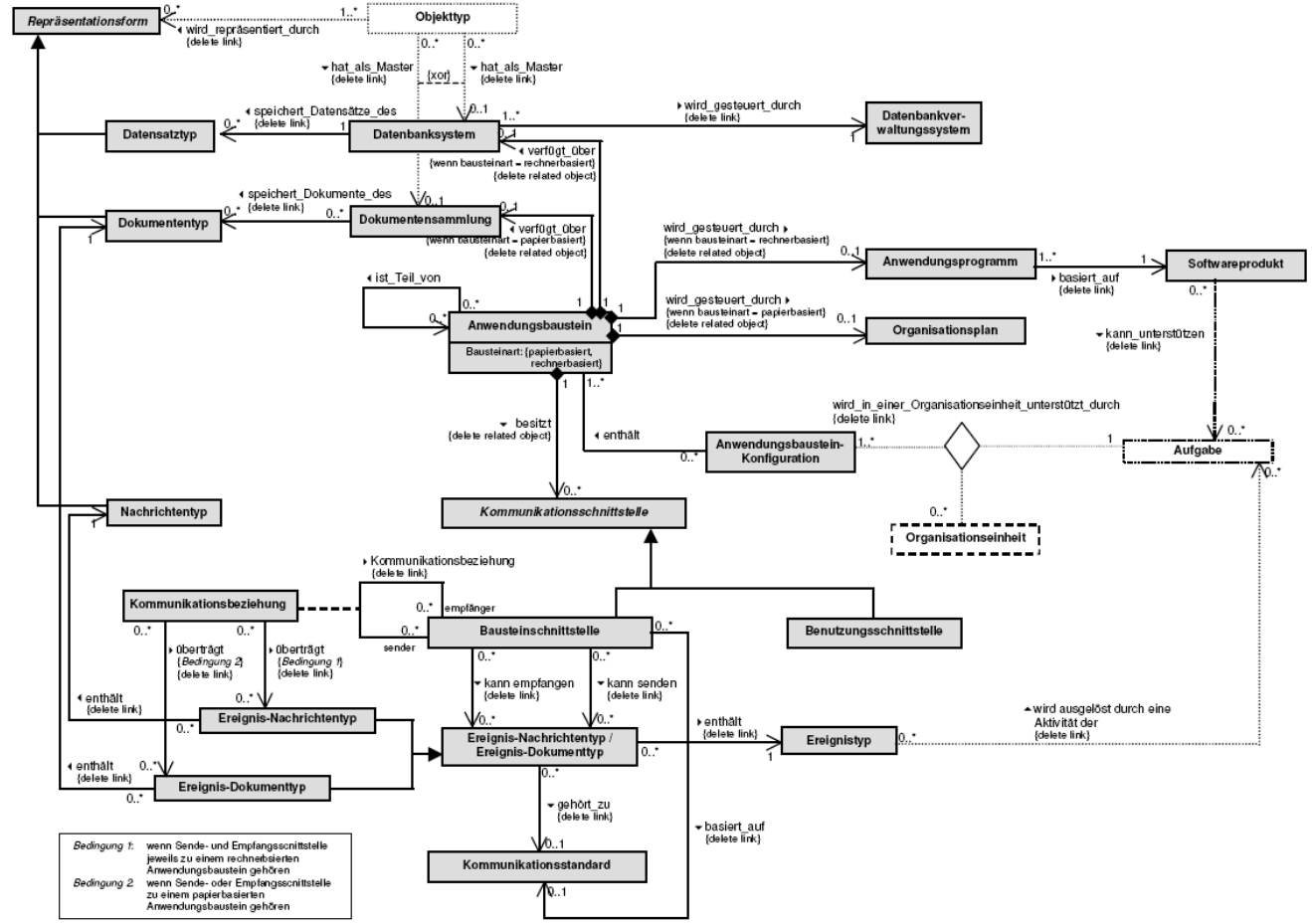


Abbildung 9-1: Das Meta-Modell der logischen Werkzeugebene

(entnommen aus [3LGM²])

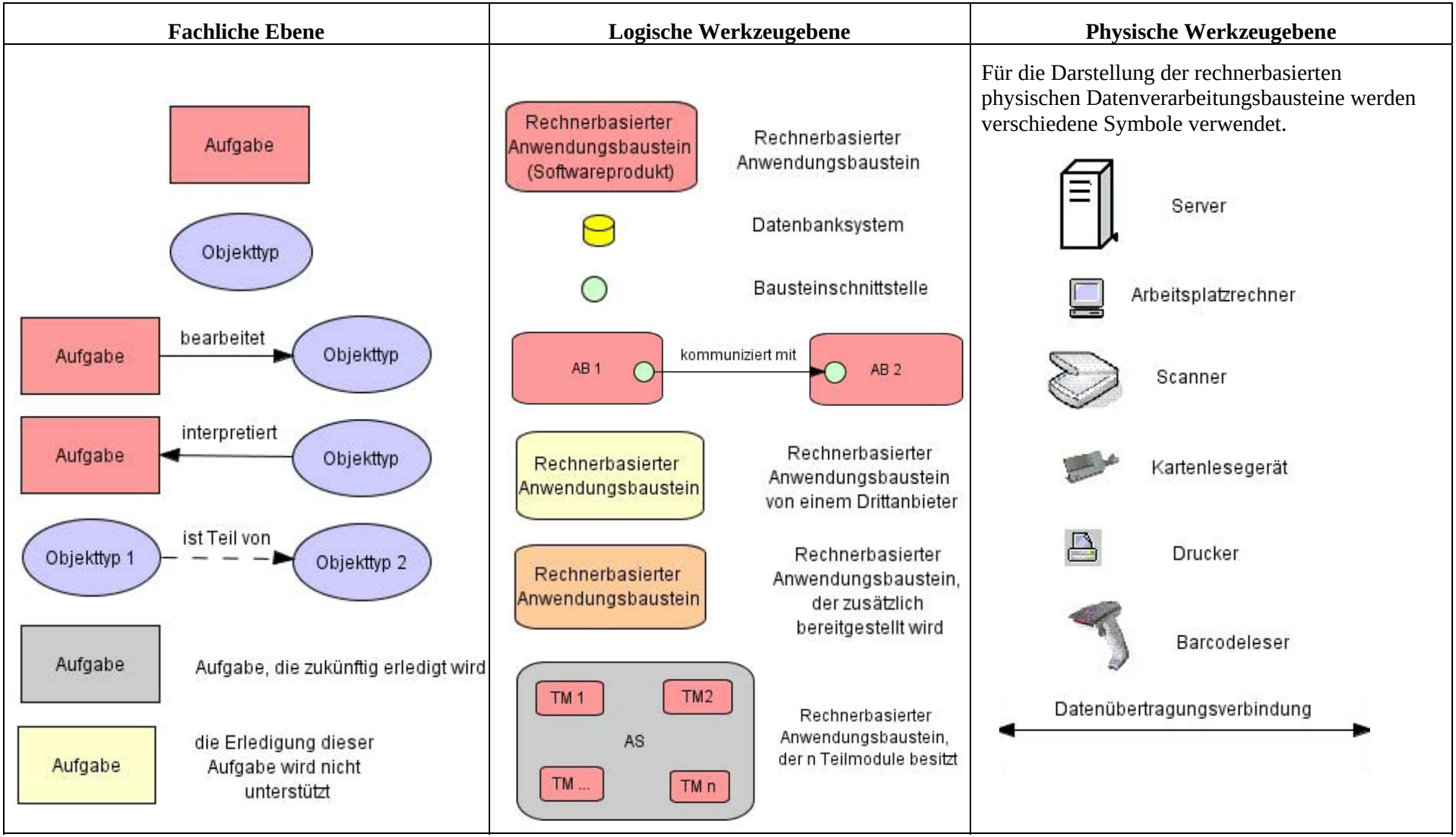


Abbildung 9-2: Legende zur graphischen Darstellung der Elemente im 3LGM²-Baukasten

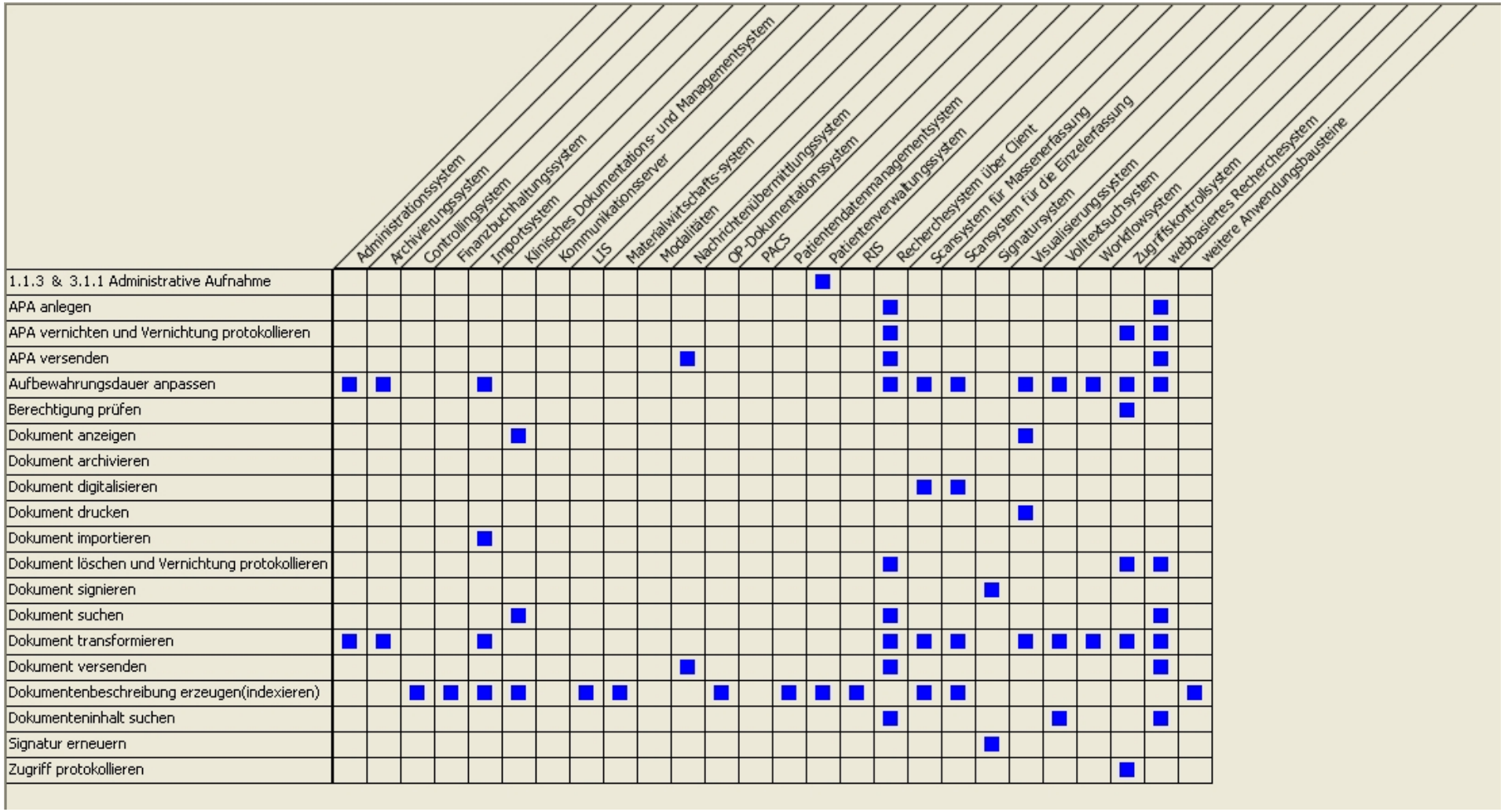


Abbildung 9-3: Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene

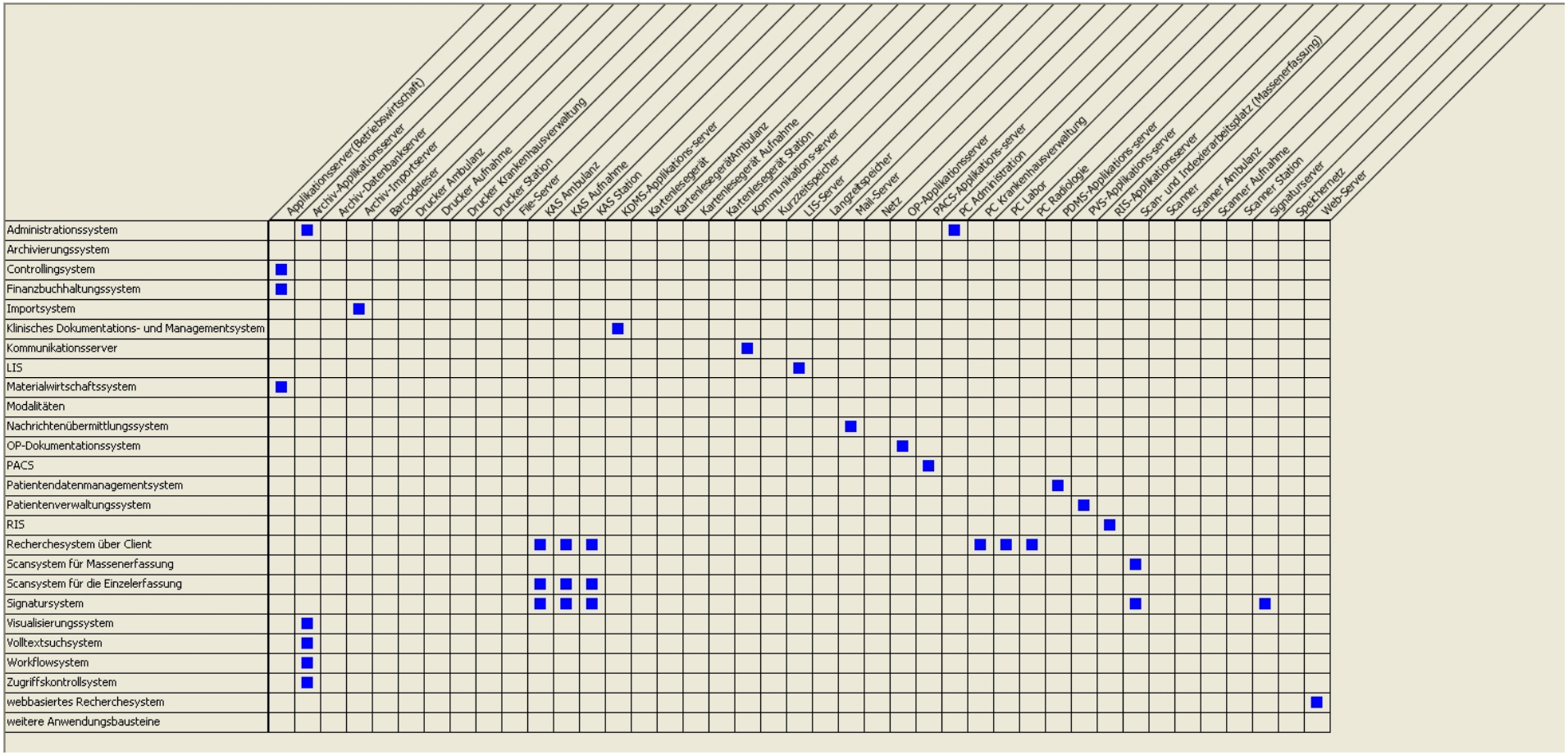


Abbildung 9-4: Inter-Ebenen-Beziehungen zwischen logischer und physischer Ebene

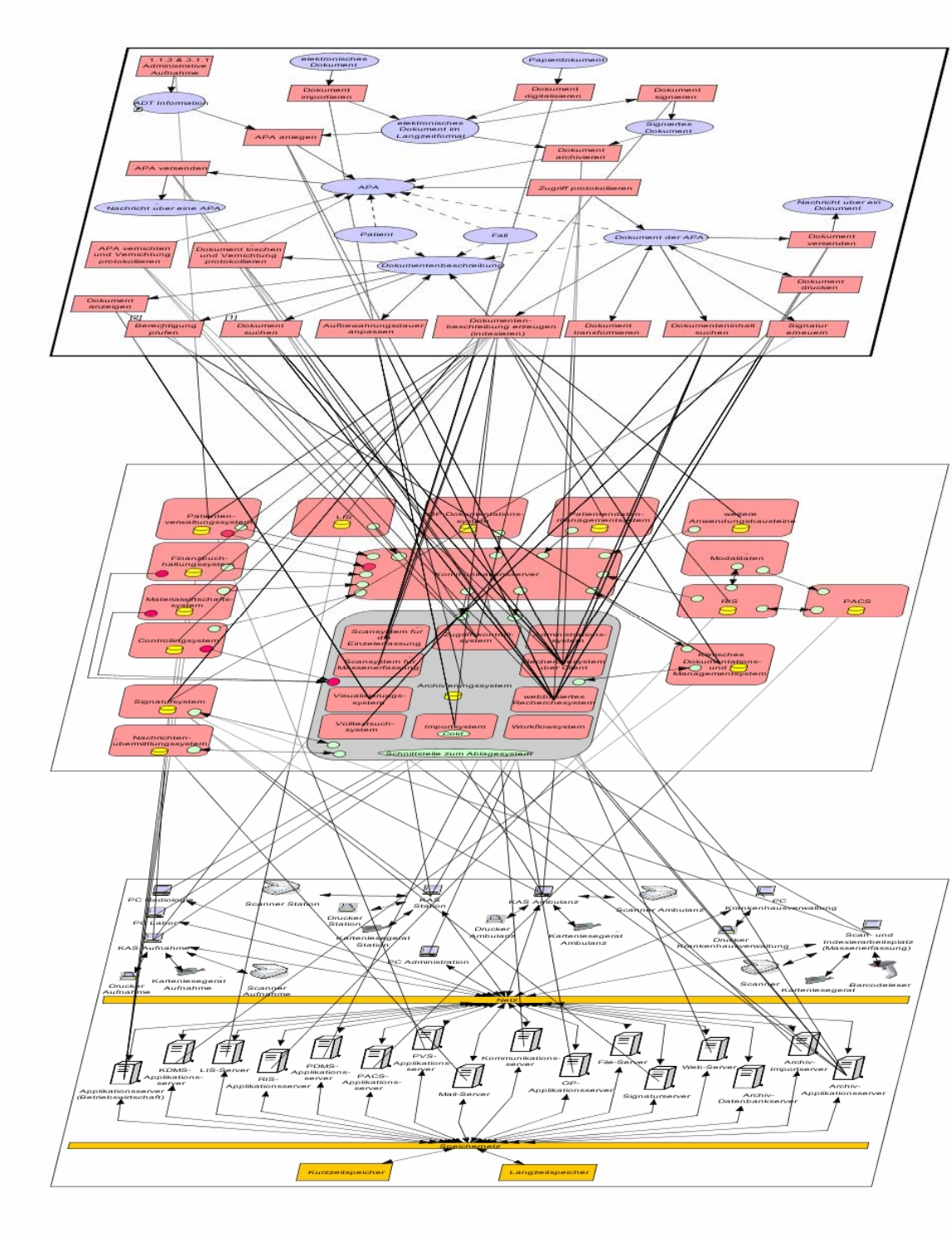


Abbildung 9-5: Referenzmodell

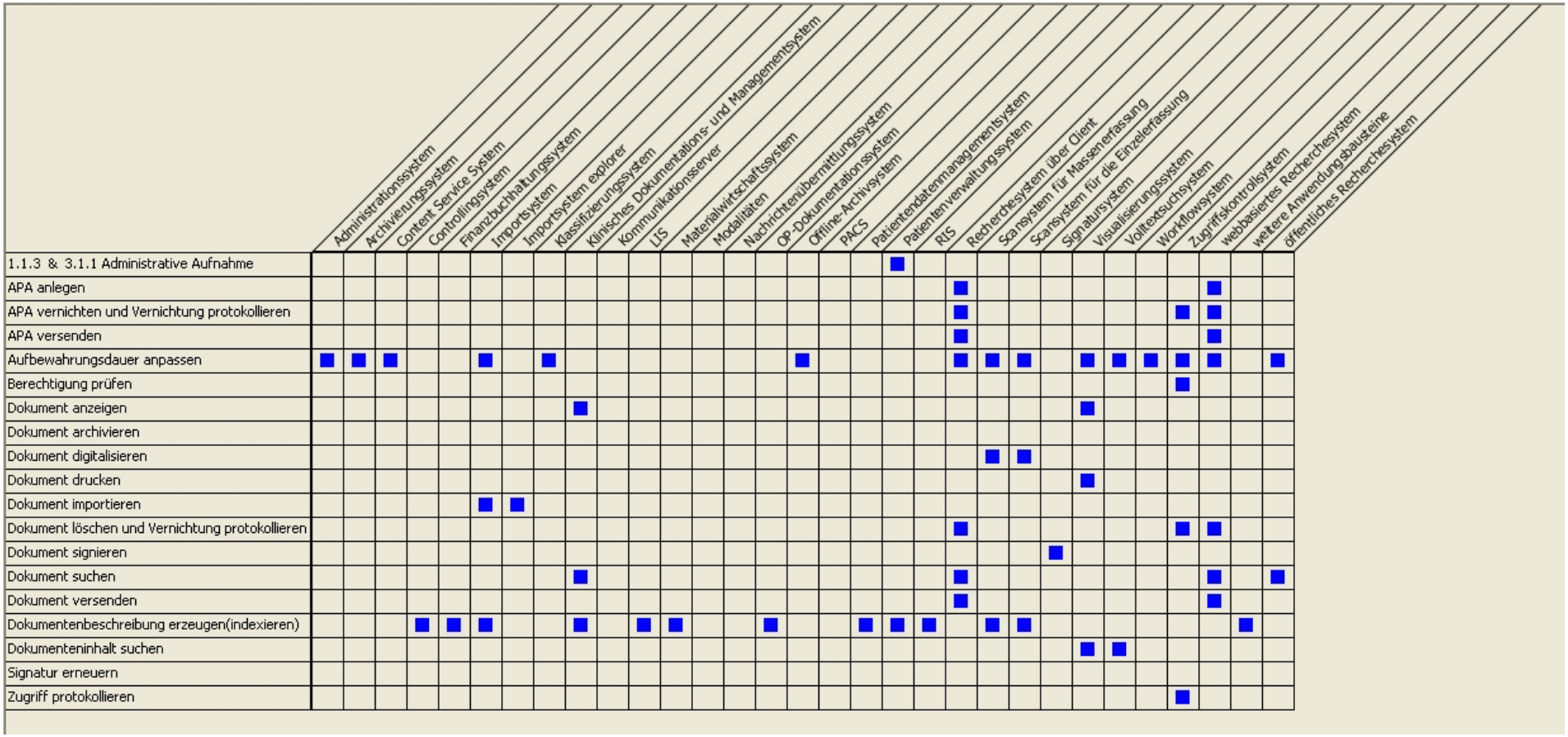


Abbildung 9-6: Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene von d.3

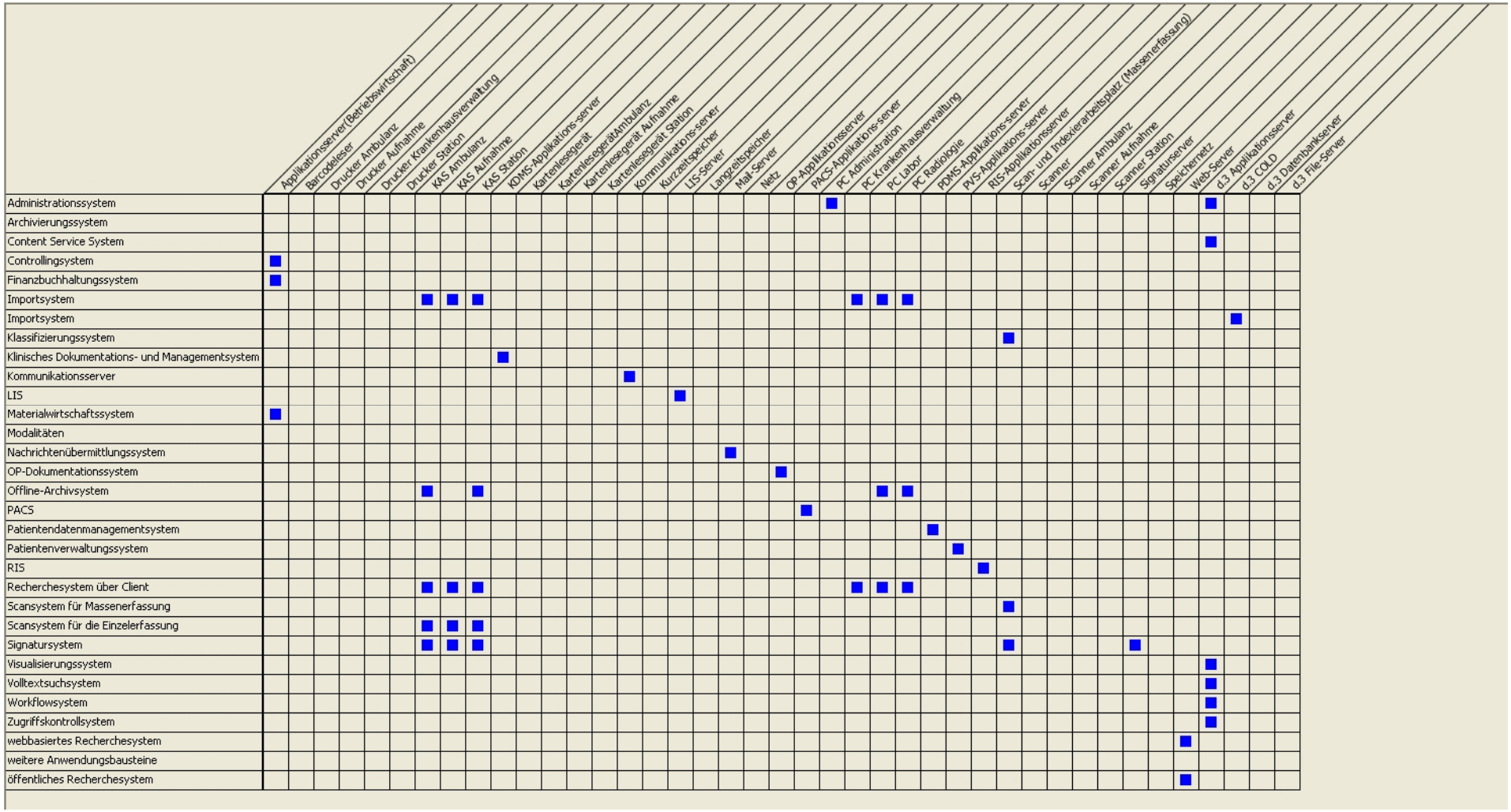


Abbildung 9-7: Inter-Ebenen-Beziehungen zwischen logischer und physischer Ebene von d.3

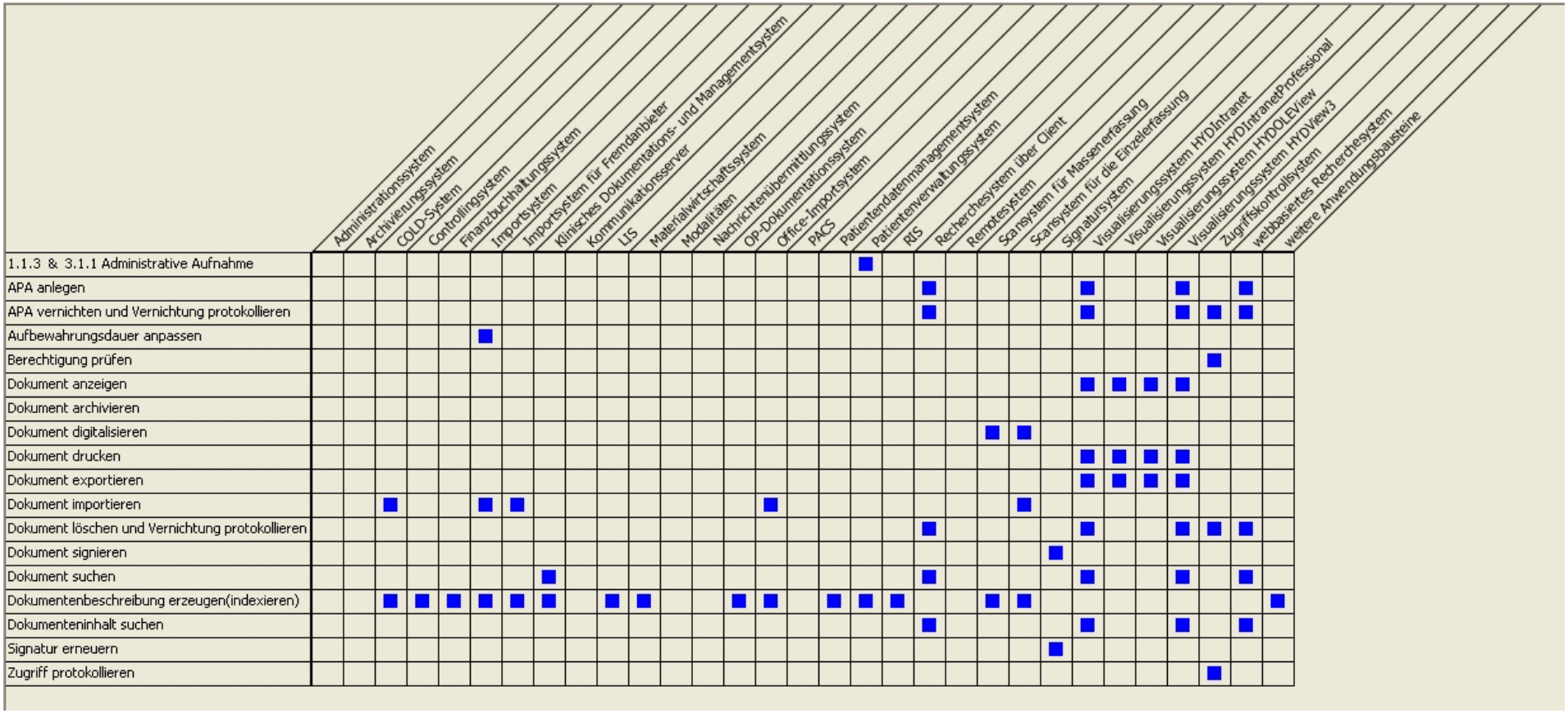


Abbildung 9-8: Inter-Ebenen-Beziehung zwischen fachlicher und logischer Ebene von HYDMedia

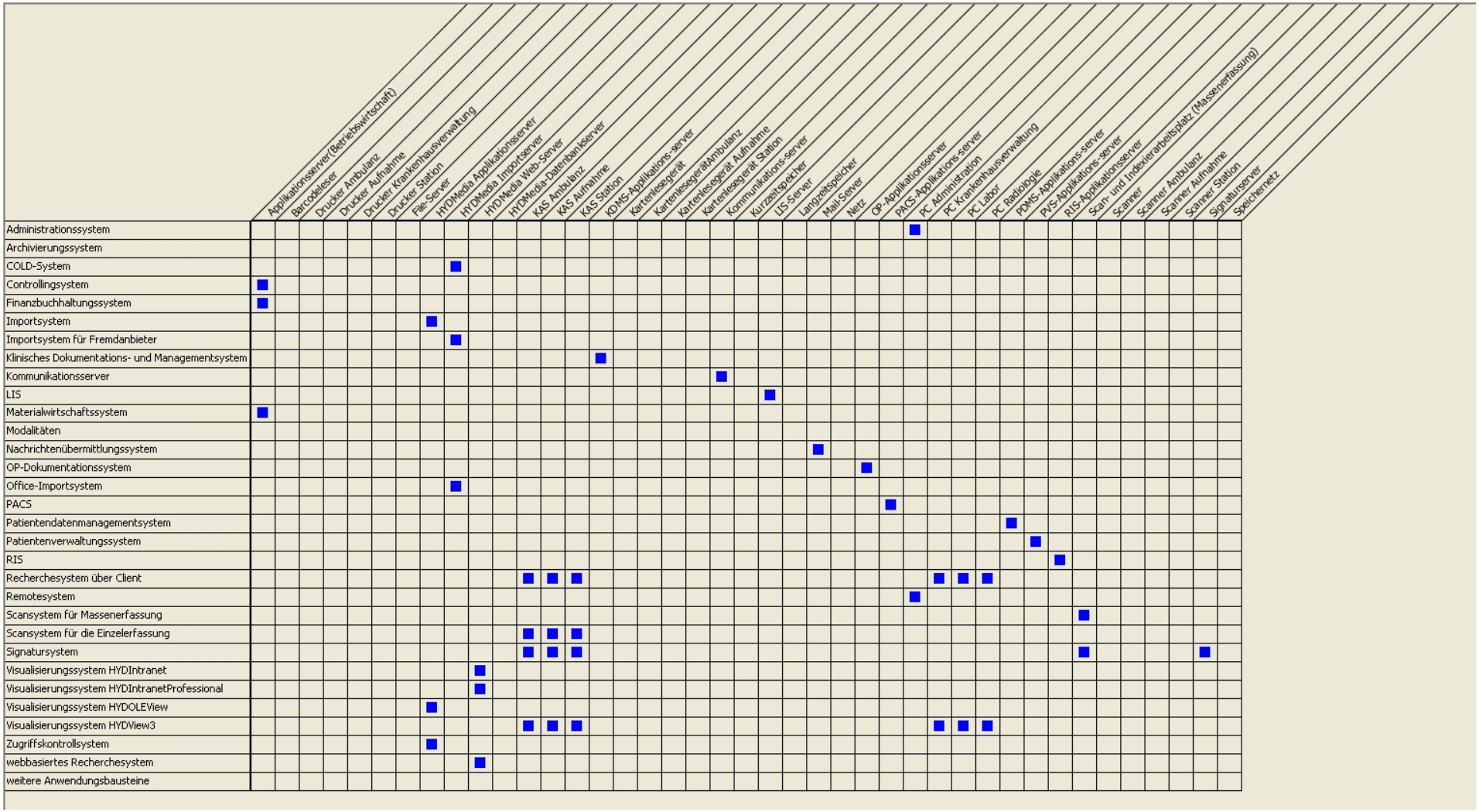


Abbildung 9-9: Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene von HYDMedia

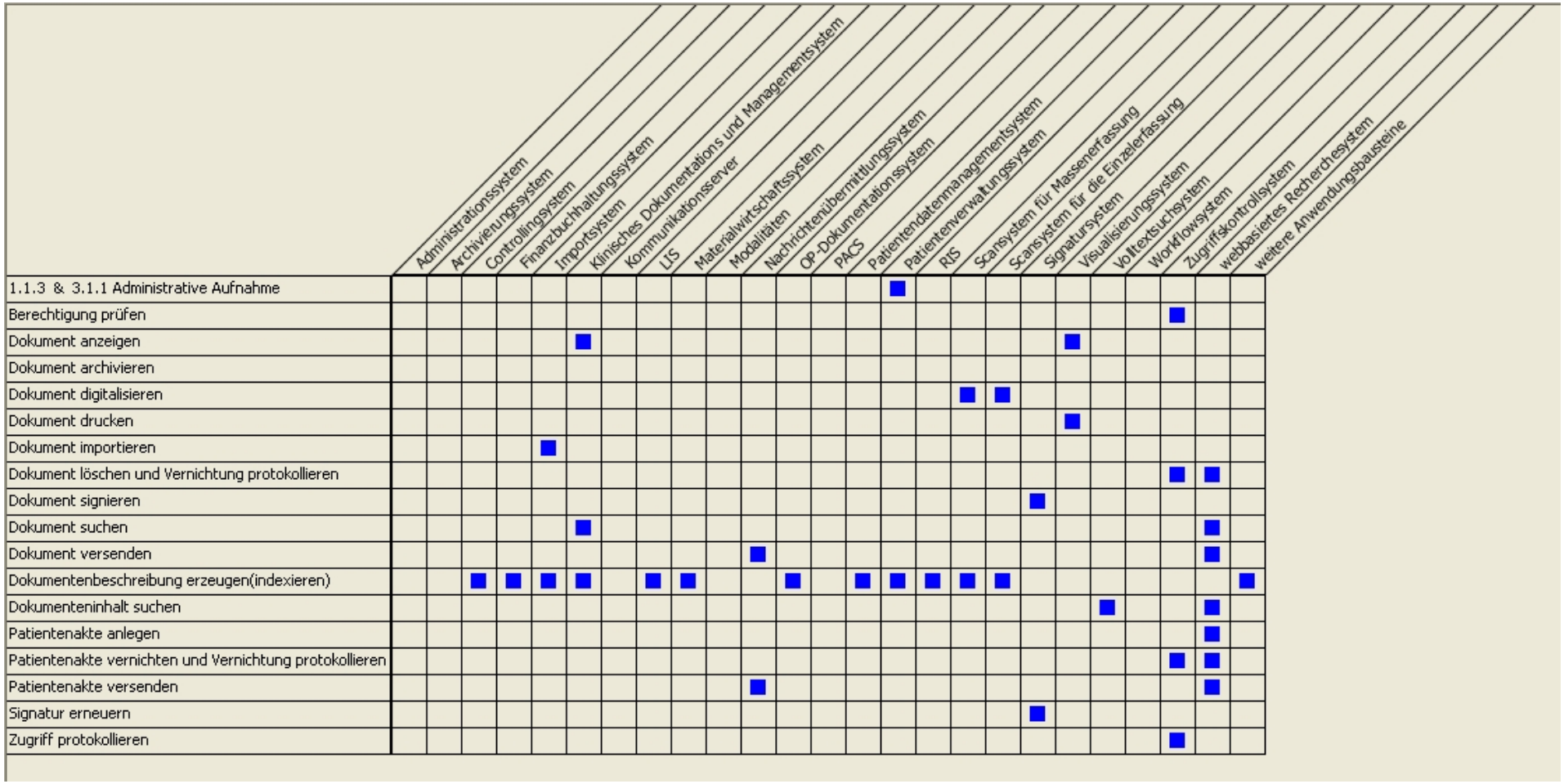


Abbildung 9-10: Inter-Ebenen-Beziehungen zwischen fachlicher und logischer Ebene der forcont factory

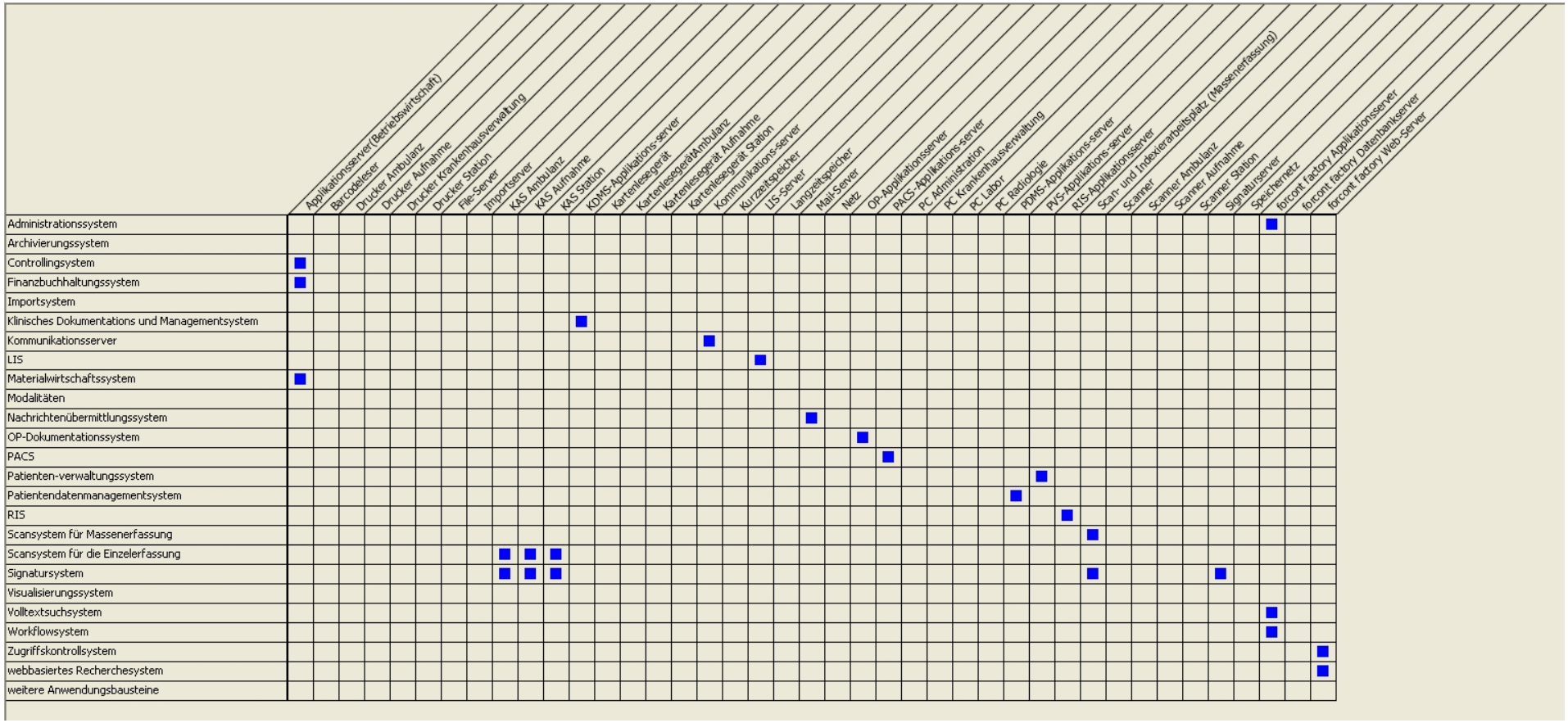


Abbildung 9-11: Inter-Ebenen-Beziehungen zwischen logischer und physischer Werkzeugebene der forcont factory

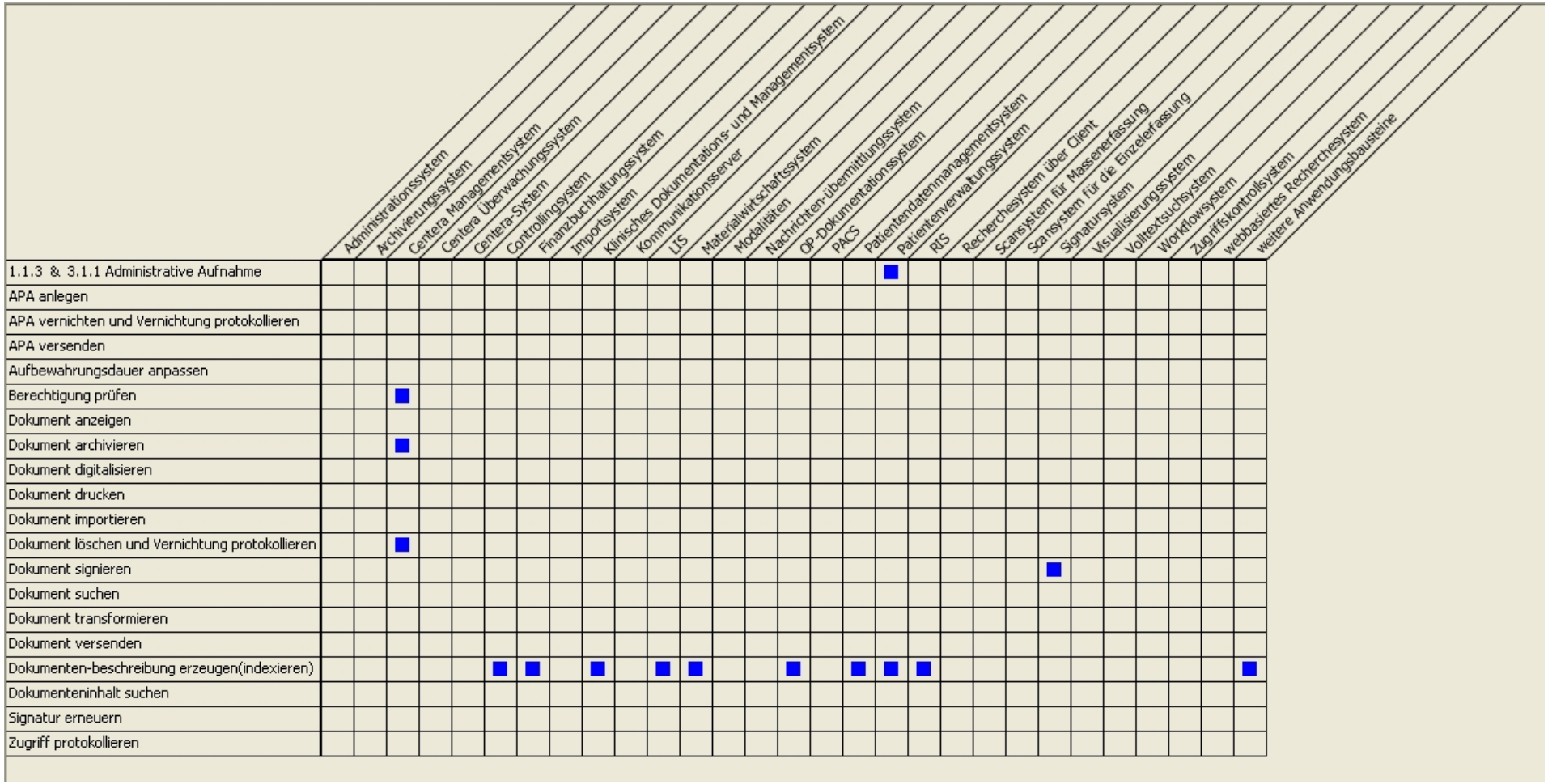
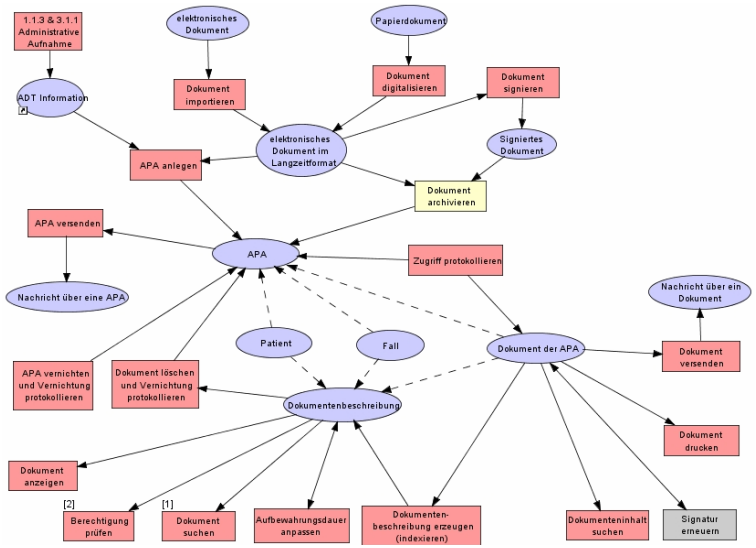
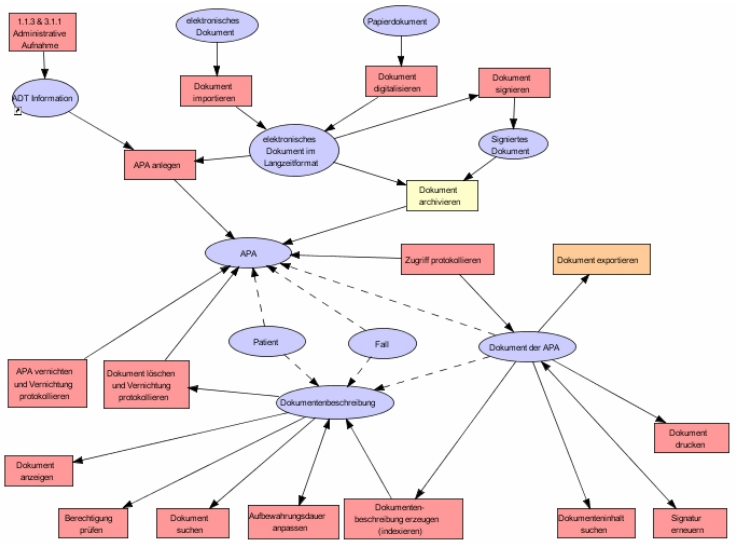


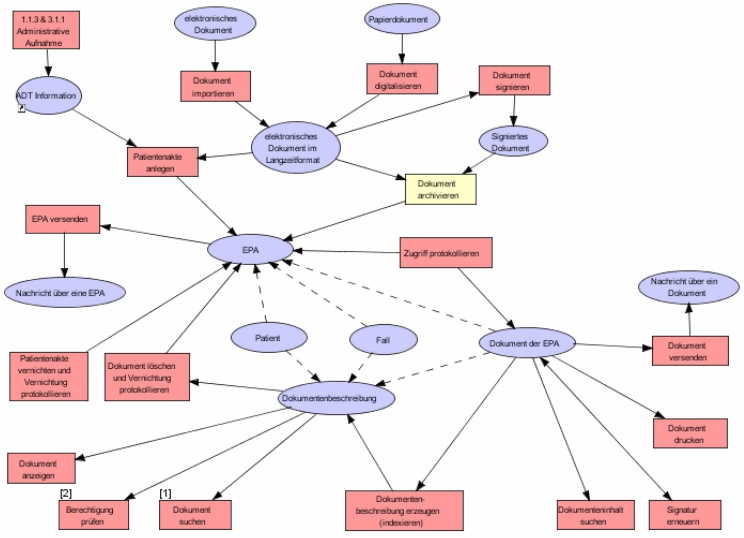
Abbildung 9-12: Inter-Ebenen-Beziehung zwischen fachlicher und logischer Ebene der EMC Centera



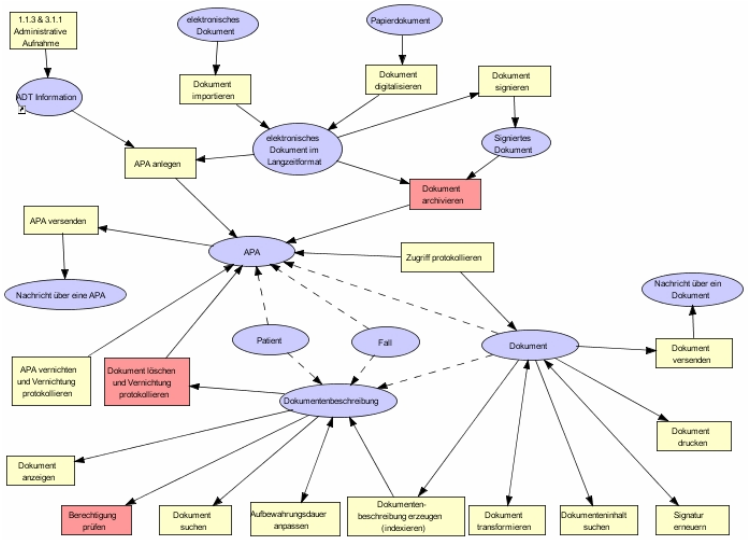
Produkt d.3



Produkt HYDMedia

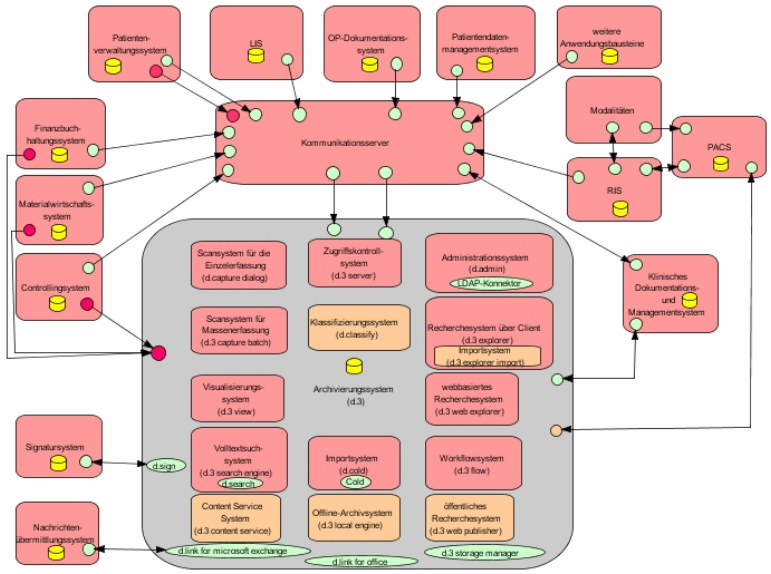


Produkt forcont factory

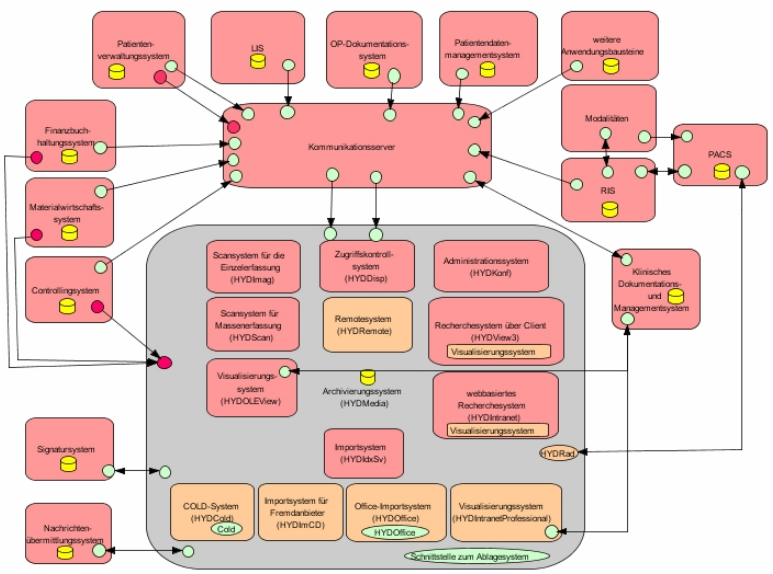


Produkt EMC Centera

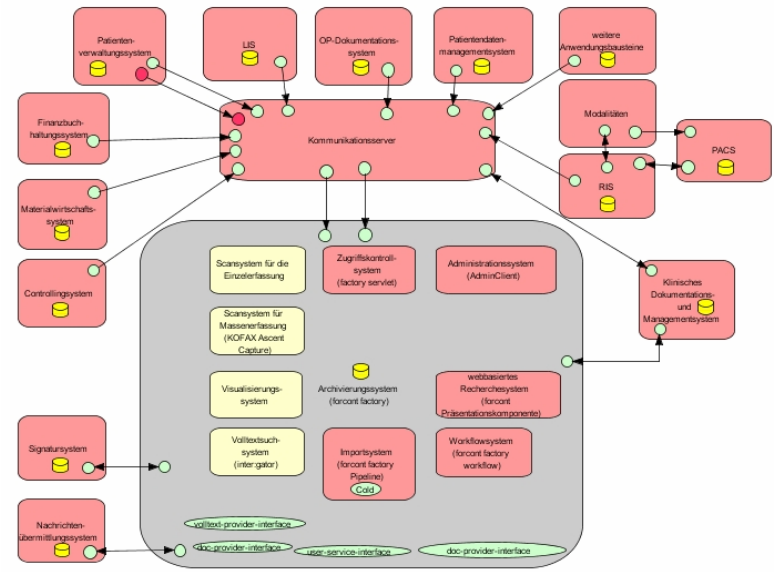
Abbildung 9-13: Vergleich der fachlichen Ebenen



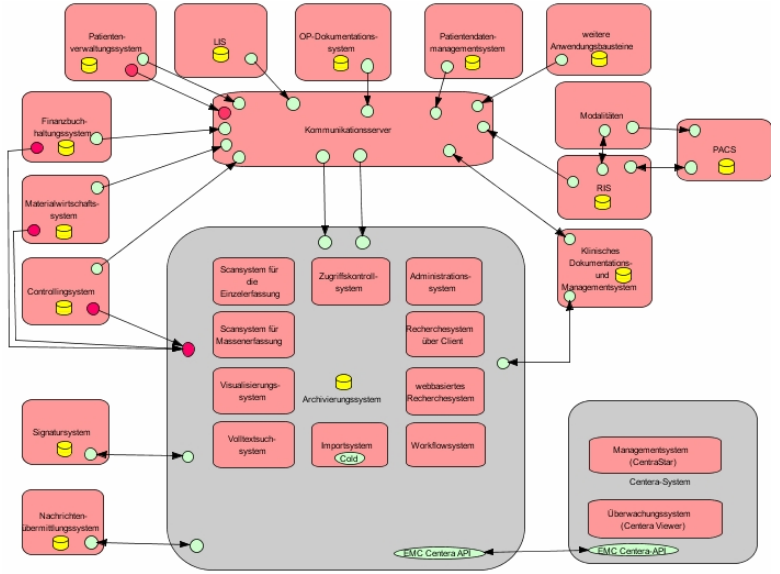
Produkt d.3



Produkt HYDMedia

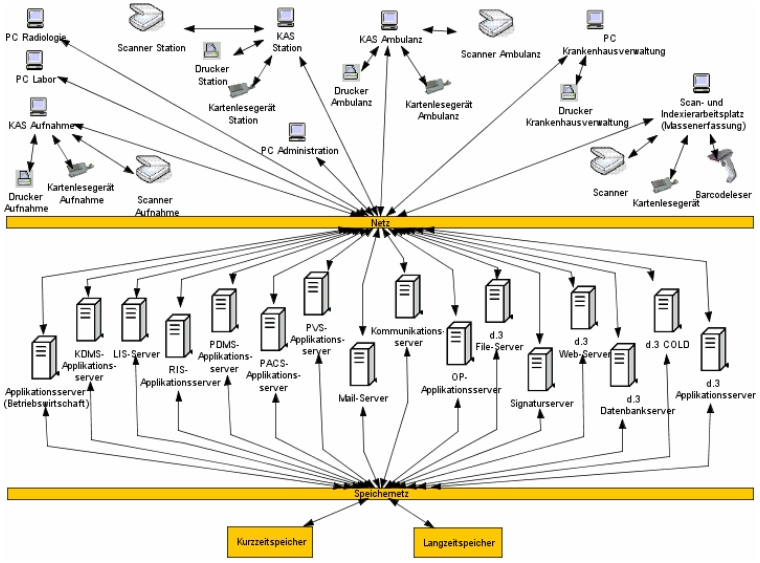


Produkt forcont factory

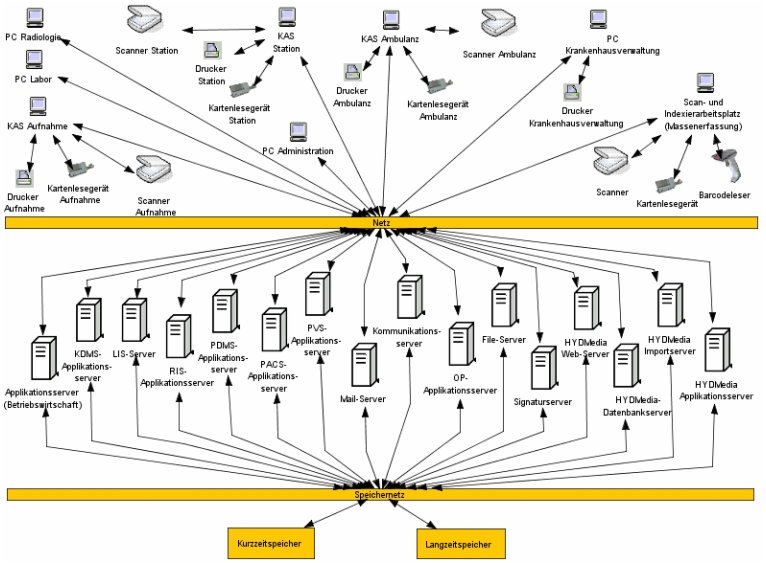


Produkt EMC Centera

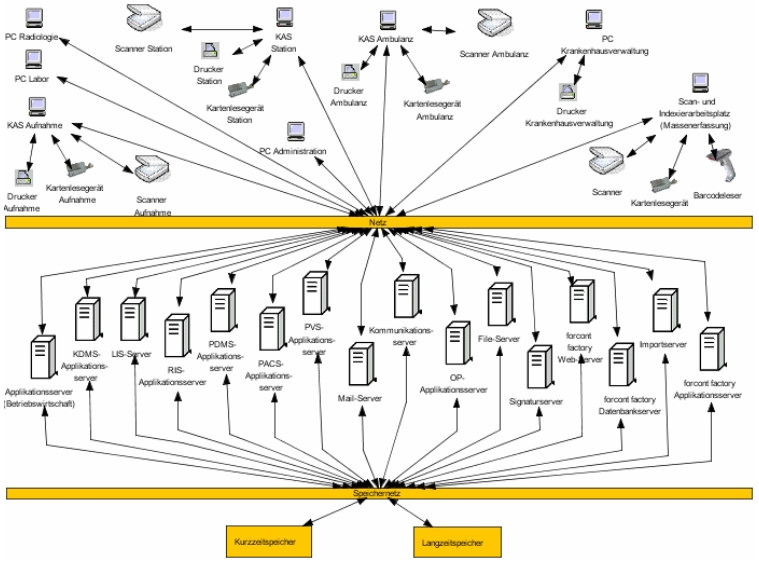
Abbildung 9-14: Vergleich der logischen Werkzeugebenen



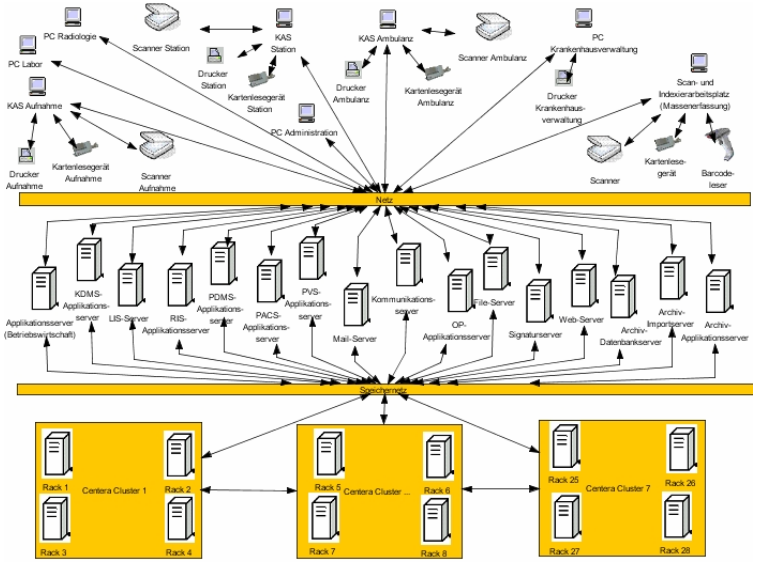
Produkt d.3



Produkt HYDMedia



Produkt forcont factory



Produkt HYDMedia

Abbildung 9-15: Vergleich der physischen Werkzeugebenen

CD-ROM als Anlage zur Diplomarbeit

Inhalt der CD-ROM:

- Diplomarbeit im PDF-Dateiformat
- Fragebogen im PDF-Dateiformat
- 3LGM^2-basiertes Referenzmodell für die digitale Archivierung von Patientenunterlagen
- 3LGM^2-Modelle der Produkte d.3, EMC Centera, forcont factory und HYDMedia
- Informationsmaterialien, die von den einzelnen Firmen zur Verfügung gestellt wurden

Literaturverzeichnis

Buch:

Ameh A. E., Shehu B.B. (2002): Medical record keeping and information retrieval in developing countries: surgeons' perspective. In: Tropical Doctor 32: 232-234.

Ball J.M., Collen F.M. (1992): Aspects of the Computer-based Patient Record. New York: Springer.

Belgian Telematics Commission (2004): Long term preservation of hospital patient records. In: Stud Health Technol Inform 110: 118-9.

Blobel B. (2005): Elektronische Patientenakte. In: Lehmann, T. Handbuch der Medizinischen Informatik. München: Carl Hanser Verlag: 649-672.

Brandner R., van der Haak M., Hartmann M., Haux R., Schmücker P. (2002): Electronic Signature for Medical Documents – Integration and Evaluation of a Public Key Infrastructure in Hospitals. In: Methods Inf Med 41: 321-330.

Brandner R., Hollerbach A., Anderl N., Gondrom T., Hochlehnert A., Barzin P. (2006a): Anwendung des Prototyps im Universitätsklinikum Heidelberg. In: Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Rechtssicherheit?: 163-175.

Brandner R., Pordesch U., Gondrom T. (2006b): Archivzeitstempelung und Neusignierung. In: Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Rechtssicherheit?: 81- 92.

Brigl B., Wendt T., Winter A. (2003): Ein UML-basiertes Metamodell zur Beschreibung von Krankenhausinformationssystemen. IMISE Reports 1/2003. Universität Leipzig.

Brigl B., Häber A., Wendt T., Winter A. (2004): Ein 3LGM^2 Modell des Krankenhausinformationssystems des Universitätsklinikums Leipzig und seine Verwertbarkeit für das Informationsmanagement. In: Rebstock M.: Modellierung betrieblicher Informationssysteme – MobIS 2004. GI-Edition: Lecture Notes in Informatics P-45: 21-41.

Brockhaus (2004): Der Brockhaus in fünf Bänden. Zehnte, neu bearbeitete Auflage, Band 1: A-Eis. Leipzig: Brockhaus GmbH.

Dick S. R., Steen B.E. (1992): Essential Technologies for Computer-based Patient Records: A Summary. In: Ball J. M., Collen F. M. Aspects of the Computer-based Patient Record. New York: Springer-Verlag: 229-261.

Dörge O. (2003): Patientenorganizer: Zentrales Navigationswerkzeug. In: Krankenhaus-IT Journal 4/2003: 2-3.

Dujat C. (1996): Zur digital-optischen Archivierung von medizinischen Dokumenten im Krankenhaus. Dissertation, Universität Heidelberg, Abteilung Medizinische Informatik.

Farnbacher W. (2004): Vom Posteingang bis in das Archiv. In: Hering R., Schäfer U.: Digitales Verwalten – Digitales Archivieren, 8. Tagung des Arbeitskreises „Archivierung von Unterlagen aus digitalen Systemen". Hamburg: Hamburg University Press.

Federal Register, Part II, Department of Health and Human Services, 45 CFR Parts 160, 162 and 164, Health Insurance Reform: Security Standards. Final Rule. Vol.68, No.34, 20.02.2003, Rules and Regulations.

Fischer-Dieskau S., Jandt S., Knopp M., Roßnagel A. (2006): Anforderungen und Trends der langfristigen Aufbewahrung von elektronischen Dokumenten. In: AWV-Information 2/2006: 7-9.

Götzer K., Schneiderath U., Maier B., Komke T. (2004): Dokumenten-Management. Heidelberg: dpunkt.

Gulbins J., Seyfried M., Strack-Zimmermann H. (2002): Dokumenten-Management. 3. überarbeitete und erweiterte Auflage. Berlin, Heidelberg: Springer.

Haas P. (2005): Medizinische Informationssysteme und Elektronische Krankenakten. Berlin, Heidelberg, New York: Springer.

Häber A., Dujat C., Schmücker P. (2005): Leitfaden für das rechnerunterstützte Dokumentenmanagement und die digitale Archivierung von Patientenunterlagen im Gesundheitswesen. Darmstadt: GIT Verlag.

Haufe, G., Schurig, A. (2000). Empfehlungen für ein Sicherheits- und Datenschutzkonzept, Sächsisches Staatsministerium für Soziales, Familie, Jugend und Gesundheit: Modellprogramm Digitalisierung bildgebender Verfahren und Bildkommunikation der Krankenhäuser im Freistaat Sachsen. Wissenschaftlicher Beirat: Dresden.

Haux R., Winter A., Ammenwerth E., Brigl B. (2004): Strategic Information Management in Hospitals. An Introduction to Hospital Information Systems. Springer: New York.

Hein M., Köhler P.T. (2002): Der IT-Reader Netzwerksicherheit. Köln: Fossil Verlag.

Henstdorf K.G., Kampffmeyer U., Prochnow J. (1999): Grundsätze der Verfahrensdokumentation nach GoBS – „Code of Practice“ zur revisionssicheren Archivierung, 1.Auflage. Bonn: VOI Verband optische Informationssysteme e.V.

Hollerbach A., Brandner R. (2003a): Kriterien und Bewertung von Datenformaten für die beweiskräftige und sichere Langzeitspeicherung medizinischer Dokumente. In: Forum der Medizin_Dokumentation und Medizin_Informatik 4/2003: 105-109.

Hollerbach A., Brandner R., Bess A., Schmücker P., Bergh B. (2005b): Electronically Signed Documents in Health Care. Analysis and Assessment of Data Formats and Transformation. In: Methods Inf Med 44: 520-527.

Hübner-Bloder G. (2005): Referenzmodell für die Fachliche Ebene des $3LGM^2$. Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT). Version 1.

Ingenerf J., Stausberg J. (2005): Klinische Arbeitsplatzsysteme. In: Lehmann, T. Handbuch der Medizinischen Informatik. München: Carl Hanser Verlag: 625-647.

Kampffmeyer U., Rogalla J. (1997): Grundsätze der elektronischen Archivierung, 2. Auflage. Darmstadt: VOI Verband optische Informationssysteme e.V.

Klingelhöller H. (2001): Dokumenten-managementsysteme. Handbuch zur Einführung. Berlin Heidelberg: Springer.

Lehmann T., Hiltner J., Handels H. (2005): Medizinische Bildverarbeitung. In: Lehmann, T. Handbuch der Medizinischen Informatik. München: Carl Hanser Verlag: 361-423.

Leiner F., Gaus W., Haux R., Knaup-Gregori P., Pfeiffer KP. (2006): Medizinische Dokumentation – Grundlagen einer qualitätsgesicherten integrierten Krankenversorgung. 5. aktualisierte Auflage. Stuttgart: Schattauer.

National Electrical Manufacturers Association (2006): Digital Imaging and Communications in Medicine (DICOM). Part 4: Service Class Specifications. Rosslyn Virgina: National Electrical Manufactures Association.

Pryor T. A. (1992): Current State of Computer-based Patient Record Systems. In: Ball J. M., Collen F. M. Aspects of the Computer-based Patient Record. New York: Springer: 67-82.

Robbe, B. (2004): SAN. Storage Area Network. Technologie, Konzepte, Einsatz komplexer Speicherumgebungen. München: Carl Hanser Verlag.

Roßnagel A., Schmücker P. (2006): Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Rechtssicherheit?. Heidelberg: Economica.

Ruotsalainen P. (2004): Security requirements in EHR systems and archives. In: Stud Health Technol Inform 103: 453-8.

Schmücker P. (1996c): Rechnerunterstützte Dokumentenmanagement- und Optische Archivierungssysteme: Marktlage und Checkliste. In: Praxis der Informationsverarbeitung im Krankenhaus 13: 147-156.

Schmücker P. (1998a): Archivierung und Präsentation von heterogenen klinischen Objekten in elektronischen Patientenakten. Dissertation, Universität Heidelberg, Institut für Medizinische Biometrie und Informatik, Abteilung Medizinische Informatik.

Schmücker P. (1998b): Erzeugung und Ablage digitaler Dokumente: Revisionsfähigkeit und Systemsicherheit. In: Praxis der Informationssysteme im Krankenhaus 15: 19-24

Schmücker P., Horst H., Pordesch U., Rossnagel A. (2006): Grundlagen. In: Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Rechtssicherheit?: 9-15.

SigG (2001): Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften. Bundesgesetzblatt Teil I Nr. 22 2001: 876-884.

VOI Verband Organisations- und Informationssysteme e. V. (2004): TÜV Informationstechnik GmbH: PK-DML - Prüfkriterien für Dokumentenmanagement-Lösungen, 2. Auflage. Bonn, Essen: VOI Verband Organisations- und Informationssysteme e. V.

VOI Verband Organisation und Informationssysteme e.V. (2005): Dokumenten-Management. Vom Archiv zum Enterprise-Content-Management. Bonn: VOI – Verband Organisation und Informationssysteme e.V.

Viebeg U. (2006): Langzeitsicherung elektronisch signierter Dokumente. AWV-Informationen 2/2006.

Von Seck C. (2003): Die elektronische Signatur im Hinblick auf die Haftung der Zertifizierungsdiensteanbieter. Marburg: Inaugural-Dissertation.

Weiß D., Böhn M., Angerhausen K., Hagn A. (2005): Dokumenten-Management. 13 Dokumenten-Management-Systeme im Vergleich. München: Oxygon.

Winter A., Winter An., Becker K., Bott O., Brigl B., Gräber S., Hasselbring W., Haux R., Jostes C., Penger O., Prokosch H., Ritter J., Schütte R., Terstappen A. (1999a): Referenzmodelle für die Unterstützung des Managements von Krankenhausinformationssystemen. In: Informatik, Biometrie und Epidemiologie in Medizin und Biologie 30(4): 173-189.

Winter A. (2004): Medizinische Begriffs- und Dokumentationssysteme - Medizinische Dokumentation. Vorlesungsskript Universität Leipzig.

Winter A., Ammenwerth E., Brigl B., Haux. R.(2005): Krankenhausinformationssysteme. In: Lehmann, T. Handbuch der Medizinischen Informatik. München: Carl Hanser Verlag: 549-623.

Zaiß A., Graubner B., Ingenerf J., Leiner F., Lochmann U., Schopen M., Schrader U., Schulz S. (2005): Medizinische Dokumentation, Terminologie und Linguistik. In: Lehmann, T. Handbuch der Medizinischen Informatik. München: Carl Hanser Verlag: 89-143.

Zivilprozessordnung (2005): Bekanntmachung der Neufassung der Zivilprozessordnung. Bundesgesetzblatt Teil I Nr. 72 2005: 3202-3378.

Internet-Publikationen:

3LGM^2, http://www.3lgm2.de/Metamodell, aufgerufen am 27.04.2006

Allgemeines Krankenhaus (AKH) Wien, http://www.akhwien.at/default.aspx?pid=27, aufgerufen am 22.09.2006

ArchiSig, http://www.archisig.de, aufgerufen am 26.04.2006

Archivas (2004): Digital Archiving Strategies for Regulatory Compliance in Healthcare, http://www.archivas.com:8080/product_info/z3_pdfs_gh23/Digital_Archiving_Strategies_HC_03_11_05.pdf, aufgerufen am 30.09.2006

Brandner R. (2005): Rechtssicherheit bei der Archivierung durch qualifizierte elektronische Signaturen. 10. Fachtagung „Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen (KIS)", http://www.informatik.fh-mannheim.de/aku/aku-daten/kis2005/Brandner_KIS%202005_Vortrag_Brandner.pdf, aufgerufen am 26.04.2006

BSI (2005): IT-Grunschutzhandbuch, http://www.bsi.de/gshb/deutsch/download/itgshb_2005.pdf, aufgerufen am 29.09.2006

BDSG: Bundesdatenschutzgesetz. Neugefasst durch Bek. v. 14.1.2003 | 66. http://www.datenschutzzentrum.de/material/recht/bdsg2001/bdsg2001.htm, aufgerufen am 04.10.2006

CMS (2004): Security 101 for Covered Entities. http://www.cms.hhs.gov/EducationMaterials/Downloads/Security101forCoveredEntities.pdf, aufgerufen am 03.10.2006

Himss (2003): Standards Insight. An Analysis of Health Information. http://www.himss.org/content/files/StandardsInsight/2003/04-2003.pdf, aufgerufen am 14.09.2006.

i.s.h.med, http://www.ishmed.de/de/html/downloads/produktblaetter.html, aufgerufen am 08.09.2006

KOFAX, http://www.dicomgroup.de/DICOM/europe/web_eur.nsf/2ffd03bb13f8663248256f39001bff18/8472187602900435c1256fe80051eaf6?OpenDocument, aufgerufen 08.09.2006

MBO-Ä (2004): (Muster-) Berufsordnung für die deutschen Ärztinnen und Ärzte (Stand 2004). http://www.bundesaerztekammer.de/30/Berufsordnung/10Mbo, aufgerufen am 04.10.2006

MI-Lexikon: Lexikon der Medizininformatik, http://www.medi-informatik.de/lex/HCM, aufgerufen am 30.06.2006.

OLG: Archivierung von Behandlungsunterlagen durch private Unternehmen, http://www.zv.uni-wuerzburg.de/datenschutz/Urteile/archiv.htm, aufgerufen am 27.05.2006

Project Consult (2004): Newsletter 20040315. http://www.project-consult.net/Files/20040315.pdf, aufgerufen am 03.10.2006

RöVo (2002): Verordnung zur Änderung der Röntgenverordnung und anderer atomrechtlicher Verordnungen. Vom 18. Juni 2002. http://online-media.uni-marburg.de/radiologie/glossar/roentgen_verordnung.pdf, aufgerufen am 21.10.2006

Sächsisches Krankenhausgesetz: Gesetz zur Neuordnung des Krankenhauswesens mit Stand vom 01. Juni 2005, http://www.saxonia-verlag.de/recht-sachsen/252_2bs.pdf, aufgerufen am 26.05.2006

SAP (2001): SAP ArchiveLink (BC-SRV-ARL). http://help.sap.com/printdocu/core/Print46c/de/data/pdf/BCSRVARL/BCSRVARL.pdf, aufgerufen am 30.06.2006

Schell W.: http://www.wernerschell.de/Rechtsalmanach/Schutz%20der%20Patientendaten/weitergabevonpatientendaten.htm, aufgerufen am 27.05.2006

TransiDoc, http://www.transidoc.de, aufgerufen am 15.06.2006

U.S. Department of Health and Human Services Office for Civil Rights: Consumer summary. http://www.hhs.gov/ocr/hipaa/consumer_summary.pdf, aufgerufen am 03.10.2006

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULDa): Das Datenschutz-Gütesiegel für IT-Produkte, http://www.datenschutzzentrum.de/download/audsieeu.pdf, aufgerufen am 26.05.2006.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULDb), http://www.datenschutzzentrum.de/guetesiegel/register.htm, aufgerufen am 26.05.2006

Informationsmaterialien zu dem Produkt d.3:

d.3 Module in der Übersicht, http://www.portal-systems.net/index.php?action=show_site&id=75, aufgerufen am 10.10.2006

d.velop AG (2005): Handbuch d.3 content service.

d.velop AG: Produktbroschüre.

d.velop AG (2005): Produkthandbuch d.3 local engine.

Informationsmaterialien zu dem Produkt HYDMedia:

HYDMedia: Das medizinische Content Management System. Rottenburg: Heydt-Verlags-GmbH.

HYDMedia (2005): White Paper. Module und Funktionalitäten. Rottenburg: Heydt-Verlags-GmbH.

Informationsmaterialien zu dem Produkt forcont factory:

forcont business technology GmbH (2006): Technical White Paper.

forcont business technology GmbH (2006): White Paper.

Informationsmaterialien zu dem Produkt EMC Centera:

EMC Corporation (2006): EMC Centera. Content-Adressed Storage. Product Description Guide.

EMC Corporation (2004): Memorial Hermann Healthcare System. Customer Profile.

EMC Deutschland GmbH (2006): EMC Centera™-Archivierungslösung.

Walsdorf O. (2005): Archivierung – Stand, Trends und Visionen.

Abbildungsverzeichnis

Tabellenverzeichnis

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Leipzig, 26. Oktober 2006

Sabine Lehmann