

«Federated Identity Management»

Optimaler Datenschutz und Datennutzung im Gesundheitswesen

Traditionell werden Patientendaten im Gesundheitswesen lokal verwaltet. Der Patient wandert durch das Gesundheitssystem, doch seine Daten verbleiben an den einzelnen Stationen – beim Arzt, im Spital oder anderswo. Heute treten deshalb Probleme zu Tage, die ein Zusammenwirken der Anbieter im Gesundheitswesen stark erschweren. Aus technischer Sicht geht es dabei meist um das Thema der Interoperabilität, also um die technischen und organisatorischen Voraussetzungen für eine Vernetzung für Datenübertragung und Datennutzung über Systemgrenzen hinweg. Im Vergleich zu anderen Wirtschaftsbereichen wie Produktion, Handel und Bankwesen, in denen es wohlgerne nicht um die Gesundheit und das Leben von Menschen geht, sind im Gesundheitswesen die Voraussetzungen für eine Interoperabilität noch kaum vorhanden.

Text: Hellmuth Broda, Liberty Alliance und Sun Microsystems, Inc.

Anforderungen im Gesundheitswesen

Speziell im Gesundheitswesen bestehen noch nie da gewesene Anforderungen an die Verfügbarkeit und die Sicherheit für die Informationsübertragung quer durch die unterschiedlichsten Organisationen. Ein modernes Gesundheitsnetz muss so aufgebaut sein, dass die Berechtigten leichten Zugang zu den relevanten Informationen haben. Beispielsweise sollte der Arzt, der ein neues Medikament verschreiben will, die gesamte Patientengeschichte und das Krankheitsbild einsehen und überprüfen können. Nur so ist er in der Lage, mögliche Nebenwirkungen, Unverträglichkeiten, Allergien und Interaktionen mit anderen Medikamenten auszuschliessen, bevor er das Rezept ausstellt. In den USA fordern die in HIPAA [1] niedergelegten Grundsätze bereits seit über zehn Jahren Nachverfolgbarkeit und umfassenden Datenschutz der Patientendaten.

Sicherer und einfacher Zugang zum Notfallausweis

Trotz allen Schutzes von Daten und Privatsphäre müssen bei einem Ereignis wichtige Gesundheitsdaten für die Notfallmedizin umgehend zur Verfügung stehen, damit das Leben des Patienten gerettet werden kann. International werden dazu heute unterschiedliche Ansätze verfolgt, von der Gesundheitskarte (s. Diskussion in Deutschland) bis hin zu Web-basierten Lösungen, wie sie heute in den USA und in Dänemark schon angeboten werden.[2] Im Zusammenhang mit der grösseren Mobilität ist es zwingend, dass solche Systeme international interoperabel werden.

«Federated Identity» im Alltag

Bankkarten

Als Anfang der 80-er Jahre Bankkarten für Geldautomaten eingeführt wurden, funktionierten diese nur bei der eigenen Bank. Es dauerte einige Jahre, bis solche Karten auch bei anderen Geldinstituten funktionierten. Damals trug man noch eine Liste der Banken bei sich, an denen die eigene Karte funktionierte. Heute kann man sich weitgehend darauf verlassen, dass die Cirrus- oder Maestro-Karten an den Bankautomaten weltweit funktionieren. Die Banken entwickelten einen technischen und Vertrags-Standard zur Abwicklung von Geschäften an Bankautomaten, über den die weltweite Zusammenarbeit und Übermittlung erst möglich wurde.

Mobiltelefonie

Die Möglichkeit des Roamings, also der Nutzung des eigenen Mobiltelefons in einem fremden Land, ist heute bereits Gewohnheit. Dies wird durch Standards und entsprechende standardisierte Abläufe geregelt. Der eigene Apparat meldet sich mit Provider-ID und SIM-ID bei einem Netzanbieter im Aufenthaltsbereich an. Dieser stellt danach eine Verbindung zum Heimatprovider her und schaltet das Handy frei, sobald der Heimatprovider die Kostenübernahme garantiert hat. Der lokale Provider weiss vom Nutzer nur die erwähnten Nummern. Er kennt weder den Namen, noch andere persönliche Daten des Nutzers.

Es bedarf eines nationalen und internationalen Standards für Interoperabilität im Gesundheitswesen

Der Aufbau eines gemeinsamen Standards für die Interoperabilität zwischen allen Dienstleistenden des Gesundheitswesens – Versicherungen, Apotheken, Spitalverwaltungen und letztlich auch den Patienten – würde die sichere, verzögerungsfreie gemeinsame Nutzung ermöglichen. Solch ein Standard muss auch die Frage des Verfallsdatums von Patienteninformationen sowie deren Verweildauer bei Dienstleistern klären. Er würde helfen, die persönlichen Daten zu schützen, organisatorische Abläufe zu vereinfachen, die Leistung des Gesamtsystems zu erhöhen und einen Beitrag zur Kostensenkung im Gesundheitswesen zu leisten.

Identitätsmanagement ist der Schlüssel

Ein für die Vernetzung von EDV-Systemen im Rahmen der Interoperabilität notwendiger gemeinsam genutzter Dienst (z. B. im Rahmen einer Service Oriented Architecture (SOA) der Bereichsinformatik) ist das Identitätsmanagement, welches das sichere Anmelden von Benutzern und den Zugriff auf Daten in ihren verschiedenen Rollen ermöglicht. Leider sind solche Systeme heute noch mehrheitlich proprietär und lokal implementiert. Sie lassen sich somit nicht ohne Weiteres mit anderen ähnlichen Identitätsmanagements-Anwendungen zusammenbringen. Man spricht hier von den Identitäts-Silos, die dazu führen, dass jeder Anwender sich bei allen involvierten Systemen separat anmelden muss. Die Zutrittsrechte auf den jeweiligen Systemen müssen so unabhängig vergeben und verwaltet werden, was einen erheblichen administrativen Aufwand erfordert und auch unter dem Gesichtspunkt der Sicherheit ein potentielles Problem darstellt. Dies erschwert den effizienten Einsatz von modernen Informations- und Kommunikationstechnologien erheblich und steht möglichen Einsparungen im Gesundheitswesen im Wege.

Die Rolle von «Federated Identity»

Im Mittelpunkt der Anstrengungen hin zu einem gemeinsamen Standard in Bezug auf die Interoperabilität steht das Konzept der Federated Identity (föderierte Identität), was dem Identitätsmanagement in einem Netz unterschiedlicher Partner entspricht. Federated Identity hilft aber nicht nur beim Aufbau eines virtuellen Netzes von Organisationen. Es ermöglicht den beteiligten Teilnehmern durch Authentifizierung auch die übergreifende Anmeldung (Single Sign-On).

Die Liberty Alliance

In anderen Wirtschaftsbereichen existierten ebensolche Herausforderungen – speziell beim Thema Identitätsmanagement. Im Jahr 2001 hat sich eine internationale Gruppe von Firmen, Institutionen, Forschungsinstituten und Regierungsbehörden zusammengefunden. Einer Initiative von Sun Microsystems folgend gründeten sie die Liberty-Allianz (<http://www.project-liberty.org>). Ziel der Liberty-Allianz ist es, einen Standard zu schaffen, der genau diese Interoperabilität zwischen unterschiedlichen Systemen ermöglicht. Die Liberty Allianz besteht heute aus ca. 190 Mitgliedern. [3]

Über eine Milliarde Identitäten werden heute weltweit unter den Liberty-Standards verwaltet. Die in diesem Zusammenhang erarbeiteten Standards lassen sich 1:1 im Gesundheitswesen einsetzen und ermöglichen die reibungslose Zusammenarbeit aller Mitwirkenden bei gleichzeitiger Einhaltung von Datenschutz und Privatsphäre.

In einer Special Interest Group der Allianz (eHealth-SIG) werden die speziellen Anforderungen aus dem Gesundheitssektor von Mitgliedern der Allianz und interessierten Teilen der Öffentlichkeit (Verbände, Verwaltungen und Dienstleistern) abgeglichen und finden in die Spezifikationen der Allianz Eingang. Und nur Standards machen eHealth für alle am Gesundheitsnetz Beteiligten sicher.

Datenschutz und Elektronische Patientenakte

Die Amerikaner sind uns auf dem Gebiet der elektronischen Patientenakte etwas voraus [4]. Gesetze und Vorschriften wie der Health Information Privacy Protection Act (HIPPA) und die Bestimmungen zum elektronischen Patientendossier lassen sich praktisch nur mit Identity- und Privacy-Management einhalten.

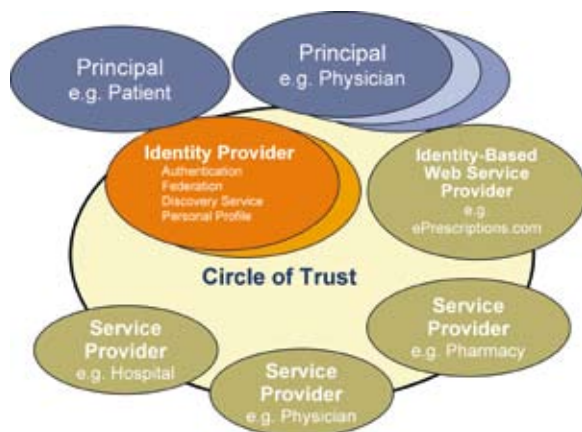
Die Markle Foundation [5] veröffentlichte 2005 Richtlinien für Systeme, welche Informationen übertragen und fordert für solche:

1. Offenheit und Transparenz
2. Zweckbindung und Minimalisierung
3. Beschränkung der Datensammlung
4. Nutzungsbindung
5. Nutzerbasierte Selbstbestimmung (Dateneignerschaft) und Kontrolle
6. Datenintegrität und -qualität
7. Sicherheitsvorkehrungen und -kontrollen
8. Rechenschaftspflicht und Aufsicht
9. Rechtsmittel

Die von der Liberty Allianz entwickelten Standards ermöglichen die Einhaltung solcher Regeln. ▶

Circle of Trust im Alltag

Ein solcher Zirkel des Vertrauens lässt sich gut mit der Situation an einer Messe vergleichen. Beim Eintritt wird man genau überprüft. Sobald man jedoch im Ausstellungsbereich drin ist, ist die Bewegungsfreiheit gross. Man kann sich mit den Anbietern austauschen, Verhandlungen führen und Geschäftsabschlüsse tätigen. Oft hat man hierzu ein Token (Messeausweis) mit RFID oder Barcode erhalten. Dieser Ausweis lässt sich an den einzelnen Ständen für die persönliche Identifikation einsetzen.



Beispiel eines Circles of Trust im Gesundheitswesen. Der Eintritt in den Circle kann situationsabhängig auch über unterschiedliche Identity Provider im Circle of Trust (z.B. Krankenkasse, Klinik, Apothekerverband) erfolgen.

«Les Chevaliers de la table ronde» – das «Circle of Trust»-Konzept

Arbeiten mehrere Partner in einem Identity-Rahmenwerk (technischer und vertraglicher Natur) zusammen, so spricht man von einem Circle of Trust. In solch einem Circle of Trust wird man sich als Nutzer typischerweise bei einem Identity Provider anmelden. Von diesem wird man dann mit sogenannten Security Assertions (Security Assertion Markup Language, SAML ein OASIS-Standard [6]) mit den jeweiligen Partnern im Circle of Trust weiterverbunden.

Im Gesundheitswesen ermöglichen die Konstrukte Federated Identity Management und Circle of Trust eine äusserst flexible Umgebung. Sie erteilen, situationsabhängig und entsprechend den Rollen der Einzelnen, die unterschiedliche Zugriffsrechte. Auch der Schutz der persönlichen Daten lässt sich damit optimal und über die unterschiedlichen Dienstleistungsanbieter und -bezügler hinweg organisieren. Die Liberty-Allianz hat die Übereinstimmung für solche Circles of Trust mit geltendem EU-Recht bestätigt [7] und veröffentlichte dieser Tage entsprechende Muster-Rahmenverträge. [8]

Einsatz von Liberty-Standards heute

Zahlreiche Organisationen weltweit setzen Liberty-Standards heute bereits im Gesundheitswesen ein. Eine Übersicht über aktuelle Implementierungen findet sich auf der Webseite <http://www.projectliberty.org/index.php/liberty/adoption/healthcare>. Unter all den dort genannten Beispielen sei auch auf MedCommons und den Free Emergency Public Health Record hingewiesen (s. Fussnote 2). Ein Beitritt zur Allianz und die Mitarbeit in den entsprechenden Gremien empfiehlt sich für alle Beteiligten (Krankenhäuser, Apothekerverbände, Ärzteschaft, Lösungsanbieter etc.). Weitere Informationen gibt es auf der Webseite der Allianz unter <http://www.projectliberty.org>, Links auf entsprechende Dokumente finden sich auf der Seite http://www.projectliberty.org/liberty/resource_center und speziell zum Thema Gesundheitswesen unter http://www.projectliberty.org/index.php/liberty/strategic_initiatives/healthcare.

Der föderalistische Ansatz der Liberty-Allianz passt nach Ansicht des Autors sehr gut zu unserem föderalen System in der Schweiz und macht mancherorts geplante hierarchische und monolithische Ansätze für Identifikationen und Zusammenarbeit im Gesundheitswesen überflüssig. Lassen Sie uns gemeinsam über den Gartenhag schauen und das übernehmen, was sich anderswo bereits bestens bewährt – zum Nutzen der Patienten, zum Wohl Aller, bei gleichzeitiger Eindämmung der Kosten. ■

1. Health Insurance Portability and Accountability Act of 1996 (<http://aspe.hhs.gov/admsimp/pl104191.htm>)
2. USA: Free Emergency Personal Health Record von MedCommons, (<http://news.biohealthmatics.com/PressReleases/2006/02/13/000000004341.aspx>), Dänemark: www.sundhed.dk
3. Für eine aktuelle Liste der Mitglieder s. http://www.projectliberty.org/index.php/liberty/membership/current_members
4. Dies gilt in weiten Bereichen von eHealth. S. hierzu: <http://www.revolutionhealth.com/>
5. Markle Foundation (2005). Framework for CFH Prototype Policy Subcommittee Documents. New York. http://www.phrconference.org/assets/consumer_principles_101105.pdf
6. Organization for the Advancement of Structured Information Standards
7. http://www.projectliberty.org/liberty/news_events/press_releases/liberty_alliance_outlines_legal_framework_for_circles_of_trust_to_comply_with_european_union_data_protection_and_privacy_laws
8. http://www.projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust

Dr. rer. nat. Hellmuth Broda

ist Sprecher der Liberty-Allianz (www.projectliberty.org) und Distinguished Director und Chief Technology Officer, Global Government Strategy bei Sun Microsystems, Inc. (www.sun.com). Er ist Einzelmitglied der Schweizerischen Akademie der Technischen Wissenschaften SATW (www.satw.ch) und dort Vizepräsident des Wissenschaftlichen Beirats und Mitglied der ICT-Kommission. Er dient als Mitglied des Fachbeirats von swissITmedical.net.