Schreier G, Hayn D, Ammenwerth E (Hrsg.). Tagungsband der eHealth2010: Health Informatics meets eHealth. 6.-7. Mai 2010, Wien. OCG Books Nr. 264. Österreichische Computer Gesellschaft. 2010

ENTWURF EINES ELEKTRONISCHEN EINWILLIGUNGSMANAGEMENTS FÜR EIN INTERSEKTORALES INFORMATIONSSYSTEM

Birkle M[1], Heinze O[1], Bergh B[1]

Kurzfassung

Der Trend im Gesundheitswesen geht im Rahmen der integrierten Versorgung immer mehr zu intersektoralen Informationssystemen. Die unterschiedlichsten gesetzlichen Bestimmungen in Deutschland stellen hohe Anforderungen an die Datenverarbeitung in solchen Systemen. Zur Achtung der Patientenrechte ist unter anderem die Implementierung eines Einwilligungsmanagements für den elektronischen, intersektoralen Datenaustausch unerlässlich. Dieser Artikel beschreibt ein dezentrales und ein zentrales Konzept für ein Einwilligungsmanagement für intersektorale Informationssysteme und geht auf die jeweiligen Vor- und Nachteile ein.

Abstract

Current healthcare trends, especially influenced by integrated care, are moving towards Personal and Electronic Health Record systems. In this context the main legal requirement in Germany is to implement an opt-in approach to consider the so called informed consent and to take patients rights into account. This article describes the concept of a technical solution for an opt-in consent management, both a centralized and a decentralized approach and discusses its advantages and disadvantages.

Keywords – informed consent, privacy, consent management, PEHR, IHE BPPC

1. Einleitung

Im Rahmen der integrierten Versorgung werden immer mehr Patienten gemeinschaftlich von verschiedenen Versorgungseinrichtungen wie niedergelassenen Ärzten, Krankenhäusern, Rehabilitationskliniken und Laboren stationär, ambulant oder aber auch in der häuslichen Umgebung kooperativ versorgt. Integrierte Versorgungsformen erfordern neue IT-Systeme, damit die neu entstandenen Prozesse in der Patientenversorgung optimal unterstützt werden können. Um die bestehenden Primärsysteme wie Krankenhausinformationssysteme (KIS) oder Praxisverwaltungssysteme (PVS) zu unterstützen, werden seit mehreren Jahren weltweit Projekte ins Leben gerufen, die entweder arztgeführte sogenannte einrichtungsübergreifende elektronische Patientenakten (eEPA) oder patientengeführte elektronische Gesundheitsakten (eGA) aufbauen, um zu versuchen, die neuen Anforderungen an Versorgungsszenarien abzubilden. Auch in Deutschland gibt es mehrere Projekte, die

[1]Zentrum für Informations- und Medizintechnik, Universitätsklinikum Heidelberg

sich diesem Thema widmen [2, 5, 6]. So wird z.B. für die Metropolregion Rhein-Neckar im Rahmen des Projektes intersektorales Informationssystem (ISIS) [6] am Universitätsklinikum Heidelberg eine persönliche einrichtungsübergreifende elektronische Patientenakte (PEPA) aufgebaut. Die PEPA basiert auf aktuellen Standards wie HL7, DICOM und IHE Profilen und gewährleistet so die Kompatibilität und Interoperabilität mit heutigen und zukünftigen Systemen. Neben den funktionalen Anforderungen sind auch die Anforderungen durch die deutsche Gesetzgebung zu beachten. Jeder Patient in Deutschland muss der elektronischen Verarbeitung seiner Daten in Informationssystemen durch das so genannte opt-in-Verfahren explizit zustimmen [8]. Im Falle der einrichtungsübergreifenden Kommunikation reicht eine Einwilligung im Rahmen des Behandlungsvertrages nicht aus. Der Gesetzgeber in Deutschland fordert eine gesonderte, adäquate Aufklärung des Patienten, damit seine Einwilligung rechtswirksam ist, der sogenannte Informed Consent [1]. Liegt dieser nicht vor, dürfen Daten aus den Primärsystemen wie KIS und PVS nicht an andere, intersektorale Systeme, übermittelt werden.

Bisher befassten sich bereits einige nationale und internationale Autoren mit der Problematik der Datenschutzkonzeption bzw. des Einwilligungsmanagements für elektronische Patientenakten.Caumanns beschreibt in [3] ein übergreifendes Sicherheitskonzept im Rahmen des Projekts elektronische Fallakte. Aber auch im internationalen Bereich beschreiben Coiera et.al [4] den Entwurf und die Implementierung von allgemeinen Einwilligungsmanagementmechanismen in elektronischen Umgebungen (sog. e-Consent). Aber auch Arbeitsgruppen wie das OASIS eXtensible Access Control Markup Language (XACML) Technical Committee befassen sich mit der Problematik des Einwilligungsmanagments [10]. Namli beschreibt in [9] erste Implementierungserfahrungen mit dem IHE BPPC Profil.

Die zurzeit am Markt befindlichen Systeme bieten bisher keine Module für ein Einwilligungsmanagement, um einen Informed Consent zu verwalten und elektronisch zu speichern. Einzig die Standardisierungsinitiative Integrating the Healthcare Enterprise (IHE) hat mit dem Basic Patient Privacy Consent (BPPC) [7] ein Profil entwickelt, das sich dieser Problematik annimmt. Ziel war es daher, eine möglichst auf Standards basierende technische Lösung für ein Einwilligungsmanagement zu finden. Dieser Artikel beschreibt die beiden gefundenen Lösungsansätze.

2. Methoden

Auf Grundlage des Datenschutzkonzeptes der PEPA des ISIS Projekts, der gefundenen Literatur und unter Berücksichtigung internationaler Standards wie HL7 und dem Integrating the Healthcare Enterprise (IHE) Profil Basic Patient Privacy Consent (BPPC) [7] wurde ein Lösungsansatz für das Einwilligungsmanagement und die Verwaltung des Informed Conest entworfen. Das IHE BPPC Profil lehnt sich an den ISO Standard 22600 – Health Informatics / Privilege Management And Access Control an, fordert jedoch nicht explizit dessen Umsetzung. Eine Implementierung dieses Profils erlaubt die Bereitstellung vordefinierter Einwilligungserklärungen die auf vordefinierten Zugriffs- bzw. Vertraulichkeitsstufen für Dokumente basieren.

Zur konkreten Entwicklung eines Lösungsansatzes wurde als Grundlage Aufbau und Struktur eines idealen Einwilligungsmanagement definiert. Anschließend wurde versucht, sich diesem Idealmodell in einer realen Implementierung auf Basis aktuell verfügbarer Standards zu nähern.

3. Ergebnisse

An das Einwilligungsmanagement für die PEPA werden einige grundlegende Anforderungen gestellt. So muss es sich nahtlos in die bestehende Systemarchitektur der PEPA einfügen und dabei die gesetzlichen Vorgaben erfüllen. Außerdem sollte es die Möglichkeit bieten, dass Patienten den Zugriff auf ihre Daten bis auf eine sehr niedrige Akteur- und Dokumentenebene regeln können. Die Analyse der Literatur und der Standards ergab, dass sich dies mit heutigen Mitteln nicht realisieren lässt. So lassen sich Einwilligungen lediglich bis auf die Ebene von Einrichtungen realisieren, nicht aber auf Akteurs- oder gar Dokumentenebene. Um ein solches Einwilligungsmanagement technisch umzusetzen gibt es zwei Möglichkeiten: Zum einen kann das Einwilligungsmanagement *dezentral*, zum anderen *zentral realisiert* werden. Bei der *dezentralen Lösung* werden die für das Einwilligungsmanagement nötigen Komponenten in den jeweiligen Primärsystemen (z.B. KIS, PVS, usw.) integriert. Das heißt jedes Primärsystem verwaltet für sich, ob ein Patient die Einwilligung in einen Datenaustausch mit der PEPA erteilt hat oder nicht. Nur wenn diese Einwilligung vorliegt, übermittelt das Primärsystem die entsprechenden Daten an die PEPA. Außerdem darf das Primärsystem nur bei vorliegen einer Einwilligung die Möglichkeit zum Aufruf der PEPA bieten. Die zweite Möglichkeit der Realisierung des Einwilligungsmanagement stellt die *zentrale Lösung* dar. Hierbei wird die Einwilligung des Patienten durch einen zentralen sogenannten Autorisierungsmanager verwaltet. Jedes an der PEPA beteiligte System muss bei dieser Form der Realisierung vor einer

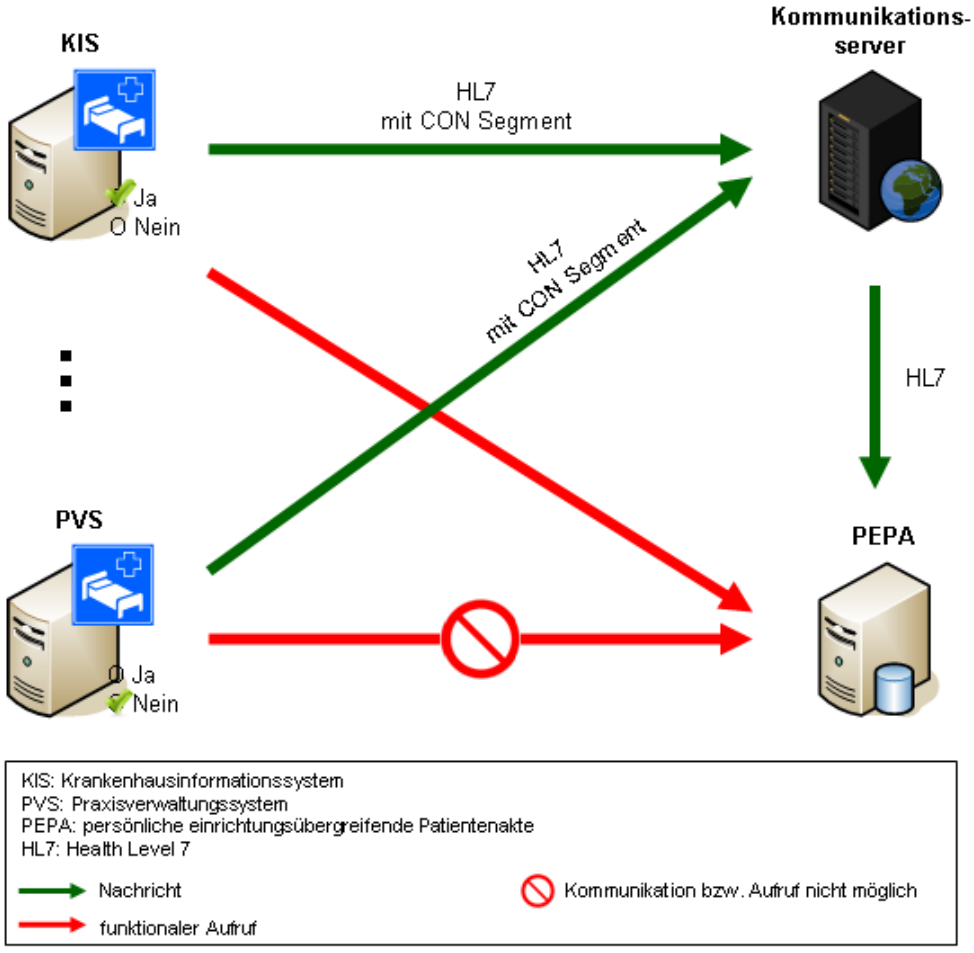

Abbildung 1: Nachrichtenfluss bei dezentraler Lösung

Transaktion beim zentralen Autorisierungsmanager anfragen, ob eine Einwilligung des Patienten vorliegt. Erst wenn der Autorisierungsmanager die Transaktion frei gibt, dürfen z.B. patientenbezogene Daten von einem Primärsystem in die PEPA übermittelt werden.

3. 1. Technische Umsetzung dezentrale Lösung

Innerhalb eines KIS kann die technische Umsetzung des dezentralen Einwilligungsmanagements wie folgt gelöst werden: Der Patientendatensatz erhält ein zusätzliches Flag. Dieses sogenannte Consent Flag wird gesetzt wenn der Patient im Sinne eines Informed Consents eine Einwilligungserklärung unterzeichnet hat. Zusätzlich zum Flag werden das Datum, die aufklärende Person und ein optionales Kommentarfeld gespeichert und Änderungen in einer History hinterlegt. Alle patientenbezogenen HL7-Nachrichten innerhalb des KIS werden um das optionale HL7 Consent Segment (CON) ergänzt. Ein Kommunikationsserver kann nun anhand dieses Segments innerhalb der übermittelten HL7-Nachrichten erkennen, ob der Patient eine Einwilligung erteilt hat oder nicht. Nur wenn dies der Fall ist, werden die Daten an die PEPA übermittelt. *Abbildung 1* stellt beispielhaft den Nachrichtenfluss bei dezentraler Lösung der Einwilligungsmanagement-Problematik dar.

3. 2. Technische Umsetzung zentrale Lösung

Der Autorisierungsmanager wird als weitere eigenständige Komponente innerhalb der Gesamtsys-

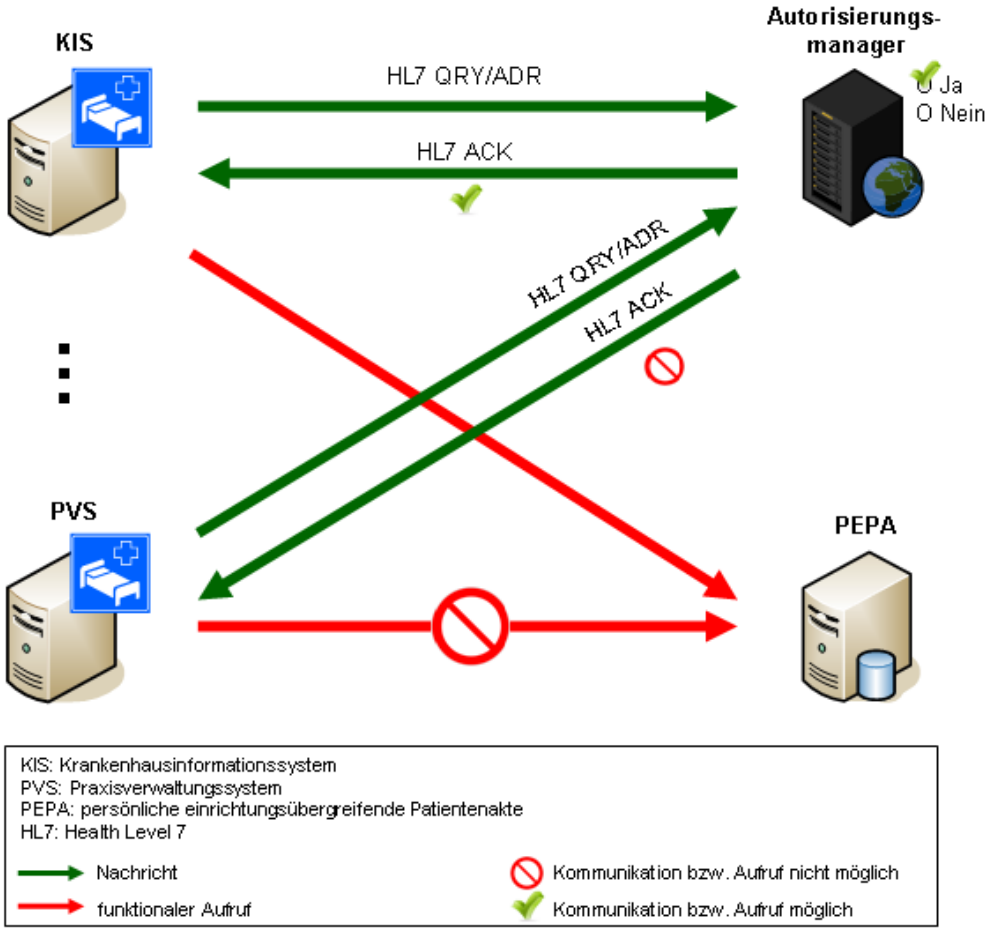

Abbildung 2: Nachrichtenfluss bei zentraler Lösung

temarchitektur implementiert und stellt mehrere Dienste zur Verfügung. Zum einen eine Schnittstelle mit der für einen bestimmten Patient hinterlegt werden kann, für welche Einrichtungen er eine Einwilligung für den Datenaustausch mit der PEPA erteilt hat. Zum Anderen kann jedes Primärsystem anfragen, ob ein bestimmter Patient eingewilligt hat, dass Daten mit der PEPA ausgetauscht werden dürfen. Praktisch sieht dies wie folgt aus: Im Vorfeld der Behandlung eines Patienten wird dieser über die Einwilligung in den Datenaustausch mit der PEPA aufgeklärt. Mit einem Consent Creator wird eine für den Patienten individualisierte Einwilligungserklärung erstellt. Der Consent Creator erfüllt hierbei zwei Aufgaben. Zum Einen erzeugt er eine Einwilligungserklärung in Schriftform, die dem Patient zur Unterschrift vorgelegt wird. Diese wird im weiteren Verlauf auf herkömmlichem Wege archiviert. Parallel hierzu parametriert er den Autorisierungsmanager mit den Einwilligungsinformationen für diesen Patienten. Dies kann zum Beispiel über eine entsprechende HL7-Nachricht geschehen. Werden nun in einem mit der PEPA verbundenen Primärsystem Daten zu diesem Patienten erzeugt, fragt das Primärsystem beim Autorisierungsmanager mittels entsprechender HL7-Query, z.B. Patient Query QRY/ADR an, ob der Patient in den Datenaustausch durch diese System eingewilligt hat. Je nach dem ob der Patient in den Datenaustausch eingewilligt hat oder nicht, sendet der Autorisierungsmanager eine positive oder negative Antwort an das Primärsystem (z.B. HL7-General Acknowledgement ACK). Bei einer entsprechenden positiven Antwort übermittelt das Primärsystem die Daten an die PEPA. Auch das Anfragen von Daten erfolgt auf die gleiche Weise. Nach einer Anfrage durch ein Primärsystem fragt die PEPA beim Autorisierungsmanager an, ob das anfragende Primärsystem berechtigt ist, Daten zu erhalten. Ist dies der Fall, bekommt es die angeforderten Daten angezeigt, andernfalls nicht. *Abbildung 2* stellt beispielhaft den Nachrichtenfluss bei zentraler Lösung der Einwilligungsmanagement-Problematik dar.

Zurzeit wird im Rahmen des ISIS-Projektes die dezentrale Lösung verwendet, da diese in ersten Piloten auf Grund der überschaubaren Zahl von beteiligten Primärsystemen schneller umzusetzen ist. Eine schnelle Umsetzung kann allerdings nur erreicht werden, da im Universitätsklinikum Heidelberg entsprechendes Know-how zur Anpassung des KIS so wie des Kommunikationsservers vorhanden ist. Für die Zukunft wird jedoch an der Umsetzung der zentralen Lösung gearbeitet.

4. Diskussion

Ein Einwilligungsmanagement für eine PEPA wie sie innerhalb des ISIS-Projekts realisiert wird, bietet dem Patienten idealer Weise, unabhängig ob eine dezentrale oder zentrale Realisierung erfolgt, die Möglichkeit den Zugriff auf seine Daten bis auf eine sehr niedrige Akteur- und Dokumentenebene regeln zu können. Nach einer ausgiebigen Literaturrecherche muss man jedoch feststellen, dass sich mit heutigen Mitteln Einwilligungen lediglich bis auf Einrichtungsebene, nicht aber auf Akteurs- oder gar Dokumentenebene realisieren lassen. Das wünschenswerte Idealmodell das ein sehr feingranulares Einwilligungskonzept vorsieht wird durch ein implementierbares Realmodell ersetzt. Diese sieht eine Einwilligung des Patienten in den Austausch seiner Daten auf Einrichtungsebene vor. Die konkrete Realisierung dieses Modells kann entweder dezentral aber auch zentral erfolgen. Sowohl die dezentrale als auch die zentrale Realisierung des Einwilligungsmanagements haben Vor- und Nachteile. Bei einer dezentralen Realisierung des Einwilligungsmanagements entstehen keine weiteren Systemkomponenten, die gepflegt werden müssen. Die Nachrichtenkommunikation mit der PEPA bleibt schlank. Nachteilig ist hierbei jedoch, dass ein erheblicher Implementierungsaufwand in den Primärsystemen entsteht. Zum Teil besteht auch gar nicht die Möglichkeit, schnell Implementierungen in Primärsystemen (z.B. PVS) durchzuführen. Durch eine zentrale Realisierung des Einwilligungsmanagements entsteht dieser Implementierungsaufwand

einmalig an zentraler Stelle. Die Primärsysteme können mittels HL7-Nachrichten mit dem Autorisierungsmanager kommunizieren und erhalten die Autorisierungsmeldungen ebenfalls als HL7-Nachrichten zurück. Der Traffic durch die zahlreichen Nachrichteninteraktionen ist jedoch nicht zu unterschätzen. Erste Tests müssen zeigen, ob der Autorisierungsmanager zu einem Flaschenhals werden kann.

Aus praktischen Überlegungen heraus ist vor allem auf längere Sicht die zentrale Lösung zu bevorzugen. Es ist davon auszugehen, dass das Netz des ISIS-Projektes ständigen Fluktuationen unterworfen ist. Das heißt es nehmen neue Einrichtungen an der PEPA teil oder beenden ihre Teilnahme und Verlassen das Netzwerk. Nur die zentrale Lösung erlaubt es das Einwilligungsmanagement für eine PEPA mit fluktuierend anzubindenden Primärsystemen mit vertretbarem Aufwand sicher zu stellen. Bei Änderungen der Systemlandschaft sind nur am Autorisierungsmanager Änderungen durchzuführen und die bisher angeschlossenen Primärsysteme bleiben davon unbehelligt. Auch der Implementierungsaufwand bei neu anzuschließenden Primärsystemen hält sich bei einer zentralen Lösung des Einwilligungsmanagements in Grenzen. Da die Kommunikation der Einwilligungen bei der zentralen Lösung komplett auf Basis von HL7-Nachrichten durchgeführt wird müssen lediglich die Nachrichtenschnittstellen der Primärsysteme entsprechend parametriert werden. Eine direkte Implementierung von Funktonalitäten im Primärsystem ist bei diesem Lösungsansatz in der Regel nicht erforderlich.

Vergleicht man die beiden Lösungsansätze hinsichtlich des Grades der Standardisierung, so kann man sagen, dass die zentrale Lösung standardisierter ist, als die dezentrale. Dies ist der Fall, da nach unserer Ansicht direkte Implementierungen in Primärsystemen immer propriätere Ansätze darstellen, auch wenn für die Implementierung Standards wie XAML eingesetzt werden. Nur bei einer zentralen Lösung des Einwilligungsmanagemtens ist sichergestellt, das der komplette Themenbereich des Einwilligungsmanagement mit einheitlichen Standards implementiert wurde. So kann die Kommunikation der Einwilligungserklärungen auf Basis von HL7-Nachrichten erfolgen und Aufbau bzw. Struktur der Einwilligungserklärungen orientieren sich an aktuellen Standards bzw. Profielen wie dem IHE BPPC Profil.

Dennoch besteht gerade im verwendeten IHE BPPC Profil noch viel Spielraum für Ergänzungen und Erweiterungen, insbesondere im Bezug auf die Umsetzung des Idealmodells. Die Problematik des BPPC Profils besteht darin, dass es auf bereits vordefinierten Zugriffs- bzw. Vertraulichkeitsstufen für Dokumente und darauf basierenden vordefinierten Einwilligungserklärungen basierte. Eine dynamische Realisierung eines Einwilligungsmanagements, das heißt es kann für jeden Patienten eine individuelle Einwilligungserklärung erstellt werden, ist somit nicht möglich.

5. Literatur

[1] ATKINS, J., Private and Public Protection: Civil Mental Health Legislation, Dunedin Academic Press Ltd., Edinburg 2006

[2] CAUMANNS, J, et.al., Elektronische FallAkten zur sicheren einrichtungsübergreifenden Kooperation, in Bundesamt für Sicherheit in der Informationstechnik: Innovationsmotor IT-Sicherheit. Tagungsband zum 10. Deutschen IT-Sicherheitskongress, 22.-24. Mai 2007, S.153-172, SecuMedia Verlag, Gau-Algesheim 2007

[3] CAUMANNS, J., Übergreifendes Sicherheitskonzept für Umsetzung und Betrieb elektronischer Fallakten, Dokument-ID: eFA-SiKo-1.2, Frauenhofer ISST, 2008

[4] COIERA, E., et.al., The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment, DOI: 10.1197/jamia.M1480, Mar–Apr; 11(2): 129–140, J Am Med Inform Assoc. 2004
[5] HAAS, P., Elektronische Patientenakte, Ein Projekt der Landesregierung Nordrhein-Westfalen gemeinsam mit Projektpartner aus Industrie und Selbstverwaltung, Projektleitpapier und Meilenstein 1.0 zur MEDIACA 2006, Nordrhein-Westfalen 2006

[6] HEINZE, O., et.al., Aufbau einer einrichtungsübergreifenden Patientenakte in der Rhein-Neckar-Region, in S. Schug und U. Engelmann (Hrsg.), Telemed 2008 Proceedings, Berlin 2008

[7] IHE INTERNATIONAL, IT Infrastructure (ITI) Technical Framework, Volume 1, Integration Profiles, Kap. 19 Basic Patient Privacy Consent Integration Profile, 2009

[8] MEIER, A., Der rechtliche Schutz patientenbezogener Gesundheitsdaten, in: Münsteraner Reihe 84, Verlag für Versicherungswirtschaft, Karlsruhe 2003

[9] NAMLI, T., et.al., Implementation Experiences on IHE XUA and BPPC, Middle East Technical University, Ankara 2006

[10] OASIS XACML TC, Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0, 2008

Corresponding Author
Markus Birkle
Center for Information Technology and Med. Engineering (ZIM), University Hospital Heidelberg
Tiergartenstraße 15, D-69121 Heidelberg
Email: markus.birkle@med.uni-heidelberg.de