

Entwicklung eines elektronischen Einwilligungsmanagementsystems für intersektorale Informationssysteme

Development of a consent management system for inter-sectoral information systems

Markus Birkle^{a,1}, Oliver Heinze^a, Björn Bergh^a

^a*Universitätsklinikum Heidelberg, Zentrum für Informations- und Medizintechnik*

Zusammenfassung. 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. Prinzipiell gibt es zwei grundlegende Ansätze ein Einwilligungsmanagement für ein intersektorales Informationssystem zu implementieren. Zum einen kann man das Einwilligungsmanagement dezentral, zum anderen zentral umsetzen. Dieser Artikel stellt beide Konzepte kurz vor und beschreibt, warum letztlich nur das zentrale Konzept zur Umsetzung auf lange Sicht in Frage kommt.

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. Basically there are two possibilities to implement a consent management. It can be implemented in a centralized or decentralized approach. This article shortly describes the concept of a centralized and a decentralized consent management approach and discusses whether in long terms only the centralized approach should be implemented.

Keywords. Electronic Health Record, Patient Data Privacy, Confidentiality, Informed Consent, eHealth

¹ Corresponding Author

Einleitung

Seit einigen Jahren gibt es im Gesundheitswesen einen grundlegenden Wandel in der Struktur der Patientenversorgung. Früher war der komplette Prozess der Patientenbehandlung einrichtungszentriert organisiert. Bei der Entwicklung dieser Prozesse und der dafür notwendigen Informatikinfrastruktur ging man davon aus, dass ein Patient von der ersten Diagnose bis zur definitiven Heilung einer Erkrankung zum überwiegenden Teil in ein und derselben Gesundheitseinrichtung behandelt wird. Dieser einrichtungszentrierte Ansatz bricht in den letzten Jahren immer mehr auf. Nicht zuletzt auf Grund des immer größer werdenden Kostendrucks im Gesundheitswesen, aber auch vor dem Hintergrund der starken Spezialisierung einzelner Gesundheitseinrichtungen, werden im Rahmen integrierter Versorgungsszenarien immer mehr Patienten gemeinschaftlich von verschiedenen Versorgungseinrichtungen stationär, ambulant oder auch in der häuslichen Umgebung kooperativ versorgt. Um bestehende Primärsysteme wie Krankenhaus-informationssysteme (KIS) oder Praxisverwaltungssysteme (PVS) zu unterstützen, werden seit mehreren Jahren weltweit Projekte ins Leben gerufen, die entweder arztgeführte sogenannte einrichtungübergreifende elektronische Patientenakten (eEPA) oder patientengeführte elektronische Gesundheitsakten (eGA) aufbauen [1, 2, 3]. Hierdurch wird versucht die neuen Anforderungen an die Versorgungsszenarien mit einer neuen und geeigneten Informatikinfrastruktur abzubilden.

Auch das Universitätsklinikum Heidelberg ist seit Jahren damit beschäftigt, die Prozesse der integrierten Versorgung technisch abzubilden. Hierzu wird im Rahmen des Projektes „Intersektorales Informationssystem (ISIS)“ eine persönliche einrichtungübergreifende elektronische Patientenakte (PEPA) aufgebaut [4]. 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. In Deutschland muss jeder Bürger der elektronischen Verarbeitung seiner Daten in Informationssystemen durch das so genannte opt-in-Verfahren explizit zustimmen [5]. Im Falle der einrichtungübergreifenden 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, den sogenannten Informed Consent [6]. Liegt dieser nicht vor, dürfen Daten aus den Primärsystemen wie KIS und PVS nicht an andere, z.B. intersektorale Systeme, übermittelt werden.

Grundlegende Voraussetzung für den rechtssicheren Betrieb eines intersektoralen Informationssystems ist aus diesem Grund die Verwaltung der Patientenaufklärung und Einwilligung, also des Informed Consents. Bei Entwurf und Entwicklung eines solchen Einwilligungsmanagementsystems müssen bereits vorhandene Standards und Profile (z.B. HL7 CDA, IHE Profile) beachtet werden. Außerdem können durch den Einsatz geeigneter Open Source Technologien hohe Lizenzkosten vermieden werden.

1. Material und Methoden

Auf Grundlage des Datenschutzkonzeptes des ISIS Projekts, der gefundenen Literatur [7, 8, 9, 10] und unter Berücksichtigung internationaler Standards wie HL7 [11] und

dem Integrating the Healthcare Enterprise (IHE) [12] Profil Basic Patient Privacy Consent (BPPC) [13] wurden verschiedene Lösungsansätze für das Einwilligungsmanagement und die Verwaltung des Informed Consents entworfen.

2. Ergebnisse

Es gibt prinzipiell zwei technische Realisierungsvarianten für ein Einwilligungsmanagement: Zum einen die dezentrale, zum anderen die zentrale Realisierung. Bei der dezentralen Realisierung (Abbildung 1) werden die für das Einwilligungsmanagement nötigen Funktionen und Komponenten in den jeweiligen Primärsystemen (z.B. KIS, PVS, usw.) integriert.

Bei der zentralen Realisierung (Abbildung 2) werden die benötigten Funktionen und Komponenten durch eine entsprechende zentrale Komponente, den Consent Manager, zur Verfügung gestellt.

2.1. Konzept dezentrales Einwilligungsmanagement

Die dezentrale Umsetzung des Einwilligungsmanagements erfordert eine Implementierung direkt in den Primärsystemen, da die Einwilligung direkt dort gespeichert wird. Das heißt, sie müssen so erweitert werden, dass sie in der Lage sind, Einwilligungen zu einem Patienten zu speichern und HL7 Nachrichten entsprechend mit einem Consent (CON) Segment zu versehen. Jedes Primärsystem kann somit für sich erkennen, ob der Patient eine Einwilligung erteilt hat, dass Daten aus diesem System zum Beispiel an eine PEPA übermittelt werden dürfen. Das Primärsystem fügt jeder seiner HL7 Nachrichten das CON Segment an. Da alle Primärsysteme in der Regel über einen Kommunikationsserver miteinander verbunden sind, kann dieser anhand des CON-Segments entscheiden, ob und zu welchem System Daten übertragen werden dürfen oder nicht (vgl. Abbildung 1).

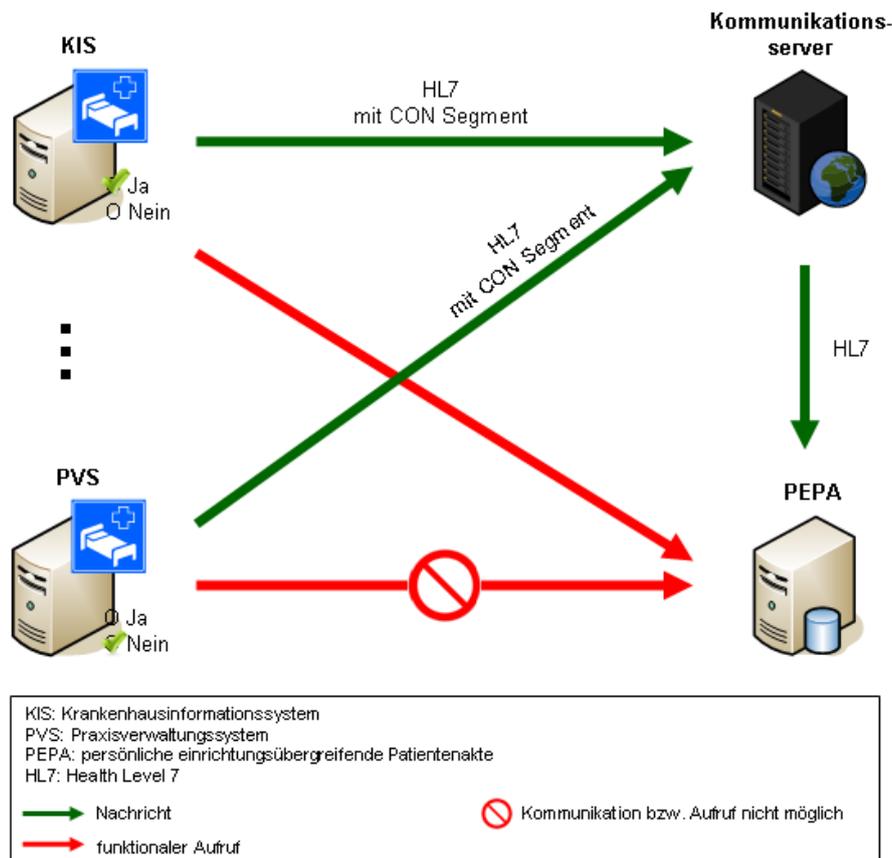


Abbildung 1. Lokalisation der funktionalen Komponenten und Nachrichtenfluss bei dezentraler Realisierung des Einwilligungsmanagements.

2.2. Konzept zentrales Einwilligungsmanagement

Beim zentralen Ansatz wird die Einwilligung in einem sogenannten Consent Manager gespeichert. Jedes Primärsystem muss vor einer Transaktion mit einer HL7-Query (z.B. Patient Query QRY/ADR) beim Consent Manager anfragen, ob der betreffende Patient eingewilligt hat, dass diese Transaktion ausgeführt wird. Je nachdem, ob der Patient in den Datenaustausch eingewilligt hat oder nicht, sendet der Consent Manager eine positive oder negative Antwort an das Primärsystem (z.B. HL7-General Acknowledgement ACK).

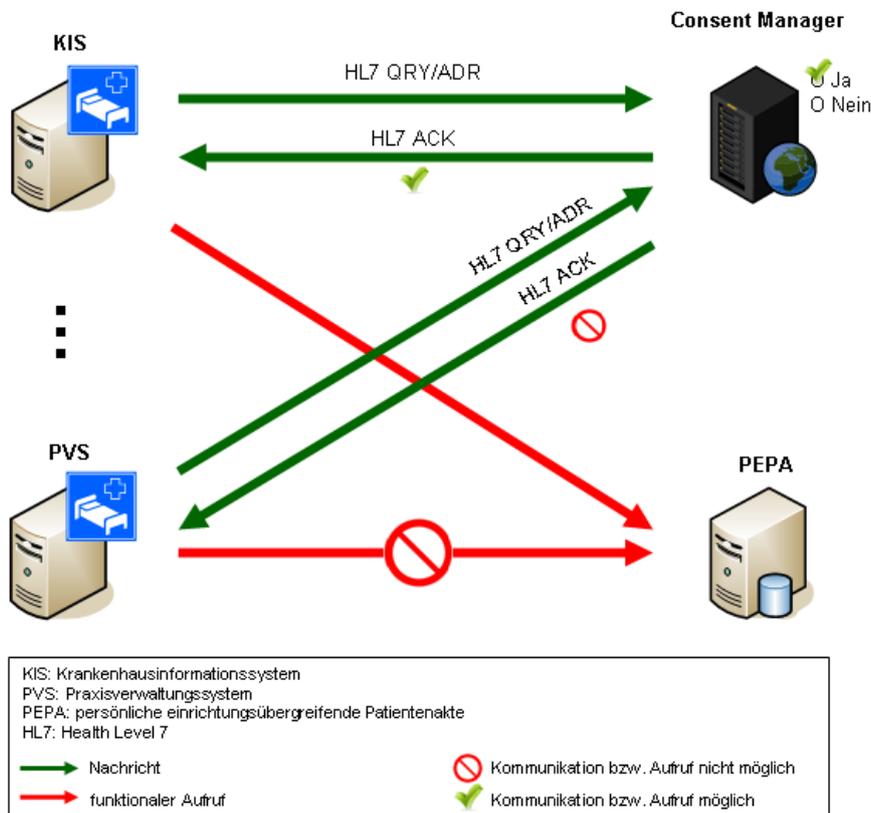


Abbildung 2. Lokalisation der funktionalen Komponenten und Nachrichtenfluss bei zentraler Realisierung des Einwilligungsmanagements.

Alle Komponenten des Einwilligungsmanagements werden idealerweise serviceorientiert unter der Nutzung von Open Source Technologien implementiert. Dadurch sind sie auf lange Sicht flexibel genug, um in einer komplexen Gesundheits-IT-Infrastruktur, wie sie zum Beispiel für regionale Gesundheitsnetzwerke benötigt wird, genutzt zu werden.

Innerhalb des Einwilligungsmanagements sind mehrere Komponenten notwendig. Zum einen eine Komponente zum Erstellen und Bearbeiten von Einwilligungserklärungen, diese Funktionalitäten bieten die Primärsysteme ebenfalls nicht. Zum anderen eine Komponente, den Consent Manager, zum Verwalten und Abfragen von Einwilligungen.

Der Consent Manager verfügt über geeignete HL7-Schnittstellen, um Einwilligungen zu empfangen und zu speichern und um diese Informationen auf geeignete Weise wieder abzufragen. Das Empfangen von Einwilligungen kann zum Beispiel mittels HL7-MDM-Nachrichten erfolgen. Hierzu werden Einwilligungserklärungen zum Beispiel in strukturierter Form als CDA-Dokument erstellt und mittels einer HL7-MDM-Nachricht an den Consent Manager übermittelt. Dieser speichert dann das CDA-Dokument und extrahiert die entsprechenden Einwilligungsinformationen aus diesem. Anfragen an den Consent-Manager können

über HL7-Query-Meldungen, zum Beispiel über die HL7-Patient-Query QRY/ADR gestellt werden. Dieser antwortet dann auf die Anfrage mit einer entsprechenden HL7-General-Acknowledgement-ACK-Nachricht.

3. Diskussion / Ausblick

Bei vielen Primärsystemen und Kommunikationsservern sind die Möglichkeiten zur Implementierung der Anforderungen eines dezentralen Einwilligungsmanagements sehr beschränkt. Sind diese jedoch gegeben, lässt sich ein dezentrales Einwilligungsmanagement schnell realisieren, wie zurzeit in Heidelberg im Rahmen des ISIS-Projektes praktiziert.

Bei der zentralen Umsetzung des Einwilligungsmanagements wird ein Consent-Manager als weitere eigenständige Komponente innerhalb der Gesamtsystemarchitektur implementiert. Er stellt alle Funktionen bzw. Dienste zur Verfügung, um Einwilligungen zu verwalten. Dadurch können beliebige Systeme, zum Beispiel über eine SOAP-Schnittstelle bei Implementierung als Web-Service, auf den Consent Manager zurückgreifen. Durch die zentrale Implementierung des Einwilligungsmanagements steigt zwar die Komplexität des Gesamtsystems, es ist jedoch weit flexibler als die dezentrale Umsetzung. Gerade in einem Gesundheitsnetzwerk kann es vorkommen, dass Primärsysteme hinzukommen oder aus dem System entfernt werden.

Auf lange Sicht erscheint aus den gerade beschriebenen Gründen nur die Implementierung eines zentralen Einwilligungsmanagements sinnvoll. Nur diese Lösung bietet die notwendige Flexibilität, um den kommenden Anforderungen an eine komplexe Gesundheits-IT-Infrastruktur gewachsen zu sein.

Eine noch nicht abschließend geklärte Frage stellt die Tatsache dar, dass der Consent-Manager als zentrale Komponente starken Belastungen ausgesetzt ist. Innerhalb des ISIS Projekts zum Beispiel fragt jedes Primärsystem vor einer Transaktion an, ob eine Einwilligung des Patienten vorliegt. Bei der als hoch zu erwartenden Anzahl von Anfragen ist es für die Funktion des Gesamtsystems entscheidend, dass der Consent-Manager stabil läuft. Fällt er aus, können die Primärsysteme keine Transaktionen mehr ausführen, da ohne eine positive Einwilligungsantwort keine Transaktionen ausgeführt werden dürfen. Auf Grund der sehr schlanken Architektur des Dienstes werden allerdings diesbezüglich keine Probleme erwartet. Letzte Klarheit werden erste Pilottests bringen.

Referenzen

- [1] Arbeitsgemeinschaft Elektronische Gesundheitsakte, *Die elektronische Gesundheitsakte in Österreich*, Wien, 2007.
- [2] J. Caumanns, et.al., Elektronische FallAkten zur sicheren einrichtungübergreifenden Kooperation, in Bundesamt für Sicherheit in der Informationstechnik: Innovationsmotor IT-Sicherheit. Tagungsband zum 10. Deutschen IT-Sicherheitskongress, 22.-24. Mai 2007, SecuMedia Verlag, Gau-Algesheim 2007, 153-172.
- [3] 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.
- [4] Heinze O, Brandner A, Bergh B (2009). Establishing a personal electronic health record in the Rhine-Neckar region. *Stud Health Technol Inform*, 150, 119.

- [5] MEIER, A., Der rechtliche Schutz patientenbezogener Gesundheitsdaten, in: Münsteraner Reihe 84, Verlag für Versicherungswirtschaft, Karlsruhe 2003.
- [6] ATKINS, J., Private and Public Protection: Civil Mental Health Legislation, Dunedin Academic Press Ltd., Edinburg 2006.
- [7] J. Caumanns., Übergreifendes Sicherheitskonzept für Umsetzung und Betrieb elektronischer Fallakten, Dokument-ID: eFA-SiKo-1.2, Fraunhofer ISST, 2008.
- [8] E. Coiera., 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.
- [9] OASIS XACML TC, Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0, 2008.
- [10] T. Namli, et.al., Implementation Experiences on IHE XUA and BPPC, Middle East Technical University, Ankara 2006.
- [11] HL7 Beutzergruppe Deutschland e.V.: <http://www.hl7.de/standard/standards.php> (Zuletzt besucht am 12.08.2010).
- [12] IHE Integrating The Healthcare Enterprise: <http://www.ihe.net/> (Zuletzt besucht am 12.08.2010)
- [13] IHE International, IT Infrastructure (ITI) Technical Framework, Volume 1, Integration Profiles, Kap. 19 Basic Patient Privacy Consent Integration Profile, 2009