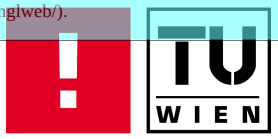

FAKULTÄT FÜR !NFORMATIK

Pseudonymisierter Arztbrief auf Basis der HL7 CDA R2 für den sicheren Austausch und die sichere Archivierung

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering & Internet Computing

eingereicht von

Markus Pehaim, BSc.
Matrikelnummer 0309108

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: O.Univ.Prof. Dr. A Min Tjoa
Mitwirkung: Dipl.-Ing. Mag. Dr. Thomas Neubauer

Wien, März 2010

(Unterschrift Verfasser) (Unterschrift Betreuer)

Erklärung der Selbstständigkeit

Markus Pehaim, BSc
Eduard-Suess-Gasse 1/30
A-1150 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, März 2010 Markus Pehaim

Danksagung

Ich möchte mich in erster Linie bei meiner Frau Katharina für ihre Unterstützung in allen sehr turbulenten Lebenslagen, die wir während der Erstellung dieser Arbeit durchgemacht haben, bedanken. Ganz herzlich möchte ich mich auch bei meinen Eltern für ihre Unterstützung während meines Studiums bedanken. Ein besonderer Dank gebührt auch Mathias, der mich die ganze Zeit durch mein Studium begleitet hat und mit dem ich so manche Übung erfolgreich bestanden habe. Dass diese Arbeit fehlerfrei vorliegt, ist ebenfalls meiner Germanistik-Gattin zu verdanken!

Man kann niemanden überholen, wenn man in seine Fußstapfen tritt.

Francois Truffaut

Kurzfassung

Der Einzug der Digitalisierung im Gesundheitswesen erfolgt mit großen Schritten da diese die Administration und Verwaltung enorm vereinfacht. Weiters hilft die Digitalisierung auf diese Weise in weiterer Folge Kosten zu sparen. Die Digitalisierung bringt jedoch nicht nur Vorteile mit sich, sondern rückt die Thematik der Privatsphäre eines Patienten in ein neues Licht. Da mittels Computernetzwerken auf digitale Patientenakten zugegriffen wird, erhöht dies die Gefahr eines Missbrauches beziehungsweise eines unautorisierten Zugriffs drastisch.

Diese Diplomarbeit beschäftigt sich mit dem auf Health Level Seven (HL7) basierenden Arztbrief. Der Arztbrief dient zum Austausch von Patienteninformationen zwischen verschiedenen Gesundheitsdienstanbietern beziehungsweise von Forschungseinrichtungen. Es werden die Daten eines Arztbriefes analysiert und entsprechend ihrer Vertraulichkeit eingestuft.

Auf Basis dieser Einstufung wird in weiterer Folge das Konzept von PIPE (Pseudonymization of Information for Privacy in e-Health) dahingehend erweitert, dass eine Anwendung dieses Services auf HL7-Dokumente ermöglicht wird. Aus diesem Grund werden neue Abläufe definiert und die Datenstruktur erweitert, um diesen neuen Anforderungen gerecht zu werden.

Mit Hilfe dieser Diplomarbeit entsteht eine Richtlinie für zukünftige Entwicklungen im Bereich des Gesundheitswesens, um eine sichere Speicherung beziehungsweise einen sicheren Austausch von Dokumenten auf Basis von HL7 zu gewährleisten. Weiters wird ein unautorisierter Zugriff auf sensible Daten verhindert und so die Privatsphäre von Patienten gewahrt.

Abstract

The advent of digitization in the health sector is making great strides as it greatly simplifies the administration and management. Furthermore the digitization will help in this way to subsequently cut costs. Digitization however brings not only advantages but also puts the issue of the patient's privacy in a new light. Being accessed via computer networks, digital patient records increases the risk of abuse or of unauthorized access drastically.

This thesis deals with the doctor's letter based upon Health Level Seven (HL7). The doctor's letter is used to exchange patient information between various health care providers or by research. We analyze the data of a discharge letter and classify them according to their confidentiality.

Based on this classification the concept of PIPE (Pseudonymization of Information for Privacy in e-Health) will be extended to allow an application of this service on HL7 documents. For this reason, new procedures are defined and the data structures are extended to meet these new requirements.

With the help of this thesis, a guideline for future developments in the field of health care arises to ensure secure storage and secure exchange of documents based on HL7. Furthermore this concept prevents unauthorized access to sensitive data and it preserves the patient's privacy.

Inhaltsverzeichnis

KAPITEL 1

Einleitung

Dieses Kapitel gibt eine Einführung in die vorliegende Diplomarbeit. Hier wird die Motivation beschrieben, ein Überblick über die Ziele dieser Diplomarbeit gegeben und die nachfolgende Struktur der Diplomarbeit dargestellt.

1.1 Motivation

Das Thema Privatsphäre ist heutzutage ein sehr wichtiges, weil die Anzahl von digital gespeicherten und via Computernetzwerken verfügbaren Daten stetig steigt. An dieser Stelle müssen wir dafür Sorge tragen, wie vertrauliche Informationen (Yee et al., 2006) sicher gespeichert werden können. Aus diesem Grund gewinnt das Thema Privatsphäre immer mehr an Bedeutung. Im Speziellen fordern moderne e-Services, wie e-Banking, e-Government und e-Health, sichere Lösungen zum Speichern und Abrufen sensibler Daten. In dieser Arbeit wird der Fokus auf e-Health, im Speziellen auf den Arztbrief, ein Teilbereich der Elektronischen Gesundheitsakte (ELGA) (IBM und Prenner, 2006), und den Datenaustausch dieser ELGA zwischen Gesundheitsdienstleistern gelegt.

ELGAs haben im Vergleich zu traditionellen Papier basierten Dokumenten eine Reihe von Vorteilen. ELGAs sparen Zeit und auch Kosten (Riedl et al., 2007c), beugen multiplen Untersuchungen vor (IBM und Prenner, 2006), können die Medikamentation verringern (IBM und Prenner, 2006) und dienen auch als Grundlage für die Forschung.

Es gibt bereits zahlreiche Anwendungen von ELGAs, welche auf Health Level Seven Clinical Document Architecture (HL7 CDA) (2, 2009) basieren. Hierzu zählen unter anderem folgende Ansätze: 1) Kuhns „Electronic medical summary“-Projekt 7 (2009),

2) die Erstellung von klinischen Dokumenten innerhalb eines Krankenhausinformationssystems (KIS) (Kim et al., 2006), 3) Entscheidungsunterstützungssysteme (engl. decision support system), welche CDA integrieren von Bilykh et al. (2006) und 4) eine kardiologische Datenkommunikation (Marcheschi et al., 2005).

Die Verwendung von ELGAs birgt nicht unbedeutende Risiken (Kotulski und Zwierko, 2005), welche zu einem Datenmissbrauch führen können. Zum Beispiel sind Forscher in der Lage die Daten, welche Sie für ihre Forschungszwecke erhalten, eindeutig Personen zuzuordnen. Ein bekanntes Beispiel, welches Datenmissbrauch aufzeigt, ist der Zugriff von Zahnärzten auf die psychiatrischen Gutachten seiner Patienten. Außerdem könnte sich ein Arbeitgeber über den Gesundheitszustand eines Bewerbers beziehungsweise eines zukünftigen Mitarbeiters informieren. Die aufgezählten Risiken müssen mit Hilfe von speziellen sicherheitstechnischen Maßnahmen minimiert werden. Diese Maßnahmen müssen bestimmten Kriterien entsprechen, um die Privatsphäre der Patienten zu schützen. Diese Maßnahmen müssen den nachfolgend aufgezählten Anforderungen entsprechen: (i) Die Daten dürfen nicht analysierbar sein, (ii) der Patient soll eine Möglichkeit zur Zugriffssteuerung seiner Daten erhalten und (iii) die Forschung soll Zugriff auf die Daten bekommen, ohne eine direkte Verbindung zum Patienten zu ermöglichen. Diese Verbindung darf nur durch autorisierte Personen/Organisationen beziehungsweise nur durch den Patienten selbst erfolgen.

Um diese Risiken zu minimieren, existieren einige Techniken. Diese sind zum Beispiel Verschlüsselung, Anonymisierung oder Pseudonymisierung. Anonymisierung und Verschlüsselung erfüllen jedoch nicht die gewünschten Anforderungen, da es möglich sein soll, eine Verbindung zwischen Daten und Person herzustellen, um den Patienten gegebenenfalls informieren zu können, wenn zum Beispiel ein Gegenmittel für eine bestimmte Krankheit entwickelt wurde. Bei verschlüsselten Daten wird der Zugriff auf die Daten der Forschung verwehrt und somit ist der Ansatz der Verschlüsselung auch keine geeignete Technik. Ein Ansatz, welcher die geforderten Anforderungen erfüllt, ist Pseudonymisierung (Kotulski und Zwierko, 2005). Hierbei wird die Verbindung zwischen Daten und Person mithilfe eines Pseudonyms versteckt. Somit ist es in weiterer Folge möglich, im Bedarfsfall diesen Link wieder herzustellen.

Nur der Eigentümer der Daten darf einen Vollzugriff auf diese erhalten. Es muss ermöglicht werden, den Zugriff auf einzelne Datensätze zu steuern. Diese Option darf allerdings nur in der Hand des Patienten liegen (Goldman und Hudson, 2000). Somit kann der Patient einen Arzt autorisieren, beziehungsweise die Rechte wieder entziehen, falls der Arzt den Zugriff auf seine klinischen Daten nicht mehr benötigt.

Da die elektronische Vernetzung im Gesundheitswesen voranschreitet, schlägt das ELGA-Konzept (IBM und Prenner, 2006) vor, elektronische Gesundheitsakten auf Basis von HL7 zu verwenden. Dieser Standard wird als Clinical Document Architecture Release 2 (CDA-R2) bezeichnet. HL7 CDA-R2 standardisiert die Dokument-Struktur, den Inhalt des Dokuments und wird zum Austausch klinischer Dokumente verwendet.

Ein klinisches Dokument, welches den CDA-R2-Standard umsetzt, muss folgende Kriterien beziehungsweise Merkmale erfüllen: (i) persistente Dokumentation, (ii) die Verantwortung für das Dokumenten-Management, (iii) die Möglichkeit das Dokument elektronisch zu signieren, (iv) definierten Inhalt, (v) Vollständigkeit des Dokuments und (vi) die menschliche Lesbarkeit (2, 2009). In unserem Ansatz wahrt dieser Kommunikations-Standard die Privatsphäre der pseudonymisierten Gesundheitsdaten.

In der Gesundheitstelematikverordnung vom 9. Dezember 2008 (6, 2008) wird die Datensicherheit anhand von Kriterien wie Identität, Rollen, Vertraulichkeit, Integrität und Dokumentationspflicht definiert. Paragraph § 3 der Verordnung betreffend der Vertraulichkeit der Daten lautet:

> § 3. (1) Die Vertraulichkeit beim elektronischen Gesundheitsdatenaustausch ist dadurch sicherzustellen, dass
>
> 1. 1. der elektronische Gesundheitsdatenaustausch über Netzwerke durchgeführt wird, die entsprechend dem Stand der Netzwerksicherheit hinreichend gegenüber unbefugten Zugriffen abgesichert sind, indem sie zumindest
>
>   a) die kryptographische Absicherung des Datenverkehrs,
>
>   b) den Netzzugang ausschließlich für eine geschlossene oder abgrenzbare Benutzergruppe sowie
>
>   c) die Authentifizierung der Benutzer vorsehen, oder
>
> 2. Protokolle und Verfahren verwendet werden, die
>
>   a) die vollständige Verschlüsselung der Gesundheitsdaten ermöglichen und
>
>   b) deren kryptographische Algorithmen in der Anlage 2 angeführt sind.

1.2 Ziele

Im Zuge dieser Diplomarbeit werden folgende Fragen beantwortet:

- Wo kann PIPE in Kombination mit HL7 implementiert werden?
- Wie kann HL7 in eine pseudonymisierte ELGA integriert werden?
- Wie sieht die optimale Synergie zwischen HL7 und Pseudonymisierung aus?
- Gibt es Probleme mit der Verwendung von Pseudonymisierung in Verbindung mit HL7?

In diesem Lösungsansatz wird ein Überblick über Privatsphäre in e-Health geben. Der Fokus der Arbeit wird auf pseudonymisierte HL7-Kommunikation zwischen den Gesundheitsdienstleistern gelegt. Hier wird als Beispiel der Arztbrief herangezogen.

Weiters wird die Integration von Pseudonymisierung in HL7 präsentiert. Aus diesem Grund wird das Konzept von CDA erläutert und die Adaptionen vorgestellt. In weiterer Folge werden typische Workflows zur Pseudonymisierung, Depseudonymisierung und zum Datenaustausch vorgestellt. Das Design zur Integration von HL7 in PIPE wird präsentiert.

Abschließend werden Fallbeispiele der pseudonymisierten Kommunikation mit HL7 vorgestellt.

1.3 Struktureller Aufbau dieser Arbeit

Diese Diplomarbeit behandelt die Wahrung der Privatsphäre von Patienten und wird anhand von Pseudonymisierung des Arztbriefes nach CDA R2 dargestellt und erläutert. Aus diesem Grund wird das Thema Privatsphäre behandelt und weiters auf die gültigen Datenschutzbestimmungen eingegangen, der Begriff e-Health genauer definiert und in Zusammenhang mit der Privatsphäre gebracht. Außerdem wird das Konzept von Health Level Seven (2, 2009) erläutert.

Nachdem die Grundlagen eingeführt und erläutert wurden, kann das Hauptaugenmerk dieser Arbeit auf PIPE (Pseudonymization of Information for Privacy in e-Health) gelegt werden und das Konzept von PIPE im Detail erläutert werden. Hierzu wird die Architektur beschrieben und auf die Struktur der Datenbank eingegangen. Im Anschluss werden typische Operationen, welche in PIPE auftreten im Detail beschrieben.

Im abschließenden Kapitel wird auf die Integration von HL7 in PIPE als Datenkommunikationsstandard eingegangen. Anfangs wird der Arztbrief einer Datenanalyse unterzogen. Im Folgenden werden die in PIPE notwendigen Adaptionen vorgestellt und ein Implementierungsvorschlag präsentiert. Einige Kommunikationsbeispiele geben einen Überblick über die Anwendungsgebiete von pseudonymisierter CDA.

KAPITEL 2

Grundlagen

Im nachfolgenden Kapitel werden Definitionen, welche für diese Arbeit relevant sind, erklärt. Zu diesen Definitionen zählen Privatsphäre, e-Health und Privatsphäre im Bereich e-Health. Weiters werden die derzeit geltenden Gesetze und Datenschutzbestimmungen erwähnt. Ebenfalls behandelt wird der klinische Standard Health Level Seven (HL7) und die damit zusammenhängende Dokumentenarchitektur Clinical Document Architecture (CDA). Die derzeit vorhandenen Sicherheitskonzepte werden aufgezeigt. Abschließend wird auf die konkrete Technologie der Pseudonymisierung als Sicherheitskonzept im Bereich e-Health eingegangen. Dieses Kapitel dient dem besseren Verständnis der nachfolgenden Kapitel.

2.1 Privatsphäre

Privatsphäre beziehungsweise das weit verbreitete Pendant *Privacy* bezeichnet den Bereich einer Person, der nicht öffentlich ist, sondern nur diese Person selbst betrifft. Privacy wurde bereits im 19. Jahrhundert von Warren und Brandeis (1890) als:

> ... the right to be let alone ... (Warren und Brandeis, 1890)

definiert. Diese Definition wurde Mitte des 20. Jahrhunderts von Westin (1968) in folgender Weise neu aufgegriffen und erweitert:

> ... the right to control when, what and how personal information is communicated to others ... (Westin, 1968)

Artikel 12 der Allgemeinen Erklärung der Menschenrechte, welche von den Vereinten Nationen (1948) veröffentlicht wurde, legt Folgendes fest:

> Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen. (3, 1948)

Rachels (1985) spricht in ihrer Publikation von der Verwendung von bestimmten Mitteln zur Erstellung eines sozialen Kontext, wenn wir in Beziehung mit anderen Menschen stehen:

> ... a means for creating social context in relationships with others ... (Rachels, 1985)

Heutzutage ist auch diese Spezifikation nicht mehr ausreichend. Kuhlen (1999) behauptet, dass Privatsphäre mehr als nur das „Recht alleine gelassen zu werden“ sein sollte. Es sollte vielmehr die Möglichkeit der Kontrolle von personenbezogenen Informationen bestehen. Weiters sollte jedem die Option gegeben werden, Informationen seiner Person betreffend zu kontrollieren und die Nutzung dieser Daten festzulegen.

2.2 Datenschutz

Die einleitenden Worte der Europäischen Kommission für Datenschutz in der Datenschutzrichtlinie 95/46/EG lauten:

> Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefwechsels. (4, 2004)

Diese Worte stellen sogleich die Grundlage des Datenschutzes dar. Der Datenschutz selbst umfasst den Missbrauchsschutz personenbezogener Daten. Unter personenbezogenen Daten sind alle Informationen zu verstehen, mit deren Hilfe es möglich ist, die Identifizierung einer Person durchzuführen. Beispiele dieser Daten sind Namen, Telefonnummern und Fotos (4, 2004). Die Datenschutzrichtline kommt bei allen kommerziellen Vorgängen zum Einsatz, die mit der Verarbeitung personenbezogener Daten in Verbindung stehen. Dazu zählen unter anderem das Erheben, Speichern und die Weitergabe von personenbezogenen Daten. Die Datenverarbeitung im privaten Umfeld, wie zum Beispiel eine Adresskartei von Freunden, ist von der Datenschutzrichtline nicht betroffen (4, 2004). Weiters kommt die Datenschutzrichtline in Bereichen wie der öffentlichen Sicherheit und der Landesverteidigung zum Einsatz (4, 2004). Die Verantwortlichen für die Datenverarbeitung sind Institutionen oder Personen, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (4,

2004). Diese müssen die in der Datenschutzrichtline definierten Vorschriften einhalten. Personenbezogene Daten dürfen nur verarbeitet werden, wenn der Betroffene seine Einwilligung dazu gegeben hat, die Daten zur Erfüllung eines Vertrages notwendig sind, die Verarbeitung gesetzlich vorgeschrieben ist, das Leben der betroffenen Person dadurch geschützt wird, oder die Aufgaben des öffentlichen Interesses wahrgenommen werden (4, 2004).

2.3 e-Health

Der Begriff e-Health wird in der heutigen Zeit sehr gerne verwendet, obwohl zu diesem Begriff keine genaueren Definitionen existieren. e-Health bezieht sich nicht direkt auf die Gesundheit der Menschen, sondern bezeichnet vielmehr Systeme und Services, die direkt oder auch indirekt mit der Gesundheit in Beziehung stehen. Eysenbach (2001) definierte e-Health wie folgt:

> e-health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology. (Eysenbach, 2001)

Die nachfolgende These, welche von Prokosch (2001) aufgestellt wurde, verdeutlicht dies:

> Der mündige Bürger wird für die elektronische Kommunikation und Integration seiner Gesundheitsdaten in Zukunft eine entscheidende Rolle einnehmen. (Prokosch, 2001)

Einer der wichtigsten Aspekte von e-Health ist der schnelle Zugriff auf Informationen zwischen autorisierten Personen (Barrows und Clayton, 1996).

2.4 Privatsphäre und Sicherheit in e-Health

Die Privatsphäre beginnt mit einem guten Verhältnis zwischen Arzt und Patient, denn zwischen diesen beiden Akteuren des Gesundheitssystems werden immer vertrauliche

Informationen ausgetauscht (Goldman, 1998). In diesem Szenario werden persönliche Informationen über sich selbst beziehungsweise Familienmitglieder preisgegeben (U.S. Congress Office of Technology Assessment, 1993). Somit ist die Privatsphäre hier besonders angreifbar, da diese Informationen in einem breiten Anwendungsfeld wiederverwendet werden können (Goldman, 1998). Ein Patient könnte dem entgegenwirken, in dem er alle Leistungen bar bezahlt. Auf diese Weise können Sachverhalte verschleiert werden, oder Behandlungen schlichtweg nicht durchgeführt werden. In weiterer Folge werden nicht alle Informationen bei einem Datenhalter gespeichert (Goldman et al., 1996). Diese Reaktion hat jedoch Auswirkungen auf die Qualität der erbrachten Leistung, wie in Tabelle 2.1 (Goldman, 1998) ersichtlich.

Elektronische Gesundheitsakten werden in der heutigen Zeit immer wichtiger und avancieren zu Schlüsselapplikationen in Krankenhausinformationssystemen (Blobel, 2004). Aus diesem Grund ist es auch wichtig, sich Gedanken über die Privatsphäre der Patienten zu machen. Sehr viele Patienten haben Angst davor, dass ihre Gesundheitsinformationen missbraucht werden und sie dadurch geschädigt werden (Goldman und Hudson, 2000). Carter (2000) zeigt einige Beispiele von Problemen mit elektronischen Gesundheitsdaten auf, die entstehen können, wenn Informationen elektronisch gesammelt, sortiert und Patienten zugeordnet werden. Zu diesen Problemen zählen unter anderem: (i) Mitarbeiter von Krankenkassen „durchstöbern“ Patientenakten, (ii) der HIV-Status wird als Information in einer Krankenhausapplikation angezeigt, selbst wenn dieser für die Behandlung unerheblich ist und (iii) Falsche Behandlung wegen einer veralteten elektronischen Patientenakte. Somit werden viele Informationen Personen zugeordnet und für unterschiedliche Anwendungen genutzt, ohne dass dies der Patient je erfährt (Goldman und Hudson, 2000). Es gibt jedoch auch bei der herkömmlichen Papier-Akte ähnliche Probleme, die nicht außer Acht gelassen werden sollen (Carter, 2000). So gehen einer amerikanischen Studie (Foundation, 1999) zufolge rund 20 Prozent der Befragten davon aus, dass ihre Gesundheitsinformationen bereits missbraucht wurden.

Auswirkungen
Schlechte Qualität der Leistung, Krankheiten können übersehen werden
Aufgrund unvollständiger Informationen ist die Diagnosefähigkeit der Ärzte eingeschränkt
Durch separate Datenhaltung seitens des Arztes können Fehler in Folgedokumenten entstehen
Datenintegrität der Informationen leidet. Daten sind nicht repräsentativ

Tabelle 2.1: Auswirkungen bei Verhinderung des Datenspeicherns bei nur einem Datenhalter (Goldman, 1998)

Barrows und Clayton (1996) definierten insgesamt vierzehn Bereiche, welche für Sicherheitsrichtlinien in e-Health von Bedeutung sind. Diese Bereiche können wiederum in vier weitere Hauptgruppen unterteilt werden. Diese sind (i) physische Sicherheitsmechanismen, (ii) programmtechnische Sicherheitsmechanismen, (iii) Richtlinien und Aktionen und (iv) Präventivmaßnahmen. Zu der Gruppe der physischen Sicherheitsmechanismen werden (i) Physische Sicherheit von Rechenzentren, (ii) Berechtigungskontrolle zu Systemressourcen, (iii) Sicherheitsmechanismen für Papier basierte Materialien und (iv) Netzwerksicherheit gezählt. Der Bereich der programmtechnischen Sicherheitsmechanismen weist die Punkte (i) Benutzerauthentifizierung, (ii) Sicherheitsmechanismen in Systeme integrieren, (iii) Benutzerprofile und (iv) Systemintegrität auf. Unter Richtlinien und Aktionen fallen die Punkte (i) Richtlinien zur Datensicherung, (ii) Juristische Belange und Haftung und (iii) Einverständniserklärung. Die vierte Hauptgruppe, die Präventivmaßnahmen vereinen (i) Datenbesitz, (ii) Problemidentifizierung und -elimination und (iii) Schulung der Benutzer.

Die US-Bürgerrechtsorganisation hat nachfolgende Prinzipien zur Wahrung der Privatsphäre im Gesundheitsbereich festgelegt (American Civil Liberties Unioin, 1994). Wenn diese befolgt werden, kann die Privatsphäre des Patienten gewährleistet werden.

1. Strict limits on access and disclosure must apply to all personally-identifiable health data, regardless of the form in which the information is maintained.
2. All personally-identifiable health records must be under an individual's control. No personal information may be disclosed without an individual's uncoerced, informed consent.
3. Health record information systems must be required to build in security measures to protect personal information against both unauthorized access and misuse by authorized users.
4. Employers must be denied access to personally-identifiable health information on their employees and prospective employees.
5. Patients must be given notice of all uses of their health information.
6. Individuals must have a right of access to their own medical and financial records, including rights to copy and correct any and all information contained in those records.
7. Both a private right of action and a governmental enforcement mechanism must be established to prevent and/or remedy wrongful disclosures or other misuse of information.

8. Establishment of a federal oversight system to ensure compliance with privacy laws and regulations.

Jeder Patient muss das Recht haben, die von ihm gespeicherten Gesundheitsinformationen zu verwalten. So sollte es möglich sein, dass ein Patient seine Daten einsehen darf. Weiters soll der Patient informiert werden, wenn jemand auf seine Daten zugreift und die Möglichkeit der Einschränkung des Zugriffs Dritter soll bestehen (Goldman und Hudson, 2000).

Es genügt nicht mehr, die Kontrolle der Rechte auf einem reinen Benutzerlevel zu realisieren (Blobel, 2004), vielmehr sind Richtlinien gefragt, welche die Privatsphäre wahren. Ein Zusammenspiel aus rollenbasiertem System, das den Zugriff und die Autorisierung steuert, und einer sicheren Kommunikation über Private Key Infrastruktur (Xenitellis, 2000), wie in der Publikation von Blobel (2004) beschrieben, ermöglicht eine Zugriffssteuerung der klinischen Daten.

Jede Gruppe von Anwendern (Mediziner, Patienten, medizinisches Personal, Apotheker und Krankenkassen) haben unterschiedliche Sicherheitsanforderungen (Bleumer und Schunter, 1997). Diese Anforderungen werden von Bleumer und Schunter (1997) in (i) Verfügbarkeit und Integrität und (ii) Vertraulichkeit und Privatsphäre unterteilt.

In Tabelle 2.2 werden die Anforderungen an Verfügbarkeit und Integrität von Medizinern, Patienten, medizinischem Personal, Apothekern und Krankenkassen angeführt. Die Anforderungen an Vertraulichkeit und Privatsphäre von Medizinern, Patienten, medizinischem Personal und Apothekern sind in Tabelle 2.3 aufgelistet.

Anwender	Verfügbarkeit und Integrität
Mediziner	Jeder Patient soll nur die ihm verschriebene Leistung erhalten. Jedes Rezept darf nur ein Mal verwendet werden.
Patient	Wenn ein Patient eine gültige Versicherungskarte, Überweisung oder ein Rezept vorweist, soll der Gesundheitsdienstanbieter die gewünschte Leistung durchführen.
med. Personal / Apotheker	Alle Ausgaben sollen von den Krankenkassen erstattet werden, sofern er mit ihnen in einem vertraglichen Verhältnis steht.
Krankenkassen	Nur registrierte Mediziner dürfen Rezepte ausstellen. Jeder Patient soll eine Leistung nur so oft in Anspruch nehmen, wie dies vorgesehen ist. Jede Krankenkasse soll die geforderten Ausgaben nur einmal rückerstatten, sofern diese für einen Versicherten ihrer Krankenkasse getätigt wurden. Krankenkassen sollen ein Limit für Rückerstattungen pro Jahr setzen dürfen.

Tabelle 2.2: Sicherheitsanforderungen per Anwendergruppe an Verfügbarkeit und Integrität (Bleumer und Schunter, 1997)

Anwender	Vertraulichkeit und Privatsphäre
Mediziner und Patient	Medizinische Behandlungen verlangen nach einem Vertrauensverhältnis zwischen Patient und Mediziner und alle Daten müssen vertraulich behandelt werden, dass diese nicht an Dritte gelangen können.
Mediziner	Krankenkassen dürfen nicht in der Lage sein, die Mediziner zu überwachen und die Leistungen für die Patienten festzulegen um dadurch Kosten zu sparen.
Patient	Gesundheitsdienstanbieter dürfen ihre Daten nicht untereinander austauschen, damit der Patient eine unabhängige zweite Meinung einholen kann.

Tabelle 2.3: Sicherheitsanforderungen per Anwendergruppe an Vertraulichkeit und Privatsphäre (Bleumer und Schunter, 1997)

2.5 Health Level Seven

Health Level Seven (HL7) ist ein vom American National Standards Institute (ANSI) (1, 2009) anerkannter Datentransfer-Standard (Dolin et al., 2006). Es sind zwei Versionen von HL7 verbreitet. HL7 V2 ist ein vage definiertes Informationsmodell, in dem nicht viele vordefinierte Felder existieren. Vielmehr gestaltet es sich vermehrt durch Freitexte (Eichelberg et al., 2005). Dieses Informationsmodell bietet eine große Flexibilität. Eine solche Flexibilität erschwert jedoch den Nachrichtenaustausch zwischen unterschiedlichen Systemen erheblich, da die Nachrichten und deren Struktur beziehungsweise deren Inhalt genau definiert werden müssen. Eine

Weiterentwicklung dieses Informationsmodells ist HL7 V3. Dieses Modell basiert auf dem sogenannten Informations-Modell (Abbildung 2.1). Die Daten sind objektorientiert dargestellt (Eichelberg et al., 2005). Diese HL7-Nachrichten können auf einfachem Weg zwischen unterschiedlichen Systemen ausgetauscht werden. Das Referenz Informations-Modell (RIM) repräsentiert die Gesamtheit aller Modelle der HL7 Domänen. Das Wurzel-Modell wird durch das RIM dargestellt. Bei HL7 gibt es eine Vielzahl von Domänen, welche in zwei große Gruppen unterteilt werden können: (i) Administration und (ii) Gesundheits- und Klinisches Management. Alle domänenspezifischen Informationen werden vom RIM abgeleitet und als Domänen-Nachrichten Informations Modell (englisch Domain-Message Information Modell D-MIM) bezeichnet. D-MIM ist eine Teilmenge von RIM und beschreibt die Nachrichten einer Domäne. Die eigentlichen Informationen einer Nachricht werden im sogenannten spezifischen Nachrichten Informations-Modell (englisch Refined-Message Informationen Model R-MIM) definiert.

2.5.1 Clinical Document Architecture

Die Clinical Document Architecture (CDA) ist ein XML[1] Dokument, das zum Austausch von Gesundheitsinformationen verwendet wird. CDA spezifiziert nicht den Inhalt eines Dokuments, sondern lediglich die Struktur und Semantik eines klinischen Dokuments. Ein CDA repräsentiert ein klinisches Dokument, wobei der Inhalt dieses klinischen Dokuments einem herkömmlichen Papier basierenden Dokument, wie zum

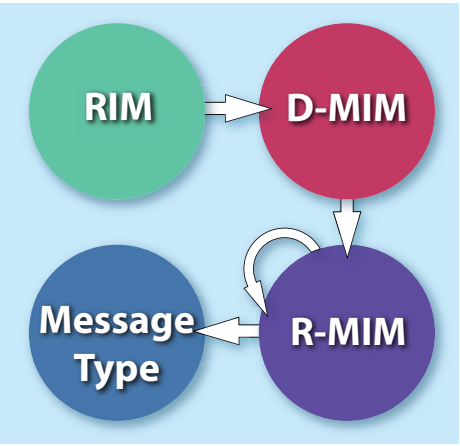

Abbildung 2.1: Referenz Informations Modell Prozess

1 Extensible Markup Language, http://www.w3.org/XML/

Beispiel dem Entlassungsbrief oder einem klinischen Befund, entspricht (2, 2009). Weiters kann CDA außerhalb des Nachrichtenübermittlungskontextes existieren und beschreibt ein eigenständiges Objekt. Es gibt derzeit zwei Versionen von CDA, Release 1 und Release 2. CDA Release 2 ist vollständig überarbeitet und bedient nun ein breiteres Spektrum an Dokumententypen. Die Informationen im Header des Dokuments wurden erweitert, somit ist es nun möglich, detailliertere Informationen abzubilden (Head, 2004). CDA Release 2 ist seit 2005 ein von ANSI standardisiertes Verfahren. Seit 2007 ist CDA Release 2 als Standard der Elektronischen Gesundheitsakte in Österreich definiert (Prenner, 2007). Ein Dokument, welches nach dem CDA Release 2-Standard erstellt wird, muss die nachfolgenden sechs Charakteristika aufweisen (Dolin et al., 2001):

- Persistente Dokumentation
- Verantwortlichkeit für das Dokumentenmanagement
- Möglichkeit das Dokument elektronisch zu signieren
- Definierten Kontext
- Vollständigkeit des Dokuments
- Für Menschen lesbar

CDA Release 2 basiert vollständig auf dem RIM. Eine schematische Darstellung eines CDAs ist in Abbildung 2.2 zu sehen.

Ein CDA ist grundsätzlich in zwei Teile unterteilt, den Header und den Body (siehe Abbildung 2.3). Der Header beinhaltet alle Informationen die der Identifizierung und Administrierung von klinischen Dokumenten dienen. Zu diesen zählen zum Beispiel allgemeine Patienteninformationen, Informationen zur Entlassung und zugeordneten Organisationen. Die Header-Informationen werden strukturiert und codiert angeführt. Der Body des Dokuments enthält die klinischen Informationen, externe Referenzen oder Freitexte und ist gekennzeichnet durch strukturierten Inhalt mit codiertem Bereich, sogenannten „sections“ (Heitmann, 2006).

Zur Differenzierung des Detailgrades werden CDAs in drei Level unterteilt. Mithilfe des ersten Levels wird nur eine eingeschränkte Interoperabilität gewährleistet. Die Informationen im Header sind strukturiert, der Body jedoch beinhaltet die klinischen Informationen lediglich als Freitext. Das zweite Level erweitert das Erste insofern, dass es auch möglich ist, den Body des Dokuments zu kodieren. Dies erweitert die Möglichkeiten der Interoperabilität des klinischen Dokuments. Im dritten Level ist das

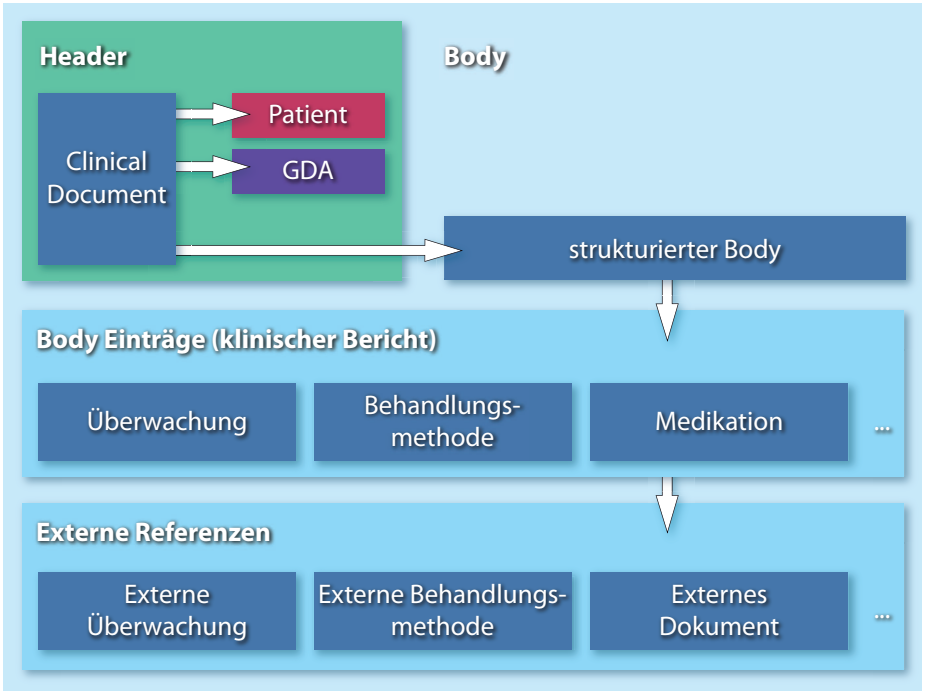

Abbildung 2.2: Schematische Darstellung eines CDA-Dokuments (Heitmann, 2006)

Dokument komplett strukturiert. Diese Struktur wird vom RIM abgeleitet. Dokumente, die nach Richtlinien des dritten Levels entworfen werden, ermöglichen eine effiziente Suche von Informationen. Diese vollständige Strukturierung hat jedoch den Nachteil, dass das Erstellen dieser Dokumente einen erheblichen Mehraufwand mit sich führt (Schanner et al., 2007).

Health Level Seven Beispiel Ein Beispiel einer XML-Nachricht ist in Abbildung 2.4 zu sehen. Das klinische Dokument ist unterteilt in Body und Header. Der Body beinhaltet die Anamnesedaten und im Header sind die Identifikatoren des Dokuments enthalten. Folgende vier Bereiche enthält ein klinisches Dokument:

- Headerdaten (H)
- Patientendaten (P)
- Erfasserdaten (A)
- Anamnesedaten (D)

Dem Header können die eigentlichen Headerdaten (H), die Patientendaten (P) und die Erfasserdaten (A) zugeordnet werden. Im Body sind die Anamnesedaten (D) zu finden.

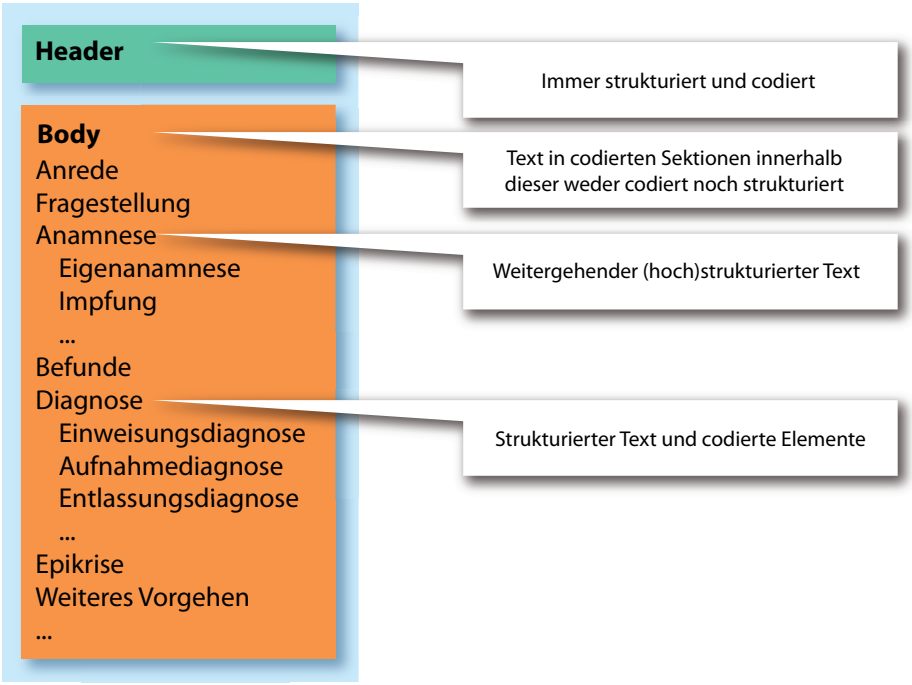

Abbildung 2.3: Aufbau eines CDA-Dokuments (Heitmann, 2006)

Das klinische Dokument wird mit dem Wurzelknoten `<ClinicalDocument>` eingeleitet. Der Header des Dokuments hat keinen spezifischen Bezeichner. Es gibt jedoch einige wichtige Elemente, welche im Header enthalten sein müssen. Zu diesen zählen `<id>`, `<authenticator>`, `<author>`, `<code>`, `<custodian>`, `<dataEnterer>`, `<effectiveTime>`, `<legalAuthenticator>` und `<recordTarget>`.

Der Body eines klinischen Dokuments ist innerhalb des `<StructuredBody>` Elements eingefasst und beinhaltet die eigentlichen klinischen Informationen. Der Body wird weiters unterteilt in unterschiedliche Bereiche, welche mit einem `<section>` Element identifiziert werden. Jeder Bereich kann eine beliebige Anzahl klinischer Daten, externer Referenzen oder Freitext-Blöcke enthalten.

2.5.2 Arztbrief auf Basis des Health Level Seven Clinical Document Architecture Release 2

Ein Arztbrief weist, wie jedes CDA-Dokument, einen Header und einen Body auf. Die Struktur des Headers ist genau definiert und enthält folgende drei Bereiche (Heitmann et al., 2006):

- ClinicalDocument Klasse

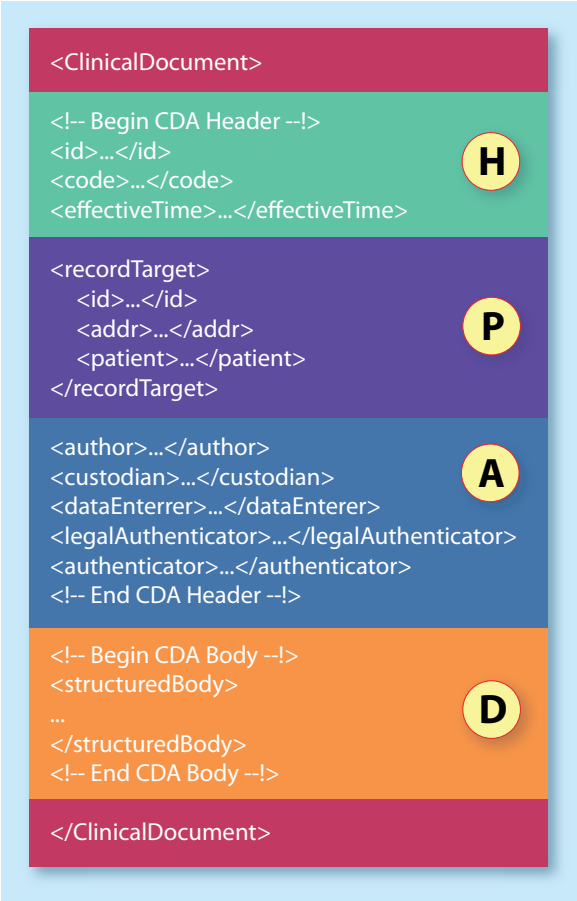

Abbildung 2.4: XML Datei

- Participations
- Act Relationships

Im ersten Bereich, der *ClinicalDocument Klasse* sind die nachfolgend aufgelisteten Informationen zwingend vorgeschrieben (Heitmann et al., 2006):

- Eine konstante Typ-Id
- Id des Dokuments
- Dokumenttyp
- Erstellungsdatum des Dokuments
- Vertraulichkeitsgrad

Die Informationen über die beteiligten Parteien eines Arztbriefes werden im Bereich *Participations* angeführt. Die dafür notwendigen Daten sind (Heitmann et al., 2006):

- Patient

- Autor der Dokumentation
- Personen bei der Dateneingabe
- Organisation, welche das Dokument erstellt hat

Die Beziehungen zwischen den beteiligten Personen sind im Bereich *Act Relationships* zu finden. Dieser Bereich beinhaltet nur den *CDA Body* als zwingend vorgeschriebenes Element (Heitmann et al., 2006).

Der Implementierungsleitfaden (Heitmann et al., 2006) schreibt vor, dass nur die dort angegebenen Elemente im Header vorkommen dürfen. Des Weiteren muss jede Person durch einen Namen, mit Hilfe dessen sie identifiziert werden kann, angegeben werden. Zusatzinformationen wie Adresse und Telefonnummer sollten ebenfalls vorhanden sein. Bei Gesundheitsdienstleistern ist die Angabe der Adresse und Telefonnummer im Gegensatz zu den Personen nicht obligatorisch. Organisationen müssen weiters noch die registrierte Organisationsidentifikationsnummer anführen.

Die medizinischen Informationen des Arztbriefes werden im Body des Dokuments angeführt.

Es steht dem Autor frei, unabhängig vom klinischen „Fall“, die aus seiner Sicht zusammengehörigen medizinischen Ereignisse eines Patienten in einem Arztbrief zusammenzustellen. Ein Arztbrief bezieht sich somit auf exakt einen Patienten und auf eine „Episode“ medizinischer Aktivitäten.

In Österreich sind die Inhalte eines Arztbriefes durch die Verordnung der Österreichischen Ärztekammer (5, 2008) genau spezifiziert.

Ein vollständiger Beispiel-Quelltext für einen Arztbrief im XML-Format befindet sich im Listing A.1. Dieser beinhaltet alle zuvor beschriebenen Elemente und demonstriert so das Erscheinungsbild des Arztbriefes.

2.5.3 Vorhandene Sicherheitskonzepte für Health Level Seven

Derzeit gibt es keine offiziellen Sicherheitsmechanismen, welche in der HL7 V3 (Abbildung 2.5)[2] direkt unterstützt werden (2, 2009).

2 http://www.hl7.org/v3ballot/html/help/v3guide/v3guide.htm

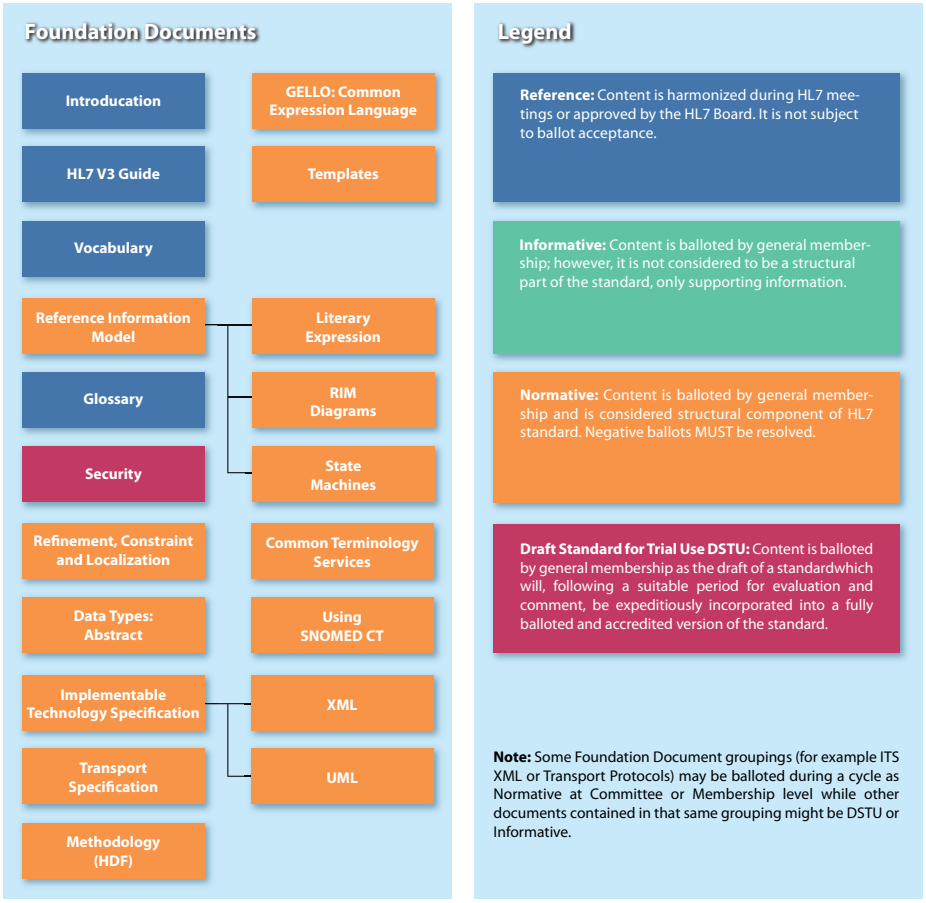

Abbildung 2.5: HL7 Komponenten (2, 2009)

Eine Empfehlung, welche von HL7 empfohlen wird, ist die Kommunikation über gesicherte Datenleitungen zu führen. Dazu wird von HL7 ein Konzept für die Verwendung von Internet Mail vorgeschlagen (Schadow et al., 1999). Hierbei wird die Nachricht entweder digital verschlüsselt, oder aber digital signiert. Dazu gibt es zwei Möglichkeiten, die Verschlüsselung durchzuführen:

1. mit Hilfe eines symmetrischen Schlüssels (Abbildung 2.6) oder
2. mit Hilfe eines asymmetrischen Schlüsselpaares (Abbildung 2.7).

Eine ähnliche Technologie, wie die soeben beschriebene, verwendet Chen et al. (2001) in seinem Artikel *Security Architecture for HL/7 Message Interchange*. Hier wird eine Abwandlung von Pretty Good Privacy (PGP) (Garfinkel, 1994) verwendet, um E-Mail-Nachrichten zu verschlüsseln.

Beide Ansätze sind für eine sichere Kommunikation sehr gut geeignet. Ein entscheidender Nachteil, den diese Sicherheitsmechanismen jedoch besitzen, ist, dass der gesamte

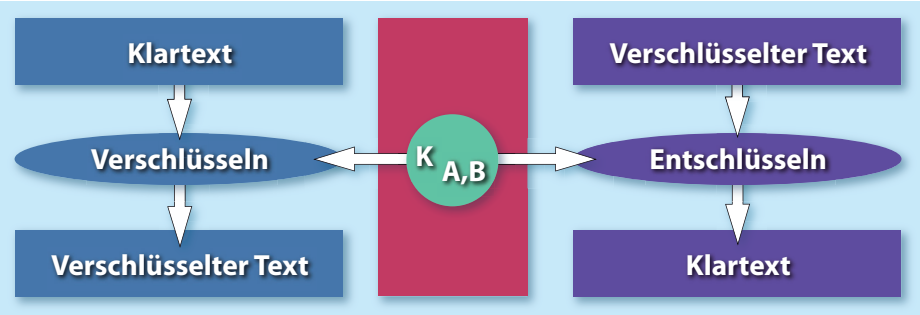

Abbildung 2.6: Symmetrische Verschlüsselung (Tanenbaum und Van Steen, 2007)

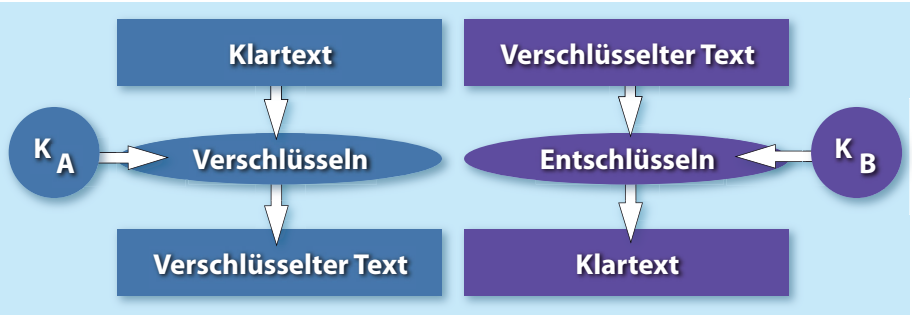

Abbildung 2.7: Asymmetrische Verschlüsselung (Tanenbaum und Van Steen, 2007)

Inhalt einer Nachricht verschlüsselt und somit nicht mehr lesbar gemacht wird. Dadurch ist dieser Ansatz nicht geeignet, für den Fall, dass diese Daten an Forschungseinrichtungen weitergereicht werden sollen. Das Ziel ist jedoch nicht das Verschlüsseln der gesamten Nachricht, sondern vielmehr eine Nachricht zu depersonalisieren. Dadurch wird es möglich, den Inhalt der Nachricht ohne eine Personenzuordnung zu lesen und diese Daten für diverse Auswertungen beziehungsweise zur Weiterverarbeitungen zu verwenden.

2.5.4 Pseudonymisierung als Sicherheitskonzept in e-Health

Um klinische Daten, wie Befunde oder Arztbriefe, für Forschungszwecke verwendbar zu machen, müssen diese zuvor depersonalisiert werden. Nach einer Depersonalisierung ist es nicht mehr möglich, von den darin enthaltenen Informationen auf eine Person Rückschlüsse zu ziehen. Pommerening (1995) unterscheidet drei Stufen der Personalisierung von Daten:

- Personenbezug
- Anonymität

- Pseudonymität

Die Ausgangssituation stellen vertrauliche Daten dar, aus denen die Identität einer Person eindeutig erkennbar ist, wodurch ein direkter Personenbezug möglich ist. Nach vollständiger Entfernung der personenbezogenen Informationen, welche in Tabelle 2.4 angeführt sind, spricht man von Anonymität. In dieser Stufe ist anhand der übrig gebliebenen Daten keine Personenzuordnung möglich. Diese Stufe der depersonalisierten Daten hat jedoch auch Nachteile. Wenn Daten an Forschungseinrichtungen weitergereicht werden, um so wichtige Erkenntnisse zu gewinnen, sollen die betroffenen Personen darüber informiert werden können. Um auch diese Anforderung zu erfüllen, gibt es die dritte Stufe, die sich Pseudonymität nennt. Ein Pseudonym ist eine nicht zuordbare künstliche Identität. Diese künstliche Identität versteckt die eigentliche Identität einer Person (Pommerening et al., 1996). Wenn ein Pseudonym nur von der betroffenen Person entschlüsselt werden kann, wird das Pseudonym als „untraceable“, also unauffindbar, bezeichnet (Pommerening et al., 1996).

Klinische Informationen oder Daten, welche eine Person betreffen, können in zwei Gruppen unterteilt werden (Pommerening et al., 1996):

- Identifikationsdaten
- Epidemiologische/Klinische Daten

Zu den Identifikationsdaten einer Person zählen unter anderem Name, Familienname, Adresse und Geburtsdatum. Die epidemiologischen beziehungsweise klinischen Daten sind jene, welche den Gesundheitszustand von Personen behandeln. Zu diesen zählen zum Beispiel Geschlecht, Berufsgruppe, Diagnosedatum und Diagnosen (Pommerening et al., 1996). In Tabelle 2.4 sind diese Identifikationsmerkmale entsprechend ihrer Sensibilität eingestuft.

Attribut	Sensibilität
Name	Sehr hoch
Geburtsdatum	Mittel
Geschlecht	Niedrig
Beruf	Mittel
Akademischer Grad	Sehr hoch
Straße	Sehr hoch
Postleitzahl	Sehr hoch
Ort	Mittel

Tabelle 2.4: Einstufung der Sensibilität von persönlichen Daten (Stolba et al., 2006)

KAPITEL 3

Pseudonymization of Information for Privacy in e-Health (PIPE)

In diesem Kapitel wird die Architektur von *Pseudonymization of Information for Privacy in e-Health*, kurz PIPE genannt, welche in (Riedl et al., 2008a,b, 2007a, 2008c,d, 2007b,c) beschrieben ist, erläutert. Dabei wird das System erklärt und die wichtigsten Abläufe anhand von Sequenzdiagrammen beschrieben.

3.1 Architektur

In den folgenden Sektionen dieses Kapitels werden die Rollen der Akteure, welche in PIPE vorkommen, erläutert. Außerdem wird auf die Hüllenarchitektur von PIPE eingegangen. Das Datenmodell wird beschrieben und die Funktionen der einzelnen Tabellen erläutert. Abschließend werden die Abläufe der PIPE-Operationen mit Hilfe von Sequenzdiagrammen beschrieben.

3.1.1 Rollen im System

Es gibt in PIPE vier Hauptrollen, die von den Akteuren eingenommen werden können. Diese sind der Patient (A), der Verwandte (B), der medizinische Dienstleister beziehungsweise eine Forschungseinrichtung (C) und der Operator (O).

Diese Hauptrollen teilen sich weiters in operative und administrative Rollen. Zu den operativen Rollen zählen:

- Patienten
- Verwandte

- Medizinische Dienstleister beziehungsweise Forschungseinrichtungen

Die administrative Rolle übernimmt der Operator.

Der Patient ist der alleinige Eigentümer seiner Daten φ_i. Der Patient kann seinen Verwandten einen Vollzugriff auf seine Daten gewähren. Der bevollmächtigte Verwandte wird im System wie ein Patient behandelt und hat dieselben Rechte wie der Patient selbst. Medizinische Dienstleister können vom Patienten bevollmächtigt werden, Anamnesen für diesen Patienten anzulegen und mit diesen zu arbeiten.

Weiters gibt es noch die Logik (L) von PIPE, die allerdings kein Akteur im eigentlichen Sinne ist. Die Logik beinhaltet die Routinen, um den Akteuren entsprechende Services anzubieten.

Jeder dieser Akteure besitzt unterschiedliche Schlüssel, die dieser zum Ver- und Entschlüsseln von Informationen verwenden kann. So besitzt jeder Akteur einen äußeren öffentlichen Schlüssel K, einen äußeren privaten Schlüssel K^{-1}, einen inneren öffentlichen Schlüssel $\widehat{K}$, einen inneren privaten Schlüssel $\widehat{K}^{-1}$ und einen inneren symmetrischen Schlüssel $\overline{K}$.

Die Logik (L) besitzt nur einen symmetrischen Schlüssel K_L.

Eine vollständige Auflistung aller System-Attribute ist in Tabelle 3.1 angeführt.

	Patient	Verwandter	Med. Dienstleister	Operator	Logik
Kürzel	A	B	C	O	L
ID	A_{id}	B_{id}	C_{id}	O_{id}	
(Äußerer öffentliche Schlüssel, privater Schlüssel)	(K_A, K_A^{-1})	(K_B, K_B^{-1})	(K_C, K_C^{-1})	(K_O, K_O^{-1})	
(Innerer öffentliche Schlüssel, privater Schlüssel)	$(\widehat{K}_A, \widehat{K}_A^{-1})$	$(\widehat{K}_B, \widehat{K}_B^{-1})$	$(\widehat{K}_C, \widehat{K}_C^{-1})$	$(\widehat{K}_O, \widehat{K}_O^{-1})$	
Innerer symmetrischer Schlüssel	$\overline{K}_A$	$\overline{K}_B$	$\overline{K}_C$	$\overline{K}_O$	K_L
Schlüsselanteil	$\sigma_\kappa(K)$				
Medizinische Daten / Anamnese	φ_i				
Pseudonym	ψ_{i_j}				
Marke	τ_v				

Tabelle 3.1: Definitionen der PIPE System Attribute (Riedl et al., 2007c)

Um den Zugriff auf die Daten φ_i auch dann zu gewährleisten, wenn die Zugriffskarte verloren ist beziehungsweise beschädigt ist, werden Teilinformationen des Schlüssels $\sigma_\kappa(K)$ an zufällig ausgewählte Operatoren verteilt und von diesen gespeichert.

Die verschlüsselten Schlüssel K der Patienten werden mit Hilfe eines Algorithmus' nach Shamir (1979) in eine definierte Anzahl von Teilen $\sigma_\kappa(K)$ aufgesplittet und an zufällig ausgewählte Operatoren verteilt.

Falls ein Akteur seine Zugriffskarte verliert, können nun die Einzelteile des Schlüssel gesammelt und wieder zusammengefügt werden. Somit hat der Akteur wieder Zugriff auf seine Daten.

3.1.2 Hüllenarchitektur

PIPE wird logisch in drei Hüllen unterteilt. Die äußerste Hülle ist die Authentifizierungsschicht, gefolgt von der mittleren Hülle, der Benutzerschicht und der innersten Hülle, der gesicherten Daten. Eine detaillierte Darstellung der Hüllenarchitektur ist in Abbildung 3.1 zu finden.

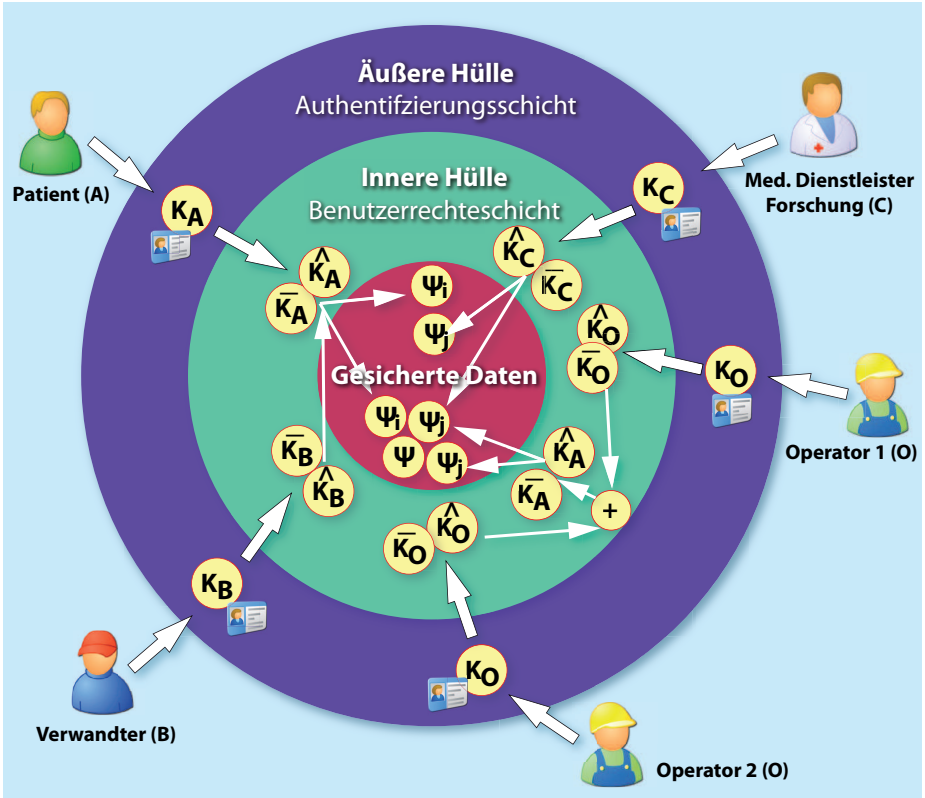

Abbildung 3.1: PIPE Hüllenarchitektur (Riedl et al., 2008c)

Diese drei Hüllen sind voneinander abhängig. Dies bedeutet konkret, dass die verschlüsselten Informationen innerhalb einer Hülle nur mit Hilfe von Informationen einer darüberliegenden Hülle zugreifbar sind. Die Informationen müssen sequentiell, beginnend von der äußersten Hülle entschlüsselt werden. Mit Hilfe der dadurch erhaltenen Informationen beziehungsweise Schlüsseln ist es möglich, auf die nächst tiefere Hülle zuzugreifen.

In der äußeren Hülle der Authentifizierungsschicht, ist der äußere öffentliche Schlüssel K auf einer Chipkarte gespeichert. Diese Chipkarte wird für die Authentifizierung des Zuganges zur Benutzerschicht verwendet.

Der innere private Schlüssel $\widehat{K}^{-1}$ in der inneren Hülle wird mit dem äußeren öffentlichen Schlüssel K verschlüsselt. Der innere symmetrische Schlüssel $\overline{K}$ wird in weiterer Folge mit dem inneren öffentlichen Schlüssel $\widehat{K}$ verschlüsselt. Um auf diese Informationen zugreifen zu können, wird das jeweilige Gegenstück, der private Schlüssel (K^{-1}, $\widehat{K}^{-1}$) verwendet. Der Ablauf des Verschlüsselungsvorganges ist in Abbildung 3.2 dargestellt.

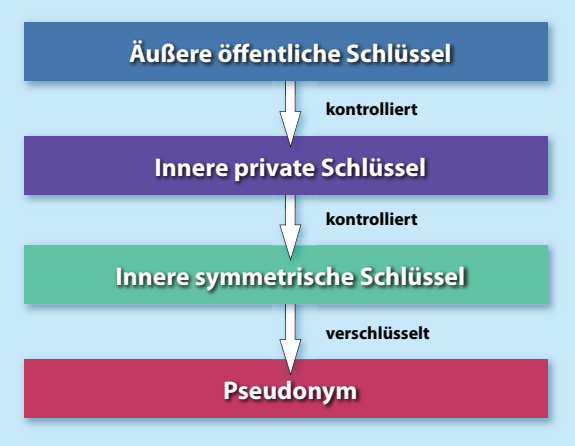

Abbildung 3.2: PIPE Verschlüsselung

Analog zum Verschlüsseln müssen die verschlüsselten Informationen entschlüsselt werden. Dieser Vorgang ist in Abbildung 3.3 dargestellt. Dazu wird der innere öffentliche Schlüssel $\widehat{K}$ mit dem äußeren privaten Schlüssel K^{-1} entschlüsselt, um mit dem erhaltenen inneren privaten Schlüssel $\widehat{K}^{-1}$ in weiterer Folge den inneren symmetrischen Schlüssel $\overline{K}$ zu entschlüsseln. Das Pseudonym ψ_{i_j} erhält man durch Entschlüsselung mit dem inneren symmetrischen Schlüssel $\overline{K}$ zurück.

Einer Anamnese φ_i können mehrere Pseudonyme ψ_{i_j} zugeordnet sein. Jede Person, die einen Zugriff auf eine bestimmte Anamnese zugewiesen bekommt, erhält ein separates

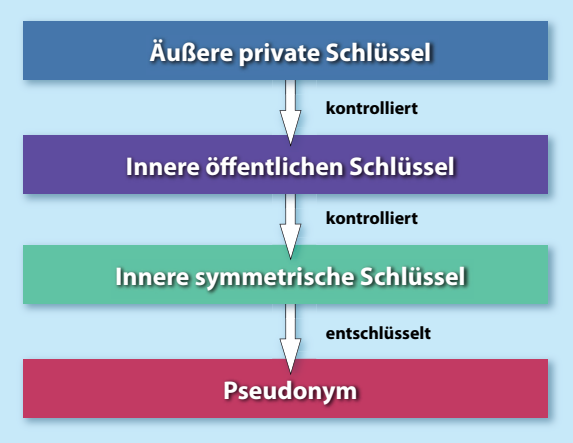

Abbildung 3.3: PIPE Entschlüsselung

Pseudonym. Somit ist es möglich, den Zugriff auf diese Anamnese durch simples Löschen des Pseudonyms, unabhängig von anderen Autorisierten, zu entziehen. Das Root-Pseudonym, welches dem Besitzer der Anamnese zugeordnet ist, kann nicht gelöscht werden. Eine Löschung des Root-Pseudonyms würde Datenleichen zur Folge haben und ist daher nicht zulässig.

3.2 Datenbank

Die Daten sind persistent in der Datenbank St abgelegt und das Kartenmanagement wird von der Logik L durchgeführt. Um die Sicherheit der Daten beziehungsweise des Kartenmanagements zu gewährleisten, müssen diese beiden Instanzen in einer vertrauenswürdigen Umgebung betrieben werden.

Der Datenspeicher wird logisch in zwei unabhängige Bereiche (St_1 und St_2), sogenannte Tablespaces, geteilt. Er kann aber auch physisch unterteilt werden. Dies gewährleistet die Datensicherheit und den Datenschutz der Benutzer (siehe Abbildung 3.4). Der Tablespace St_1 beinhaltet alle Informationen, um die beteiligten Akteure zu identifizieren. Es finden sich hier auch die allgemeinen Tabellen, welche das PIPE-System für den Betrieb benötigt (*Identification*, *UserMapping*, *Relations*, *Pseudonyms*). Im zweiten Tablespace St_2 werden die pseudonymisierten Daten (*Records*) gespeichert. Eine direkte Verlinkung der beiden Tablespaces St_1 und St_2 ist nicht vorgesehen und daher auch nicht möglich.

Die Tabelle *Identification* beinhaltet alle zur Operation des PIPE-Systems notwendigen Daten. Zu diesen Daten zählen der *Innere öffentliche Schlüssel*, der *verschlüsselte*

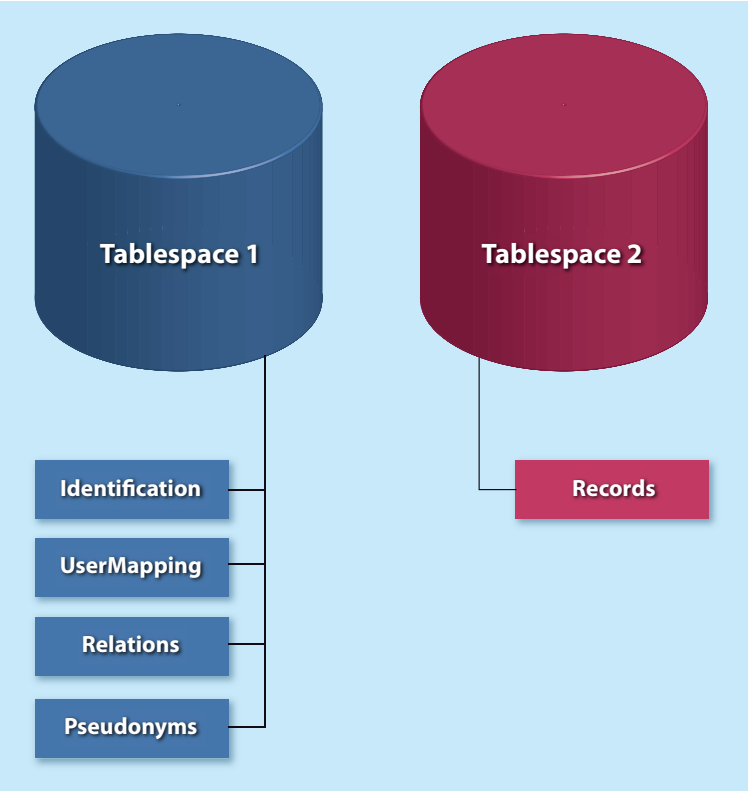

Abbildung 3.4: Schematische Darstellung der PIPE Datenbank

innere private Schlüssel und der *verschlüsselte symmetrische Schlüssel* der Akteure.

In der *UserMapping*-Tabelle sind die Verlinkungen zwischen externen Benutzer und internen Akteure gespeichert. Die externen Benutzer sind User von den existierenden Applikation, in denen PIPE integriert wurde. Die internen Akteure sind Benutzer von PIPE. Mit Hilfe dieser Zuordnung können einem internen Akteur mehrere externe Applikationen zugeordnet werden.

Die Beziehungen zwischen PIPE-Akteuren sind in der *Relations*-Tabelle gespeichert. Zu diesen Beziehungen zählen die Patient-Arzt- und die Patient-Verwandte-Beziehung.

Pseudonyme, welche von PIPE erstellt wurden, werden verschlüsselt in der *Pseudonyms*-Tabelle abgelegt. Weiters werden den Pseudonymen bestimmte Schlüsselwörter zugeordnet, um ein späteres Auffinden der verschlüsselten Pseudonyme zu ermöglichen.

Die eigentlichen Daten, welche nur in pseudonymisierter Form vorliegen, werden in der sogenannten *Records*-Tabelle gespeichert. Eine direkte Zuordnung zu den Akteuren ist durch die Anwendung der Pseudonymisierung nicht möglich.

3.3 Abläufe von typischen PIPE-Operationen

In den nachfolgenden Kapiteln werden Abläufe von typischen PIPE-Operationen beschrieben. Um die Veranschaulichung dieser Operationen zu vereinfachen, werden zur Unterstützung Sequenzdiagramme verwendet.

Folgende PIPE-Operationen werden nachfolgend näher erläutert:

- Einen Akteur zu PIPE hinzufügen
- Eine Anamnese in PIPE anlegen
- Eine Anamnese aus PIPE lesen
- Eine Anamnese für einen anderen Akteur freigeben
- Die Freigabe einer Anamnese annullieren

PIPE wird in drei Schichten, die *Administrations*-Schicht, die *PIPE-API* und die *Service*-Schicht, unterteilt. Die Administrations-Schicht dient dazu, neue Akteure im System anzulegen. Die PIPE-API stellt Funktionen zur Verfügung, die es ermöglichen, neue Anamnesen anzulegen und die Zugriffsrechte dieser Anamnesen zu verwalten. Die Administrations-Schicht und die PIPE-API existieren parallel und greifen auf die Service-Schicht zu.

Weiters wird die Applikation, in der PIPE integriert wurde, als *Ursprungssystem* bezeichnet. Die nachfolgenden Kapitel behandeln die zuvor angeführten Abläufe. Dazu werden diese in einem Sequenzdiagramm dargestellt. Die Prozeduraufrufe, welche in diesen Sequenzdiagrammen enthalten sind, richten sich an die Namensgebung des jeweiligen Application Programming Interface (API)[1]. Es stellen die Administrations-Schicht und die Service-Schicht je eine eigene API zur Verfügung. Die API der Administrations-Schicht wird vom Ursprungssystem verwendet, um die Funktionen von PIPE zu nützen. Die API der Service-Schicht wird nur von der Administrations-Schicht verwendet. Um die Übersichtlichkeit zu wahren, werden die Parameter beim Funktionsaufruf weggelassen. Stattdessen findet sich eine Beschreibung der Paramter in den Begleittexten.

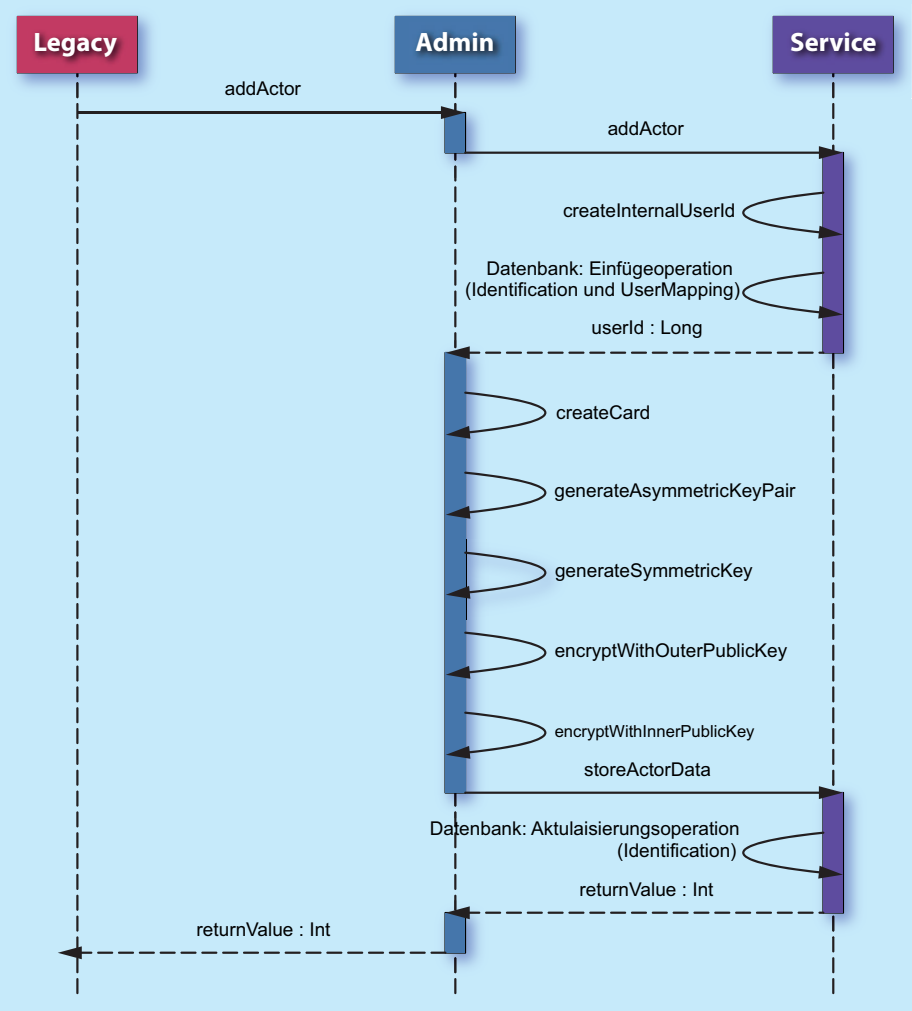

Abbildung 3.5: Sequenzdiagram: Einen Akteur zu PIPE hinzufügen

3.3.1 Einen Akteur zu PIPE hinzufügen

Akteure des PIPE-Systems sind Benutzer, die eine bestimmte Rolle in PIPE einnehmen. Es ist auch möglich, diese Akteure einem externen Ursprungssystem zuzuordnen.

Beim Hinzufügen eines neuen Akteurs zum PIPE-System werden automatisch alle notwendigen Schlüssel erstellt. Der innere private Schlüssel ($\widehat{K}^{-1}$) und der innere symmetrische Schlüssel ($\overline{K}$) werden mit dem äußeren privaten Schlüssel (K^{-1}), welcher auf einer Smartcard gespeichert wurde, in der Datenbank verschlüsselt abgelegt. Zudem erfolgt die Verknüpfung des neuen Akteurs zu einem Benutzer des Ursprungssystem. Es ist zusätzlich möglich, einen Akteur von PIPE mit mehreren Benutzern von unter

1 http://en.wikipedia.org/wiki/API

Umständen unterschiedlichen Ursprungssystemen zu verknüpfen.

Eine Vorbedingung dieser Funktion ist, dass der Akteur noch nicht im System existiert. Das Ergebnis der Operation ist ein neu angelegter Akteur.

Wie in Abbildung 3.5 ersichtlich, wird der Aufruf *addActor* vom Ursprungssystem über die Administrations-Schicht bis hin zur Service-Schicht durchgereicht. Als Parameter werden zwei Identifikatoren übergeben, zum einen der Identifikator des Ursprungssystems, das dem PIPE-System bereits bekannt sein muss und zum anderen der Identifikator des Benutzers des Ursprungssystems. Dieser Benutzer wird mit dem neu hinzugefügten PIPE-Akteur verknüpft.

Die Service-Schicht generiert einen neuen eindeutigen internen Bezeichner, der in der Datenbank gespeichert wird. Der neu generierte Identifikator wird dann zur Administrations-Schicht als Ergebnis der Operation zurückgesandt. Die Administrations-Schicht erstellt nun nacheinander die Smartcard, das asymmetrische Schlüsselpaar und den symmetrischen Schlüssel. Der innere private Schlüssel ($\widehat{K}^{-1}$) wird nun mit dem äußeren öffentlichen Schlüssel (K) und der innere symmetrische Schlüssel ($\overline{K}$) mit dem inneren öffentlichen Schlüssel verschlüsselt ($\widehat{K}$).

Als letzter Schritt werden nun die zuvor gespeicherten Akteur-Daten aktualisiert und die Schlüssel (der innere öffentliche Schlüssel, der verschlüsselte innere private Schlüssel und der verschlüsselte innere symmetrische Schlüssel) in der Datenbank gespeichert. Der Rückgabewert dieser Funktion ist positiv, wenn der Akteur erfolgreich angelegt werden konnte, andernfalls negativ.

3.3.2 Eine Anamnese in PIPE anlegen

Die Anlage einer Anamnese in PIPE erfordert zunächst eine Pseudonymisierung, bevor sie in das System eingefügt werden kann. Die Anamnese wird dem Patient zugeschrieben, welcher der alleinige Eigentümer dieser Daten ist und somit die Zugriffsrechte verwaltet. So kann nur der Patient selbst entscheiden welcher Arzt, welche medizinische Einrichtung oder welches Forschungsinstitut Zugriff auf selektierte Anamnesen erhält.

Die Vorbedingung dieser Funktion ist, dass diese Anamnese noch nicht im System gespeichert wurde. Das Ergebnis der Operation ist eine neu angelegte Anamnese.

Der Aufruf von *addData* ist in Abbildung 3.6 dargestellt und wird vom Ursprungssystem zur PIPE-API durchgereicht. Diese Funktion hat 4 Parameter: (i) der Identifikator

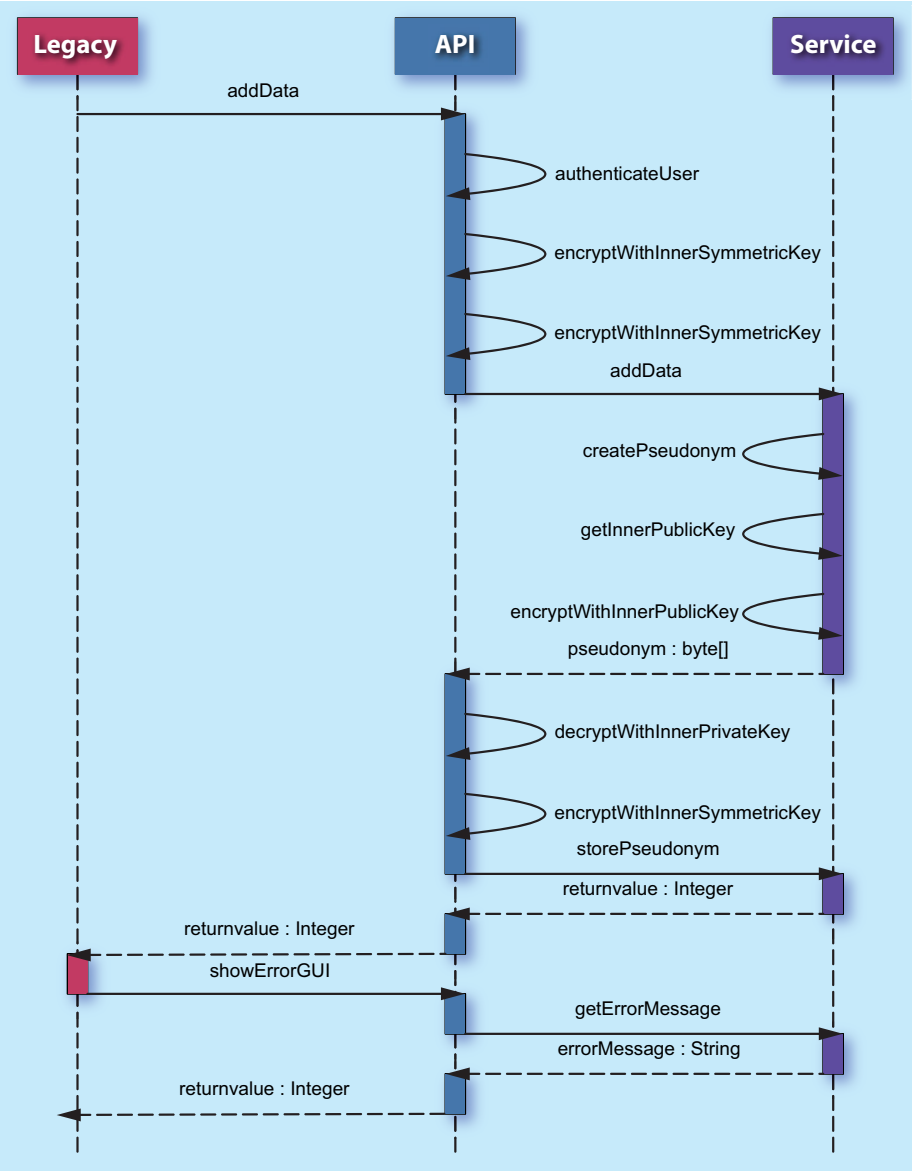

Abbildung 3.6: Sequenzdiagramm: Eine Anamnese in PIPE anlegen

des Ursprungssystem, welcher PIPE bekannt ist, (ii) der Identifikator des Benutzer vom Ursprungssystems, (iii) die eigentlichen Anamnese-Daten und (iv) Schlüsselworte. Die Schlüsselwörter dienen dazu, um die pseudonymisiert abgespeicherte Anamnese wieder auffinden zu können. In der PIPE-API muss sich der Akteur zuerst bei PIPE authentifizieren um eine neue Sitzung (engl. session) zu erstellen.

Im nächsten Schritt verschlüsselt der innere symmetrische Schlüssel die interne Benutzerkennung. Zudem kommt es zu einer Verschlüsselung der einzelnen Schlüsselwörter mit dem inneren symmetrischen Schlüssel. Anschließend werden die Daten gemeinsam mit den verschlüsselten Schlüsselwörtern an die Service-Schicht weitergereicht.

In der Service-Schicht wird ein Pseudonym erstellt und der innere öffentliche Schlüssel ausgelesen. Das neu erstellte Pseudonym wird nun mit dem inneren öffentlichen Schlüssel verschlüsselt und an die PIPE-API als Antwortnachricht gesandt.

Das verschlüsselte Pseudonym wird in der PIPE-API mit dem inneren privaten Schlüssel entschlüsselt und im Anschluss mit dem inneren symmetrischen Schlüssel verschlüsselt.

Im letzten Schritt wird das verschlüsselte Pseudonym mit der verschlüsselten Benutzerkennung und den verschlüsselten Schlüsselwörtern an die Service-Schicht übergeben und dort in der Datenbank persistiert.

Der Rückgabewert dieser Funktion ist positiv, wenn die Anamnese erfolgreich angelegt wurde. Im Fehlerfall ist der Rückgabewert negativ und eine entsprechende Meldung wird ausgegeben.

3.3.3 Eine Anamnese aus PIPE lesen

Um eine pseudonymisierte Anamnese aus dem PIPE-System auslesen zu können, sind zwei voneinander abhängige Schritte notwendig. Zuerst muss das Pseudonym ermittelt werden, mit welchem die Daten im zweiten Schritt aus der Datenbank ausgelesen werden. Um das Pseudonym ermitteln zu können, müssen sämtliche Schlüsselwörter angegeben werden, mit welchen es pseudonymisiert in der Datenbank abgelegt wurde.

In Abbildung 3.7 wird das Sequenzdiagramm für den ersten Schritt *searchData* des Lesevorgangs einer Anamnese dargestellt. Abbildung 3.8 visualisiert den zweiten Schritt *retrieveData*, der zum Lesen einer Anamnese notwendig ist.

Die Vorbedingung der Funktion searchData ist, dass die Schlüsselwörter ausgewählt werden. Das Ergebnis der Operation ist ein Pseudonym für die entsprechende Anamnese.

Der Funktion searchData werden drei Parameter übergeben. Diese sind der Identifikator des Ursprungssystem, der Identifikator des Benutzers vom Ursprungssystem, und die Schlüsselwörter, die mit der gesuchten Anamnese in Verbindung stehen. In der PIPE-API muss sich der Akteur zuerst bei PIPE authentifizieren, um eine neue Sitzung zu erstellen. Im Anschluss daran werden die Benutzerkennung und die Schlüsselwörter einzeln je mit dem inneren symmetrischen Schlüssel verschlüsselt an die Service-Schicht weitergereicht. Das Ergebnis dieser Funktion ist ein Array mit

verschlüsselten Pseudonymen, die von der PIPE-API einzeln entschlüsselt und der Ursprungsapplikation übergeben werden.

Die Funktion retrieveData hat die Funktion searchData zur Vorbedingung und liefert als Ergebnis die gewünschte Anamnese.

Im zweiten Schritt des Anamnese Lesens wird die Funktion retrieveData aufgerufen. Die Parameter dieser Funktion setzen sich aus dem Identifikator des Ursprungssystems, dem Identifikator des Benutzers vom Ursprungssystem und dem Pseudonym der Anamnese zusammen. In der PIPE-API muss sich der Benutzer zunächst authentifizieren, um eine neue Sitzung zu erstellen, bevor der Funktionsaufruf an die Service-Schicht weitergereicht wird. In der Service-Schicht werden die Daten aus der Datenbank gelesen und als Rückgabewert zunächst an die PIPE-API und dann an das Ursprungssystem weitergereicht.

3.3.4 Eine Anamnese für einen anderen Akteur freigeben

Mit Hilfe dieser Funktion kann Zugang zu einer Anamnese gewährt werden. Dies ist die eigentliche Hauptfunktionalität von PIPE. Akteure können auf diese Weise genau beeinflussen, welcher Akteur Rechte für ausgewählte Anamnesen erhält. Das dazugehörige Sequenzdiagramm ist in Abbildung 3.9 dargestellt.

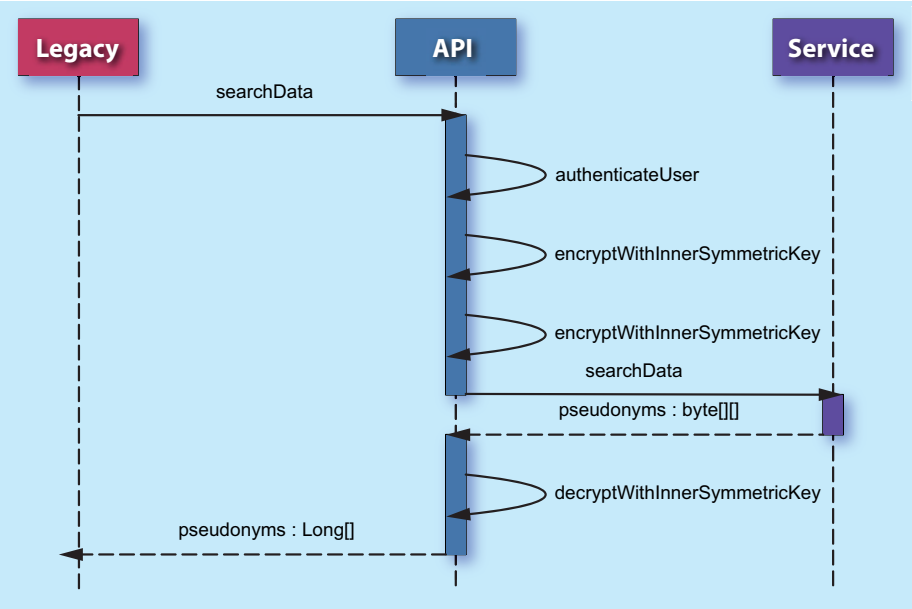

Abbildung 3.7: Sequenzdiagramm: Eine Anamnese in PIPE suchen

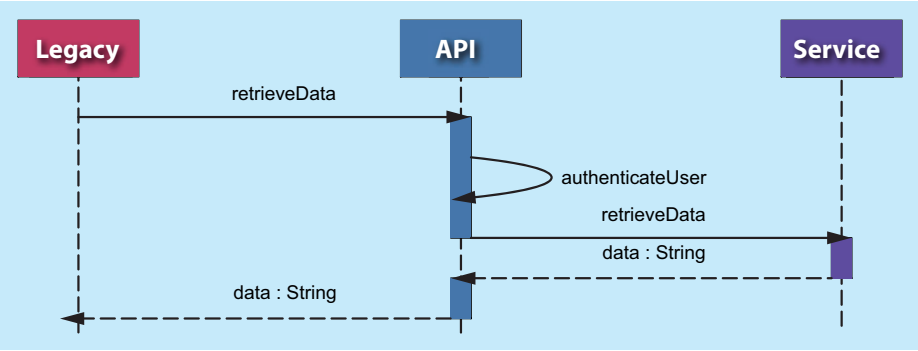

Abbildung 3.8: Sequenzdiagramm: Eine Anamnese aus PIPE lesen

Die Vorbedingung dieser Funktion ist, dass noch keine Zuordnung der Anamnese zu einen Akteur stattgefunden hat. Das Ergebnis ist das Recht des neuen Akteurs auf die spezifizierte Anamnese zugreifen zu können.

Die Aufrufparameter von *addDataRelation* setzen sich aus dem Identifikator des Ursprungssystem, dem Identifikator des Benutzers vom Ursprungssystem, dem Identifikator des zu autorisierenden Benutzers des Ursprungssystems, dem Wurzel-Pseudonym, den Identifikatoren der Schlüsselwörter des Wurzel-Pseudonyms und den Schlüsselwörtern des neuen Pseudonyms zusammen.

In der PIPE-API muss sich der Akteur, welcher Besitzer des Wurzel-Pseudonyms ist, am System anmelden, um eine neue Sitzung zu erstellen. Im nächsten Schritt muss sich auch der zweite Akteur, der die Zugriffsrechte für die Anamnese erhalten wird, am System anmelden. Dies ist notwendig um auf die privaten Schlüssel des zweiten Akteurs zugreifen zu können. In den nächsten Schritten dieser Funktion werden je die internen Benutzeridentifikatoren mit den jeweiligen inneren symmetrischen Schlüsseln verschlüsselt. So wird in der Sitzung des Ursprungs-Akteurs seine eigene Benutzeridentifikation als auch die Benutzeridentifikation des neu zu autorisierenden Akteurs mit dem inneren symmetrischen Schlüssel verschlüsselt. Die gleichen Operationen werden nun in der Sitzung des zweiten Akteurs durchgeführt. Auch hier werden die Benutzeridentifikatoren mit dem inneren symmetrischen Schlüssel verschlüsselt. Im Anschluss daran werden die Schlüsselwörter mit den jeweiligen inneren symmetrischen Schlüsseln der Akteure verschlüsselt. Die soeben verschlüsselten Daten werden gemeinsam mit dem Wurzel-Pseudonym an die Service-Schicht übergeben.

In der Service-Schicht wird ein neues Pseudonym erstellt und der innere öffentliche Schlüssel des zu autorisierenden Akteurs aus der Datenbank gelesen. Dieser innere öffentliche Schlüssel verschlüsselt das zuvor erstellte Pseudonym und retourniert es an

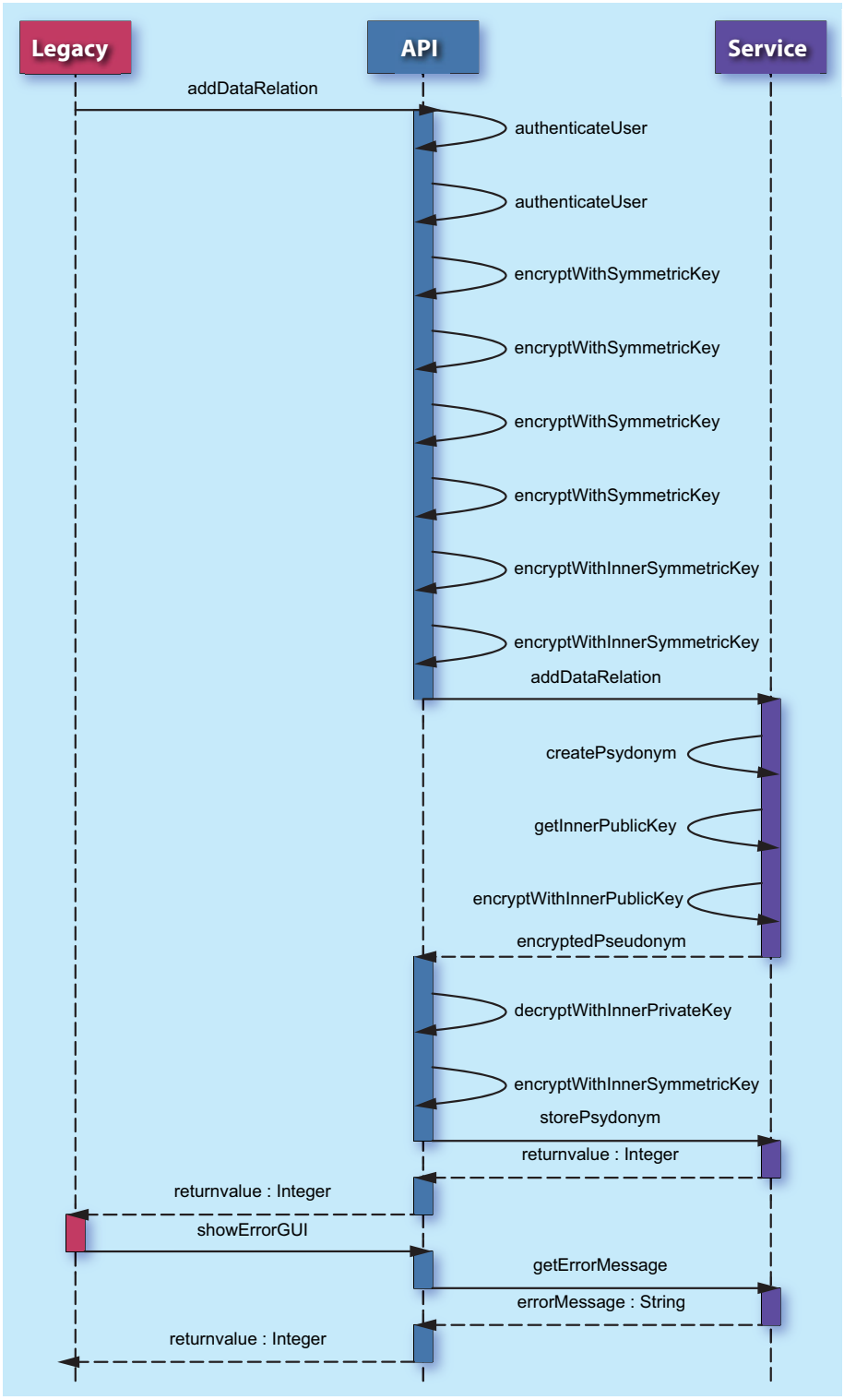

Abbildung 3.9: Sequenzdiagramm: Eine Anamnese für einen anderen Akteur freigeben

die PIPE-API.

Das verschlüsselte Pseudonym wird mit dem inneren privaten Schlüssel des zu autorisierenden Akteurs in der PIPE-API entschlüsselt. Im Anschluss wird das Pseudonym mit dem inneren symmetrischen Schlüssel verschlüsselt und an die Service-Schicht gesandt. In der Service-Schicht wird das verschlüsselte Pseudonym persistent in der Datenbank abgelegt.

Bei erfolgreicher Freigabe der Anamnese ist der Rückgabewert dieser Funktion positiv. Der Rückgabewert ist im Fehlerfall negativ. Im negativen Fall wird eine Meldung ausgegeben.

3.3.5 Die Freigabe einer Anamnese annullieren

Um die Zugriffsrechte für eine Anamnese einem Akteur entziehen zu können, wird die Funktion *revokeDataRelation*, welche in Abbildung 3.10 dargestellt ist, verwendet.

Um diese Funktion ausführen zu können, muss ein Akteur über bestimmte Zugriffsrechte für eine Anamnese verfügen. Nach der Ausführung der Funktion werden dem Akteur diese Zugriffsrechte entzogen und in weiterer Folge kann der Akteur nicht mehr auf diese Anamnese zugreifen.

Der Funktionsaufruf von revokeDataRelation erfolgt vom Ursprungssystem mit den Parametern Identifikator des Ursprungssystems, dem Identifikator des Akteurs vom Ursprungssystem, dem Identifikator des zu annullierenden Akteurs des Ursprungssystems und des Pseudonyms der betreffenden Anamnese. Dieser Aufruf wird an die PIPE-API weitergereicht, dort muss sich der Akteur, welcher Besitzer der Anamnese ist, authentifizieren, um eine neue Sitzung zu erzeugen. Im nächsten Schritt wird der interne Benutzeridentifikator des Besitzers ermittelt, anschließend wird der Akteur gesucht, dem die Zugriffsrechte entzogen werden. Diese beiden Benutzeridentifikatoren werden mit dem inneren symmetrischen Schlüssel verschlüsselt. Anschließend werden diese Daten an die Service-Schicht weitergereicht, um nach der gewünschten Anamnese zu suchen. Dieser Aufruf liefert alle betroffenen verschlüsselten Pseudonyme. Diese entschlüsselt die PIPE-API mit dem inneren symmetrischen Schlüssel. Das entschlüsselte Pseudonym wird im Anschluss daran an die Service-Schicht geschickt. Dieses Pseudonym entschlüsselt dann in der PIPE-API der innere symmetrische Schlüssel. Abschließend wird das entschlüsselte Pseudonym aus der Datenbank entfernt und der ehemals autorisierte Akteur verliert den Zugriff auf diese Daten.

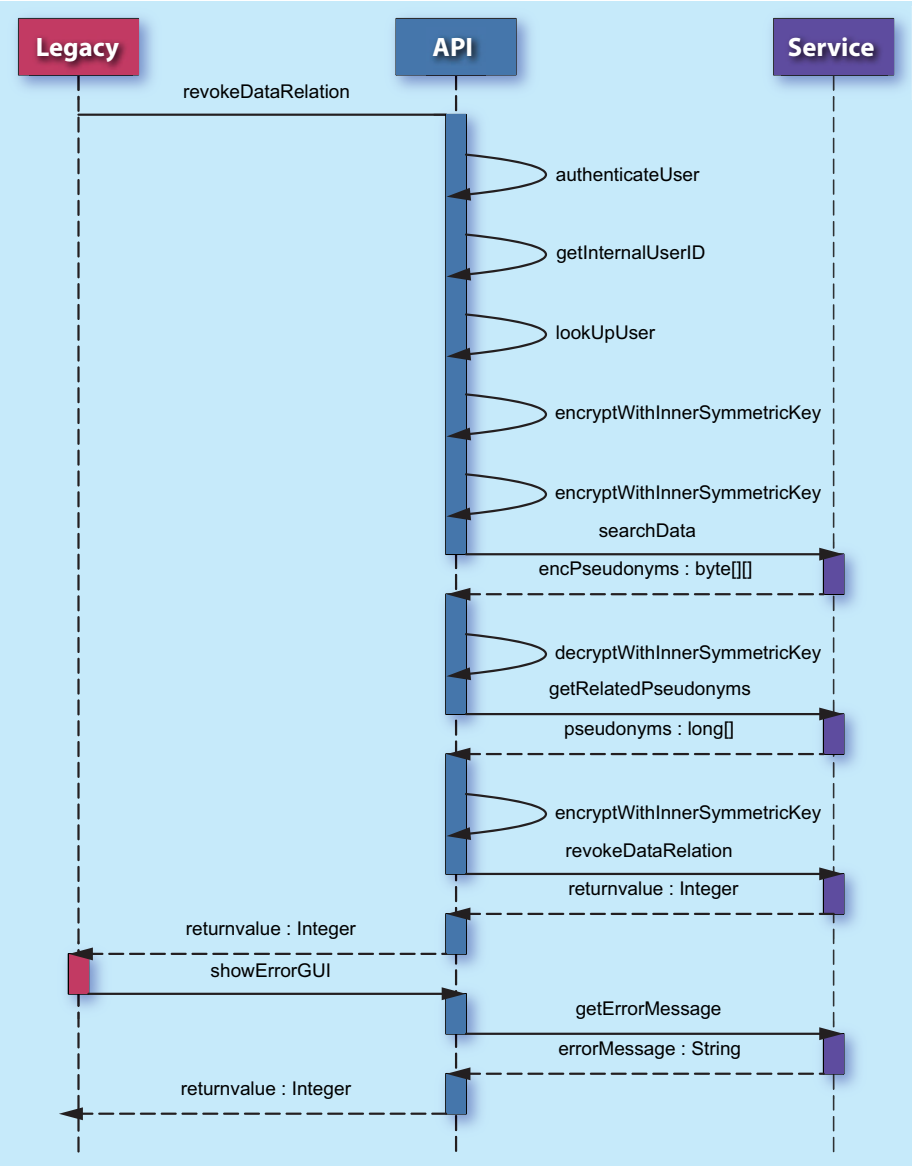

Abbildung 3.10: Sequenzdiagramm: Die Freigabe einer Anamnese annullieren

Der Rückgabewert dieser Funktion ist positiv, wenn es zu einer erfolgreichen Annullierung kommt. Andernfalls ist der Rückgabewert negativ. Im negativen Fall wird eine Meldung ausgegeben.

KAPITEL 4

PIPE in den Arztbrief auf Basis von HL7 CDA R2 integrieren

Dieses Kapitel behandelt die Integration von PIPE in den Arztbrief, der auf Basis von HL7 CDA R2 aufgebaut ist. Zu Beginn werden die Daten, welche für einen Arztbrief in Österreich relevant sind, aufgelistet. Diese Daten werden bezüglich der Möglichkeit der Pseudonymisierung analysiert. Hierbei werden die relevanten Daten den einzelnen Bereichen des Arztbriefes zugeordnet. Im Speziellen wird auf die Header-Informationen, welche primär für die Pseudonymisierung relevant sind, eingegangen. Diese Analyse wird in drei Bereiche aufgeteilt: (i) die Allgemeinen Dokumenteninformationen, (ii) die Beteiligten Parteien und (iii) den Body. Anschließend wird auf den Prozess der Pseudonymisierung eingegangen und relevante Workflows präsentiert.

4.1 Datenanalyse des Arztbriefes

In diesem Abschnitt werden die Daten, welche in einem Arztbrief enthalten sind, anhand des in Listing A.1 angeführten Arztbriefes und der Implementierungsdokumentation (Elga, 2008, Heitmann et al., 2006) analysiert. Die von der Initiative Elga aufgelisteten obligatorischen Felder für einen österreichischen Arztbrief (5, 2008) werden den jeweiligen Sektionen eines Arztbriefes zugeordnet. Die Sensibilität der enthaltenen Informationen werden anhand der in Tabelle 2.4 definierten Stufen eingeordnet. Das Augenmerk der Analyse wird hierbei auf die Daten im Header gelegt. Der Body wird nur soweit analysiert, um eine Gefährdung der Pseudonymisierung durch Freitexte zu vermeiden.

Der Arztbrief kann in zwei Bereiche unterteilt werden, den Header und den Body. Der Header kann weiters in sechs Sektionen gegliedert werden (Heitmann et al., 2006):

1. Allgemeine Dokumenteninformation
2. Beteiligte Parteien
    a) Patient
    b) Autor
    c) Verwaltende Organisation
    d) Empfänger
    e) Unterzeichner

Die Informationen können nun betreffend ihrer Sensibilität differenziert werden. So sind die direkt identifizierbaren Sensibilitätsdaten Informationen über den Patient. Weniger sensibel sind die Daten betreffend des Autors, der verwaltenden Organisation, des Empfängers und des Unterzeichners. Da hier kein direkter Schluss auf einen bestimmten Patienten möglich ist.

In den nachfolgenden Abschnitten werden alle Bereiche durchleuchtet, um eventuell sensible Daten aufzudecken. Hierbei wird zuerst der jeweilige Abschnitt kurz erklärt und der entsprechende Auszug aus dem im Anhang A.1 angeführten Arztbrief aufgelistet. Die einzelnen Tags werden genau erklärt und anschließend das Ergebnis zusammengefasst. Die Zusammenfassung ist tabellarisch aufgebaut und enthält die einzelnen Elemente. Jedes Element wird kurz beschrieben und die Einstufung der Sensibilität mit Hilfe der vier Abstufungen *Sehr hoch*, *Hoch*, *Mittel*, *Niedrig* und *Keine* vorgenommen.

Zur deutlicheren Hervorhebung der sensiblen Daten, welche der Sensibilitätsstufe *Sehr hoch*, *Hoch* und *Mittel* angehören, sind diese in den einzelnen Listing-Auszügen farblich markiert. So sind die der Sensibilitätsstufe *Sehr hoch* und *Hoch* zuzuordnenden Informationen, rot markiert, und die der Sensibilitätsstufe *Mittel* zuzuordnenden Daten sind blau hervorgehoben.

4.1.1 Daten im österreichischen Arztbrief

Die Daten des österreichischen Arztbriefes werden in zwei unterschiedliche Gruppen von Informationen aufgeteilt: (i) Die Grunddaten und (ii) die Detaildaten. Jeder dieser Bereiche hat Felder, die auszufüllen sind beziehungsweise ausgefüllt werden können. Diese Anforderungen an den Arztbrief listet die Initiative Elga (5, 2008) auf. Diese

Auflistung basiert auf Beschlüssen der Verordnung der Österreichischen Ärztekammer (VO der ÖÄK).

Zu den zwingend erforderlichen Feldern der Grunddaten eines Arztbriefes gehören das Briefdatum, der Patientenname, das Geburtsdatum des Patienten, die Patienten Aufnahmezahl, die Zeitspanne des stationären Aufenthalts, die entlassende Station, der stationsführende Oberarzt, die Entlassungsdiagnose, der Verlauf und die Wechselwirkungen, die letzte Medikation beziehungsweise die Therapieempfehlung, das geplante Prozedere und die empfohlenen Kontrollen (5, 2008).

Die Detaildaten dienen der genaueren Spezifikation der Anamnese und umfassen die Aufnahmeumstände, ein Kennzeichen einer Notfallaufnahme, das Transportmittel bei Aufnahme, die Transportart, die Transportbegleitpersonen, die krankheitsrelevante Anamnese, die durchgeführte Diagnostik, die durchgeführten Operationen und Eingriffe, die Entlassungsrichtlinien, der Entlassungszustand, die Belastbarkeit, ein Kennzeichen, ob ein Pflegebericht beigefügt wurde, der diktierende Arzt und der vidierende Arzt (5, 2008).

Diese Daten werden den Dokumentenbereichen: (i) Allgemeine Dokumenteninformation, (ii) Beteiligte Parteien und (iii) Body zugeordnet. Diese Bereiche werden in den nachfolgenden Sektionen näher beschrieben. Während das Briefdatum den allgemeinen Informationen zugeordnet ist, zählen Patientendaten und alle beteiligten Ärzte beziehungsweise Stationen zu den beteiligten Parteien. Alle Daten betreffend der Aufnahme, Anamnese und Entlassung finden sich im Body des Arztbriefes.

4.1.2 Allgemeine Dokumenteninformation

Der Bereich der allgemeinen Dokumenteninformationen beinhaltet Daten, die das XML-Dokument selbst betreffen und näher spezifizieren. Diese Daten lassen keine direkten Rückschlüsse auf den Urheber beziehungsweise die beteiligten Personen zu. Listing 4.1 zeigt den entsprechenden Auszug des Arztbriefes.

Der Header eines Arztbriefes beginnt mit den allgemeinen Informationen (Listing 4.1), die das Dokument selbst betreffen. Eingeleitet ist das klinische Dokument mit einem `<typId>`-Tag, dieser ist fix vorgegeben und muss der erste Tag im Arztbrief sein. Die weltweit eindeutige Dokumenten-Identifikations-Nummer wird im `<id>`-Tag angegeben. Dieses Element enthält zwei Attribute, die Id, welche in der Erzeugungsanwendung

verwendet wird, (`@extension`-Attribut) und die Id der Erzeugungsanwendung (`@root`-Attribut). Jeder Arztbrief ist einem bestimmten Typ mittels `<code>`-Tag zugeordnet[1]. Optional kann ein Titel (`<titel>`-Tag) angegeben werden, der die Klinik wie auch den Autor des Dokuments enthalten kann. Das Erstelldatum des Dokuments ist im `<effectiveTime>`-Tag angeführt. Die Einstufung der Vertraulichkeit des Dokuments erfolgt mittels des `<confidentialityCode>`-Tag. Weiters kann die Sprache des Dokuments mit Hilfe des `<languageCode>`-Tag definiert werden. Dokumente können zu einem Dokumentensatz zusammengefasst werden. Dieser Satz wird innerhalb einer Version des Dokuments, welche im `<versionNumber>`-Tag angegeben ist, mit Hilfe des `<setId>`-Tag definiert.

```
 4 <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
   <id extension="35" root="1.2.276.0.24.0.5.0.1339551403.3.1.1550751403"/>
 6 <code code="34106-5" codeSystem="2.16.840.1.113883.6.1"/>
   <title>Entlassbericht</title>
 8 <effectiveTime value="20060529153213"/>
   <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
10 <languageCode code="de-DE"/>
   <setId extension="35" root="1.2.276.0.24.0.5.0.1339551403.3.2.1550751403
       "/>
12 <versionNumber value="1"/>
```

Listing 4.1: Arztbrief: Allgemeine Informationen

Eine Einstufung der Sensibilität, der in diesem Header-Bereich enthaltenen Informationen, ist in Tabelle 4.1 zusammengefasst.

Tag	Kurzbeschreibung	Erforderlich	Sensibilität
`<typId>`	Fix vorgegebener Tag	Ja	Keine
`<templateId>`	Template Id	Nein	Niedrig
`<id>`	Weltweit eindeutige Dokument Id	Ja	Mittel
`<code>`	Typisierung des Dokuments	Ja	Niedrig
`<titel>`	Titel des Dokuments	Nein	Sehr hoch
`<effectiveTime>`	Erstellungsdatum	Ja	Niedrig
`<confidentialityCode>`	Vertraulichkeitsgrad	Ja	Niedrig
`<languageCode>`	Dokumentensprache	Nein	Niedrig
`<setId>`	Id des Dokumentensets	Nein	Mittel
`<versionNumber>`	Versionsnummer des Dokuments	Nein	Niedrig

Tabelle 4.1: Arztbrief-Header: Allgemeine Informationen

Der allgemeine Teil des Dokumenten-Headers beinhaltet insgesamt zwei Informationen, welche bei der Pseudonymisierung des Dokuments berücksichtigt werden

1 siehe Tabelle 3 Implementierungsleitfaden (Heitmann et al., 2006) Seite 45-46

müssen. Das ist zum einen die *Id* und die *setID* des Dokuments und zum anderen der *Titel* des Dokuments. Die Id stellt eine sensible Information dar, da hier auf den Erzeuger Rückschlüsse gemacht werden können. Der optionale Titel kann, da dieser ein reines Freitext-Feld ist, personenbezogene Daten enthalten und sollte somit der Sensibilitätsstufe *Sehr hoch* zugeordnet werden.

4.1.3 Beteiligte Parteien

Die beteiligten Parteien eines Arztbriefes umfassen Personen und Organisationen, die direkt oder auch indirekt mit dem Arztbrief und somit auch mit dem Patienten in Verbindung stehen. Dabei können folgende Rollen eingenommen werden:

1. Patient
2. Autor
3. Verwaltende Organisation
4. Empfänger
5. Unterzeichner

In den nachfolgenden Abschnitten werden diese Rollen durchleuchtet und auf ihre Sensibilität hin untersucht.

4.1.3.1 Patient

Der Patienten-Bereich ist der für die Pseudonymisierung wichtigste Teil des Arztbriefes. Dieser beinhaltet alle Informationen, die den Patient eindeutig identifizieren. Daher ist auf diesen Bereich besonderes Augenmerk zu legen. Das Listing 4.2 zeigt ein Beispiel, welches nachfolgend einer Analyse unterzogen ist.

```
   <recordTarget>
14   <patientRole>
       <id extension="123419520917" root="1.2.276.0.76.3.1.13.99"/>
16     <id extension="M5" root="1.2.276.0.24.0.5.0.1339551403.2.6.1"/>
       <id extension="5" root="1.2.276.0.24.0.5.0.1339551403.2.1.1550751403
           "/>
18     <id extension="5" root="1.2.276.0.24.0.5.0.1339551403.2.5.1"/>
       <addr use="HP">
20       <streetName>Kölner Wiesenweg</streetName>
         <houseNumber>44</houseNumber>
22       <postalCode>52349</postalCode>
         <city>Düren</city>
24       <country>Deutschland</country>
       </addr>
26     <telecom use="HP" value="tel:+4924212356532"/>
```

```
      <patient>
28      <name>
          <given>Karl</given>
30        <family>Krummbein</family>
        </name>
32      <administrativeGenderCode code="M" codeSystem="
            2.16.840.1.113883.5.1"/>
        <birthTime value="19520917"/>
34    </patient>
      <providerOrganization>
36      <id extension="927834" root="1.2.276.0.76.3.1.13.79"/>
        <name>Medizinische Klinik am Waldpark</name>
38      <telecom use="WP" value="tel:+492421435621"/>
        <addr use="WP">
40        <streetName>Roonstraße</streetName>
          <houseNumber>30</houseNumber>
42        <postalCode>52351</postalCode>
          <city>Düren</city>
44        <country>Deutschland</country>
        </addr>
46    </providerOrganization>
    </patientRole>
48 </recordTarget>
```

Listing 4.2: Arztbrief: Patient-Tag

Der <recordTarget>-Tag beinhaltet die Informationen des Patienten, welche im <patientRole>-Tag angeführt werden. Der <id>-Tag beinhaltet die Identifikations-Nummer des Patienten in diversen Systemen. Die Systeme sind wie bereits bei den allgemeinen Informationen als @root-Attribut angegeben. Hier kann zum Beispiel die Sozialversicherungsnummer enthalten sein. Die Adresse des Patienten befindet sich im <addr>-Tag. Der <telecom>-Tag beinhaltet die Telefonnummer des Patienten. Der Name, das Geburtsdatum und das Geschlecht des Patienten sind im <patient>-Tag zu finden. Die für den Patienten zuständige Heilberuf-Organisation ist im <providerOrganisation>-Tag angeführt.

Eine Einstufung der Sensibilität für die Daten des Patienten ist in Tabelle 4.2 zusammengefasst.

Tag	Kurzbeschreibung	Erforderlich	Sensibilität
<id>	Id des Patienten in der Anwendung	Ja	Sehr hoch
<addr>	Adresse des Patienten	Nein	Sehr hoch
<telecom>	Telefonnummer des Patienten	Nein	Sehr hoch
<patient>	Patienteninformation	Nein	Sehr hoch
<providerOrganisation>	Organisation, die den Patienten betreut	Nein	Niedrig

Tabelle 4.2: Arztbrief-Header: Patient

Generell sind alle Informationen, die in diesem Block angeführt sind der Sensibilitätsstufe *Sehr hoch* zuzuordnen. Eine Abstufung der Sensibilität kann in den Stufen *Sehr*

hoch und *Hoch* vorgenommen werden. So sind der *Name*, die *Id*, die *Adresse* als *Sehr hoch*, das Geburtsdatum als *Mittel* und das *Geschlecht* als *Niedrig* einzustufen.

4.1.3.2 Autor

Der Urheber des Arztbriefes wird als Autor bezeichnet. Listing 4.3 zeigt den betroffenen Bereich des Arztbriefes aus Listing A.1.

```
   <author>
50   <time value="20060529"/>
     <assignedAuthor>
52       <id extension="MM" root="
             1.2.276.0.24.0.5.0.1339551403.1.6.1550751403"/>
         <id extension="4533355" root="1.2.276.0.76.3.1.13.89"/>
54       <assignedPerson>
           <name>
56           <prefix qualifier="AC">Dr.</prefix>
             <given>Medina</given>
58           <family>Medorn</family>
           </name>
60       </assignedPerson>
         <representedOrganization>
62         <name>Medizinische Klinik am Waldpark</name>
           <telecom use="WP" value="tel:+492421435621"/>
64         <addr use="WP">
             <streetName>Roonstraße</streetName>
66           <houseNumber>30</houseNumber>
             <postalCode>52351</postalCode>
68           <city>Düren</city>
             <country>Deutschland</country>
70         </addr>
         </representedOrganization>
72   </assignedAuthor>
   </author>
```

Listing 4.3: Arztbrief: Autor-Tag

Der Zeitpunkt der Dokumentation wird im `<time>`-Tag festgehalten. Wie jede Rolle im Arztbrief besitzt auch der Autor eine Id (`<id>`-Tag), welche für die jeweilige Anwendung eindeutig ist. Der `<assignedPerson>`-Tag repräsentiert die Person, welche als Autor des Dokuments verantwortlich ist. Diese Person ist einer Organisation zugeordnet, die im `<representedOrganization>`-Tag eingetragen ist.

In Tabelle 4.3 ist die Einstufung der Sensibilität der Daten des Autors in Bezug auf die Patienten-Sicherheit zusammengefasst.

Die Informationen des Autors werden gänzlich der Sensibilitätsstufe *Niedrig* zugeordnet, da diese keinen direkten Rückschluss auf den Patienten zulassen.

Tag	Kurzbeschreibung	Erforderlich	Sensibilität
<functionCode>	Funktion des Autors	Ja	Niedrig
<time>	Zeitpunkt der Dokumentation	Ja	Niedrig
<id>	Id des Autors in der Anwendung	Ja	Niedrig
<addr>	Adresse des Autors	Nein	Niedrig
<telecom>	Telefonnummer des Autors	Nein	Niedrig
<assignedPerson>	Personendaten des Autors	Nein	Niedrig
<providerOrganisation>	Daten der Autor-Organisation	Nein	Niedrig

Tabelle 4.3: Arztbrief-Header: Autor

4.1.3.3 Verwaltende Organisation

Die Verwaltung eines Dokuments obliegt einer Organisation, die Daten dieser sind im <custodian>-Tag eingetragen. Listing 4.4 zeigt ein Beispiel eines solchen Eintrags.

```
74 <custodian>
     <assignedCustodian>
76     <representedCustodianOrganization>
         <id extension="927834" root="1.2.276.0.76.3.1.13.79"/>
78       <name>Medizinische Klinik am Waldpark</name>
         <telecom use="WP" value="tel:+492421435621"/>
80       <addr use="WP">
           <streetName>Roonstraße</streetName>
82         <houseNumber>30</houseNumber>
           <postalCode>52351</postalCode>
84         <city>Düren</city>
           <country>Deutschland</country>
86       </addr>
       </representedCustodianOrganization>
88   </assignedCustodian>
   </custodian>
```

Listing 4.4: Arztbrief: Verwaltende Organisation-Tag

Jede Organisation besitzt innerhalb einer Anwendung ihre eindeutige Id (<id>-Tag). Weiters können der Name (<name>-Tag) sowie die Adresse (<addr>-Tag) einer Organisation angegeben werden.

Eine Einstufung der Sensibilität für die Daten der verwaltenden Organisation in Bezug auf den Patienten ist in Tabelle 4.4 zusammengefasst.

Sämtliche Informationen dieses Tags werden der Sensibilitätsstufe *Niedrig* zugeordnet. Diese Daten lassen keinen direkten Schluss auf den Patienten zu.

Tag	Kurzbeschreibung	Erforderlich	Sensibilität
<id>	Id der Organisation in der Anwendung	Ja	Niedrig
<name>	Name der Organisation	Nein	Niedrig
<telecom>	Telefonnummer der Organisation	Nein	Niedrig
<addr>	Adresse der Organisation	Nein	Niedrig

Tabelle 4.4: Arztbrief-Header: Verwaltende Organisation

4.1.3.4 Empfänger

Der Empfänger eines Arztbriefes ist ein Arzt einer im Arztbrief definierten Organisation. Es sind nur Empfänger eingetragen, die auch tatsächlich diesen Arztbrief erhalten, und direkt bei der Erstellung des Dokuments erfasst werden. Mögliche Empfänger, die unter Umständen diesen Arztbrief erhalten könnten, sind nicht vorgesehen und werden somit auch nicht berücksichtigt.

```
<informationRecipient typeCode="PRCP">
  <intendedRecipient>
    <id extension="9182736" root="1.2.276.0.76.3.1.13.89"/>
    <informationRecipient>
      <name>
        <prefix qualifier="AC">Dr.</prefix>
        <given>Detlef</given>
        <family>Insulaner</family>
      </name>
    </informationRecipient>
    <receivedOrganization>
      <telecom use="WP" value="tel:+49242136318"/>
      <addr use="WP">
        <streetName>Hauptstr.</streetName>
        <houseNumber>3</houseNumber>
        <postalCode>52355</postalCode>
        <city>Düren</city>
        <country>Deutschland</country>
      </addr>
    </receivedOrganization>
  </intendedRecipient>
</informationRecipient>
```

Listing 4.5: Arztbrief: Empfänger-Tag

Der <id>-Tag identifiziert innerhalb einer Anwendung eindeutig den Empfänger. Ein Empfänger wird mit dem Namen (<informationRecipient>-Tag) und der zuständigen Organisation (<receivedOrganisation>-Tag) angegeben.

Tabelle 4.5 fasst die Einstufung der Sensibilität der Daten des Empfängers in Bezug auf den Patienten zusammen.

Tag	Kurzbeschreibung	Erforderlich	Sensibilität
<id>	Id der Organisation in der Anwendung	Nein	Niedrig
<informationRecipient>	Empfänger der Nachricht	Nein	Niedrig
<receivedOrganization>	Organisation des Empfängers	Nein	Niedrig

Tabelle 4.5: Arztbrief-Header: Verwaltende Empfänger

Diese Informationen sind der Sensibilitätsstufe *Niedrig* zugeordnet, da hier kein direkter Bezug zum Patienten vorliegt.

4.1.3.5 Unterzeichner

Maximal eine Person kann einen Arztbrief unterzeichnen. Diese Person ist dann gesetzlich für den Inhalt verantwortlich. Der zugehörige Codeschnippsel ist im nachfolgenden Listing 4.6 angeführt.

```
112 <legalAuthenticator>
      <time value="20060529153202"/>
114   <signatureCode code="I"/>
      <assignedEntity>
116     <id extension="MM" root="
            1.2.276.0.24.0.5.0.1339551403.1.6.1550751403"/>
        <id extension="4533355" root="1.2.276.0.76.3.1.13.89"/>
118     <assignedPerson>
          <name>
120         <prefix qualifier="AC">Dr.</prefix>
            <given>Medina</given>
122         <family>Medorn</family>
          </name>
124     </assignedPerson>
        <representedOrganization>
126       <name>Medizinische Klinik am Waldpark</name>
          <telecom use="WP" value="tel:+492421435621"/>
128       <addr use="WP">
            <streetName>Roonstraße</streetName>
130         <houseNumber>30</houseNumber>
            <postalCode>52351</postalCode>
132         <city>Düren</city>
            <country>Deutschland</country>
134       </addr>
        </representedOrganization>
136   </assignedEntity>
    </legalAuthenticator>
```

Listing 4.6: Arztbrief: Unterzeichner-Tag

Der Zeitpunkt der Unterzeichnung wird im <time>-Tag angegeben. Weiters wird ein <signatureCode>-Tag, der die Unterschrift typisiert[2] definiert. Die Id des Unterzeichners (<id>-Tag) ist eindeutig innerhalb der angegebenen Anwendung. Der Unterzeichner ist mit Name (<assignedPerson>-Tag) und der zugehörigen Organisation (<representedOrganisation>-Tag) angegeben.

Eine Einstufung der Sensibilität für die Daten des Unterzeichners in Bezug auf den Patienten ist in Tabelle 4.6 zusammengefasst.

Tag	Kurzbeschreibung	Erforderlich	Sensibilität
<time>	Zeitpunkt der Unterschrift	Ja	Niedrig
<signatureCode>	Typisierung der Unterschrift	Ja	Niedrig
<id>	Id des Unterzeichners	Nein	Niedrig
<addr>	Adresse des Unterzeichners	Nein	Niedrig
<telecom>	Telefonnummer des Unterzeichners	Nein	Niedrig
<assignedPerson>	Name des Unterzeichners	Nein	Niedrig
<representedOrganization>	Organisation des Unterzeichners	Nein	Niedrig

Tabelle 4.6: Arztbrief-Header: Unterzeichner

Diese Information sind der Sensibilitätsstufe *Niedrig* zugeordnet, da hier kein direkter Bezug zum Patienten vorliegt.

4.1.4 Body

Im Body sind die eigentlichen medizinischen Informationen des Arztbriefes enthalten. Es ist nicht möglich, diese Informationen einer Person zuzuordnen, wenn diese nicht im Text des Bodys namentlich genannt werden. Listing 4.7 zeigt ein Problem auf, dass bei der Eingabe von Freitexten auftreten kann.

```
138 <component>
      <structuredBody>
140     <component>
          <section>
142         <code code="X-SALUT" codeSystem="2.16.840.1.113883.6.1"/>
            <text> Sehr geehrte Frau Kollegin, sehr geehrter Herr Kollege, <
                br/>
```

2 ”Unterschrift erforderlich”, ”unterschrieben” beziehungsweise ”beabsichtigt das Dokument zu unterschreiben”

```
144             <br/> wir berichten über unseren Patienten, Karl Krummbein,
                    geboren am 17.09.1952, der sich vom 25.01.2006 bis
                    17.02.2006 bei uns in stationärer Behandlung befand.
                </text>
146           </section>
            </component>
148         ...
```

Listing 4.7: Arztbrief: Body-Tag

Der Inhalt des Bodys ist prinzipiell der Sensibilitätsstufe *Niedrig* zugeordnet, da hier kein Rückschluss auf den Patienten möglich ist.

Es muss jedoch darauf geachtet werden, dass in den Freitextinformationen des Bodys keine Patientendaten wie zum Beispiel der Name oder das Geburtsdatum eingegeben werden, da ansonsten die Pseudonymisierung gefährdet ist.

4.1.5 Ergebnis der Datenanalyse

Bei der Pseudonymisierung des Arztbriefes ist besonderes Augenmerk auf die Patientendaten zu legen. Diese erlauben es, den Arztbrief direkt einer Person zuzuordnen. Wenn eine Pseudonymisierung angestrebt wird, muss dafür Sorge getragen werden, dass keine Patienteninformationen in den Freitextfeldern des Arztbriefes enthalten sind. Zu diesen Freitextfeldern zählen zum Beispiel der Titel des Dokuments oder die Freitextfelder des Bodys.

Die der Sensibilitätsstufe *Mittel* zugeordneten Informationen lassen keinen Schluss auf den Patient zu. Bei der Pseudonymisierung sind daher primär die Informationen des Patienten zu berücksichtigen. Im weiteren Schritt muss auch angedacht werden, die übrigen Informationen zu bearbeiten. So sollten vor einer Pseudonymisierung die Freitextfelder, soweit möglich, auf Daten des Patienten hin untersucht werden und diese gegebenenfalls automatisch entfernt beziehungsweise der Ersteller des Dokuments darauf hingewiesen werden. Der Ersteller sollte bei einer Benachrichtigung handeln und seine Eingaben entsprechend überarbeiten.

Das detaillierte Ergebnis der Datenanalyse des Arztbriefes ist in nachfolgender Tabelle 4.7 zusammengefasst.

Um eine Pseudonymisierung zu ermöglichen, wird empfohlen, den Titel nicht manuell zu befüllen, um auf diese Weise der Eingabe von personenbezogenen Daten vorzubeugen. Weiters sollten Dienstanweisungen dafür Sorge tragen, dass die Autoren keine personenbezogenen Daten (Name, Adresse, Geburtsdatum, ...) in die Freitextfelder

Bereich	Sensibilität
Allgemeine Dokumenteninformation	Sehr hoch
Patient	Sehr hoch
Autor des Dokuments	Mittel
Verwaltende Organisation	Mittel
Beabsichtigter Empfänger	Mittel
Unterzeichner	Mittel

Tabelle 4.7: Arztbrief-Header: Zusammenfassung Datenanalyse

des Arztbriefes eingeben. Ein simpler Check während des Speicherns des Arztbriefes kann den Autor auffordern, diese Daten wieder zu entfernen und den Vorgang des Speicherns anschließend zu wiederholen. Dieser Check greift auf die Informationen des zugeordneten Patienten zu und durchsucht die Freitexte auf diese Daten.

4.2 Pseudonymisierung des Arztbriefes

In den nachfolgenden Kapiteln wird der Ablauf der Integration der Pseudonymisierungs-Funktion eines Arztbriefes in das bestehende PIPE beschrieben. Es gibt insgesamt drei Haupt-Funktionen, welche für eine Pseudonymisierung eines Arztbriefes erforderlich sind:

- Pseudonymisierung des Arztbriefes
- Despeudonymisierung des Arztbriefes
- Datenaustausch zwischen GDAs

Weiters wird die grundlegende Architektur kurz erläutert und die Anforderungen an das zugrunde liegende Datenmodell beschrieben und erweitert.

Um eine Implementierung durchführen zu können, werden die neuen Funktionen, welche dafür benötigt werden, detailliert beschrieben und deren Implementierung mit Hilfe von Sequenzdiagrammen und Funktionsbeschreibungen erläutert. Es werden die Parameter und Rückgabewerte der einzelnen Funktionen angeführt.

4.2.1 Architektur

Die Systemarchitektur, in welche PIPE integriert wird, führt eine zusätzliche Schicht zwischen ELGA und den Gesundheitsdienstanbietern (GDA) (IBM und Prenner, 2006) ein. Das Service von PIPE ist als Ergänzung zu der bestehenden Struktur von ELGA

zu sehen. Mit Hilfe dieses Services kann ein pseudonymisierter Arztbrief gespeichert werden. Diese zusätzliche Schicht hält am geplanten dezentralen Dokumentenkonzept von ELGA fest. Das heißt, dass PIPE keine vollständigen Dokumente speichert. In PIPE werden lediglich die Informationen, welche zur Wiederherstellung des vollständigen Arztbriefes notwendig sind, persistent gespeichert. Des weiteren kann der Patient mittels PIPE den Zugriff auf den Arztbrief selbst steuern.

PIPE greift auf die vorhandenen Informationen des Gesundheitsdienstanbieter-Index und des Patienten-Index zu. Diese Informationen werden dazu verwendet, um den Header des Arztbriefes zu erstellen. Die Zuordnungstabelle *UserMapping* speichert in PIPE die dazugehörigen Schlüssel während die Beziehungen zwischen den beteiligten Personen in der *Relations*-Tabelle persistiert werden. Da jedoch auch eine Zuordnung der unterschiedlichen Rollen im Arztbrief notwendig ist, muss die *Identification*-Tabelle um ein Attribut, welches die Rolle in einem Arztbrief beschreibt, erweitert werden. Abbildung 4.1 stellt die geänderte Struktur dieser Tabelle dar.

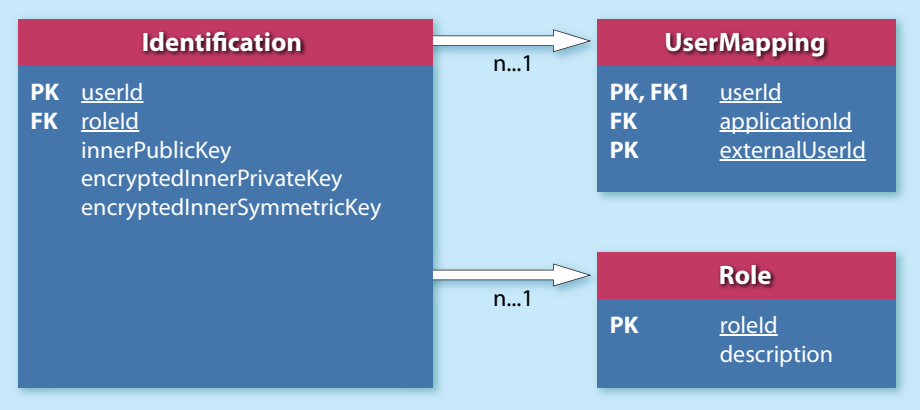

Abbildung 4.1: Änderungen an der Identification-Tabelle

Die eigentlichen medizinischen Daten des Arztbriefes, der Body, werden nicht im PIPE-Service gespeichert. Es wird, der ELGA-Konformation entsprechend, lediglich eine Referenz zu den Daten im jeweiligen Fremdsystem abgelegt. Die Informationen dieser Referenz werden beim Zusammensetzen des Arztbriefes vom Gesundheitsdienstanbieter abgerufen und über eine gesicherte Leitung zum Empfänger übertragen.

4.2.2 Ablauf der Pseudonymisierung

Der Ablauf der Pseudonymisierung wurde grundsätzlich in Kapitel 3.3.2 beschrieben. Diese Beschreibung beinhaltet den standardisierten Ablauf einer herkömmlichen Pseudonymisierung. Um jedoch einen Arztbrief zu pseudonymisieren, sind zusätzliche

Schritte notwendig. Es müssen zuerst die entsprechenden Tags entfernt werden, bevor die eigentliche Pseudonymisierung durchgeführt werden kann. Da diese Informationen nicht im Dokument sondern im PIPE-Service persistent gespeichert werden.

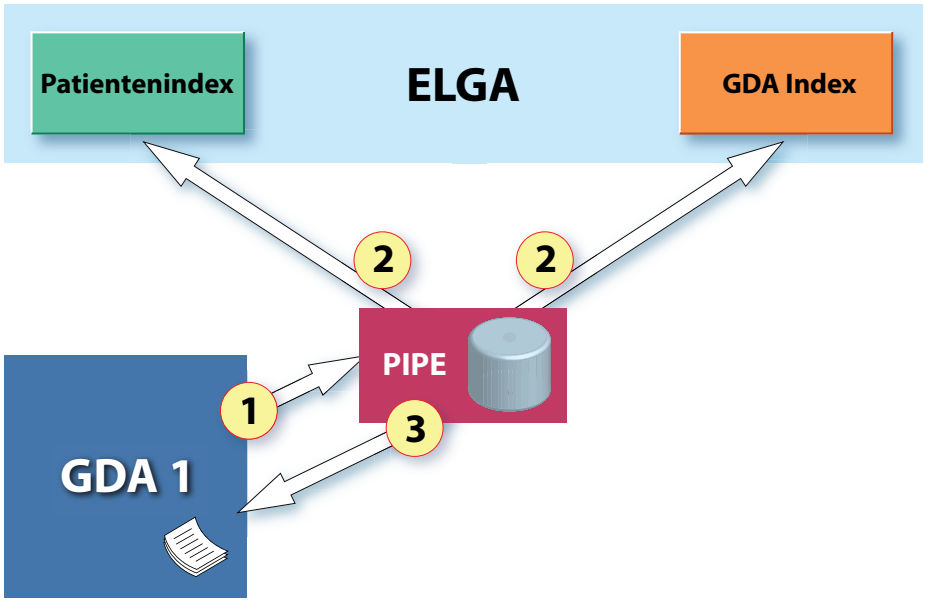

Abbildung 4.2: Ablauf bei Pseudonymisierung

Abbildung 4.2 zeigt den Ablauf der Pseudonymisierung eines Arztbriefes. Für die Pseudonymisierung relevant sind die Schritte *1*, *2* und *3*. Im ersten Schritt wird der Arztbrief an PIPE gesendet. Im nächsten Schritt werden die Informationen der Personen von ELGA aus dem Patienten- beziehungsweise dem Gesundheitsdienstanbieter-Index gelesen. Diese Informationen werden benötigt, um eine Zuordnung der Personen mit Hilfe des PIPE-Services zu ermöglichen. Im zweiten Schritt verarbeitet das PIPE-Service diese Informationen. Dazu werden die Personen im PIPE-Service angelegt (Abschnitt 3.3.1), falls dies noch nicht erfolgte. Für jede identifizierte Person wird ein Eintrag in der *Relations*-Tabelle erstellt. Danach werden die Daten – in unserem Fall eine Referenz beziehungsweise ein Link zum Body des Dokuments – gespeichert (siehe Abschnitt 3.3.2), um im Anschluss daran die Beziehungen dieser Personen, welche für den Arztbrief relevant sind, zu persistieren (siehe Abschnitt 3.3.4). Im letzten Schritt informiert PIPE die aufrufende Applikation über den Status der Operation und die aufrufende Applikation speichert den Body des Arztbriefes.

Abbildung 4.3 zeigt das Sequenzdiagramm zu diesem Usecase. Es wird eine neue Funktion in der API `addDataNew` angesprochen, welche die bereits integrierten Funktionen `addData`, `addDataRelation` und `addActor` vereint und um die Funktionen `getRolesInDocument`, `lookUpActor`, `getPatient`, `getGDA` und `removeRolesInDocument`

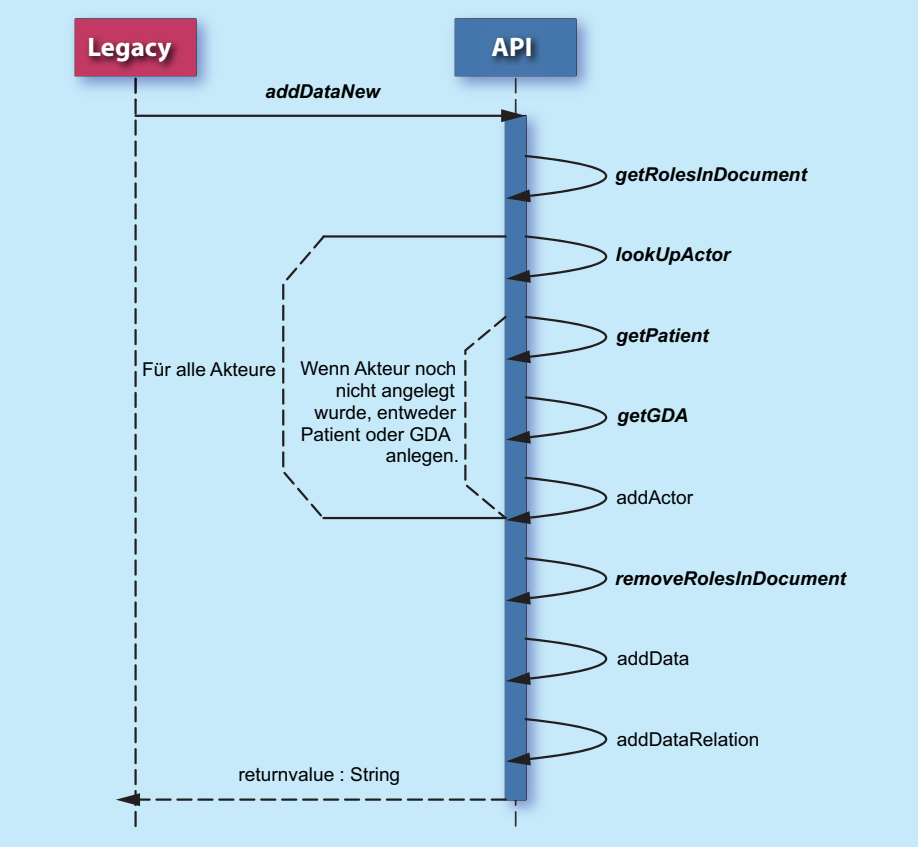

Abbildung 4.3: Sequenzdiagramm: Einen Arztbrief pseudonymisiert ablegen

erweitert. Die nachfolgenden Sektionen widmen sich diesen neuen Funktionen näher und beschreiben diese im Detail.

4.2.2.1 getRolesInDocument

Hierbei handelt es sich um eine neue Funktion in PIPE. Diese durchsucht den übergebenen Arztbrief und extrahiert die im Header enthaltenen Patienten-/GDA-Informationen. Das Ergebnis dieser Funktion ist ein Array mit allen enthaltenen Rollen und Identifikationsnummern aus dem Patienten-/GDA-Index.

Das gesamte Dokument wird auf die in Kapitel 4.1.3 angeführten Tags hin untersucht. Für jeden gefundenen Tag wird im Anschluss die Identifikationsnummer aus dem Patienten-/GDA-Index ermittelt.

Die Aufrufparameter sind in Tabelle 4.8 und die Rückgabewerte in Tabelle 4.9 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument

Tabelle 4.8: Parameter: getRolesInDocument

Wert	Typ	Kommentar
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument enthaltenen Rollen

Tabelle 4.9: Rückgabewert: getRolesInDocument

4.2.2.2 getPatient

Diese neue Funktion dient zum Auslesen der Identifikationsnummer aus dem Patientenindex. Hierzu wird in diesem nach einem Patienten mit Hilfe von Namen, Geburtsdatum und Sozialversicherung gesucht. Das Ergebnis dieses Aufrufs ist die Identifikationsnummer des Patientenindex. Diese wird für die Zuordnung zum internen Akteur verwendet.

Die Aufrufparameter sind in Tabelle 4.10 und die Rückgabewerte in Tabelle 4.11 angeführt.

Name	Typ	Kommentar
name	String	Der Name, der zu suchenden Person
[dateOfBirth]	Date	Das Geburtsdatum der zu suchenden Person
[socialSecurityNumber]	Long	Sozialversicherungsnummer

Tabelle 4.10: Paramter: getPatient

Wert	Typ	Kommentar
> 0	Long	Die externe Identifikationsnummer des Patienten-Index
< 0	Long	Fehlercode

Tabelle 4.11: Rückgabewert: getPatient

4.2.2.3 getGDA

Diese neue Funktion dient zum Auslesen der Identifikationsnummer aus dem GDA-Index. Hierzu wird in diesem nach einem GDA mit Hilfe des Namens und des Organisationsnamens gesucht. Als Ergebnis wird die Identifikationsnummer im GDA-Index zurückgeliefert. Diese wird für die Zuordnung zum internen Aktuer herangezogen.

Die Aufrufparameter sind in Tabelle 4.12 und die Rückgabewerte in Tabelle 4.13 angeführt.

Name	Typ	Kommentar
name	String	Der Name, der zu suchenden Person
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.12: Paramter: getGDA

Wert	Typ	Kommentar
> 0	Long	Die externe Identifikationsnummer des GDA-Index
< 0	Long	Fehlercode

Tabelle 4.13: Rückgabewert: getGDA

4.2.2.4 removeRolesInDocument

Diese Funktion ermöglicht die Entfernung aller Rollen aus dem Dokument, damit der Arztbrief im Anschluss pseudonymisiert gespeichert werden kann. Hierbei werden alle Tags aus dem Header entfernt, welche zuvor ermittelt und zwischengespeichert wurden. Diese Funktion bereitet den Arztbrief soweit auf, dass dieser ohne jeglichen Personenbezug - also anonymisiert - in der Datenbank des GDA abgelegt werden kann.

Die Aufrufparameter sind in Tabelle 4.14 und die Rückgabewerte in Tabelle 4.15 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument zu löschenden Rollen
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.14: Paramter: removeRolesInDocument

Wert	Typ	Kommentar
document	String	Das anonymisierte XML-Dokument

Tabelle 4.15: Rückgabewert: removeRolesInDocument

4.2.3 Ablauf der Depseudonymisierung

Da ein pseudonymisierter Arztbrief nur noch aus dem Body besteht und alle personenbezogenen Informationen entfernt wurden, ist es notwendig, diese Informationen zu sammeln und im Anschluss zusammenzufügen. Dadurch wird der vollständige Arztbrief hergestellt, mit dem in gewohnter Weise gearbeitet werden kann.

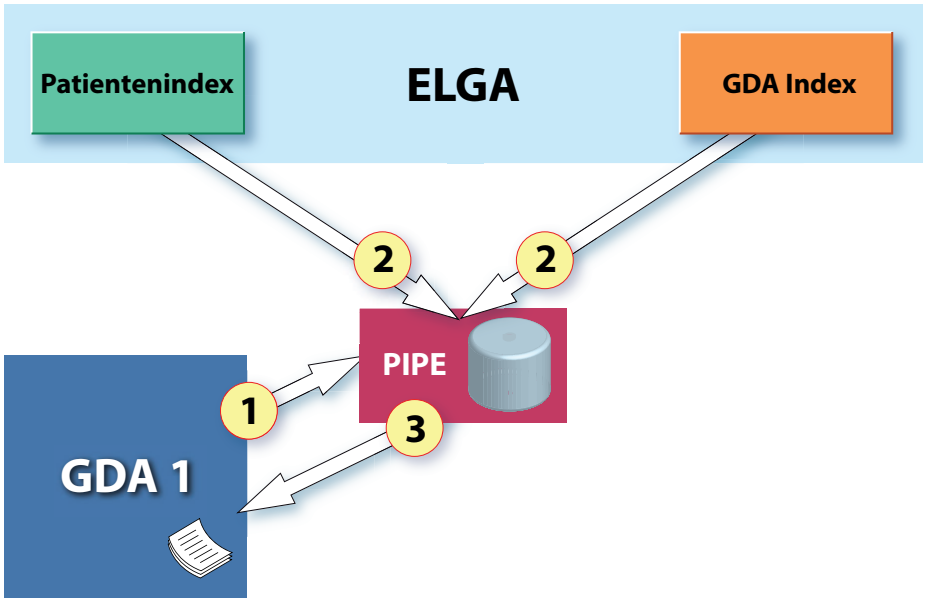

Abbildung 4.4: Ablauf bei Depseudonymisierung

Die Depseudonymisierung wurde bereits in Kapitel 3.3.3 erläutert. Um jedoch die Erweiterungen des pseudonymisierten Arztbriefes zu unterstützen, muss dieser Ablauf entsprechend erweitert werden. Diese Erweiterung ist in Abbildung 4.4 visualisiert. Im ersten Schritt sendet die Fremdapplikation eine Anfrage an PIPE. PIPE sucht nun mit Hilfe der Schlüsselwörter den Arztbrief. Im zweiten Schritt müssen die Akteurdaten aus dem PIPE-Service ausgelesen werden. Die ausgelesenen Akteurdaten welche dazu benutzt werden, um die eigentlichen Informationen dieser Akteure aus ELGA zu erhalten sind in Form einer Referenz beziehungsweise eines Links im System abgelegt. Dazu wird auf den Patienten- beziehungsweise auf den Gesundheitsdienstanbieter-Index zugegriffen. Weiters werden die jeweiligen Rollen der Akteure, mit Ausnahme des Patienten – welcher Eigentümer des Arztbriefes ist – geliefert. Mit Hilfe dieser Informationen kann nun der Header des Arztbriefes zusammengesetzt werden. Sämtliche Informationen wie Adresse, Geburtsdatum, Telefonnummern, ... werden aus dem globalen ELGA-Index verwendet. Im letzten Schritt fügt das PIPE-Service den Body des Dokuments mit Hilfe der gespeicherten Referenz hinzu und sendet den Arztbrief

an die Fremdapplikation.

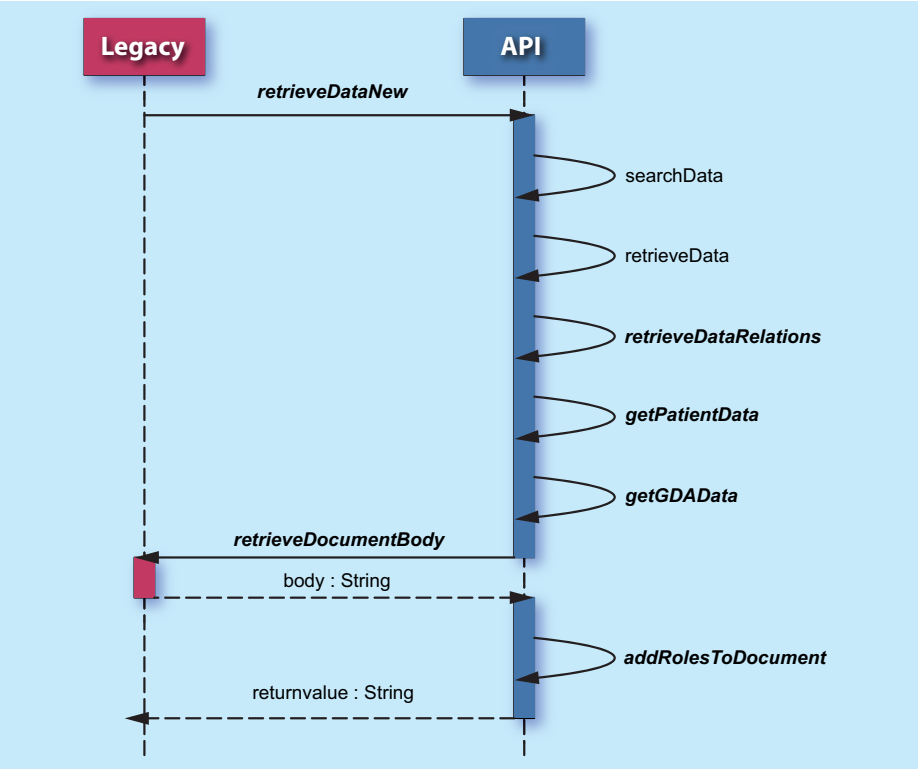

Abbildung 4.5: Sequenzdiagramm: Einen Arztbrief depseudonymisieren

Um wieder den ursprünglichen Arztbrief zu erhalten, in dem alle Informationen der beteiligten Akteure enthalten sind, müssen die in Abbildung 4.5 angeführten Operationen durchgeführt werden. Die Funktion `retrieveDataNew` vereint die Funktionsaufrufe der bereits in PIPE vorhandenen Funktionen `searchData` und `retrieveData` mit den neu hinzugefügten Funktionen `retrieveDataRelations`, `getPatientData`, `getGDAData` und `addRolesToDocument`. Eine nähere Erläuterung findet sich in den nächsten Sektionen.

4.2.3.1 retrieveDataRelations

Eine Extrahierung der Daten aus der Datenbank ist notwendig, um alle Rollen wieder in den Arztbrief einzufügen. Dies geschieht mit Hilfe dieser Funktion.

Die Aufrufparameter sind in Tabelle 4.16 und die Rückgabewerte in Tabelle 4.17 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument zu löschenden Rollen
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.16: Paramter: retrieveDataRelations

Wert	Typ	Kommentar
document	String	Das anonymisierte XML-Dokument

Tabelle 4.17: Rückgabewert: retrieveDataRelations

4.2.3.2 getPatientData

Nach der Extrahierung aller Rollen kommt es zu einer Selektion der zugehörigen Daten. Die Daten für den Patienten werden direkt aus dem Patientenindex verwendet. Diese Funktion bietet die Möglichkeit eine Abfrage auf diesen Patientenindex durchzuführen.

Die Aufrufparameter sind in Tabelle 4.18 und die Rückgabewerte in Tabelle 4.19 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument zu löschenden Rollen
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.18: Paramter: getPatientData

Wert	Typ	Kommentar
document	String	Das anonymisierte XML-Dokument

Tabelle 4.19: Rückgabewert: getPatientData

4.2.3.3 getGDAData

Die Daten der GDA werden ebenfalls aus dem entsprechenden Index, dem GDA-Index, selektiert. Diese Informationen werden im Anschluss daran in den Arztbrief eingefügt.

Die Aufrufparameter sind in Tabelle 4.20 und die Rückgabewerte in Tabelle 4.21 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument zu löschenden Rollen
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.20: Paramter: getGDAData

Wert	Typ	Kommentar
document	String	Das anonymisierte XML-Dokument

Tabelle 4.21: Rückgabewert: getGDAData

4.2.3.4 addRolesToDocument

Diese Funktion fügt die zuvor selektierten Daten des Patienten und der GDA wieder in den Arztbrief ein. Das Ergebnis dieser Funktion ist der vollständige Arztbrief, mit dem in gewohnter Weise gearbeitet werden kann.

Die Aufrufparameter sind in Tabelle 4.22 und die Rückgabewerte in Tabelle 4.23 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument zu löschenden Rollen
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.22: Paramter: addRolesToDocument

Wert	Typ	Kommentar
document	String	Das anonymisierte XML-Dokument

Tabelle 4.23: Rückgabewert: addRolesToDocument

4.2.4 Ablauf des Datenaustausches

Der Austausch eines pseudonymisierten Arztbriefes erfordert spezielle Mechanismen, da nur autorisierte Personen auf diese Daten zugreifen können. Ein Austausch kann

auch über Systemgrenzen hinweg geschehen, sofern der empfangende Gesundheitsdienstanbieter ebenfalls das PIPE-Service verwendet.

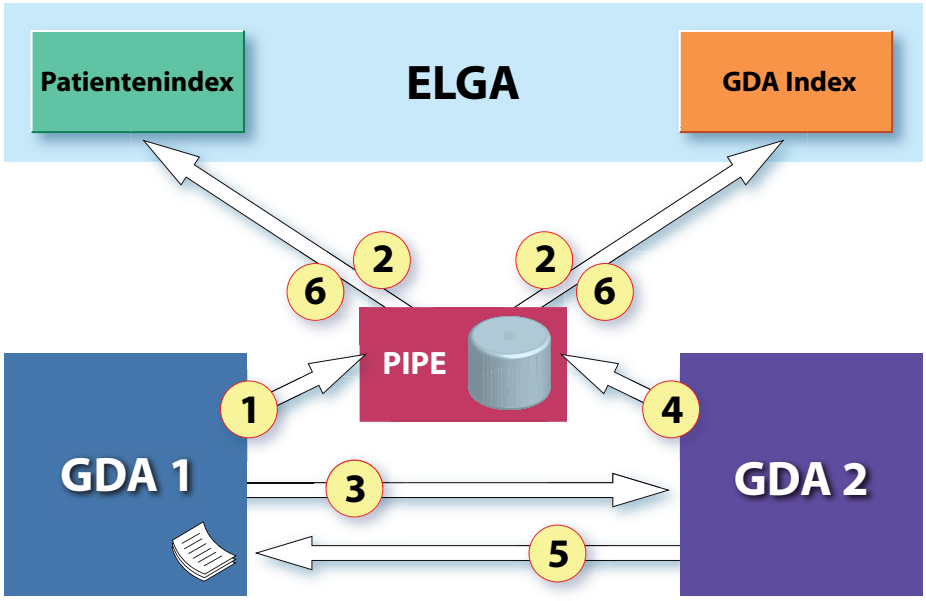

Abbildung 4.6: Ablauf bei Datenaustausch

Der Austausch eines Arztbriefes vereint die Schritte der Pseudonymisierung und Depseudonymisierung miteinander und erweitert diese entsprechend um das Senden einer Benachrichtigung an den Empfänger der Nachricht. Der Ablauf eines Datenaustausches ist schematisch in Abbildung 4.6 dargestellt. Nach der Pseudonymisierung (Beschrieben in Kapitel 4.2.2) wird eine Nachricht an den Empfänger des Arztbriefes geschickt, welcher einen Hinweis enthält, dass ein neuer Arztbrief abrufbereit ist. Der Empfänger sucht nun im PIPE-System mit Hilfe der definierten Schlüsselworte nach diesem Arztbrief und depseudonymisiert (Beschrieben in Kapitel 4.2.3) diesen. Um den Body des Arztbriefes zu erhalten, folgt der Empfänger der Referenz und ruft über eine gesicherte Datenleitung den Inhalt ab. Abschließend kommt es zu einer Zusammenfügung aller Informationen im lokalen System und das Ergebnis ist der Vollständige Arztbrief.

Auch der Usecase aus Empfängersicht vereint die Usecases der Pseudonymisierung und Depseudonymisierung. Zusätzlich werden die Funktionen `sendMessage` und `getBody` verwendet, welche in den nachfolgenden Sektionen detailliert beschrieben sind.

4.2.4.1 sendMessage

Diese Funktion versendet eine Nachricht an den Empfänger des Arztbriefes. Diese Nachricht enthält eine Information, dass ein neuer Arztbrief zur Abholung bereit steht.

Die Aufrufparameter sind in Tabelle 4.24 und die Rückgabewerte in Tabelle 4.25 angeführt.

Name	Typ	Kommentar
GDA	String	Der Empfänger des Arztbriefes

Tabelle 4.24: Paramter: sendMessage

Wert	Typ	Kommentar
< 0	Long	Fehlercode

Tabelle 4.25: Rückgabewert: sendMessage

4.2.4.2 getBody

Diese Funktion fordert den Body des Dokuments vom Datenhalter an. Dies geschieht über den im PIPE-Service gespeicherten Link. Der Empfänger-GDA fügt den Body dem wiederhergestellten Header an und erhält so den vollständigen Arztbrief.

Die Aufrufparameter sind in Tabelle 4.26 und die Rückgabewerte in Tabelle 4.27 angeführt.

Name	Typ	Kommentar
document	String	Das gesamte XML-Dokument
role	Long[][]	Array aller Identifikationsnummern der im XML-Dokument zu löschenden Rollen
[nameOfOrganization]	String	Name des GDA, optional

Tabelle 4.26: Paramter: getBody

Wert	Typ	Kommentar
document	String	Das anonymisierte XML-Dokument

Tabelle 4.27: Rückgabewert: getBody

KAPITEL 5

Zusammenfassung und Ausblick

Die Digitalisierung findet im Gesundheitswesen Einzug. Die Daten in Krankenhäusern beziehungsweise Arztpraxen werden vermehrt digital gespeichert. Diese digital gespeicherten Daten werden in weiterer Folge für den Austausch von Daten zwischen verschiedenen Gesundheitseinrichtungen verwendet. Herkömmliche Kommunikationsmechanismen bieten meist nur geringen Schutz vor unautorisiertem Zugriff.

- Wo kann PIPE in Kombination mit HL7 implementiert werden?

Um diese Frage zu beantworten, wurden die Strukturen von HL7, im Speziellen des Arztbriefes auf Basis der CDA R2 analysiert. Die enthaltenen Daten wurden auf Sensibilität hin untersucht und entsprechend eingestuft. Diese Einstufung ermöglicht nun die gezielte Verwendung von PIPE in Kombination mit HL7. Da PIPE ein Service ist und die Grunddaten von Patienten- beziehungsweise von Gesundheitsdienstanbietern zur Verfügung stellt, kann PIPE sehr gut mit HL7 kombiniert werden. So können alle personenbezogenen Daten entfernt werden, bevor der Arztbrief pseudonymisiert abgelegt wird. Bei einem Aufruf des pseudonymisierten Arztbriefes fügt PIPE die zuvor entfernten Daten wieder hinzu und stellt das vollständige Dokument zur Verfügung. Es ist jedoch zwingend notwendig, dass jegliche Freitextinformation frei von Patienteninformationen ist, um einen Schutz der Privatsphäre gewährleisten zu können.

- Wie kann HL7 in eine pseudonymisierte ELGA integriert werden?

Da es sich bei PIPE um ein Service handelt, welches auf sehr einfache Art und Weise in bestehende Applikationen eingebunden werden kann, ist die Integration ohne großen Aufwand möglich. Die Ursprungsapplikation muss nur dahingehend angepasst werden,

dass sie die entsprechenden Funktionen der PIPE-Service-API aufrufen kann. Der Aufruf muss beim Speichern und beim Lesen von Arztbriefen erfolgen. So kann der Arztbrief sehr einfach pseudonymisiert werden. Der Empfänger benötigt ebenfalls diese Erweiterungen in seiner Applikation, um den pseudonymisierten Arztbrief wieder zu depseudonymisieren und lesbar zu machen. Da es sich bei den PIPE-Funktionen um autarke Funktionen handelt, kann das Einbinden durch einen simplen Aufruf erfolgen. Dieser Aufruf kann ohne weitere Modifikation der Ursprungsapplikation erfolgen.

- Wie sieht die optimale Synergie zwischen HL7 und Pseudonymisierung aus?

HL7 und Pseudonymisierung sind für sich gesehen zwei mächtige Instrumente. Während HL7 für einen effektiven Datenaustausch verantwortlich ist und somit umfangreiche Dienstleistungen zur Verfügung stellt, kümmert sich Pseudonymisierung um das sichere Speichern von Daten. Die Sicherheit der Pseudonymisierung bezieht sich auf die Privatsphäre des Patienten. So ist es damit nicht möglich einen direkten Bezug zwischen Arztbriefen und Patienten herzustellen. Diese beiden Instrumente lassen sich sehr gut miteinander kombinieren und ergänzen sich somit prächtig. Dabei wird die vielschichtige Schnittstelle HL7 um ein Sicherheitskonzept erweitert, um die Privatsphäre der Patienten zu schützen. Hierbei wird einerseits die Struktur von HL7 zum effektiven Speichern der Informationen und andererseits die Pseudonymisierungsfunktionalität von PIPE für die sichere Ablage der Daten verwendet. Somit ist es in weiterer Folge auch möglich diese pseudonymisierten Arztbriefe mittels ungesicherter Datenleitung zwischen Gesundheitsdienstanbietern auszutauschen. Ein vermeintlicher Angreifer kann die übertragenen pseudonymisierten Daten keinem Patienten zuordnen.

- Gibt es Probleme mit der Verwendung von Pseudonymisierung in Verbindung mit HL7?

Wie bereits erwähnt, gibt es eine große Schwierigkeit, die im Zusammenhang mit Pseudonymisierung und HL7 steht. Ärzte müssen beim Erfassen von Daten für den Arztbrief Sorge tragen keine personenbezogenen Daten im Freitextbereich einzugeben, da dies die Pseudonymisierung des Dokuments gefährdet. Dieses Problem kann durch Arbeitsanweisungen gelöst werden. Mit Hilfe dieser kann der Gesundheitsdienstleister definieren, dass händische Eingaben von personenbezogenen Daten verboten sind und diese Eingaben nur im Headerbereich ausgewählt werden dürfen.

Da PIPE Pseudonymisierung als Grundlage hat und das Konzept vorsieht, dass in der Regel nur eine Person den Vollzugriff auf die pseudonymisierten Daten besitzt, müssen effektive Mechanismen entwickelt werden, um einem Datenverlust vorzubeugen.

Dieser Datenverlust kann beispielsweise durch einen simplen Verlust der Schlüsselkarte geschehen, da ohne den darauf gespeicherten Schlüssel kein Zugriff auf Daten möglich ist.

Weiters muss PIPE entsprechend zertifiziert werden, um auch standardmäßig in Neuimplementierungen Einsatz zu finden. Damit sich PIPE im Gesundheitssektor etablieren kann, sollte PIPE als Standard anerkannt werden. Dadurch wird eine Verbreitung und eine effektive Nutzung gewährleistet. Nur wenn jeder Arzt PIPE in seinem System verwendet, kann es zu einem sicheren Austausch von Arztbriefen kommen.

Literaturverzeichnis

1, Internet: American National Standards Institute. http://www.ansi.org, 2009. URL http://www.ansi.org.

2, Internet: Health Level Seven. http://www.hl7.org, 2009. URL http://www.hl7.org.

3, Internet: Allgemeine Erklärung der Menschenrechte. http://www.un.org/Depts/german/grunddok/ar217a3.html, 1948. URL http://www.un.org.

4, Internet: Datenschutzrichtlinie 95/46/EG der Europäischen Union. http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-austria_de.pdf, 2004. URL http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-austria_de.pdf.

5, Internet: Inhalte von Arztbriefen. http://www.initiative-elga.at, 2008. URL http://www.initiative-elga.at.

6, Internet: 451. Verordnung: Gesundheitstelematikverordnung (GTelV). http://ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2008_II_451/BGBLA_2008_II_451.html, 2008. URL http://ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2008_II_451/BGBLA_2008_II_451.html.

7, Internet: Electronic Medical Summary. http://www.e-ms.ca, 2009. URL http://www.hl7.org.

American Civil Liberties Unioin: *Toward a New Health Care System: The civil liberties issues in brief.* ACLU Free Reading Room (ISBN 0-914031-24-4), New York, 1994. URL http://www.skepticfiles.org/aclu/health_r.htm.

Barrows, Randolph C. und Clayton, Paul D.: Privacy, Confidentiality, and Electronic Medical Records. In: *Journal of the American Medical Informatics Association*,

Band 13:S. 139–148, 1996. URL http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=116296&blobtype=pdf.

Bilykh, Iryna, Jahnke, Jens H., McCallum, Glen und Price, Morgan: Using the Clinical Document Architecture as Open Data Exchange Format for Interfacing EMRs with Clinical Decision Support Systems. In: *CBMS '06: Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*. IEEE Computer Society, Washington, DC, USA, 2006, S. 855–860. ISBN 0-7695-2517-1. doi: http://dx.doi.org/10.1109/CBMS.2006.166.

Bleumer, G. und Schunter, M.: Privacy Oriented Clearing for the German Health Care System. In: *Personal Information Security, Engineering and Ethics*, S. 175–194, 1997. URL citeseer.ist.psu.edu/bleumer97privacy.html.

Blobel, Bernd: Authorisation and access control for electronic health record systems. In: *International Journal of Medical Informatics*, Band 73:S. 251–257, 2004.

Carter, Meredith: Privacy and Public Confidence in an e-Health Era. In: *Health Issues*, Band 64:S. 12–16, 2000. URL http://www.healthissuescentre.org.au/docs/jacarter64.pdf.

Chen, TS, Liao, BS, Lin, MG und Gough, TG: Security Architecture for HL/7 Message Interchange. In: *MEDINFO 2001*, Band 84:S. 1247–1251, 2001.

Dolin, Robert H., Alschuler, Liora, Beebe, Calvin, Biron, Paul V., Boyer, Sandra Lee, Essin, Daniel, Kimber, Elliot, Lincoln, Tom und Mattison, John E.: The HL7 Clinical Document Architecture. In: *J Am Med Inform Assoc.*, Band 8:S. 552–569, 2001. URL http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=130066.

Dolin, Robert H., Alschuler, Liora, Boyer, Sandy, Beebe, Calvin, Behlen, Fred M., Biron, Paul V. und Shabo, Amnon: HL7 Clinical Document Architecture, Release 2. In: *J Am Med Inform Assoc.*, Band 13, 2006. URL http://www.jamia.org/cgi/reprint/M1888v1.

Eichelberg, Marco, Aden, Thomas, Riesmeier, Jörg, Dogac, Asuman und Laleci, Gokce B.: A survey and analysis of Electronic Healthcare Record standards. In: *ACM Comput. Surv.*, Band 37(4):S. 277–315, 2005. ISSN 0360-0300. doi:http://doi.acm.org/10.1145/1118890.1118891. URL http://portal.acm.org/citation.cfm?id=1118890.1118891.

Elga, Initiative: 2008. URL http://www.initiative-elga.at/.

Eysenbach, Gunther: What is e-health? In: *Journal of Medical Internet Research*, Band 3, 2001. URL `http://www.jmir.org/2001/2/e20/`.

Foundation, California HealthCare: *Medical Privacy and Confidentiality Survey.* California HealthCare Foundation, 1999.

Garfinkel, Simson: *Pgp : Pretty Good Privacy.* O'Reilly, Sebastopol, 1994. ISBN 9781565920989.

Goldman, J: Protecting privacy to improve health care. In: *Health Aff*, Band 17(6):S. 47–60, 1998. doi:10.1377/hlthaff.17.6.47. `http://content.healthaffairs.org/cgi/reprint/17/6/47.pdf`, URL `http://content.healthaffairs.org/cgi/content/abstract/17/6/47`.

Goldman, J., Mulligan, D., for Democracy, Center und Technology: *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality.* Center for Democracy & Technology, 1996.

Goldman, Janlori und Hudson, Zoe: Virtually Exposed: Privacy And E-Health. In: *Health Affairs*, Band 19:S. 140–148, 2000. URL `http://content.healthaffairs.org/cgi/reprint/19/6/140.pdf`.

Head, Brad: What is CDA? In: *Electronic Medical Summary Project - Phase 2*, 2004.

Heitmann, Kai U.: Arztbrief, eRezept - Sciphox Spezifikationen für die Einführung der elektronischen Gesundheitskarte. Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen (KIS), 2006.

Heitmann, Kai U., Kassner, Andreas, Gehlen, Erich, Görke, Hans-Joachim und Heidenreich, Georg: Implementierungsleitfaden Arztbrief auf Basis der HL7 Clinical Document Architecture Release 2 für das deutsche Gesundheitswesen. VHitG, 2006.

IBM und Prenner, Engelbert: *Machbarkeitsstudie betreffend Einfuehrung der elektronischen Gesundheitsakte (ELGA) im österreichischen Gesundheitswesen.* IBM, Bundesgesundheitsagentur, 2006.

Kim, Hwa Sun, Tran, Tung und Cho, Hune: A Clinical Document Architecture (CDA) to Generate Clinical Documents within a Hospital Information System for E-Healthcare Services. In: *CIT '06: Proceedings of the Sixth IEEE International Conference on Computer and Information Technology (CIT'06).* IEEE Computer Society, Washington, DC, USA, 2006, S. 254. ISBN 0-7695-2687-X. doi:http://dx.doi.org/10.1109/CIT.2006.2.

Kotulski, Zbigniew und Zwierko, Aneta: Secure protocol architectures through the concept of pseudonymization. Technischer Bericht, Euro-ngi, 2005. URL `http://eurongi.enst.fr/archive/127/JRA634.pdf`.

Kuhlen, Rainer: *Die Konsequenzen von Informationsassistenten*. Suhrkamp-Verlag, Frankfurt Am Main, 1999. ISBN 3518290436. URL `http://www.inf-wiss.uni-konstanz.de/People/RK/Publikationen1995-2000/informationsassistenten.pdf`.

Marcheschi, P., Mazzarisi, A., Dalmiani, S. und Benassi, A.: New standards for cardiology report and data communication: an experience with HL7 CDA release 2 and EbXML. In: *Computers in Cardiology, 2005*, S. 383–386, 2005. URL `{http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1588117}`.

Pommerening, K., Miller, M., Schmidtmann, I. und Michaelis, J.: Pseudonyms for Cancer Registries. In: *METHODS OF INFORMATION IN MEDICINE*, Band 35:S. 112–121, 1996.

Pommerening, Klaus: Pseudonyme - ein Kompromiss zwischen Anonymisierung und Personenbezug. In: *Medizinische Forschung - Ärztliches Handeln*, S. 329–333, 1995.

Prenner, Engelbert: Standards im österreichischen Gesundheitswesen. BMGFJ - I/A/15 (Gesundheitstelematik), 2007.

Prokosch, Hans Ulrich: KAS, KIS, EKA, EPA, EGA, E-Health: Ein Plädoyer gegen die babylonische Begriffsverwirrung in der Medizinischen Informatik. In: *Informatik, Biometrie und Epidemiologie in Medizin und Biologie*, Band 32:S. 371–382, 2001. URL `http://www.imi.med.uni-erlangen.de/team/download/mis_begriffsdefinitionen.pdf`.

Rachels, James: Why privacy is important. In: , S. 194–201, 1985.

Riedl, B., Grascher, V., Fenz, S. und Neubauer, T.: Pseudonymization for improving the Privacy in E-Health Applications. In: *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, S. 255–255, 2008a. ISSN 1530-1605. doi:10.1109/HICSS.2008.366.

Riedl, B., Grascher, V., Kolb, M. und Neubauer, T.: Economic and Security Aspects of Applying a Threshold Scheme in e-Health. In: *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, S. 39–46, 2008b. doi:10.1109/ARES.2008.175.

Riedl, B., Grascher, V. und Neubauer, T.: Applying a Threshold Scheme to the Pseudonymization of Health Data. In: *Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on*, S. 397–400, 2007a. doi:10.1109/PRDC.2007.24.

Riedl, Bernhard, Grascher, Veronika und Neubauer, Thomas: A Secure e-Health Architecture based on the Appliance of Pseudonymization. In: *JOURNAL OF SOFTWARE*, Band 3(2):S. 23–32, 2008c.

Riedl, Bernhard, Grascher, Veronika und Neubauer, Thomas: Pseudonymization for improving the privacy in e-Health applications. In: *41st Hawaii International Conference on System Sciences*. 2008d.

Riedl, Bernhard, Neubauer, Thomas und Boehm, Oswald: Datenverarbeitungssystem zum Verarbeiten von Objektdaten. In: , 2007b. Austrian-Patent, No. A 503 291 B1, 2007-09-15.

Riedl, Bernhard, Neubauer, Thomas, Goluch, Gernot, Boehm, Oswald, Reinauer, Gert und Krumboeck, Alexander: A secure architecture for the pseudonymization of medical data. In: *Ares 2007*. 2007c.

Schadow, Gunther, Rishel, Wesley J. und Tucker, Mark C.: *Secure HL7 Transactions using Internet Mail*. Health Level Seven, 1999.

Schanner, Alexander, Otter, Heinz, Philippi, Theresa und Hurch, Martin: Die elektronische Gesundheitsakte in Österreich - Ausblick auf die erste Umsetzungsphase. Arbeitsgemeinschaft Elektronische Gesundheitsakte, 2007.

Shamir, Adi: How to Share a Secret. In: *Communications of the ACM*, Band 22:S. 612–613, 1979.

Stolba, Nevena, Banek, Marko und Tjoa, A Min: The Security Issue of Federated Data Warehouses in the Area of Evidence-Based Medicine. In: *ares*, Band 0:S. 329–339, 2006. doi:http://doi.ieeecomputersociety.org/10.1109/ARES.2006.132.

Tanenbaum, Andrew und Van Steen, Maarten: *Distributed Systems: Principles and Paradigms*. Prentice Hall International, Englewood Cliffs, 2007.

U.S. Congress Office of Technology Assessment: *Protecting Privacy in Computerized Medical Information*. OTA-TCT-576. U.S. Government Printing Office, 1993. URL `http://www.mccurley.org/papers/9342.PDF`.

Warren, Samuel D. und Brandeis, Louis D.: The right to privacy. In: *Harvard Law Review*, Band 4:S. 193–220, 1890. URL `http://www.niatec.net/Publications/wyndrose/CASMAT/PRIV/RTPRIV.doc`.

Westin, Alan: *Privacy and freedom*. Atheneum, London, 1968. ISBN 9780370013251. URL `http://meteor.bibvb.ac.at/F?func=find-b&find_code=IDN&local_base=acc01&request=AC01259161`.

Xenitellis, Symeon: *The Open-source PKI Book*. 2000. URL `http://ospkibook.sourceforge.net`.

Yee, George, Korba, Larry und Song, Ronggong: Ensuring Privacy for E-Health Services. In: *ares*, S. 321–328, 2006. doi:http://doi.ieeecomputersociety.org/10.1109/ARES.2006.59.

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

ANHANG A

Arztbrief-XML-Source

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="vhitg-cda-v3.xsl" ?>
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/voc"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:hl7-org:v3 ../schemas/CDA.xsd">
  <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
  <id extension="35" root="1.2.276.0.24.0.5.0.1339551403.3.1.1550751403"
      />
  <code code="34106-5" codeSystem="2.16.840.1.113883.6.1"/>
  <title>Entlassbericht</title>
  <effectiveTime value="20060529153213"/>
  <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
  <languageCode code="de-DE"/>
  <setId extension="35" root="
      1.2.276.0.24.0.5.0.1339551403.3.2.1550751403"/>
  <versionNumber value="1"/>
  <recordTarget>
    <patientRole>
      <id extension="789987" root="1.2.276.0.76.3.1.13.99"/>
      <id extension="M5" root="1.2.276.0.24.0.5.0.1339551403.2.6.1"/>
      <id extension="5" root="
          1.2.276.0.24.0.5.0.1339551403.2.1.1550751403"/>
      <id extension="5" root="1.2.276.0.24.0.5.0.1339551403.2.5.1"/>
      <addr use="HP">
        <streetName>Kölner Wiesenweg</streetName>
        <houseNumber>44</houseNumber>
        <postalCode>52349</postalCode>
        <city>Düren</city>
        <country>Deutschland</country>
      </addr>
      <telecom use="HP" value="tel:+4924212356532"/>
      <patient>
        <name>
          <given>Karl</given>
          <family>Krummbein</family>
        </name>
        <administrativeGenderCode code="M" codeSystem="
            2.16.840.1.113883.5.1"/>
        <birthTime value="19520917"/>
      </patient>
      <providerOrganization>
        <id extension="927834" root="1.2.276.0.76.3.1.13.79"/>
        <name>Medizinische Klinik am Waldpark</name>
        <telecom use="WP" value="tel:+492421435621"/>
        <addr use="WP">
```

```
            <streetName>Roonstraße</streetName>
41          <houseNumber>30</houseNumber>
            <postalCode>52351</postalCode>
43          <city>Düren</city>
            <country>Deutschland</country>
45        </addr>
        </providerOrganization>
47    </patientRole>
    </recordTarget>
49  <author>
      <time value="20060529"/>
51    <assignedAuthor>
        <id extension="MM" root="
            1.2.276.0.24.0.5.0.1339551403.1.6.1550751403"/>
53      <id extension="4533355" root="1.2.276.0.76.3.1.13.89"/>
        <assignedPerson>
55        <name>
            <prefix qualifier="AC">Dr.</prefix>
57          <given>Medina</given>
            <family>Medorn</family>
59        </name>
        </assignedPerson>
61      <representedOrganization>
          <name>Medizinische Klinik am Waldpark</name>
63        <telecom use="WP" value="tel:+492421435621"/>
          <addr use="WP">
65          <streetName>Roonstraße</streetName>
            <houseNumber>30</houseNumber>
67          <postalCode>52351</postalCode>
            <city>Düren</city>
69          <country>Deutschland</country>
          </addr>
71      </representedOrganization>
    </assignedAuthor>
73  </author>
    <custodian>
75    <assignedCustodian>
        <representedCustodianOrganization>
77        <id extension="927834" root="1.2.276.0.76.3.1.13.79"/>
          <name>Medizinische Klinik am Waldpark</name>
79        <telecom use="WP" value="tel:+492421435621"/>
          <addr use="WP">
81          <streetName>Roonstraße</streetName>
            <houseNumber>30</houseNumber>
83          <postalCode>52351</postalCode>
            <city>Düren</city>
85          <country>Deutschland</country>
          </addr>
87      </representedCustodianOrganization>
    </assignedCustodian>
89  </custodian>
    <informationRecipient typeCode="PRCP">
91    <intendedRecipient>
        <id extension="9182736" root="1.2.276.0.76.3.1.13.89"/>
93      <informationRecipient>
          <name>
95          <prefix qualifier="AC">Dr.</prefix>
            <given>Detlef</given>
97          <family>Insulaner</family>
          </name>
99      </informationRecipient>
        <receivedOrganization>
101       <telecom use="WP" value="tel:+49242136318"/>
          <addr use="WP">
103         <streetName>Hauptstr.</streetName>
            <houseNumber>3</houseNumber>
105         <postalCode>52355</postalCode>
            <city>Düren</city>
```

```
107           <country>Deutschland</country>
            </addr>
109       </receivedOrganization>
        </intendedRecipient>
111   </informationRecipient>
      <legalAuthenticator>
        <time value="20060529153202"/>
        <signatureCode code="I"/>
115     <assignedEntity>
          <id extension="MM" root="
              1.2.276.0.24.0.5.0.1339551403.1.6.1550751403"/>
117       <id extension="4533355" root="1.2.276.0.76.3.1.13.89"/>
          <assignedPerson>
119         <name>
              <prefix qualifier="AC">Dr.</prefix>
121           <given>Medina</given>
              <family>Medorn</family>
123         </name>
          </assignedPerson>
125       <representedOrganization>
            <name>Medizinische Klinik am Waldpark</name>
127         <telecom use="WP" value="tel:+492421435621"/>
            <addr use="WP">
129           <streetName>Roonstraße</streetName>
              <houseNumber>30</houseNumber>
131           <postalCode>52351</postalCode>
              <city>Düren</city>
133           <country>Deutschland</country>
            </addr>
135       </representedOrganization>
        </assignedEntity>
137   </legalAuthenticator>
      <component>
139     <structuredBody>
          <component>
141         <section>
              <code code="X-SALUT" codeSystem="2.16.840.1.113883.6.1"/>
143           <text> Sehr geehrte Frau Kollegin, sehr geehrter Herr Kollege,
                    <br/>
                <br/> wir
145                       berichten über unseren Patienten, Karl Krummbein
                              , geboren am 17.09.1952, der
                          sich vom 25.01.2006 bis 17.02.2006 bei uns in
                              stationärer Behandlung befand.
147                   </text>
            </section>
149       </component>
          <component>
151         <!-- Diagnosen, Level 2 -->
            <section>
153           <code code="29308-4" codeSystem="2.16.840.1.113883.6.1"/>
              <title>Codierte Diagnosen</title>
155           <text>
                <table>
157               <thead>
                    <tr>
159                   <th>Diagnose</th>
                      <th>ICD Code</th>
161                   <th>Lokalisation</th>
                      <th>Zusatz</th>
163                 </tr>
                  </thead>
165               <tbody>
                    <tr>
167                   <td>
                        <content ID="diag-D10">Traumatische
169                                     Symphysensprengung</content>
                      </td>
```

```
171                   <td>S33.4</td>
                      <td/>
173                   <td/>
                    </tr>
175                 <tr>
                      <td>
177                     <content ID="diag-D11">Fraktur des Os sacrum</
                            content>
                      </td>
179                   <td>S32.1</td>
                      <td>L</td>
181                   <td/>
                    </tr>
183                 <tr>
                      <td>
185                     <content ID="diag-D12">Nicht näher bezeichnete
                                                Niereninsuffizienz, incl.
                                                    Niereninsuffizienz,
                                                    nicht als
187                                             akut oder chronisch
                                                    bezeichnet, Urämie o.n.A
                                                    .</content>
                      </td>
189                   <td>N19</td>
                      <td/>
191                   <td/>
                    </tr>
193                 <tr>
                      <td>
195                     <content ID="diag-D9">Fraktur: Sonstige und multiple
                                 Teile
                                                des Beckens, incl. Laterale
                                                    Kompressionsfraktur,
197                                             Malgaigne-Fraktur,
                                                    Schmetterlingsbruch,
                                                    Sonstige
                                                komplexe Beckenfrakturen</
                                                    content>
199                   </td>
                      <td>S32.89</td>
201                   <td>L</td>
                      <td/>
203                 </tr>
                  </tbody>
205             </table>
              </text>
207           <entry>
                <!-- codierte Diagnose, Level 3 -->
209             <observation classCode="OBS" moodCode="EVN">
                  <code code="29308-4" codeSystem="2.16.840.1.113883.6.1"/>
211               <statusCode code="completed"/>
                  <effectiveTime>
213                 <low value="200605031557"/>
                  </effectiveTime>
215               <value code="S33.4" codeSystem="1.2.276.0.76.5.311"
                        codeSystemName="icd10gm2006" xsi:type="CD">
                    <originalText>
217                   <reference value="#diag-D10"/>
                    </originalText>
219               </value>
                </observation>
221           </entry>
              <entry>
223             <!-- codierte Diagnose, Level 3 -->
                <observation classCode="OBS" moodCode="EVN">
225               <code code="29308-4" codeSystem="2.16.840.1.113883.6.1"/>
                  <statusCode code="completed"/>
227               <effectiveTime>
```

```
                    <low value="200605031557"/>
229               </effectiveTime>
                  <value code="S32.1" codeSystem="1.2.276.0.76.5.311"
                      codeSystemName="icd10gm2006" xsi:type="CD">
231                 <originalText>
                      <reference value="#diag-D11"/>
233                 </originalText>
                  </value>
235               <targetSiteCode code="L" codeSystem="
                      2.16.840.1.113883.3.7.1.7"/>
                </observation>
237           </entry>
              <entry>
239             <!-- codierte Diagnose, Level 3 -->
                <observation classCode="OBS" moodCode="EVN">
241               <code code="29308-4" codeSystem="2.16.840.1.113883.6.1"/>
                  <statusCode code="completed"/>
243               <effectiveTime>
                    <low value="200605031557"/>
245               </effectiveTime>
                  <value code="N19" codeSystem="1.2.276.0.76.5.311"
                      codeSystemName="icd10gm2006" xsi:type="CD">
247                 <originalText>
                      <reference value="#diag-D12"/>
249                 </originalText>
                  </value>
251             </observation>
              </entry>
253           <entry>
                <!-- codierte Diagnose, Level 3 -->
255             <observation classCode="OBS" moodCode="EVN">
                  <code code="29308-4" codeSystem="2.16.840.1.113883.6.1"/>
257               <statusCode code="completed"/>
                  <effectiveTime>
259                 <low value="200605031556"/>
                  </effectiveTime>
261               <value code="S32.89" codeSystem="1.2.276.0.76.5.311"
                      codeSystemName="icd10gm2006" xsi:type="CD">
                    <originalText>
263                   <reference value="#diag-D9"/>
                    </originalText>
265               </value>
                  <targetSiteCode code="L" codeSystem="
                      2.16.840.1.113883.3.7.1.7"/>
267             </observation>
              </entry>
269         </section>
          </component>
271       <component>
            <!-- Prozeduren, Level 2 -->
273         <section>
              <code code="X-PROC" codeSystem="2.16.840.1.113883.6.1"/>
275           <title>Codierte Maßnahmen</title>
              <text>
277             <table>
                  <thead>
279                 <tr>
                      <th>Datum</th>
281                   <th>Maßnahme</th>
                      <th>OPS Code</th>
283                 </tr>
                  </thead>
285               <tbody>
                    <tr>
287                   <td>30.01.2006</td>
                      <td>
289                     <content ID="proc-P5">Offene Reposition einer
                            Beckenrand-
```

```
                                                  und Beckenringfraktur: Durch
                                                       Platte, vorderer
291                                             Beckenring</content>
                    </td>
293                 <td>5-798.4</td>
                  </tr>
295               <tr>
                    <td>25.01.2006</td>
297                 <td>
                      <content ID="proc-P6">Computertomographie des
                          Abdomens mit
299                                             Kontrastmittel</content>
                    </td>
301                 <td>3-225</td>
                  </tr>
303             </tbody>
              </table>
305         </text>
          </section>
307     </component>
        <component>
309       <section>
            <code code="10164-2" codeSystem="2.16.840.1.113883.6.1"/>
311         <title>Anamnese vom 25.01.2006</title>
            <text> Laut Aussage des Patienten bei Aufnahme sei er am
                19.01.2006 von seinem
313                     eigenen Trecker auf Beckhöhe überrollt worden.
                            Herr Krummbein arbeitete
                        zunächst wie gewohnt weiter und stellte sich
                            erst heute wegen
315                     persistierender Schmerzen und Schwellung beider
                            Beine bei seinem Hausarzt
                        Herrn Dr. Merz vor. Dieser überwies Herrn
                            Krummbein in die Notfallambulanz
317                     des Kreiskrankenhauses Düren. Nach
                            intensivmedizinischer Überwachung in der
                        Nacht wurde der Patient unfallchirurgisch
                            versorgt. </text>
319       </section>
        </component>
321     <component>
          <section>
323         <code code="8648-8" codeSystem="2.16.840.1.113883.6.1"/>
            <title>Therapie und Verlauf vom 17.02.2006</title>
325         <text> Bei der Aufnahme fand sich ein ca. 20 x 20 cm großes
                Hämatom am linken
                        Unterbauch und in der Nähe des Beckenkamms. Es
                            fiel eine deutlich ödematöse
327                     Schwellung beider Beine li &gt; re auf. Außerdem
                             konnte ein
                        Beckenkompressionsschmerz bei instabilem Becken
                            ausgelöst werden. Die
329                     periphere Durchblutung, Motorik und Sensibilität
                             waren intakt. <br/>
              <br/>
331                     Aufgrund steigender Kreatinin-Werte wurde
                            zunächst ein Abdomen CT mit
                        Kontrastmittel veranlasst. Hier zeigte sich eine
                             ausbleibende Anreicherung
333                     der linken Niere. Die Kollegen der urologischen
                            Klinik legten daraufhin am
                        25.01.2006 einen Double-J-Katheter und empfahlen
                             einen Farbduplex der
335                     Nierenarterie sowie eine retrograde Darstellung
                            der ableitenden Harnwege im
                        Verlauf des stationären Aufenthaltes. <br/>
337           <br/> Am 30.01.2006 wurde die
```

```
                            offene Reposition der Beckenrand- und
                                Beckenringfraktur mit Platte vorderer
339                         Beckenring durchgeführt. Die Drainagen konnten
                                zeitgerecht entfernt werden.
                            Die Wundheilung erfolgte primär. Die FKDS und
                                IVP zeigten eine wieder
341                         regelrechte Perfusion und Ausscheidung der
                                linken Niere. <br/>Die
                            Mobilisation erfolgte über das linke Bein,
                                verzögerte sich jedoch aufgrund
343                         orthostatischer Dysregulation und mangelnder
                                Compliance des Patienten.
                            Intermittierend berichtete Herr Krummbein über
                                pseudoradikuläre Parästhesien
345                         des rechten Beines. Unter Neurotin-Medikation
                                bildeten sich diese jedoch
                            vollständig zurück. <br/>
347               <br/> Augrund des wiederholten Bakteriennachweises
                            im Urin wird eine Antibiotikatherapie mit
                                Tavanic 500 veranlasst. <br/>Am
349                         18-02-2006 kann wir Herrn Krummbein bei
                                allgemeinem Wohlbefinden in die
                            stationäre Rehabilitationseinrichtung nach
                                Nümbrecht verlegt werden. Zu
351                         diesem Zeitpunkt sind die Wundverhältnisse
                                reizlos und die
                            Entzündungslaborparameter liegen im Normbereich.
353                             <br/>
                  <br/>Pelvis<renderMultiMedia referencedObject="EXD9001_17"/>
355             </text>
                <entry>
357               <observationMedia ID="EXD9001_17" classCode="OBS" moodCode="
                      EVN">
                    <id extension="9001_17" root="
                        1.2.276.0.24.0.5.0.1339551403.4.3.1550751403"/>
359                 <value mediaType="image/jpeg" xsi:type="ED">
                      <reference value="9001_17.JPG"/>
361                 </value>
                  </observationMedia>
363             </entry>
              </section>
365         </component>
            <component>
367           <section>
                <code code="18776-5" codeSystem="2.16.840.1.113883.6.1"/>
369             <title>Procedere vom 17.02.2006</title>
                <text> bitte vervollständigen </text>
371           </section>
            </component>
373         <component>
              <section>
375             <code code="18776-5" codeSystem="2.16.840.1.113883.6.1"/>
                <title>Procedere vom 29.05.2006</title>
377             <text> Wir bitten um regelmäßige Wund- und Befundkontrollen
                    sowie die
                            Fortführung der Thromboseprophylaxe bis zur
                                Vollbelastung unter
379                         entsprechender Laborkontrolle. Des Weiteren
                                empfehlen wir eine
                            Röntgenkontrolle der osteosynthetisch versorgten
                                 vorderen Beckenringfraktur
381                         zur Stellungs- und Durchbauungskontrolle nach
                                Beendigung der stationären
                            Reha. Zusätzlich sollte antibiotische Therapie
                                für insgesamt 5 Tage
383                         fortgeführt werden. <br/>
                  <br/> Bei Beschwerdepersistenz sollte die
```

```
385                         Wiedervorstellung in der Urologie bei liegendem
                                Double-J erfolgen. Der
                            Double-J-Katheter soll auf Anraten der Urologen
                                3 Wochen nach Entlassung
387                         entfernt werden. </text>
          </section>
389       </component>
          <component>
391         <section>
              <code code="10183-2" codeSystem="2.16.840.1.113883.6.1"/>
393           <title>Medikation</title>
              <text> Pantozol 20 mg Tabletten; Dosis: 1-0-0 <br/>Voltaren
                  Resinat Kps.; Dosis:
395                         1-0-1 <br/>Bifiteral sirup 500ml Fla.; Dosis:
                                1-0-0 <br/>Tavanic 500 mg
                            Tbl.; Dosis: 1-0-0 für 5 Tage <br/>Clexane-40
                                0.4 ml Fertigspritze </text>
397         </section>
          </component>
399     </structuredBody>
      </component>
401 </ClinicalDocument>
```

Listing A.1: Source eines Arztbriefs