Nr. 29/2011 · 25.10.2011

Jahrgang 2011 · ISSN 1616-8909

HL7-Mitteilungen

Offizielle Mitteilung der HL7-Benutzergruppen in Deutschland · Österreich · Schweiz · Luxemburg

CTS2 in Theorie und Praxis

Konzept der eHealth-Plattform für Luxemburg

Security- und Privacy-Standards

HL7-Benutzergruppen
Deutschland · Österreich
Schweiz · Luxemburg

Fachbeiträge

Aus den Ländern

Ankündigungen

HL7-Infobroschüre verfügbar

Ab sofort können Sie unsere HL7-Infobroschüre bestellen. Sie informiert kurz und bündig über HL7 als Kommunikationsstandard für das Gesundheitswesen, HL7-Version 2.x, HL7-Version 3, Dokumente im Gesundheitswesen, über weitere HL7-Standards in Auszügen und beleuchtet schließlich neuere Entwicklungen, Kooperationen sowie Terminologien. Dazu werden die Merkmale und Ziele von HL7 und die HL7-Benutzergruppe in Deutschland e. V. genauer beschrieben.

Die Infobroschüre kann bei der Geschäftsstelle angefordert werden und ist für Mitglieder von HL7 Deutschland, Österreich, der Schweiz oder Luxemburg kostenfrei (ein Exemplar).

Impressum

Vorsitzender

PD Dr. Bernd Blobel (Regensburg)

E-Mail: bernd.blobel@klinik.uni-regensburg.de

1. Stellvertretender Vorsitzender

Dr. Kai U. Heitmann (Köln)

E-Mail: hl7@kheitmann.de

2. Stellvertretender Vorsitzender

Thomas Norgall (Erlangen)

E-Mail: nor@iis.fraunhofer.de

Herausgeber
HL7-Benutzergruppe Deutschland e. V.
Bernd Blobel (Regensburg)
V.i.S.d.P.

Postanschrift
HL7-Benutzergruppe in Deutschland e. V.
An der Schanz 1
50735 Köln
Telefon: (0700) 7777-6767
Telefax: (0700) 7777-6761
E-Mail: info@hl7.de
Internet: www.hl7.de

Redaktion
Dr. Kai U. Heitmann
HL7-Benutzergruppe in Deutschland e. V.
An der Schanz 1
50735 Köln

Referent für Öffentlichkeitsarbeit
Karl-Heinz Gobrecht
Health-Comm GmbH
Dachauer Str. 11
80335 München

Textbeiträge in dieser Ausgabe
Dr. Udo Altmann, Dr. Stefan Benzschawel, Priv.-Doz. Dr. Bernd Blobel, Prof. Dr. Peter Haas, Dr. Georg Heidenreich, Dr. Kai Heitmann, Alexander Mense, Robert Mützner, Thomas Norgall, Dr. Frank Oemig, Dr. Stefan Sabutsch, Tony Schaller, Bernd Schütze, Dr. Peter Seifter, Thomas Wälti

Fotos
Fotolia.com © Yvann K, Mihai-Bogdan Lazar, babimu), Butch, Andrey Kuzmin, Xuejun li.
Dank an Stefan Benzschawel.

Layout, Satz und Druck
LUP AG
Filzengraben 15–17
50676 Köln

Verlag und Vertrieb
Eigenverlag und Eigenvertrieb

Auflage
800 Stück

Erscheinungsweise
etwa viermonatlich

Manuskripte
Senden Sie Zuschriften direkt an die Redaktion. Für unverlangt eingesendete Beiträge gehen wir keine Verpflichtung zur Veröffentlichung ein und wird keine Haftung übernommen. Die Redaktion behält sich vor, aus technischen Gründen Kürzungen oder Veränderungen vorzunehmen. Namentlich gekennzeichnete Beiträge geben die Meinung der Verfasser wieder.

Anzeigen
Anfragen nach Anzeigen für Produkte und Dienstleistungen sowie Stellenanzeigen richten Sie bitte an die Redaktion. Es gilt die Preisliste vom 17.07.2007.

Inhaltsverzeichnis

Offizielle Mitteilung der HL7-Benutzergruppen in Deutschland · Österreich · Schweiz · Luxemburg

Fachbeiträge

Aus den Ländern

Ankündigungen/Bekanntmachungen

Rubriken

Richtigstellung Ausgabe 28/2011

Der Autor des Artikels in unseren Mitteilungen 28/2011 über ProRec Austria auf Seite 29 ist nicht Stefan Sabutsch, sondern Dr. Alexander Hörbst.

Exclusiv für Mitglieder: unsere HL7-Standard-DVD

Die HL7-Standard-DVD 10/2010 enthält die Originale der HL7-Standards und andere HL7-Dokumente sowie die bisher von der HL7-Benutzergruppe erstellten (und in der Regel abgestimmten) Implementierungsleitfäden und weiter gehende Informationen.

Als Mitglied der HL7-Benutzergruppe in Deutschland e. V. erhalten Sie diese DVD auf Anfrage einfach und kostenlos.

Faxen Sie uns das Anforderungs-Formular (downloadbar auf hl7.de) ausgefüllt zurück oder senden Sie es an die Geschäftsstelle.

Thomas Norgall

Zum Verständnis des scheinbar Selbstverständlichen…

…möchten wir mit dieser Ausgabe der HL7-Mitteilungen beitragen. Deshalb behandeln wir in diesem Heft die Grundlagen für die Bereitstellung all jener Dienste und Funktionen, welche die Akteure eines modernen Gesundheitswesens im Alltag unter Wahrung von Datenschutz und Sicherheit unterstützen, informieren, verbinden und integrieren. Dass solche „unsichtbaren" Infrastrukturen und erst recht die ihnen zugrundeliegenden Standards angemessener Wahrnehmung und Würdigung durch ihre Nutzer meist entgehen, liegt in der Natur der Sache und des Menschen – Motivation genug, einmal „hinter die Kulissen" zu blicken.

Um die für medizinische Behandlung und Forschung, Prozessgestaltung und Abrechnung erforderlichen Informationen und Daten einrichtungsübergreifend systematisch und sicher erfassen, handhaben und nutzen zu können, ist ein Netz von Datenbanken, Servern, Registern etc. erforderlich. Durchgängige Basisdienste und Strukturen sind für die Kommunikation und Kooperation erforderlich, die auf übergreifenden Festlegungen beruhen. Solche Festlegungen können zwar prinzipiell durch die beteiligten Akteure auf Projektebene, in Fachgesellschaften, Industrieverbänden, Selbstverwaltung etc. vereinbart werden, zumindest für organisations- und hersteller-übergreifende, flächendeckende, oft auch internationale Anwendung unabdingbar ist jedoch die Orientierung an übergreifenden Standards. Dass selbst die Durchsetzung international anerkannter Normen in der Praxis häufig nur bei flankierender Rahmensetzung durch die Politik gelingt, sei hier nur am Rande erwähnt.

Funktion und Effizienz, Nutzbarkeit und Akzeptanz von Infrastrukturen sind stets direkt abhängig von der Qualität der zugrunde liegenden Festlegungen, Standards bzw. Normen. Keine Organisation kann das gesamte Spektrum relevanter Domänen und Betrachtungsebenen alleine abdecken. Die Entwicklung von Nachrichtenaustausch zum umfassenden Interoperabilitätsparadigma steigert jedoch die Bedeutung der Zusammenarbeit von HL7 mit anderen Normungs- bzw. Standardisierungsorganisationen wie ISO, CEN, IHTSDO, WHO etc. Dementsprechend bilden Standards von HL7 und anderen Organisationen die Basis einer wachsenden Zahl nationaler und internationaler Infrastrukturprojekte und -plattformen.

Einige Beispiele aus Deutschland, Luxemburg und der Schweiz werden Sie auf den folgenden Seiten kennenlernen. Weitere Einblicke liefern unsere Website, die Mitarbeit in unseren Technischen Komitees und das Interoperabilitätsforum – oder der Besuch unserer bevorstehenden Jahrestagung in Göttingen. Ich freue mich darauf, Sie dort zu begrüßen!

Thomas Norgall
2. Stellv. Vorsitzender HL7 Deutschland

▶ Thomas Norgall

Standardisierungs-experten auf der conhIT in Berlin

Die HL7-Benutzergruppe in Deutschland ist auch im nächsten Jahr auf der conhIT vom **24. bis 26. April 2012 in Berlin** mit einem Stand vertreten. Merken Sie sich diesen Termin schon einmal vor.

Wir informieren über Themen wie CDA (standardisierte Dokumente), HL7-Version 3, HL7 v2 sowie Semantik und Terminologien, beleuchten praxisbezogene Aspekte wie Geräteeinbindung und -kommunikation, Behandlung von Pharmazieprodukten, HL7-Version 3 im Routineeinsatz in Deutschland usw.

Termine

Treffen des Interoperabilitätsforums
Das Interoperabilitätsforum wurde gemeinsam von der HL7-Benutzergruppe in Deutschland (den technischen Komitees), IHE Deutschland sowie der AG Interoperabilität des VHitG und dem Fachbereich Medizinische Informatik des DIN initiiert. Auf diesen Treffen werden Fragen und Probleme der Interoperabilität in der Kommunikation zwischen verschiedenen Anwendungen vorgestellt, Lösungsansätze dafür eruiert und darauf aufbauend entsprechende Aktivitäten festgelegt. Die Punkte werden themenweise besprochen und sind nicht abhängig von der dafür zuständigen Gruppe.

In 2011 und 2012 sind folgende Termine für das Treffen des Interoperabilitätsforums vorgesehen:

- 5.–6. Dezember 2011 in Göttingen
- 26.–27. März 2012 in Berlin
- 18.–19. Juni 2012 in Köln
- 27.–28. September 2012 (Ort folgt)
- 29.–30. November 2012 in Göttingen

Weitere Termine:

15. November 2011
RIMBAA Out-of-Cycle Meeting
Amsterdam (NL)

29. November – 1. Dezember 2011
1st ISO IT Forum
Genf (CH)

15.–20. Januar 2012
Working Group Meeting
San Antonio, TX (US)

13.–18. Mai 2012
Working Group Meeting
Vancouver, BC (CA)

21.–25. Mai 2012
IHE connect-a-thon
Bern (CH)

24.–26. April 2012
conhIT
Berlin

Bitte schauen Sie auch in den gemeinsamen Terminkalender des Interoperabilitätsforums (interoperabilitaetsforum.de), des Kompetenznetzes eHealth-Standards (kompetenznetz-ehealth-standards.de) und HL7-Deutschland (hl7.de).

Bernd Blobel

Die Welt der Security- und Privacy-Standards

Einleitung

Kommunikation und Kooperation zwischen Einrichtungen des Gesundheitswesens und ihren Mitarbeitern, künftig sogar unter Einbeziehung der Patienten, ist Vertrauenssache. Das erforderliche Vertrauen kann aus der Vertrautheit mit den beteiligten Personen und ihren Handlungsbedingungen, aus dem Vorhandensein klarer Anweisungen, Regelungen und Vorschriften und ihrer Kontrolle, oder garantiert durch gesetzliche Regelungen mit Strafbewehrungen entstehen. Aufgrund dieser Bedeutung von Datenschutz und Datensicherheit wollen wir uns hier etwas eingehender mit der Problematik und den erforderlichen Maßnahmen beschäftigen. Mit zunehmender Anwendung von Informations- und Kommunikationstechnologien (IKT) über Organisations-, regionale und sogar nationale Grenzen hinweg erhöht sich die Verwundbarkeit der Organisationen und ihrer Strukturen (Gesamtheit der schützenswerten Objekte) und nimmt die Bedrohung von Datenschutz und Datensicherheit zu.

Bedrohungen von Datenschutz und Datensicherheit sind objektive Möglichkeiten für passive und aktive, fahrlässige und intendierte Angriffe auf Informations- und Kommunikationssysteme, die das subjektiv empfundene bzw. zumindest teilweise objektivierbare Risiko und somit das Vertrauen in ein System, die Kommunikations- und Kooperationspartner und die Informationen sowie Dienste beeinflussen. Das objektivierbare Risiko beschreibt die berechnete Prognose eines möglichen Schadens oder Verlustes hinsichtlich Eintrittswahrscheinlichkeit und Konsequenzen, wobei der Schaden finanzieller, materieller, aber auch ideeller Art (z. B. Reputations- und Vertrauensverlust) sein kann. Da die Bedrohungen nicht vollständig aus der Welt geschafft werden können, gibt es kein Null-Risiko. Datenschutz und Datensicherheit müssen so organisiert und implementiert werden, dass ein als akzeptabel definiertes Risiko nicht überschritten wird.

In weitgefasster, in der internationalen Praxis aber gut bewährter Weise bezeichnen wir den Komplex der rechtlichen, organisatorischen, funktionalen, medizinischen, sozialen, ethischen und technischen Regulierungen für Datenschutz und Datensicherheit als Security & Privacy Policy [1]. Da man nicht alles verbindlich regulieren kann, wurden durch die IMIA (International Medical Informatics Association) die Prinzipien zum fairen Umgang mit Informationen (Fair Information Principles) und die

ethischen Leitlinien (Code of Ethics for Health Information Professionals) definiert [2].

Bei Datenschutz- und Datensicherheit können wir rechtliche und politische, organisatorische und technische Aspekte unterscheiden. Wir wollen uns in diesem Beitrag auf die organisatorischen und technischen Aspekte beschränken und die entsprechenden Standards kurz beleuchten. Für eine weitergehende, auch die rechtlichen und politischen Aspekte einbeziehende Betrachtung sei auf das Handbuch für Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen verwiesen [3].

Wenn man bei der Kommunikation sensitiver Information zwischen IKT-Systemen und ihrer Verwendung und Verarbeitung in Anwendungssystemen unterscheidet, kann man die Konzepte,

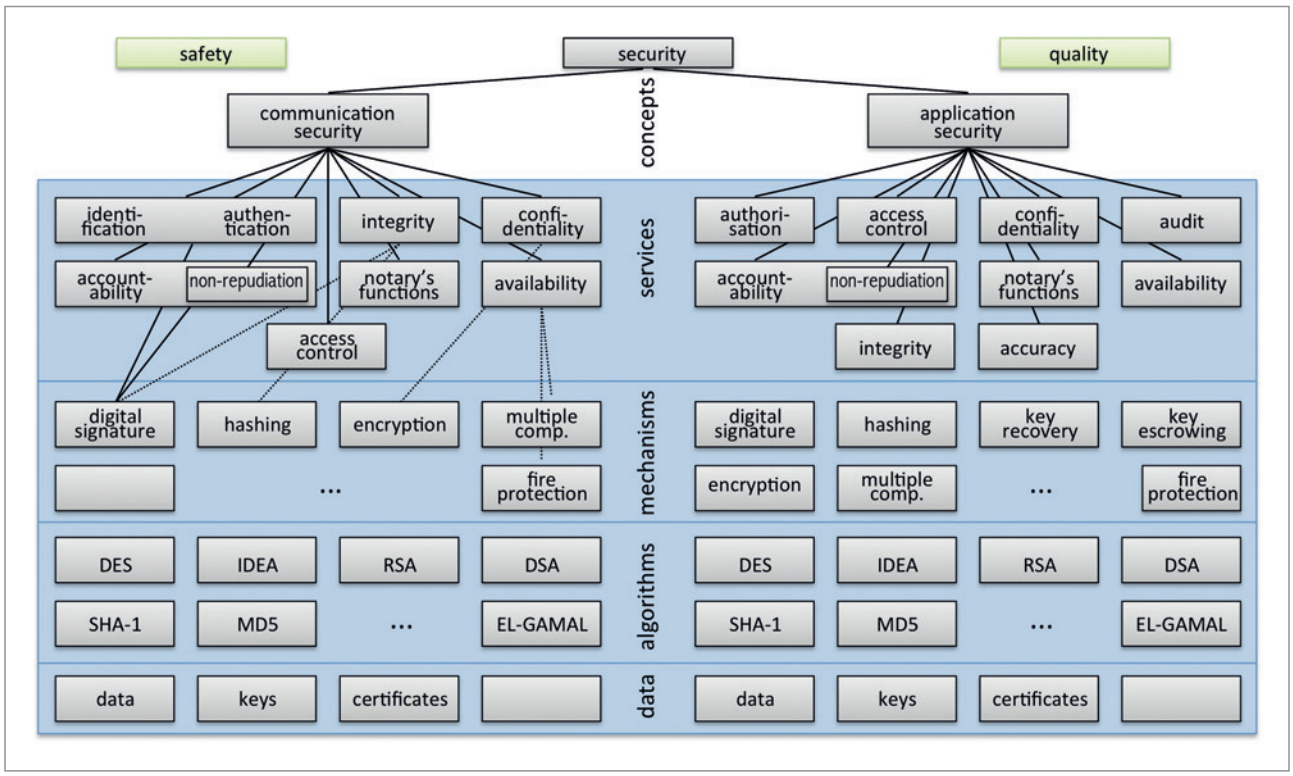


Abbildung 1: Schichtenarchitektur der Security und Privacy Services

Dienste, Mechanismen, Algorithmen und Objekte für Datenschutz und Datensicherheit – die alle standardisiert sein müssen – wie folgt zusammenfassen (Abbildung 1).

Während die Konzepte der Kommunikationssicherheit nicht domänenspezifisch sind und deshalb keine speziellen Standards und Spezifikationen benötigen (auch wenn das von Einigen immer wieder forciert wird), sondern von den existierenden und in Entwicklung befindlichen domänenübergreifenden Standards vollständig abgedeckt werden, sind die Konzepte der Anwendungssicherheit hochgradig von den Datenobjekten, deren vielschichtigen sozialen, ethischen und psychologischen Implikationen für die Betroffenen sowie der zugrunde liegenden Policies abhängig. Das Konzept der Identifikation und Authentifizierung der beteiligten Akteure im weitesten Sinne (Personen, Organisationen, Systeme, Geräte, Anwendungen, Komponenten) ist sowohl für den Zugriff auf Systeme im Kontext der Kommunikationssicherheit als auch den danach möglichen Zugriff auf Informationsobjekte und Funktionen im Kontext der Anwendungssicherheit fundamental.

Security- und Privacy-Konzepte

Kommunikationssicherheitskonzepte

Wie Abbildung 1 entnommen werden kann, müssen wir folgende Basisdienste für Kommunikationssicherheit gewährleisten: Authentifizierung vorgegebener Identitäten sowie Verfügbarkeit (Sicherung gegen Vorenthaltung), Vertraulichkeit (Sicherung gegen unautorisierte Kenntnisnahme), Integrität (Sicherung gegen unautorisierte Veränderungen) und Verbindlichkeit einschließlich Unbestreitbarkeit (verifizierbare Verknüpfung der Informationen und Prozesse mit Akteuren) kommunizierter Informationen. Während traditionell die Authentifizierung von Akteuren und Vertraulichkeit der Informationen im Fokus der Datensicherheitsbemühungen standen, gewinnen in einer verteilten, interoperablen Welt durch die wachsende Abhängigkeit von verlässlichen Informationen neben dem ID-Management die Verfügbarkeit und Integrität zunehmend an Bedeutung. Wie bereits ausgeführt, ist der erste Service für die gerichtete Kommunikation und Kooperation, aber auch für die Gewährleistung von Anwendungssicherheits- und Privacy-Diensten grundlegend.

Das Erfordernis der Identifikation betrifft in einer verteilten eHealth-Umgebung jede Komponente, alle möglichen Zustände und jedes Ereignis, aber auch Prozessschritte, Assoziationen etc. Generell beinhaltet Identifikation die Verknüpfung eines Identifikators (d. h. eines identifizierenden Merkmals) mit einem Objekt. Ein Objekt ist identifiziert, wenn es aus einer Gruppe von Objekten selektiert werden kann. Der Identifikator kann z. B. ein Name, eine Zahl oder ein Statement sein, wobei das Konzept der Identifikation von der Eindeutigkeit der Identifikator-Objekt-Beziehung innerhalb eines ID-Management-Raumes ausgeht, d. h., es darf hier zu einem Identifikator nur ein Objekt geben. Das ID-Management erfordert eine diesen Raum umfassende Autorität, wobei der Raum eine Organisation, eine Region, ein Land oder auch die globale Landschaft sein kann. Selbstverständlich kann ein Objekt – z. B. in Abhängigkeit von verschiedenen Rollen – verschiedene Identifikatoren haben. So haben wir eine Personalausweisnummer und eine Kranken-

versichertennummer. Beide beziehen sich auf das gleiche Objekt (dieselbe Person), zum einen in seiner Rolle als Bürger und zum anderen in seiner Rolle als Krankenversicherter. Im Sinne der Datensicherheit muss diese beanspruchte Identität überprüfbar sein. Das kann durch eine Beglaubigung (Zertifikat) durch eine dafür zuständige, nachprüfbare Autorität (z. B. das Einwohnermeldeamt, welches das Zertifikat Personalausweis mit seinem Siegel beglaubigt), durch Wissen, welches nur die mit dem Identifier verknüpfte Person haben kann (z. B. das Passwort zu einem Nutzernamen), durch Besitz eines individuellen Tokens (z. B. ein Schlüssel für ein Schließfach, eine Smartcard) oder durch eine individuelle Eigenschaft des Objekts (Stimme, Handschrift, Gang, biometrische Parameter wie Iris, Gesicht, Fingerabdruck, genetischer Code) geschehen. Dabei muss auch im Falle des Rückgriffs auf Eigenschaften die Eindeutigkeit sorgfältig geprüft werden, bevor man sich für einen derartigen Authentifizierungsmechanismus entscheidet. So ist der menschliche Fingerabdruck nur in einem bestimmten Lebensabschnitt eindeutig. Auch die Iris kann Veränderungen unterliegen, wie von [4] berichtet. Schließlich muss für alle Authentifizierungsdienste die Fälschungssicherheit analysiert und bei der Entscheidung für einen bestimmten Mechanismus berücksichtigt werden. Bei Identifikationstests unterscheiden wir zwei Varianten: die Identifikation und die Verifikation. Bei der Identifikation wird die Identität gegen alle in einer Datenbank gespeicherten identifizierenden Merkmale analysiert, während bei der Verifikation die Identität gegen ein beglaubigtes Muster (z. B. auf einer Smartcard gespeicherter zertifizierter Fingerabdruck der Person) geprüft wird. Letztgenannter Mechanismus birgt weniger Security- und Privacy-Risiken als der erstgenannte (Datensammlung) und sollte deshalb bevorzugt werden.

Die Sicherung der Verfügbarkeit, der Vertraulichkeit, Integrität und Verbindlichkeit einschließlich Unbestreitbarkeit der kommunizierten Informationen und bezogenen Prozesse sind technisch lösbare Dienste. Dabei kommen zunehmend kryptografische Mechanismen zum Einsatz, die mit testbaren mathematischen Algorithmen einen Schlüssel auf ein Objekt manipulationsfrei anwenden. Das Objekt kann dabei ein signiertes Dokument (digitale Signatur), ein von einer entsprechenden autorisierten Stelle signiertes Nutzerzertifikat, der Fingerprint eines Dokuments (Hash-Wert) und seine Signierung (Manipulation des Dokuments resultiert in einem anderen Hash-Wert, der mit dem manipulationsfrei signierten Hash-Wert des Originaldokuments verglichen und so Integritätsverlust nachgewiesen werden kann) u. ä. sein. Notariatsdienste sind z. B. von einer autorisierten Stelle signierte Zeitstempel etc.

Die meisten der Kommunikationssicherheitsdienste werden auf den Ebenen 1–6 des ISO OSI Modells realisiert, was die Domänenunabhängigkeit unterstreicht. Gleiches gilt natürlich für die Mechanismen, die für die Dienste-Realisierung implementiert werden sowie für die Algorithmen, die dafür abgearbeitet werden. Beispiele für derartige domänenunspezifische, technische Spezifikationen finden sich in der Übersicht am Ende des Beitrags. Leider wurden derartige Spezifikationen „missbräuchlich“ und fälschlich auch im CEN TC 251 Health Informatics entwickelt. Als solches Negativbeispiel wäre der dreiteilige Standard EN 13608 „Health informatics – Security for healthcare communication“ zu nennen, der von der deutschen CEN-Delegation von Anfang an sehr kritisch begleitet und auf ihr Betreiben inzwischen zurückgezogen wurde. Er ist deshalb auch nicht in der Übersicht enthalten. Leider sind nicht alle unnützen, die gültigen und ausreichenden Basis-Standards inkonsistent wiederholenden Spezifikationen zu verhindern.

Anwendungssicherheitskonzepte

Die Mechanismen und Algorithmen zur Sicherung der Verfügbarkeit, Verbindlichkeit und Integrität von gesammelten, gespeicherten, wiedergefundenen, verarbeiteten, gesicherten und ggf. gelöschten Informationen – also im Anwendungskontext – entsprechen denen der Kommunikationssicherheitsdienste. Wie die zugrunde liegenden Services sind auch sie nicht spezifisch für das Gesundheits- und Sozialwesen.

Besonderheiten im Gesundheitswesen auf Grund des besagten besonderen Charakters der Prozesse und Informationen gelten aber für die Policy-anhängigen Dienste, d. h., die durch Gesetzlichkeiten, berufsständische Festlegungen, ethische Prinzipien, aber auch persönlich Erwartungen, Präferenzen etc. geregelte Prozesse. Hier sind insbesondere die Autorisierung und Zugriffskontrolle, aber auch das Audit zu nennen. Benutzte Mechanismen, Algorithmen, aber auch Repräsentationsmittel wie Beschreibungs- und Modellierungssprachen (z. B. UML, XML, SAML, XACML, BPML) sind wiederum domänenunspezifisch, werden in der Regel in anderen Domänen entwickelt und im Gesundheitswesen nachgenutzt. Das schließt jedoch Grundlagenentwicklungen in unserer Domäne nicht aus, wie der grundlegende dreiteilige Standard ISO 22600 „Health informatics – Privilege management and access control“ beweist. Hier wurde vor Jahren ein architekturbezogenes, ontologisch begründetes generisches Policymodell entwickelt, welches sich – wenn zurzeit auch nur in Teilen – in neuesten SOA-Spezifikationen wiederfindet.

Bei der Zuweisung von Privilegien sind Qualifikationen, Dienststellungen, die Einbeziehung in bestimmte Prozesse bzw. Beziehungen zum Datensubjekt wesentlich, die in Rollen zusammengefasst werden. Nach ISO TS 21298 „Health informatics – Structural and functional roles“ beschreiben Rollen ein Set von Kompetenzen und/oder Performanzen, die mit einer Aufgabe verbunden sind. Rollen zwischen Personen und Organisationen sind eher statisch definiert. Sie werden laut ISO TS 21298 als strukturelle oder organisatorische Rollen bezeichnet. Rollen im Kontext einer Aktion sind hoch-dynamisch und werden in ISO TS 21298 als funktionelle Rollen definiert. Da bei Datenschutz- und Datensicherheitsverstößen

nicht die Möglichkeit, sondern der Vollzug relevant ist, sind vor allem die funktionellen Rollen bedeutsam im Kontext des in diesem Beitrag behandelten Gegenstandes. Die Instanzen der Privilegien sind die Erlaubnisse bzw. Verpflichtungen zu bestimmten Aktionen. Anwendbare Regeln einschließlich der für kontextuelle, Umgebungs- und andere Einflüsse werden in Policies fixiert. Policies werden über Zugriffskontrollmechanismen (Zugriffsbeschränkungen) durchgesetzt. Daraus resultieren die einschlägigen Zugriffskontrollmodelle mit aufsteigender Policy-Komplexität wie das Mandatory Access Control (MAC) Modell (militärische, ranggesteuerte Rechtehierarchie), Discretionary Access Control (DAC) Modell (Rechteeigner weist anderen Rechte zu, delegiert Rechte), Role-Based Access Control (RBAC) Modell (Rollen definieren Privilegien anstelle einer individuellen Privilegienzuweisung, was das Privileg-Management wesentlich vereinfacht, jedoch nicht von der Fallkontrolle befreit).
Die zunehmende Komplexität und die bessere Abbildung der Anforderungen werden in den traditionellen Zugriffskontrollmodellen durch einen Übergang von strukturellen zu funktionellen Rollen sowie einen Übergang zu größerer Granularität gemeistert. Das macht der Vergleich der früheren groben Rollen gemäß der Leitungshierarchie in Strukturen im Gesundheitswesen mit dem für verschiedene strukturelle Rollen auf Aktivitäten und Arbeitsschritte fein aufgeschlüsselten funktionellen Rollen des HL7-RBAC-Katalogs deutlich. Die Perfektion dieser Entwicklung ist die freie und dynamische Definition von Policies unter Berücksichtigung kontextueller und Umgebungsbedingungen, wie es ISO 22600 ermöglicht. Durch die definierte Meta-Policy (Policy-Ontologie) ist ein umfassendes Security- und Privacy-Management möglich. Für weitere Informationen siehe zum Beispiel [5] und [6].

Privacy-Konzepte

Privacy – d. h. der Schutz der Privatsphäre – ist im Gesundheits- und Sozialwesen wegen der sozialen und psychologischen, unter Umständen auch der politischen Implikationen von Zuständen und Prozessen für den Betroffenen und sein Umfeld ein besonders geschütztes Gut. Viele Prozesse erfordern seine informierte, d. h. bewusste Einwilligung, wobei eine Ablehnung in der Regel keine Nachteile zeitigen darf. Die Einwilligung oder auch deren Beschränkung ist eine spezifische Policy, die mit anderen zutreffenden Policies harmonisiert werden muss (ISO 22600).

Ein wichtiges Privacy-Konzept ist die De-Identifikation von Objekten, d. h., die Trennung des Identifikators vom Objekt bzw. seiner informationellen Repräsentation (z. B. die Entfernung von Namen und weiteren demografischen Angaben aus dem Datensatz), bzw. im Falle von Kompromittierungen bzw. zur Risikominderung die Veränderung der Identifikatoren für ein Objekt (die Schaffung einer neuen Identität (neuer Nutzername/Passwort-Kombination, neuer Ausweis/Lebenslauf für eine gefährdete Person, die Veränderung ihrer identifizierenden Merkmale). Bei der De-Identifikation sind zwei unterschiedliche Mechanismen möglich: die Anonymisierung und die Pseudonymisierung. Dabei kann ein Klassenmerkmal wie Beruf durchaus zum Individualmerkmal werden, wenn die Menge der möglichen Instanzen des Merkmals klein genug ist, der Beruf des Individuums z. B. Bundeskanzlerin ist oder das Objekt an einer absolut seltenen, ggf. sogar offensichtlichen Krankheit leidet. Die Anonymisierung schließt eine Re-Identifikation (mit verhältnismäßigem Aufwand) aus. Dabei ist zu beachten, dass nach der mathematischen Theorie von komplexen Merkmalsräumen eine 100%ige Anonymisierung komplexer Objekte unmöglich ist, da die Merkmalskombination selbst einmalig sein kann und damit eine identifizierende Charakteristik aufweist. Mit anderen Worten, je mehr Informationen wir über einen Patienten sammeln (z. B. die Gesamtheit eines lebenslangen EHR oder genetische Informationen, die ja für sich schon einen Authentifizierungsmechanismus anbieten), umso unmöglicher ist die De-Identifikation (d. h. sowohl die Anonymisierung als auch die Pseudonymisierung) der Informationen über diese Individuen. Dann bleibt nur die verschärfte Anwendung von Sicherheitsmechanismen oder die Beschränkung von Datensammlungen, ihre Separierung in nicht verlinkte Teildatenmengen etc. Bei der Pseudonymisierung wird der interpretierbare (das zugehörige Objekt direkt oder indirekt, d. h. über öffentlich zugängliche Referenzen identifizierende) Identifikator durch einen nicht interpretierbaren Identifikator ersetzt. Nur einer Vertrauensstelle, die die Referenztabelle vorhält, ist eine Re-Identifikation möglich. Das Pseudonym kann dabei willkürlich definiert oder durch einen speziellen (z. B. kryptografischen) Algorithmus reproduzierbar ermittelt werden. Letzteres ist z. B. beim Fortschreiben von Datensätzen in klinischen oder epidemiologischen Registern erforderlich. Die folgenden Bilder (nach Pommerening) beschreiben die Pseudonymisierungskonzepte für die sekundäre Nutzung persönlicher

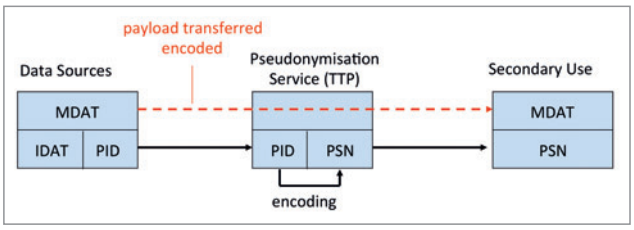


Abbildung 2: Pseudonymisierung für die einmalige sekundäre Verwendung von klinischen Informationen

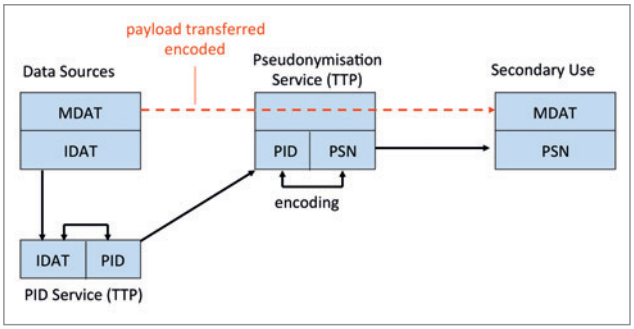


Abbildung 3: Pseudonymisierung mit möglicher Re-Identifikation

medizinischer Daten für unterschiedliche Use Cases nach ISO/IEC 25237 „Health informatics – Pseudonymisation practices for the protection of personal health information and health related services“. Dieser Standard wurde dem Pseudonymisierungskonzept der TMF für klinische Register entlehnt und entsprechend weiterentwickelt.

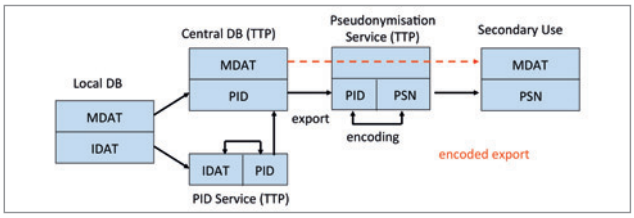


Abbildung 4: Pseudonymisierung für eine zentralisierte Datenbank
Legende für die Abbildungen: MDAT medical data, IDAT identification data, PID personal identifier (unique), PSN pseudonym.

Einordnung der Datenschutz- und Datensicherheitsstandards

Generell kann man hinsichtlich der Typen von Datenschutz- und Datensicherheitsstandards und -spezifikationen sowie der zuständigen Standardisierungsgremien (Standards Development Organizations – SDOs) folgende Grobeinteilung vornehmen:

Spezifikationstyp	SDOs (Auswahl)
Domänenübergreifende technisch/ technologische Standards	ISO/IEC, ETSI, NIST
Domänenspezifische Spezifikationen	HL7, ISO TC 215, CEN TC 251, ASTM, IHTSDO, WHO
Domänenübergreifende architekturbezogene Spezifikationen	OMG, TOG
Domänenübergreifende prozessbezogene Spezifikationen	OASIS
Internetbezogene Spezifikationen	W3C, IETF
Business/Trading Spezifikationen und Instanzen	UN, CENELEC, GS1

Tabelle 1: Security- und Privacy-Spezifikationstypen und zuständige SDOs

Manch Leser mag IHE in Tabelle 1 vermissen. IHE ist jedoch keine Standards entwickelnde Organisation, sondern spezifiziert Interoperabilitätsprofile auf der Basis existierender Standards, die von den in Tabelle 1 aufgeführten SDOs entwickelt wurden. Dabei ist die Verschränkung zwischen HL7 und IHE besonders intensiv, was sich sowohl auf globalem Level als auch regional und national deutlich manifestiert. Hier sei an die enge Kooperation zwischen HL7 Deutschland und IHE Deutschland erinnert, die sich mittlerweile sogar in gemeinsamen Jahrestagungen niederschlägt. Natürlich gibt es datenschutz- und datensicherheitsrelevante IHE-Spezifikationen. Einige davon sind in der Übersicht am Ende des Beitrags aufgelistet. Darüber hinaus hat IHE auch White Papers und Nutzer-Handbücher zum Gegenstand dieses Artikels entwickelt.

Im Folgenden wird ein kleiner Teil der mehrere Hunderte relevanter Standards um Datenschutz und Datensicherheit im Gesundheitswesen aufgelistet. Weitergehende Übersichten und zusätzliche Informationen finden sich zum Beispiel in der Datenbank des europäischen BioHealth-Projektes [7].

Domänenunspezifische technische Spezifikationen

- ISO/IEC 7498 Information technology – OpenSystems Interconnection
- ISO/IEC 9594:2001 Information technology – Open Systems Interconnection – The Directory
- ISO/IEC 10118 Information technology – Security techniques – Hash-functions
- ISO/IEC 10181 Information technology – Open Systems Interconnection – Security frameworks for open systems
- ISO/IEC 10736 Information technology, Telecommunications and information exchange between systems, Transport layer security protocol
- ISO/IEC 10745 Information technology, Open Systems Interconnection, Upper layers security model
- ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
- ETSI ETR 277 (March 1996) Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems
- ETSI ETR 278 (March 1996) Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2
- ETSI SR 002 176 V1.1.1 (2003-03) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures
- ETSI SR 002 298 V1.1.1 (2003-12) Response from CEN and ETSI to the “Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach”
- ETSI TR 101 375 V1.1.1 (1998-09) Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)
- ETSI TR 101 690 V1.1.1 (1999-08) Security Algorithms Group of Experts (SAGE); Rules for the management of the GSM CTS standard Authentication and Key Generation Algorithms (CORDIAL)
- ETSI TR 101 740 V1.1.1 (1999-08) Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)
- ETSI TR 102 038 V1.1.1 (2002-04) TC Security – Electronic Signatures and Infrastructures (ESI); XML format for signature policies
- ETSI TR 102 047 V1.2.1 (2005-03) International Harmonization of Electronic Signature Formats

- ETSI TR 102 272 V1.1.1 (2003-12) Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies
- ETSI TS 101 862 V1.3.3 (2006-01) Qualified Certificate profile
- ETSI TS 101 733 Electronic Signature Formats
- ETSI TS 101 903 V1.2.2 (2004-04) XML Advanced Electronic Signatures (XAdES)
- ETSI TS 102 023 V1.2.1 (2003-01) Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
- ETSI TS 102 176-1 V1.2.1 (2005-07) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
- ETSI TS 102 176-2 V1.2.1 (2005-07) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices

Spezifikationen von Anforderungen und Evaluierungen

- ISO/IEC 15408-1:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
- ISO/IEC 15408-2:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
- ISO/IEC 15408-3:2005 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements

Spezifikationen für Information Security Management Systeme

- ISO/IEC NP 27000 Information technology – Information security management – fundamentals and vocabulary
- ISO/IEC 27001:2005 (revised version of BS 7799 Part 2:2002) Information technology – Security techniques – Information security management systems (ISMS) – Requirements
- ISO/IEC 27002 (Previous ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27003 ISMS Implementation guidance
- ISO/IEC 27004 ISMS measurements
- ISO/IEC 27005 ISMS Risk assessment
- ISO 27799 Health informatics – Information security management in health using ISO/IEC 27002 (domänenspezifisch)

Leitlinien

- ISO/IEC TR 13335-3:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security
- ISO/IEC TR 13335-4:2000 Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards
- ISO/IEC TR 13335-5:2001 Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security

Domänenunspezifische Security- & Privacy-Infrastrukturstandards

- X.1051 ISMS Telecoms requirements
- ISO/IEC 18028 Information technology – Security techniques – IT network security
- ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
- ITU-T X.841 | ISO/IEC 15816:2002 – Security information objects for access control
- ITU-T X.842 | ISO/IEC 14516:2002 – Guidelines on the use and management of Trusted Third Party services
- ITU-T X.843 | ISO/IEC 15945:2002 – Specification of TTP services to support the application of digital signatures
- CORBA Security Services (CORBA)
- Common Security Interoperability Services (CORBA)

Domänenunspezifische Privacy-Standards und Modellierungsspezifikationen

- Extensible Access Control Markup Language (XACML) v2.0, February 2005
- XACML Profile for Role Based Access Control (RBAC): Committee Draft 01 (normative; 13 February 2004)
- Security Assertion Markup Language (SAML) v2.0, March 2005
- SAML 2.0 profile of XACML, November 2004
- Security Provisioning Markup Language (SPML) V1.0, (OASIS 200306), October 2003
- OASIS 200201 Directory Services Markup Language (DSML) v2.0
- OASIS XACML eXtensible Access Control Markup Language TC v2.0 (XACML)

Spezifikationen von Anforderungen und Evaluierungen für das Gesundheitswesen

- ISO/NP TS 14441-1 Health informatics – Security and privacy requirements for compliance testing of EHR systems (1–2)
- CEN ENV 12924 Medical Informatics – Security Categorisation and Protection for Healthcare Information Systems
- ISO/TS 21547:2010 Health informatics – Security requirements for archiving of electronic health records – Principles

Security- und Privacy-Infrastrukturstandards für das Gesundheitswesen

- ISO 17090 Health informatics – Public key infrastructure (1–3)
- ISO 21091 Health informatics – Directory services for security, communications and identification of professionals and patients
- ISO TS 21298 Functional and structural roles

- Resource Access Decision Service (CORBA)
- Clinical Object Access Service (CORBA)

Privacy-Standards für das Gesundheitswesen

- ISO/TS 22857:2004 Guidelines on data protection to facilitate trans-border flow of personal health information
- ISO 22600 Health informatics – Privilege management and access control (1–3)
- ISO/IEC TS 25237 Health Informatics: Pseudonymisation Practices for the Protection of Personal Health Information and Health Related Services
- ISO/DIS 27789 Health informatics – Audit trails for electronic health records
- EN 14484:2004 Health informatics – International transfer of personal health data covered by the EU data protection directive – High level security policy
- CEN EN 14485 Health Informatics – Guidance for handling personal health data in international applications in the context of the EU Data Protection Directive
- CEN ENV Health Informatics – Accountability and audit trail mechanism for healthcare information systems
- ASTM E1987-98 Standard guide for individual rights regarding health information

ID-Management-Standards

- Person Identification Service CORBA
- Entity Identification Service (HL7/CORBA)
- Master Patient Index (HL7)
- International Object Identifier (UNO)
- LOINC (Regenstrief Institute/HL7)
- Standard guide for properties of a Universal Healthcare Identifier (ASTM)
- ASTM E1714-00 Standard guide for properties of a Universal Healthcare Identifier

Datenschutz- und datensicherheitsrelevante IHE-Spezifikationen

- Audit Trail and Node Authentication (ATNA)
- Basic Patient Privacy Consents (BPPC)
- Consistent Time (CT)
- Cross-Community Access (XCA)
- Cross-Enterprise Document Reliable Interchange (XDR)
- Cross-Enterprise User Assertion (XUA)
- Enterprise User Authentication (EUA)
- Patient Administration Management (PAM)
- Patient Demographic Query HL7 V3 (PDQ V3)
- Patient Demographics Query
- Patient Identifier Cross-Referencing (PIX)
- Patient Identifier Cross-Reference HL7 V3 (PIX V3)
- Cross-Community Patient Discovery (XCPD)
- Cross-Enterprise User Assertion – Attribute Extension (XUA++)
- Document Digital Signature (DSG)
- Document Encryption (DEN)
- Healthcare Provider Directory (HPD)
- Notification of Document Availability (NAV)
- XAD-PID Change Management (XPID)

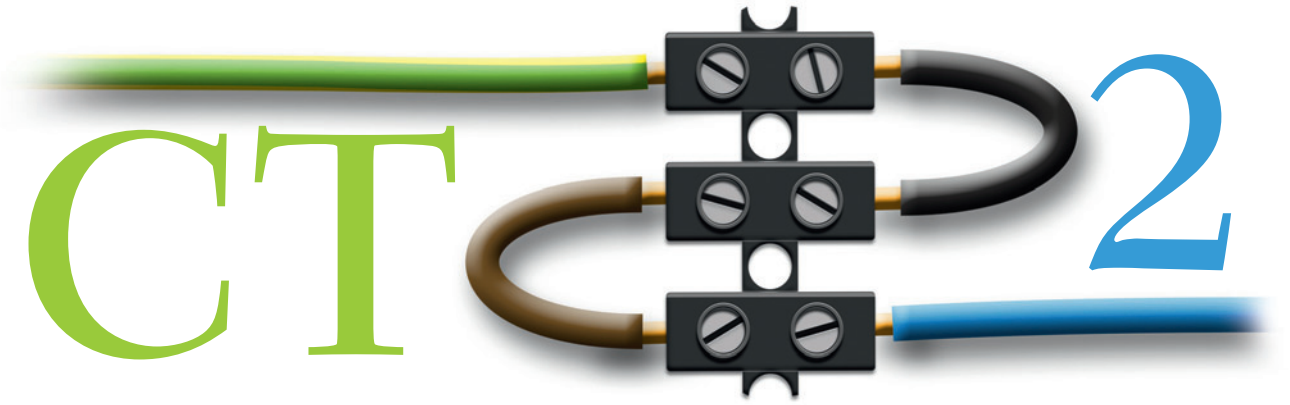
Diskussion

Der Autor stellt sich mit dem vorliegenden Beitrag der Herausforderung, den aufgrund seiner technischen, aber auch rechtlichen, regulatorischen, organisatorischen, sozialen und psychologischen Komponenten extrem komplexen Gegenstand von Datenschutz und Datensicherheit im Allgemeinen sowie speziell im Gesundheitswesen zu strukturieren und dadurch etwas verständlicher zu machen, ohne ihn umfassend behandeln zu können. Es wurde deutlich, dass es viele (teilweise zu viele) Standards und öffentlich zugängliche Spezifikationen (Publicly Available Specifications – PAS) gibt. Dennoch sind einige Fragen ungelöst, was eine unüberschaubare Community aus verschiedensten Domänen motiviert, sich auf diesem bedeutsamen Feld zu engagieren. Schon das Behalten der Übersicht ist ein hoher Anspruch, umso mehr das durchgängige und umfassende Verständnis der existierenden und in Entwicklung befindlichen Lösungen. Die große Gruppe der deutschen Experten spielt sowohl domänenübergreifend als auch domänenspezifisch eine gute Rolle im internationalen Geschäft. Die Nutzergemeinde ist gut beraten, sich dieser reichen Ressourcen zu bedienen und nicht die Räder irgendwie neu zu erfinden.

Priv.-Doz. Dr. Bernd Blobel
eHealth Competence Center, Regensburg (DE)

Referenzen:

[1] B.Blobel, F.Roger-France: A Systematic Approach for Analysis and Design of Secure Health Information Systems. International Journal of Medical Informatics 62 (3) (2001) pp. 51–78.
[2] International Medical Informatics Association (IMIA): The IMIA Code of Ethics for Health Information Professionals http://www.imia.org
[3] C.Bake, B.Blobel, P.Münch (Hrsg.): Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 3. überarbeitete und erweiterte Auflage. DATAKONTEXT-FACHVERLAG GmbH, Frechen 2009.
[4] John Daugman, University of Cambridge (Persistence of Iris Pattern Recognition)
[5] B.Blobel, R.Nordberg, J.M.Davis, P.Pharow: Modelling privilege management and access control. International Journal of Medical Informatics 75, 8 (2006) pp. 597–623.
[6] B.Blobel: Intelligent security and privacy solutions for enabling personalized telepathology. Diagnostic Pathology 2011, 6 (Suppl 1):S4.
[7] The BioHealth Project Consortium: Security and Identity Management Standards in eHealth including Biometrics http://biohealth.helmholtz-muenchen.de



Peter Haas, Robert Mützner

CTS2 in Theorie und Praxis

Einleitung

In verteilten Anwendungsumgebungen, aber auch im Web 2.0 wird immer deutlicher, dass ein sinnvolles elektronisches Miteinander ohne eine gemeinsame Semantik kaum möglich ist. Interoperabilität auf Basis eines wie auch immer technisch realisierten Datenaustausches zwischen Systemen erfordert nicht nur eine definierte Syntax für den Austausch, sondern auch eine gemeinsam verbindlich zu nutzende Semantik. Semantik-Missmatches sind heute das größte Problem bei der Interoperabilität, die semantische Integrität wie sie für Datenbanksysteme bekannt ist, muss auch in großen verteilten Umgebungen gewahrt werden. Diese Semantik findet sich zum Großteil in attributbezogenen zu verwendenden Ordnungssystemen von einfachen kleinen Vokabularen bis hin zu umfassenden Taxonomien oder mehrachsigen semantischen Bezugssystemen wieder. Bei vielen hundert bis tausenden Teilnehmern bzw. Teilnehmersystemen lässt sich diese Semantik aber nicht mehr manuell konsentieren und verteilen – z. B. via CDs oder informalen E-Mail-Nachrichten. Es wird daher ein informatisches Artefakt notwendig, das es allen Teilnehmersystemen ermöglicht, Semantik maschinenabrufbar und – lesbar zu beziehen bzw. die lokale Semantik mit der globalen Semantik zu synchronisieren. So kann ein in semantischer Hinsicht „selbstlernendes“ Gesamtsystem entstehen, in dem die einzelnen Teilnehmersysteme die gesamte Semantik nicht per se kennen müssen, sondern auch bei Bedarf – also wenn z. B. eine Nachricht, ein Dokument o. Ä. mit nicht bekannter Semantik eintrifft – automatisiert nachladen können. Hierzu sollten Terminologieserver zum Einsatz kommen, die über ein sehr generisches Datenmodell verfügen müssen, um beliebige und verschieden komplexe Ordnungssysteme verwalten und via Webservices in diesen verteilten Umgebungen verfügbar machen zu können. Der Standard Common Terminology Services Version 2 (CTS 2) spezifiziert ein solches Modell und die zugehörigen Diensteklassen und Dienste.

CTS2 – Historie und Grundstruktur

CTS2 – Common Terminology Services – ist eine HL7-OMG-Spezifikation, die ein Klassenmodell sowie die notwendigen Dienste spezifiziert, um Terminologien und Ontologien z. B. mittels eines Terminologieservers verwalten und diese in verteilten Umgebungen via Webservices verfügbar machen zu können. Der Standard ist eine Weiterentwicklung von CTS 1.0. Neu hinzugekommen ist beispielsweise ein Versionisierungskonzept. Aufgeteilt ist der Standard in zwei Modelle, die im Folgenden kurz beschrieben werden.

Conceptual Model

Das Conceptual Model stellt das Datenmodell in Form eines Klassenmodells dar, welches eine hohe Generizität bietet. Es ermöglicht die Verwaltung von Vokabularen, Konzepten und deren Beziehungen, Cross-Mappings und Value Sets. Die wesentlichen Submodels zeigt Abbildung 1.

Auf oberster Ebene stehen die einzelnen Vokabulare. Jedes Vokabular enthält mehrere, unterschiedliche Konzepte. Diese

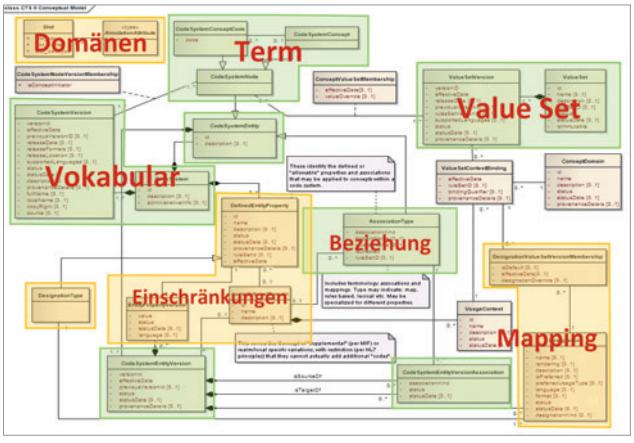


Abbildung 1: CTS2 Submodels

Konzepte können einzelne Begriffe einer Terminologie, Begriffskomplexe oder Beziehungen sein. Jedes Konzept kann in Beziehung mit einem anderen Konzept stehen. Dabei ist es irrelevant, ob sich beide Konzepte im gleichen Ordnungssystem befinden oder nicht. Man spricht im zweiten Fall auch von Cross-Mapping.

Value Sets fassen unterschiedliche Konzepte aus einem oder mehreren Ordnungssystemen zusammen, sie bilden quasi einen View auf die Semantik. Die Komplexität eines Value Sets kann von einer flachen Liste von Konzeptcodes von einem Ordnungssystem bis hin zu einer unbegrenzten, hierarchischen Sammlung von Konzepten aus unterschiedlichen Ordnungssystemen reichen. Dabei gilt zu beachten, dass jede Sammlung von Konzepten in einem Value Set einzigartig bleiben sollte.

Eine Besonderheit von CTS2 ist die Versionisierung, welche nicht nur auf Vokabular-, sondern auch auf Konzept- und Value Set-Ebene stattfindet. Ein Vokabular kann so in Echtzeit weiterentwickelt werden, um zu einem bestimmten Zeitpunkt in eine komplett neue Vokabular-Version überführt zu werden. Vorteile liegen in der hohen Aktualität der Einträge, ohne dass alte Datenzusammenhänge verloren gehen.

Functional Model

Das Functional Model spezifiziert die Dienste, welche ein Terminologieserver anbieten sollte. Die verfügbaren Dienste werden in vier Klassen bzw. Szenarien eingeordnet: Administrative Szenarien (Administration), Zugriff-Szenarien (Search), Pflege-Szenarien (Authoring) und Konzept-Szenarien (Association), was eine Übersicht zu der Vielzahl von Diensten erleichtert.

„Administration“ bietet funktionale Methoden für Terminologie-Administratoren an, die den Terminologieserver mit Inhalt füllen oder bei entsprechender Erweiterung auch Benutzer und Rechte verwalten. Es können Inhalte importiert, exportiert sowie Benachrichtigungen über neue oder geänderte Inhalte für Nutzer verwaltet werden. „Search“ umfasst das Retrieval von Vokabularen, Begriffen, Beziehungen und Value Sets. Unterschiedliche Filter helfen bei der Einschränkung der Datenmenge bei Suchanfragen. „Authoring“ befasst sich mit der Pflege von Vokabularen, Begriffen, Beziehungen und Value Sets. Im Gegensatz zu „Search“ ist es hier möglich, dediziert Inhalte in den Terminologieserver einzustellen und Einträge zu pflegen. „Association“ ist für die Verwaltung der Beziehungen zwischen Begriffen sowie dem Cross-Mapping zuständig. Es beschreibt die Möglichkeit, Beziehungen abzufragen, zu erstellen sowie Beziehungen zwischen Vokabularen zu pflegen. Dies ist nicht ganz konsequent, da für Beziehungen hier Methoden des „Authoring“ und des „Search“ zusammengefasst sind.

Die Aufteilung der Dienste in die vier Diensteklassen bietet den Vorteil der Modularisierbarkeit. Unterschiedliche Benutzer mit einzelnen Rollen müssen nur die für sie wichtigen Dienste verwenden. Die Last der Anfragen kann auf verschiedene Services verteilt werden, so dass der Betrieb des Terminologieservers performanter wird. Jede Diensteklasse hat dabei unterschiedliche Zugriffsrechte, so dass Benutzer auch nur für bestimmte Klassen zugelassen werden können.

Das Projekt und die Vorgehensweise

Im Rahmen eines vom BMG geförderten F&E-Projektes wurde auf Basis des Standards CTS2 ein Terminologieserver sowie eine Kollaborationsumgebung zur webbasierten Entwicklung von Terminologien durch viele Benutzer implementiert. Mittels des Terminologieservers können beliebige Ordnungssysteme bzw. deren Inhalte sowie Value Sets verwaltet und in einer verteilten Umgebung zur Verfügung gestellt werden. Dazu wurden auch einige erweiternde Anpassungen am Modell vorgenommen. Der darauffolgende Diensteentwurf und die Implementierung setzten den Standard schließlich in Form eines Terminologieservers um, indem das Klassenmodell in ein Datenbankmodell überführt wurde, die Dienste im Detail geschnitten und dann implementiert wurden.

Anpassungen an CTS2

Das Datenmodell musste im Wesentlichen um Login-Informationen für eine Lizenzüberprüfung sowie die Lizenzinformationen selbst, um Beziehungstypen für die Unterscheidung zwischen ontologischen, taxonomischen oder Cross-Mapping-Beziehungen sowie deren Leserichtung und um Übersetzungen für Begriffe erweitert werden. Damit ist der implementierte Server auch multilingual.

Das Datenmodell und die Dienste wurden um die beschriebenen Änderungen im Datenmodell erweitert. Dazu entstand ein neues Szenario „Authorization“, welches für die Anmeldung am System verantwortlich ist. Für das Qualitätsmanagement entstand ein weiteres Szenario: „Reporting“. So lassen sich in generischer Weise Statistiken erstellen.

Entwurf

Eine große Hilfe für spätere Anwender des Terminologieservers stellt eine Dienste-Attribut-Matrix dar. Sie enthält auf der Horizontalen die in CTS2 spezifizierten Dienste, auf der Vertikalen die Datentypen und den logischen Zusammenhang zwischen Attributen und Diensten (Abbildung 2). In der Matrix werden die Kardinalitäten eingetragen. So sieht ein Entwickler in übersichtlicher Weise, welcher einzelne Dienst welche Muss- und Kann-Angaben beim Request erwartet und welche Ergebnisse dieser zurückliefert. So wurden alle CTS2-Dienste in eine Matrix übertragen und mit Inhalten gefüllt. Diese war sodann Basis für die Entwicklung der lauffähigen Dienste.

Implementierung

Auf Basis des Datenmodells, der Dienste sowie der oben genannten Matrix wurde der Terminologieserver in der Programmiersprache Java umgesetzt. Dabei gibt die Dienste-Attribut-Matrix vor, welche Attribute welchem Service mitgegeben wer-

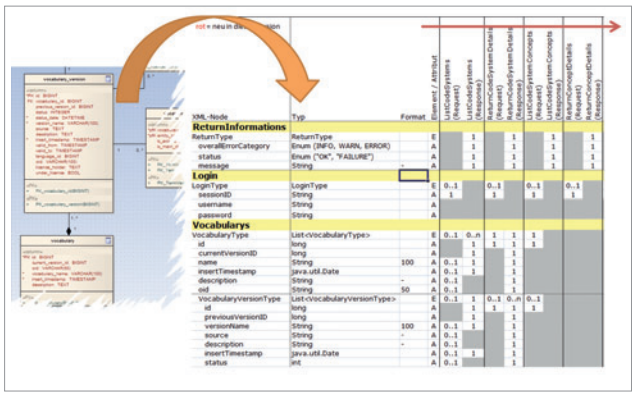


Abbildung 2: Vom Klassenmodell zu den Services

den. Diese Parameter werden zu Beginn auf Korrektheit geprüft, Fehlermeldungen weisen so präzise auf die Ursachen von Problemen hin.

Ergebnisse

Es wurde ein Terminologieserver auf Basis von CTS 2 implementiert, mittels dem semantische Bezugssysteme beliebiger Komplexität sowie Value Sets und Begriffsbeziehungen von Informationssystemen auf Basis von Webservices je nach Berechtigungen verwaltet und abgerufen werden können. Wesentliche Funktionalitäten sind Dienste zur Administration und Pflege von Vokabularen bzw. Ordnungssystemen inkl. Metadaten, ontologischen Beziehungen, Cross-Mappings sowie Value Sets. Außerdem wird die vollständige Versionisierung von Vokabularen, Vokabulareinträgen und Value Sets unterstützt sowie die Berücksichtigung von Lizenzbedingungen für semantische Bezugssysteme. Die wichtigsten 33 Services (siehe Tabelle 1) sind so erfolgreich implementiert worden und sind nun öffentlich erreichbar unter http://www.term.mi.fh-dortmund.de:8080/Terminologieserver/.

Search/Access	Authoring/Curation	Administration
ListCodeSystems	CreateCodeSystem	ImportCodeSystem
ListCodeSystemConcepts	MaintainCodeSystemVersion	ImportCodeSystemRevision
ReturnConceptDetails	UpdateCodeSystemVersionStatus	ImportValueSetVersion
ListConceptAssociationTypes	CreateConcept	Import AssociationVersion
ReturnConceptAssociationTypeDetails	MaintainConcept	ExportConceptAssociation
ListValueSets	UpdateConceptStatus	ExportCodeSystemContent
ReturnValueSetDetails	CreateConceptAssociationType	ChangeCodeSystemStatus
ListValueSetContents	MaintainConceptAssociationType	
CheckConceptValueSetMembership	CreateValueSet	
ListConceptDomains	MaintainValueSet	
ReturnConceptDomainDetails	UpdateValueSetStatus	
ListUsageContexts	CreateConceptDomain	
ReturnUsageContextDetails	MaintainConceptDomain	
ListConceptDomainBindings	CreateUsageContext	
CheckConceptDomainMembership	MaintainUsageContext	
	ListConceptAssociations	
	ComputeTransitiveClosure	
	ComputeSubsumtionrelationship	
	ReturnConceptAssociationDetails	
	UdateConceptAssociationStatus	
	CreateConceptAssociation	

Tabelle 1: Übersicht Dienste

Komponenten

Eine Administrationsumgebung für den Terminologieservern ermöglicht die wesentlichen Einstellungen wie die Verwaltung von Benutzern oder die Verwaltung von Lizenzen über Dialogfunktionen vorzunehmen. Diese Dialogfunktionen nutzen aber auch selbst die realisierten Dienste.

Die in Administration beschriebenen Import- und Export-Schnittstellen wurden mittels ClaML (Classification Markup Language) – einem CEN-Standard [1] zum Austausch von Klassifikationen – implementiert. Der ICD 10-GM wurde so beispielhaft vollständig importiert. Nach Bedarf können auch weitere Ordnungssysteme importiert werden.

Die Interoperabilität zwischen Terminologieserver wurde anhand 2 konkreter Anbindungen für Vokabulare der Notfalldaten an ein KIS und an ein Arztpraxisinformationssystem gezeigt. Es handelt sich dabei um das ClinicCentre von iSOFT sowie das Arztpraxissystem von Duria. Zudem wurde der Terminologieserver in die FH-eigene Web-Krankenakte ophEPA erfolgreich eingebaut.

Beispiele

1. Die Methode „ListCodeSystems()“ wird aufgerufen, um eine Liste mit allen im Terminologieserver verfügbaren Vokabularen zu erhalten (ohne Anmeldung nur lizenzfreie)
   a. Aufruf: Es werden keine Parameter mitgegeben
   b. Antwort: eine Liste der verfügbaren Ordnungssysteme

2. Die Methode „ListCodeSystemConcepts()“ wird aufgerufen, um alle Konzepte des Vokabulars „ICD 10-GM“ abzurufen
   a. Aufruf: die Vokabular-ID 11 wird mitgegeben (ICD 10-GM, erhalten aus dem vorherigen Aufruf)
   b. Antwort: eine Liste mit verfügbaren Konzepten des ICD 10-GM

3. Die Methode „ReturnConceptDetails()“ wird aufgerufen, um Details zu dem Begriff „Blutegelbefall o.n.A.“ abzurufen
   a. Aufruf: die Konzept-ID 29603 wird mitgegeben (ID erhalten aus dem vorherigen Aufruf)
   b. Antwort: alle Details zum Konzept „Blutegelbefall o.n.A.“

Ein weiteres, vermutlich das am meisten benötigte Szenario wäre die Synchronisation der lokalen mit der globalen Semantik, bezogen auf ein oder mehrere Vokabulare. Hierzu müsste das Primärsystem zu festgelegten Zeiten (z. B. immer nachts um 23 Uhr) die Liste der Konzepte eines Ordnungssystems abrufen, deren Änderungsdatum größer als der letzte Abrufzeitpunkt ist, und dann für diese die Details nachladen. Im Grunde wäre dieser Algorithmus sehr einfach. Die äußere Schleife läuft über die lokalen Ordnungssysteme, die synchronisiert werden sollen, damit die Methode „ListCodeSystemConcepts()“ mit den Parametern Vokabular-ID und ab-Datum aufgerufen werden kann. Die nächste innere Schleife muss dann über die zurück-

gegebenen Konzepte laufen und die Details nachladen. So kann dann in einfacher Weise auch bei zig- bis hundertausenden von Teilnehmersystemen neue oder zu ändernde Semantik einfach deployed werden. Unterjährig z. B. einen neuen ICD-Code wie „Schweinegrippe“ einzufügen, ist dann kein Problem: ein Eintrag im Terminologieserver und alle wissen kurz danach Bescheid. Dass dies z. B. real sein kann, zeigt die Meldung der Ärztezeitung vom 3.5.2009:

Schweinegrippe nun mit ICD-Code von der WHO
KÖLN (ava). Die Weltgesundheitsorganisation (WHO) hat entschieden, dass Influenza-Fälle, die durch eine Infektion mit dem Schweinegrippe-Virus A/H1N1 hervorgerufen werden, mit dem ICD-10-Kode J09 zu kodieren sind. Das teilte das Deutsche Institut für Medizinische Dokumentation und Information am Donnerstag mit.

Der Text zu dieser schon bestehenden Schlüsselnummer J09 (Grippe durch nachgewiesene Vogelgrippe-Viren) wird entsprechend angepasst. Durch den neuen ICD-Code sollen Schweinegrippe-Fälle schnell statistisch identifizierbar sein.

Natürlich ändert sich die ICD nicht laufend, aber für viele kleinere Vokabulare in der Gesundheitstelematik ist eine größere Dynamik zu erwarten.

In der Regel sollten die Primärsysteme in ihrer lokalen Vokabularverwaltung die IDs des Terminologieservers auf jeder Granularitätsstufe mitführen.

Lessons learned

Zusammenfassend können folgende Aspekte genannt werden:

- CTS2 ist ein umfangreicher und exzellenter Standard für die Implementierung eines Terminologieservers.
- Das Klassenmodell von CTS2 ist derart generisch, dass beliebige Ordnungssysteme bis hin zu einfachen Ontologien verwaltet werden können.
- Die Klassifikation der Dienste ist hilfreich und kann auch für andere Diensteserver so übernommen werden.
- CTS2 beschreibt nicht im Detail die Diensteschnittstellen selbst, diese müssen bei der Entwicklung auf Basis des Klassenmodells spezifiziert werden, wofür sich eine Dienste-Attribut-Matrix gut eignet.
- Für einen professionellen kommerziellen Betrieb muss das Klassenmodell um administrative Informationen zu Benutzern und Lizenzinformationen erweitert werden.
- Eine zusätzliche Absicherung der Services mittels WS-Security ist notwendig
- Weitere Erweiterungen des Klassenmodells für Multilingualität und bessere Beschreibung von Beziehungen sind sinnvoll, da rekursive Multilingualität via Cross-Mappings nicht performant ist.
- Die Praktikabilität konnte an zwei beispielhaften Interoperabilitätsszenarien mit Primärsystemen gezeigt werden.
- Ein serviceorientierter Ansatz ist sinnvoll und ermöglicht auch die physische Verteilung von Semantik auf mehrere Terminologieserver, hierfür wäre jedoch ein Broker zu entwickeln.

Zusammenfassung

Die Zurverfügungstellung bzw. Verteilung von Semantik in verteilten Systemen ist für die semantische Interoperabilität und damit für einen wertschöpfenden Betrieb interoperierender Informationssysteme unabdingbar. Hierfür bieten sich Terminologieserver an, für die durch CTS2 ein internationaler Standard vorliegt. Zur Implementierung wurde im konkreten Fall das Klassenmodell des Standards in ein Datenbankmodell überführt und mittels einer Dienste-Attribut-Matrix die Diensteschnittstellen spezifiziert und implementiert. Für einen professionellen Betrieb wurden kleinere Erweiterungen des CTS2-Klassenmodells notwendig. Der realisierte Lösungsansatz wurde anhand eines Szenarios (Nofalldatenvokabulare) mit zwei Primärsystemen evaluiert und kann als gut praktikabel bezeichnet werden. Die Entwicklung des CTS2-Terminologieservers wurde vom Bundesministerium für Gesundheit unterstützt.

Prof. Dr. Peter Haas, Robert Mützner
Fachbereich Informatik, Fachhochschule Dortmund (DE)

Referenzen:

[1] CEN/TC 251. Investigation of syntaxes for existing interchange formats to be used in healthcare. CENT/TC 251/PT 004 Final document. Bruxelles (36 rue de Stassart, B-1050) : CEN/TC 251, 2007-01.

Georg Heidenreich

Klinische Register

Der Artikel führt zunächst in die Aufgaben und Merkmale von klinischen Registern ein und beschreibt dann einige Aspekte im Hinblick auf die elektronische Unterstützung von Registern durch standardisierte Profile der Initiative Integrating the Healthcare Enterprise IHE ([1]).

Abgrenzung und Charakterisierung

Klinische Register sind personenbezogene medizinische Datensammlungen mit genauer Fokussierung auf definierte (Krankheits)fälle, wobei die typische Nutzung lediglich Auswertungen „über alle“ Patienten umfasst und diese Auswertungen prozessual getrennt von der Behandlung der erfassten Patienten erfolgt.

Charakterisierend für klinische Register ist also die Ausrichtung auf eine überwiegende Zahl von lesenden Zugriffen außerhalb des Behandlungszusammenhangs.

Geschickterweise sind die schreibenden Zugriffe zur Erzeugung von Datensätzen meist eng mit der Behandlung verbunden, so dass Doppelerfassung weitgehend vermieden wird. Die Fähigkeit eines klinischen Informationssystems (KIS), passende Meldesätze auszuleiten, kann eine bedeutende IT-Anforderung sein.

Die wichtigste Eigenschaft von klinischen Registern ist die Vergleichbarkeit der erfassten Fälle; diese basiert natürlich auf qualitätsgesicherten Datenfeldern mit definierter Erfassungssystematik, wobei durch registerspezifische Scores für wichtige Felder die ursprünglichen Originaldaten weiter verdichtet und verbessert werden können ([2]).

In diesem Zusammenhang gibt es das Zugriffsszenario der Qualitätssicherung durch die sogenannte „study nurse“ (bei der pflegenden Organisation) mit Zugriff auf den erfassten Fall (Lesen/Schreiben) und sogar auf Quelldaten (Lesen) mit den Aktionen Kontrolleingabe, Korrektur und Freigabe, teilweise bis auf Feldebene.

Warum braucht man ein klinisches Register?

Die systematische Sammlung der Erfahrung von Behandelnden über viele Fälle ist sehr wertvoll zur Verfeinerung der Diagnostik, zur Differenzierung von Krankheitsbildern sowie zur Vorbereitung von Studien zu Therapien.

Eine typische Auswertung ist das Data Mining für die klinische Forschung, zur Findung von Korrelationen (Ursachen) und Wirkungsweisen (Therapie). Diese Ergebnisse müssen durch nachfolgende Studien erhärtet werden, damit sich sichere medizinische Schlüsse ziehen lassen. Besonders Fehlschlüsse aus Ko-Faktoren kann man mit Vergrößerung der Fallzahl im Register prinzipiell nicht aufdecken: Eine geeignete klinische Studie hilft da weiter.

Eine andere Art von Auswertung verfolgt lediglich die Ausbreitung einer Erkrankung aus einer mehr statistischen Sicht, dabei kann die Betrachtung von Korrelationen mit nicht-medizinischen Merkmalen – wie Wohnort, Alter, Beruf, soziales Umfeld, Umweltfaktoren, Freizeitverhalten etc. – bedeutsam sein.

Im Hinblick auf die Ziele späterer (medizinischer) Auswertungen sollten auch nicht zuzuordnende (medizinische) Faktoren im Datenschema berücksichtigt und bei der Meldung erfasst werden.

Eine große Bedeutung für die Qualität der erfassten Datensätze haben standardisierte klinische Terminologien, da sie durch eine systematische Fragestellung und klar definierte Konzepte bereits bei der Erfassung von Fällen hilfreich sind und nach Auswertungen die Interoperabilität bei der weiteren Verarbeitung fördern.

Charakterisierung

Die Aufgabe eines klinischen Registers kann also mit „krankheitsbezogene Beobachtung“ umschrieben werden: Durch die Fallzahl wird der Einzelfall überwunden, allerdings bis zur klinischen Evidenz fehlt noch einiges (an Studien).

Methodisch ermittelter Inhalt von Registern stellt die Vergleichbarkeit von Beobachtungen her, während große Fallzahlen im Register die Wiederholbarkeit von Beobachtungen sichern.

Klinische Register sind in folgenden Situationen besonders geeignet:

- Krankheiten mit hohem Forschungsbedarf (epidemiologisch)
- Verfolgung langandauernder Patientenhistorien
- Erkrankungen mit stark diversifizierten Ausprägungen und Verläufen.

Bedarf in der Epidemiologie

Epidemiologische Register sind für Erkrankungen mit erhöhtem Forschungsbedarf ausgelegt und haben meist ein überregionales Einzugsgebiet (landesweit, auch bundesweit).

Oft ist die Therapieunterstützung eine gewünscht Folge der Auswertungen, jedoch selten für die erfassten Patienten – was zum einen an der Länge der Abläufe vom Fall über die Evidenz bis zur Therapie liegt, zum anderen auch daran, dass die Rückmeldung (etwa über Risiken) teilweise auch für die Patienten und deren Angehörige problematisch sein kann.

Die sogenannten „Kompetenznetze“ zu einem benannten Krankheitsbild arbeiten oft mit eigenen Studienregistern, wobei eben nicht nur seltene, sondern auch häufige Erkrankungen („Volkskrankheiten“) im Fokus sind.

Ein sehr wichtiges Ziel von epidemiologischen Registern ist eine hohe quantitative Abdeckung: Idealerweise werden alle Fälle der Zielgruppe erfasst, um jede Korrelation durch die Auswahl einer Untermenge zu vermeiden ([3]).

Die epidemiologische Auswertung muss regelmäßig vorab im Hinblick auf ethische Aspekte beurteilt werden. Grundsätzlich sind rein epidemiologische Auswertungen nicht ethikkommissionspflichtig, speziell, wenn die Anfragen lediglich anonyme Antworten ohne Datum sowie mit klassifizierten Merkmalen vorsehen.

Speziell hypothesen-gestützte Anfragen an ein klinisches Register machen die Bewertung durch die Ethikkommission notwendig, ansonsten wird gemäß registerspezifischer Genehmigungsprozesse meist ein registerspezifisches „Board“ die Anfrage bewerten.

Abdeckung der Historie

Für die Verfolgung längerdauernder Krankheitsverläufe sind langfristige Register notwendig, die eindeutige persönliche (identifizierende) Merkmale berücksichtigen, damit die Situationen „Umzug“, „Arztwechsel“ und auch „Klinikwechsel“ geeignet verfolgt werden können.

Charakteristisch für langfristige Register ist somit die zusätzliche Erfassung (und gegebenenfalls Pseudonymisierung) von zur Identifikation geeigneten Personendaten – zum Auffinden von bereits erfassten Fällen.

Grundlage der langfristig laufenden Register ist die Verstetigung, d. h. die kontinuierliche Pflege der Register (via Verträge oder gesetzliche Regeln) durch eine Organisation, deren Betrieb nachhaltig gesichert ist.

Die nationale Kohorte

Ein Spezialfall unter den langfristigen Registern ist die vom BMBF geförderte einzurichtende „Nationale Kohorte“ mit einer großen Menge (200.000 Personen) an „gesunden“ – genauer: nicht näher diagnostizierten – Personen als Stichprobe zur Verfolgung von sehr weit verbreiteten („Volks“)krankheiten, zur Ermittlung früh erkennbarer Risikoindikatoren sowie zur Entwicklung von Vorbeugemaßnahmen ([4]).

Man wird ja noch träumen dürfen:
Das ideale Register ([5])

Der – sicherlich unerreichbare – Traum vom idealen Register formuliert die Ziele, die bei Einrichtung und Betrieb klinischer Register nicht aus dem Auge verloren gehen sollten:

- Alle klinisch relevanten Angaben sind als Felder im Datenschema erfasst.
- Alle betroffenen Patienten sind im Register erfasst.
- Der Inhalt kann unabhängig von Abrechnungsfragen erhoben werden.
- Alle medizinischen (oder sonst wie für das Register relevanten) Angaben sind hochstrukturiert und mit standardisierten Terminologien codiert.
- Ein On-demand-Berichtgenerator liefert Daten für die Qualitätsverbesserung.
- Sicherer Zugriff unterstützt die Szenarien Meldung, Erfassung, Pflege, QS-Freigabe, Auswertung, sowie Behandlung.

- Leicht konfigurierbare Schnittstellen erlauben die systematische, interoperable Kommunikation zu anderen IT-Systemen im Gesundheitswesen.
- Kundenspezifisch anpassbare Abläufe, Masken und Schemata machen das Register flexibel.
- Eine „clinical care guidelines"-Rule Engine, die wie ein Arzt denkt, nicht wie ein Rechner, hilft bei Diagnose und Therapie.
- Point-of-care Funktionen machen die Visite wirksamer.
- Automatisierte Werkzeuge übernehmen die Patienteneinbestellung, planen Termine und buchen benötigte Räume.
- Skalierbare Performanz erlaubt „weiches" Wachstum der Bestände und Funktionen.

Anwendbare Regeln

Wie sieht der rechtliche und ethische Rahmen für die Einrichtung und den Betrieb klinischer Register aus? Der Betrieb von Registern wird gefordert von vertraglichen Pflichten der meldenden Stellen sowie deren Anerkennungsvoraussetzungen („Fachzentrum"), gesetzlichen Meldepflichten, speziell für bestimmte Register sowie allgemein von der ärztlichen Ethik im Hinblick auf die bestmögliche Behandlung.

Regelmäßig einschränkend für die Art der Sammlung beziehungsweise Auswertung von Daten in Registern wirken die Aspekte der Vertraulichkeit von personenbezogenen Daten, also die ärztliche Schweigepflicht, die EU-Verfassung (Schutz von persönlichen medizinischen Daten) sowie die national und regional anwendbaren Datenschutzgesetze und Datenschutzregelungen.

Informationstechnische Aspekte

- Die technische Identifikationen durch die Vergabe der OID für ein Register von Objekten (hier: das Register) unterstützt die Interoperabilität. Der Betreiber bzw. die datenverantwortliche Organisation stellt dazu einen Antrag an das DIMDI ([6]), woraufhin das DIMDI eine neue OID vergibt und in einem technischen OID-Index den Servicezugang (URL) und den Kontakt (technischer Administrator des Betreibers) publiziert.
- Definition des Datenschemas
- Einrichtung eines wirksamen Pseudonymisierungsverfahrens (siehe [7], [8])
- Use Cases und Portale für Anlegen, Pflege, QS/Freigabe, Auswertungen, Behandlung: Als Folge der für Register typischen Trennung von Erfassen der Fälle und den Auswertungen findet der erzeugende Prozess wie auch der korrigierende Prozess total getrennt vom typischen lesenden Zugriff statt – und zwar schon auf der Prozessebene.
- Terminologie-Server zur Unterstützung standardisierter klinischer Terminologien
- elektronisch unterstützte Klassifikation/k-Anonymisierung
- nachträgliche Erweiterung des Datenschemas bei Revisionen des Registers

Anwendbare IHE-Profile

Das Profil IHE XDS (Cross-Enterprise Document Sharing) als zentraler Baustein unterstützt die Zusammenführung von verteilt gehaltenen Datensätzen in einer (technischen) „Registry". Für klinische Register sind dabei zwei Varianten denkbar:

a) Die Metadaten der XDS-Registry werden im Hinblick auf das klinische Datenschema des Registers erweitert, so dass die Registry nun wirklich zum Register wird. Diese Konnation machte mich zum Autor dieses Artikels. Dringend zu empfehlen ist dabei die Verwendung von „Stored Queries", denn die Umsetzung von Registeranfragen in Anfragen an ein Datenschema muss unbedingt die Aspekte der Vertraulichkeit berücksichtigen: Eine direkte Eingabemöglichkeit frei formulierter Queries wäre ein Sicherheitsleck.

b) Die Datensätze des Registers werden in einem oder mehreren Repositories gehalten. Die Metadaten enthalten ausdrücklich keine Merkmale des Registers; nur das Pseudonym als einziges fallbezogenes Merkmal. Selbst das Metadatum „Erfassungsdatum" sollte zuvor umgeformt werden. Ohne weitere Maßnahme kommt hierbei dem Repository die Aufgabe der Umsetzung von Anfragen zu; eine Funktionalität die klar über XDS hinausgeht. Eine Abhilfe könnte eine registerspezifische Stelle zur sicheren Generierung von Anfragen sein, als Abweichung vom XDS-Profil bei der Bearbeitung von Queries.

Immer eine gute Wahl ist das Profil IHE ATNA (Audit Trail and Node Authentication) zur standardisierten Knoten- und Benutzer-Identifizierung, wobei die technischen „Benutzer" für Auswertungen wegen der Offenheit der tatsächlich anzunehmenden Auswerter idealerweise Platzhalter für berechtigte Inhaber der Rolle „Auswerter" sein sollten.

IHE PIX (Patient Identity Cross Referencing) realisiert die Generierung von Fall-Identitäten und unterstützt die Pseudonymisierung. Der Akteur „Patient Identity Source" realisiert dabei den PID-Generator. Das Pseudonym kann mit PIX übrigens als „demographisches Merkmal" gespeichert werden, da keine Antworten des PIX-Managers mit solchen Merkmalen vorgesehen sind.

Das Profil IHE EUA (Enterprise User Authentication) beschreibt eine Login-Verwaltung mit der Trennung von „Rechte-Herausgeber" und „geschützter Funktion" im Hinblick auf die Nutzung des sogenannten single-sign-on, etwa für Anfragen in einem System von XDS-Repositories.

Andrew Hinchley

Understanding Version 3

A primer on the HL7 Version 3 Healthcare Interoperability Standard

Normative Edition

4th completely revised edition, 120 pages

The Version 3 development by HL7 represents a major worldwide landmark in the developments of standards for electronic information flows in healthcare. It has already received substantial endorsement in a number of countries and also now forms the basis for an ISO international standard on healthcare message development.

The V3 documentation is substantial and not easy to get familiar with. HL7 UK decided to sponsor the development of this Primer to help its membership get started on V3. Great care was taken in writing and revising the material to ensure that anyone using the Primer should be able to rapidly get to grips with the key elements of the V3 methodology.

Since its original publication in 2003, the Primer has sold more than 2500 copies and has been translated into French and Japanese. During this time the Version 3 standard has changed significantly. This Primer has been completely revised and updated to reflect this and to align with the Normative Edition of the standard. It is essential reading not only for newcomers to HL7, but for purchasers of previous editions of the Primer.

Through this Primer, we hope that many more thousands of people throughout the world will be in a position to understand the implications of HL7 Version 3 and how it can help with development of healthcare communications in their organisation.

Andrew Hinchley
Understanding Version 3
ISBN 3-933819-21-0 • € 26 • please contact us at info@hl7.de for orders

Dank

Diese Arbeit entstand mit viel Hilfe von Frau Prof. Dr. med. Sylvia Thun (Köln), Prof. Bernd Blobel sowie Dr. med. Rainer Röhrig (Gießen), denen ich hier ausdrücklich danken möchte.

Dr. Georg Heidenreich
Siemens AG, Healthcare Sector, Quality & Technology, Erlangen (DE)

Quellen:

[1] Integrating the Healthcare Enterprise Int. (Hrsg.), „Information Infrastructure Domain“: Die genannten IHE-Profile gehören zur Domäne „IT Infrastructure“ und sind unter http://www.ihe.net/Technical_Framework/index.cfm#IT definiert, eine kurze Aufgabenstellung der einzelnen Profile findet man unter www.ihe.net zum Thema „Profiles“.

[2] Paul-Ehrlich-Institut (Hrsg.) „Deutsches Hämophilieregister“ (DHR) unter www.pei.de. Ein Register, dessen Aufgaben und Inhalte gut dokumentiert sind.

[3] Kassenärztliche Bundesvereinigung, Berlin, (Hrsg.), „Arztbibliothek“: www.arztbibliothek.de/themenschwerpunkt/themen-von-a-z/medizinregister. Eine Übersicht über klinische Register gibt die „Arztbibliothek“ unter dem Thema „Medizinregister“. Die Arzbibliothek wird gemeinsam von KBV&BÄK publiziert.

[4] Deutsches Krebsforschungszentrum (Hrsg.), „Die nationale Kohorte“ (auch: Helmholtz-Kohorte) wird unter www.Nationale-Kohorte.de vorgestellt.

[5] Das „ideale Register“ (zumindest als Idee) findet man unter CieloMedSolutions.com, mittlerweile ein Bereich der Advisory Board Company, Washington/DC.

[6] Das Deutsche Institut für Medizinische Dokumentation und Information (DIMDI) im Bereich des BMG präsentiert sich unter dem Auftritt www.dimdi.de und bietet die OID-Vergabe unter www.dimdi.de/static/de/ehealth/oid/index.htm an.

[7] B. Blobel „Die Welt der Privacy- und Security-Standards“ HL7-Mitteilungen, HL7-Benutzergruppe e. V., Köln, 2011. Dies ist ein Beitrag von B. Blobel in diesem Heft zur Vorstellung der Umsetzung von IT-Themen, insbesondere Pseudonymisierung und Anonymisierung.

[8] „Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin.“ beschreiben C.-M. Reng, P. Debold, Ch. Specker, K. Pommerening, erschienen in: Medizinisch-Wissenschaftliche Verlagsgesellschaft, München 2006, ISBN 3939069043.

Tony Schaller

Herstellerunabhängige Konformität von Dokumenten mit medizinischen Inhalten

Mit HL7 CDA, IHE Content Profiles und Schematron heute Realität

Der Einsatz von Standards war in der Vergangenheit nicht immer unproblematisch. Dies insbesondere deshalb, weil die individuellen Softwareentwickler jedes Herstellers klinischer oder medizinischer Softwaresysteme tausende von Zeilen von Spezifikationen nach ihrem Verständnis bestmöglich in die Logik ihrer Applikationen überführen müssen. Ohne die insgesamt großartige Leistung von Programmierern und Softwareherstellern schmälern zu wollen, ist trotz allem guten Willen aller Beteiligten beim Programmieren der entsprechenden Algorithmen ein entsprechender Interpretationsspielraum vorhanden, der sich später hinsichtlich Interoperabilität negativ auswirken kann. Dies ist in der Natur der Sache begründet und betrifft insbesondere den Datenaustausch mit Softwaresystemen anderer Hersteller, aber auch mit anderen Institutionen, welche die gleiche Software einsetzen.

Im Zuge der immer lauter werdenden Forderungen nach betriebs-, regions- und landesübergreifendem Datenaustausch und den zukünftigen, dezentralen, elektronischen Patientendossiers besteht demzufolge auch ein immer größer werdendes Bedürfnis nach Dokumenten mit konformanten medizinischen Inhalten. Weil mit der globalen Mobilität unserer Gesellschaft sich Sender und Empfänger von Dokumenten mit Informationen zum Gesundheitszustand eines Patienten nicht notwendigerweise kennen, sind keine bilateralen Absprachen möglich. Ein zukünftiger Leser eines Dokuments ist also darauf angewiesen, dass das Dokument vom Sender so bereitgestellt worden ist, dass er es auch lesen und verstehen kann, ohne dass dem Dokumentenempfang Verhandlungen oder gar ein Integrationsprojekt vorangegangen sind.

Mit der Bereitstellung von Geschäftsregeln in Form von Schematron und einer dreistufigen, automatisierbaren Validierung von HL7 CDA-Dokumenten ist heute eine herstellerunabhängige Konformanz von Dokumenten mit medizinischen Inhalten möglich. Die HL7-Benutzergruppe Schweiz hat mit CDA-CH-II (eCH-0121) eine weitere Spezifikation publiziert, welche eine Reihe von medizinischen Dokumenten und Formularen, sowie wiederverwendbare Teilbereiche wie z. B. Deklaration von Medikation, Arbeitgeber etc. beinhaltet. Diese Spezifikation wurde mit zahlreichen, praxisbezogenen Beispielen rund um das fiktive Fallbeispiel „Auffahrunfall“ angereichert. Sowohl Spezifikation, wie auch die begleitendenden Beispieldokumente sind auf hl7.ch in Deutsch, Französisch, Italienisch und Englisch publiziert.

▶ Tony Schaller

Nachfolgend werden einige Elemente etwas näher betrachtet, die im Zusammenhang mit der herstellerunabhängigen Konformanz von Dokumenten mit medizinischen Inhalten wichtig sind. Weitere Informationen können im Internet gefunden werden (siehe Kasten).

IHE Content Profiles

IHE (Integrating the Healthcare Enterprise) ist eine internationale Initiative zur Verbesserung des technischen Datenaustausches von IT-Systemen im Gesundheitswesen. Bei IHE geht es nicht darum, neue Standards zu entwickeln, sondern existierende Standards wie zum Beispiel HL7 anzuwenden. Dazu wurden Technical Frameworks (TF) erarbeitet, die beschreiben, wie die existierenden Kommunikationsstandards eingesetzt werden sollen, um einen fehlerfreien Datenaustausch zu ermöglichen. In einem IHE Technical Framework werden in Form von Integrationsprofilen Anwendungsszenarien beschrieben, in denen Interaktionen zwischen mehreren Computersystemen erforderlich sind.

Neben den eigentlichen Transaktionen werden auch Dokumenteninhalte beschrieben. Dazu stellt IHE sogenannte Content Profiles zur Verfügung. Die Content Profiles referenzieren auf den zu verwendenden Standard (heute in vielen Fällen HL7 CDA R2) und deklarieren zusätzlich nebst der gewünschten Struktur des Dokuments auch zwingende und optionale Inhalte sowie zu verwendende Codesysteme. IHE Content Profiles existieren in zahlreichen Technical Frameworks. Aktuelle Beispiele sind etwa die Content Profiles „Immunization Content (IC)“ für Impfdaten im IHE TF „Patient Care Coordination (PCC)“ oder „Dispense (DIS)“,

„Prescription (PRE)“, „Pharmaceutical Advice (PADV)“ für medikamentöse Verordnungen und Abgaben im IHE TF „Pharmacy (PHAR)“.

Mit der Anwendung von IHE-Integrationsprofilen, insbesondere auch der Content Profiles im Gesundheitswesen, kann die Qualität der Patientenversorgung erhöht werden.

Schematron

Schematron ist eine XML-Technologie, die vom World Wide Web Consortium (W3C) definiert und ISO normiert worden ist. Auf eine detaillierte Einführung in Schematron und die Nennung technischer Details wird an dieser Stelle verzichtet. Wichtig erscheint hier vor allem der Zusammenhang zu HL7 CDA und den IHE Content Profiles. Schematron ermöglicht nämlich die automatisierbare Validierung von Geschäftsregeln und damit die Prüfung der Umsetzung von IHE Content Profiles und anderer HL7 CDA Templates wie diejenigen im Fallbeispiel „Auffahrunfall“ rund um CDA-CH-II. Mittels Schematron lassen sich Geschäftsregeln in XML abbilden und automatisiert prüfen. Mittels XML Transformation wird ein XML-Dokument **(Prüfling)** – im vorliegenden Kontext ein HL7 CDA Dokument – über die Schematronregeln **(Geschäftsregeln)** in ein **Prüfresultat** überführt, welches dann ebenfalls im XML-Format vorliegt und deshalb durch eine Software weiterverarbeitet resp. dargestellt werden kann.

Der große Vorteil liegt nun darin, dass die Geschäftsregeln nicht von jedem Softwarehersteller individuell implementiert werden, sondern vom Herausgeber einer Dokumentenvorlage oder eines Formulars definiert werden. Damit liegen die Verantwortlichkeiten an einer einzigen und gleichzeitig an der richtigen Stelle. Softwareprodukte verschiedener Hersteller prüfen mit denselben, identischen Regeln. Der Interpretationsspielraum, der bisher oft zu Unstimmigkeiten geführt hat, wird eliminiert und es liegt auf der Hand, dass damit eine wesentlich höhere Konformanz erreicht wird.

3-stufige Validierung von HL7 CDA-Dokumenten

An den internationalen IHE Connectathons in Europa, Nordamerika und Asien wird die Testsoftware „Gazelle“ eingesetzt. Die Prüfungen von HL7 CDA-Dokumenten, welche nach den Vorgaben der verschiedenen IHE Content Profiles durch Gazelle vorgenommen werden, werden nach folgendem 3-stufigen Validierungskonzept implementiert:

1. Schemakonformität:
Die CDA-Dokumente werden gegenüber dem XML-Schema von HL7 CDA R2 validiert. Damit wird geprüft, ob das Dateiformat korrekt ist und den Vorgaben von W3C (wohlgeformtes XML) und den Vorgaben von HL7 CDA (Schemakonformität) entspricht.

2. Konformität gegenüber dem Modell von HL7 V3 und CDA:
Die CDA-Dokumente werden mittels dem Open Source Produkt CDAInstanceValidator gegenüber dem HL7 Model Interchange Format (MIF) geprüft. Damit wird geprüft, ob die verwendeten Inhalte im Dokument den Vorgaben aus dem HL7 Reference Information Model (RIM) entsprechen. Dabei werden unter anderem auch vorgegebene Wertemengen aus HL7-spezifischen Codesystemen validiert (z. B. Geschlecht, Zivilstand etc.).

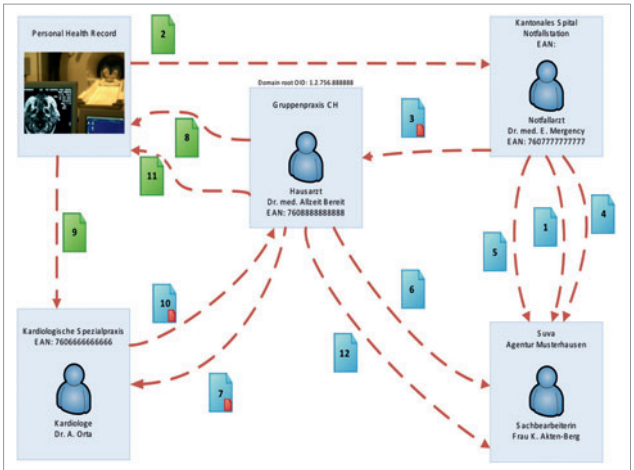
3. Konformität gegenüber den Geschäftsregeln:
Die CDA-Dokumente werden mittels Schematronregeln gegenüber den Vorgaben der verantwortlichen Stellen für die entsprechenden Dokumenteninhalte validiert (z. B. IHE Content Profiles). Damit wird geprüft, ob das Dokument den vom Herausgeber der Vorlage beschriebenen Geschäftsregeln entspricht.

Dieses mehrstufige Validierungsverfahren erlaubt die Sicherstellung einer sehr hohen Konformanz auf hohem Detaillierungsgrad, ohne die Individualität von Dokumentenvorlagen oder Formularen einzuschränken. Hinzu kommt, dass die Validierung vollumfänglich unabhängig von den einzelnen Softwareanbietern durchgeführt werden kann. Bei Anwendung dieses Validierungsverfahrens kann deshalb der Interpretationsspielraum der beteiligten Systeme auf ein noch nie dagewesenes Minimum beschränkt werden.

CDA-CH-II

Die international verfügbaren IHE Content Profiles decken zahlreiche Anwendungsfälle ab. Dennoch existieren in der Schweiz Prozesse, Dokumentenvorlagen und Formulare, für welche keine IHE Content Profiles existieren. Rund um HL7 CDA-CH ist deshalb eine Reihe von helvetisierten CDA-Vorlagen entstanden. Die Arbeitsresultate wurden aus konkreten Anwendungsfällen heraus entwickelt und erarbeitet. Die Arbeitsresultate sind kompatibel zu HL7 und IHE. Durch den Einsatz von CDA-Dokumenten, welche diesen Arbeitsresultaten entsprechen, können wichtige Prozesse wie der Austausch von Medikations- und Notfalldaten oder Unfallversicherungsformulare bezüglich Interoperabilität wesentlich verbessert werden. Nachfolgende Grafik illustriert den Dokumenten-Workflow des Fallbeispiels „Auffahrunfall“, welches als Grundlage für die Entwicklung der heute verfügbaren CDA Templates diente:

Die nachfolgende Abbildung zeigt auf, welche Teile von allgemeinem Interesse sind (blau) und welche nicht von CDA-CH-II behandelt bzw. spezifiziert werden (rot). Im oberen Bereich sind wichtige Dokumenttypen des Unfallversicherers aufgeführt (Arbeitsunfähigkeitszeugnis, ärztlicher Zwischenbericht und HWS-Unfallbericht), darunter im linken Abschnitt die eines Datendienstleisters, welcher Stammdaten für die Medikamentenverschreibung anbietet und rechts daneben die Domäne eines



Legende:

1. Dokumentationsbogen für Erstkonsultation nach kranio-zervikalem Beschleunigungstrauma
2. Auszug aus persönlichem Patientendossier
3. Spitalaustrittsbericht
4. Behandlungsmeldung an die Suva
5. Arbeitsunfähigkeitszeugnis an die Suva
6. Arztzeugnis UVG
7. Untersuchungsanmeldung an Kardiologen
8. Eintrag in persönliches Patientendossier (Diagnosen und Medikamente)
9. Auszug aus persönlichem Patientendossier
10. Befundrückmeldung des Kardiologen an den Hausarzt
11. Eintrag in persönliches Patientendossier (aktualisierte Diagnosen und Medikamente sowie Laborwerte)
12. Ärztlicher Zwischenbericht an die Suva

Abbildung 1: Dokumenten-Workflow Fallbeispiel Auffahrunfall

Notfallkontaktes, der auf Notfalldaten aus einem Patientendossier (unten rechts) angewiesen ist. Basis aller Überlegungen bildet das HL7 Reference Information Model (RIM) und die HL7 Clinical Document Architecture (CDA). Diese dienten dem Bundesverband Gesundheits-IT (bvitg) e. V. in Deutschland (früher Verband der Hersteller von IT-Lösungen für das Gesundheitswesen, VHitG) als Grundlage für die Gestaltung eines CDA-Arztbriefes, der wiederum Pate stand für die Schweizer Spezifikation CDA-CH.

OpenSource Repository

Die HL7-Benutzergruppe Schweiz stellt alle verfügbaren Schematronregeln, XML Stylesheets und Beispiel-CDA-Dokumente in einem OpenSource Repository zur Verfügung (siehe Kasten) und empfiehlt allen Interessierten, diese zu nutzen – sie sind kostenlos, öffentlich und frei verfügbar.

Die HL7-Benutzergruppe Schweiz nimmt gerne weitere Elemente in das Repository auf. Voraussetzung dafür ist, dass diese der Spezifikation CDA-CH-II entsprechen. Wo verfügbar, sollen diese Elemente zusätzlich auf IHE Content-Profiles basieren.

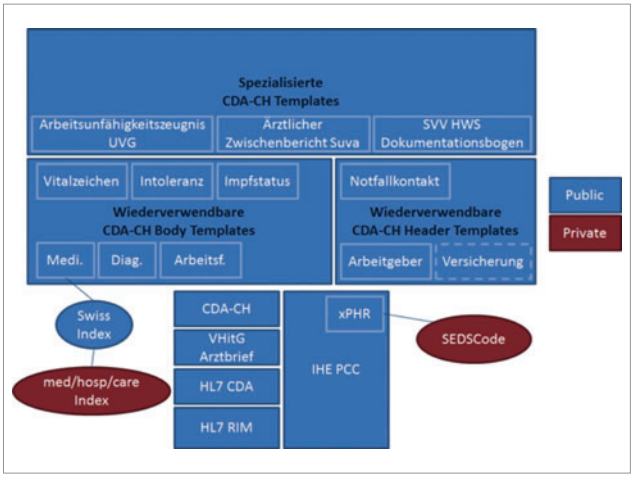


Abbildung 2: Komponenten CDA-CH, Etappe II

Ausblick

Die Projektgruppen rund um die HL7-Benutzergruppe Schweiz widmen sich derzeit der Konkretisierung von Impfungen (elektronischer Impfausweis) und Laborbefunden (insbesondere auch für den Bereich Mikrobiologie). Dabei werden die verfügbaren IHE Content Profiles „Immunization Content" (IC) und „Sharing Laboratory Reports" (XD-LAB) analysiert und gegebenenfalls weiterentwickelt resp. helvetisiert. Darüber hinaus arbeitet die Projektgruppe Labor auch an einem Auftragsverfahren mit HL7 V3 und an der Helvetisierung von Katalogdaten der Laboratorien.

Tony Schaller, medshare GmbH, Thun-Allmendingen, Schweiz
Projektleiter der HL7-Benutzergruppe Schweiz und IHE Suisse

Weitere Informationen

Publikationen der HL7-Benutzergruppe Schweiz:

- CDA-CH und CDA-CH-II Spezifikationen: http://www.hl7.ch/publikationen0
- Supporting Documents: http://www.hl7.ch/publikationen0/cda-templates.html
- Open Source Repository: https://hl7ch.svn.sourceforge.net/svnroot/hl7ch

Weitere Quellen für nützliche Elemente rund um CDA und Schematron:

- ISO/IEC 19757-3:2006 (Schematron): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40833
- CDA Validierung in Gazelle: http://gazelle.ihe.net/node/43
- NIST CDA Guideline Validation: http://xreg2.nist.gov/cda-validation/validation.html
- CDA Validator medshare: http://ws1.medshare.net/xmlvalidator
- Sammlung weiterer nützlicher Links: http://hl7book.net/index.php?title=CDA

Bernd Schütze, Udo Altmann, Frank Oemig

HL7 zur Datenübermittlung in der Onkologie

Die Mission

Derzeit werden in der Onkologie Daten zu Forschungs- und Qualitätssicherungszwecken in verschiedenen Formaten an die jeweiligen Organisationen übermittelt. Typischerweise basieren diese entweder auf dem CSV- oder dem XML-Format, wie die nachstehende Tabelle zeigt:

Empfänger	Datenaustauschformat
Klinische Krebsregister [1]	CSV, XML
Epidemiologische Krebsregister [2]	XML
AQUA-Institut [3]	CSV
Deutsches Onkologie Centrum [4]	XML
Gesellschaft für Pädiatrische Onkologie und Hämatologie [5]	CSV
Kassenärztliche Bundesvereinigung [6]	XML
Kassenärztliche Bundesvereinigung [7]	SCIPHOX
Arbeitsgruppe Tumordatenschnittstellen Niedersachsen [8]	XML

Die in dieser Domäne nicht vereinheitlichten und inkompatiblen Schnittstellen zur Datenübermittlung verursachen daher einen hohen Aufwand bei den Herstellern von Informationssystemen in der Onkologie. Bedingt durch diese Schnittstellenvielfalt und die hohe Komplexität der onkologischen Dokumentation existieren nur wenige elektronische Dokumentationssysteme für die Onkologie, die zumindest einen Teil der Daten zum Export zur Verfügung stellen können.

Aus diesem Grund initiierte die Deutsche Krebsgesellschaft die Einrichtung einer Arbeitsgruppe, welche die Datenübermittlung in der Onkologie optimieren und dabei internationale Standards nutzen sollte. Zur Arbeitsgruppe gehören Mitarbeiter der Datenempfänger, d. h. Mitarbeiter

- der Arbeitsgemeinschaft Deutscher Tumorzentren (ADT),
- der Gesellschaft epidemiologischer Krebsregister in Deutschland e. V. (GEKID),
- des AQUA-Institutes für angewandte Qualitätsförderung und Forschung im Gesundheitswesen GmbH
- der Deutschen Krebsgesellschaft (DKG) sowie
- dem Deutschen Onkologie Centrum (DOC).

Zugleich unterstützen sowohl Mitarbeiter von Herstellern von Informationssystemen in der Onkologie als auch Mitglieder von

Standardisierungsgremien wie IHE und HL7 die Arbeitsgruppe mit ihrem Fachwissen.

Die Arbeitsgruppe soll den Bedarf hinsichtlich der Datenkommunikation analysieren und homogenisieren und daraus ein standardisiertes onkologisches Domänenmodell erstellen. Daraus soll ein generisches Kommunikationsmodell für die Onkologie abgeleitet werden, das auf international anerkannte und verwendete Kommunikationsstandards abgebildet und dann durch die Hersteller von onkologischen Informationssystemen sowie die Datenempfänger implementiert wird. Als Arbeitsgrundlage dienten die Erhebungsbögen der in der Einführung genannten Organisationen. Dies heißt:

- der Basisdatensatz der ADT,
- der organspezifische Datensatz Darm der ADT,
- der organspezifische Datensatz Mamma-CA der ADT,
- der Datensatz Mammachirurgie des AQUA-Instituts,
- der Benchmarking-Datensatz Mammakarzinom des DOC,
- der Benchmarking-Datensatz Darm des DOC und
- der Mindestdatensatz der GeKiD.

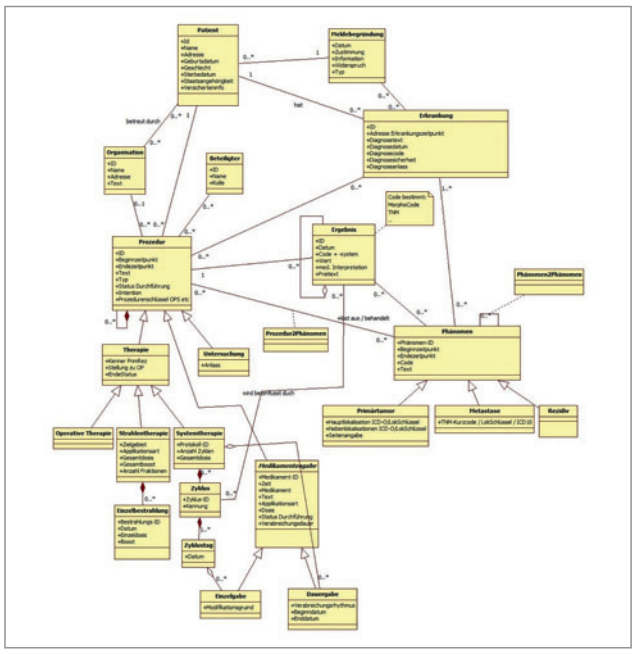


Abbildung 1: Allgemeines Domänen-Modell für die Onkologie

Ergebnisse

Als Zielsetzung für die Arbeiten sollten die Möglichkeiten des internationalen Datenaustausches im Bereich der onkologischen Qualitätssicherung oder Forschung berücksichtigt werden, weshalb der Datensatz auf dem internationalen Standard HL7 basiert. Innerhalb dieses Standards hat die Gruppe sich für die Datenübermittlung mittels CDA (Clinical Document Architecture) entschieden, weil in der Onkologie Daten zu einem Patienten dokumentartig übermittelt werden, sei es als mehr oder weniger strukturierter Arztbrief oder im Sinne einer Meldung an Krebsregister oder Qualitätssicherungsorganisationen. CDA bietet den meldenden Ärzten den großen Vorteil, die zu übermittelnden Daten, die sowohl in Textform als auch strukturiert in den Berichten enthalten sein können, vor dem Versand einzusehen und damit kontrollieren zu können.

In einem Initialtreffen wurden die derzeitigen Anforderungen zusammengetragen und miteinander verglichen. Schnell stellte sich heraus, dass der ADT-Basisdatensatz Angaben enthält, die bei jeder Tumordokumentation benötigt werden. Aus den Angaben wurden entsprechend dem IHE-Weg „Story-Boards“ entwickelt, so dass der Datenfluss in der Onkologie dargestellt wird. In den daraus entwickelten Sequenzdiagrammen wurden Akteure und Nachrichten dargestellt.

Basierend auf den daraus gewonnenen Erkenntnissen und den im ADT-Basisdatensatz enthaltenen Anforderungen wurde ein generisches Domänen-Modell für die Onkologie (s. Abb.1) erstellt. Ausgehend von diesem allgemeinen Modell wurden die organspezifischen Anforderungen hinzugefügt. Hierbei konzentrierte sich die Gruppe zuerst auf die Tumorentitäten Mammakarzinom und kolorektales Karzinom, da die von ADT, DOC und AQUA schon erstellten Ausarbeitungen dafür genutzt werden konnten.

Parallel hierzu entschied sich die Gruppe, die Anforderungen der GEKID als ersten Datensatz beispielhaft für die anderen Anforderungen darzustellen. Da in Baden-Württemberg ein Bedarf bzgl. der Datenübermittlung zum epidemiologischen Krebsregister besteht, wird hier die erste Umsetzung einer HL7-Datenübermittlung im 3. und 4. Quartal 2011 getestet. Bei dieser Umsetzung wird auf die im Diagnoseleitfaden schon erarbeiteten Ergebnisse zur Abbildung onkologischer Diagnosen gemäß der TNM-Klassifikation in HL7 zurückgegriffen [9].

Diskussion

Die unterschiedlichen Datenaustauschformate, welche derzeit zur Qualitätssicherung und Forschung in der Onkologie gegenwärtig eingesetzt werden, erlauben den Softwareherstellern nicht, alle benötigten Schnittstellen im Rahmen einer sinnvollen Kosten-Nutzen-Relation zu berücksichtigen. Hier schafft die Initiative der Krebsgesellschaft mit einem gemeinsamen Datenaustauschformat die Möglichkeit, dass durch eine breitere Umsetzung des Austauschformates durch die Industrie die onkologische Forschung wie auch die Qualitätssicherung in der Versorgung besser untersucht und Optimierungspotentiale aufgezeigt werden können.

Mit der Entscheidung des HL7-Einsatzes zum Datenaustausch steht Deutschland international nicht alleine da. Auch das National Program of Cancer Registries in den USA setzt auf HL7 als Datenaustauschformat [10, 11]. Die North American Association of Central Cancer Registries (NAACCR) hat bei ihren Untersuchungen bzgl. der Nutzung von CDA festgestellt, dass bei den bei ihnen anfallenden Datenmengen unter der Nutzung von CDA zwar die Verarbeitungszeit bzgl. der automatisierten Datenverarbeitung bedingt durch den strukturellen Aufbau der XML-Struktur angestiegen ist, jedoch hinsichtlich der Interoperabilität der Gewinn sehr hoch ist [12].

In der IHE-Domäne „Quality, Research and Public Health (QRPH)“ wird derzeit an einem Profil für Krebsregister gearbeitet: „Physician Reporting to a Public Health Repository – Cancer Registry“ [13]. QRPH wählt einen anderen Weg als die NAACCR, aber es werden auch hier die CDA Content Modules genutzt. Es wird versucht, die Ergebnisse aus Deutschland einzubringen, damit dieses stark auf Amerika zugeschnittene Profil auch international nutzbar wird.

Durch die Abbildung der Anforderungen an einen einheitlichen Datensatz im HL7-Format wird einerseits die Komplexität und damit auch der Aufwand der Schnittstellenimplementierung reduziert, andererseits auch der Internationalisierung sowohl im Bereich der Forschung wie auch der internationalen Qualitätssicherung Rechnung getragen.

Bernd Schütze
Universitätsklinikum Düsseldorf (DE)

Dr. Udo Altmann
Arbeitsgemeinschaft Deutscher Tumorzentren ADT
Klinikum der Justus Liebig Universität, Göttingen (DE)

Dr. Frank Oemig
AGFA HealthCare GmbH, Bonn (DE)

Literatur:

[1] Arbeitsgemeinschaft Deutscher Tumorzentren e. V (ADT) [Online] 2009 [Zitiert 2011-09-07] Verfügbar unter http://www.tumorzentren.de/

[2] Gesellschaft der epidemiologischen Krebsregister in Deutschland e. V. (GEKID) [Online] 2010 [Zitiert 2011 -09-07] Verfügbar unter http://www.gekid.de/

[3] AQUA – Institut für angewandte Qualitätsförderung und Forschung im Gesundheitswesen GmbH – Chirurgie bei Mammakarzinom [Online] 2010 [Zitiert 2011-09-07] Verfügbar unter http://www.sqg.de/ergebnisse/leistungsbereiche/chirurgie-bei-mammakarzinom.html

[4] Deutschen Onkologie Centrum (DOC) [Online] 2010 [Zitiert 2011-09-07] Verfügbar unter http://www.brustcentrum.de/cms/default.aspx?CID=6^

[5] Gesellschaft für Pädiatrische Onkologie und Hämatologie (GPOH): GPOH Basisdatensatz [Online] 2002 [Zitiert 2011-09-07] Verfügbar unter http://www.kinder-krebsinfo.de/e1676/e1806/e5133/index_ger.html

[6] Kassenärztliche Bundesvereinigung (KBV): DMP-Brustkrebs [Online] 2011 [Zitiert 2011-09-13] Verfügbar unter http://www.kbv.de/ita/4287.html

[7] Kassenärztliche Bundesvereinigung (KBV): Hautkrebs-Screening [Online] 2011 [Zitiert 2011-09-13] Verfügbar unter http://daris.kbv.de/daris/link.asp?ID=1003754654

[8] Arbeitsgruppe Tumordatenschnittstellen Niedersachsen. TuDaSch-XML. [Online] 2007 [Zitiert 2011-09-13] Verfügbar unter http://www.mh-hannover.de/7511.html

[9] HL7-Benutzergruppe in Deutschland e. V. – Diagnoseleitfaden. [Online] 2010 [Zitiert 2011-09-08] Verfügbar unter http://www.hl7.de/download/documents/diagnosen/Diagnoseleitfaden-v0.99f.pdf

[10] National Program of Cancer Registries (NPCR) [Online] 2011 [Zitiert 2011-09-07] Verfügbar unter http://www.cdc.gov/cancer/npcr/tools/registryplus/mp.htm

[11] National Program of Cancer Registries (NPCR) – Clinical Document Architecture (CDA) Pilot Project [Online] 2011 [Zitiert 2011-09-07] Verfügbar unter http://www.cdc.gov/cancer/npcr/informatics/cda/index.htm

[12] National Program of Cancer Registries (NPCR): Interoperability Questions and Issues [Online] 2010 [Zitiert 2011-09-07] Verfügbar unter http://www.naaccr.org/LinkClick.aspx?fileticket=g-CQtd3lQIo%3D&tabid=230&mid=679

[13] IHE "Quality, Research and Public Health (QRPH)". Physician Reporting to a Public Health Repository – Cancer Registry. [Online] 2011 [Zitiert 2011-09-08] Verfügbar unter http://www.ihe.net/Technical_Framework/upload/IHE_QRPH_Suppl_PRPH_Ca_Rev2-1_2011-09-02.pdf

Joachim Dudeck Award erstmals vergeben

Anlässlich der International HL7 Interoperability Conference IHIC 2011 in Lake Buena Vista wurde erstmals der Joachim Dudeck Award vergeben. Mit dem Preis, der von nun an jährlich im Rahmen der IHIC im Gedenken an Joachim Dudeck, Gründer, langjähriger Vorsitzender und erstes Ehrenmitglied der HL7-Benutzergruppe in Deutschland e. V. sowie erster Affiliate Director im HL7 Board of Directors und Initiator der Internationalen HL7-Interoperabilitätskonferenzen verliehen wird, werden außerordentliche Leistungen von Nachwuchswissenschaftlern bei der Entwicklung und Implementierung von HL7-basierten Interoperabilitätslösungen sowie für die Förderung der Anwendung von HL7 und seine Harmonisierung mit anderen Standards gewürdigt. Der erste Preisträger ist Mario E. Cortés aus Cali, Kolumbien, Mitglied des dortigen Affiliate, der mit seinen Koautoren Diego M. Lopez und Bernd Blobel für den Beitrag „The Unified File Format for HL7 Electronic Documents – DUFF" ausgezeichnet wurde.

Mario E. Cortés aus Cali, Kolumbien

Integrierte IT-Lösungen von Agfa HealthCare

ORBIS NICE 360°

Die 360° Sichtweise wird bei Agfa HealthCare GROSS geschrieben!

ORBIS von Agfa HealthCare ist das ganzheitliche System zur Steuerung Ihrer Klinikprozesse. Diese einzigartige Applikationslandschaft für das Gesundheitswesen wird heute bereits in 950 Krankenhäusern von über 500.000 Anwendern täglich genutzt.

Mit ORBIS sind Sie schon heute auf die Zukunft bestens vorbereitet – hin zu übergreifenden Prozessabläufen mit Blick auf klinische Behandlungspfade, Integrierte Versorgung und die Bildung von Medizinischen Versorgungszentren.

Die 360° Sicht bezieht auch unsere Speziallösungen für Intensivmedizin und Diagnostik (Radiologie, Kardiologie u.a.) mit ein, womit Agfa HealthCare einmal mehr Maßstäbe setzt.

Nehmen auch Sie uns beim Wort und lassen Sie ORBIS zum Fundament Ihrer krankenhausweiten Informationslogistik werden. Selbstverständlich mit Integration Ihrer bereits bestehenden IT-Systeme, falls Sie sich von diesen nicht trennen wollen.

ORBIS. Ein System. Eine Philosophie. Ein Gesicht.

Schulungen

Hinweis: In der ersten Hälfte des Jahres 2012 (genaue Termine werden noch bekannt gegeben) veranstaltet das Zentrum für Telematik im Gesundheitswesen ZTG (Bochum) in Zusammenarbeit mit Ringholm bv zwei Kurse in Deutschland:

8.– 9. Mai 2011
Einführungsseminar in HL7-Version 2.x

13. – 14. Juni 2011
HL7-Version 3 und CDA

Termine:

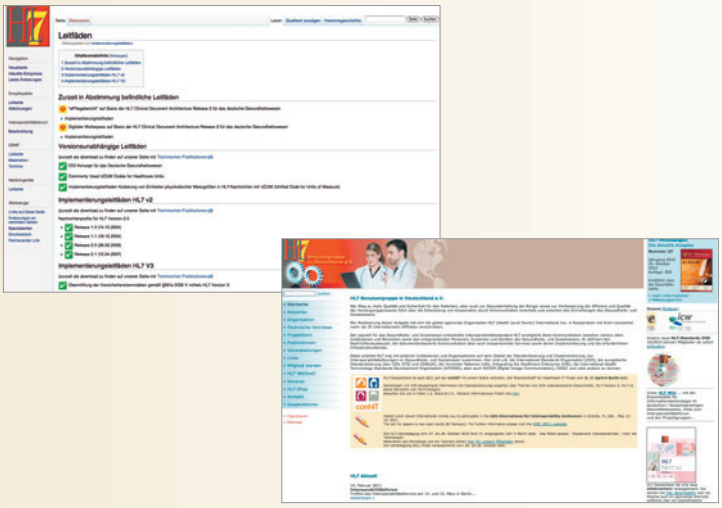
20. März 2012
An Overview of Healthcare Interoperability Standards, Thun (CH)

21. – 22. März 2012
HL7-Version 3 und CDA, Thun (CH)

Besuchen Sie unsere
HL7-Internetseiten unter

www.hl7.de
wiki.hl7.de
online

mit weiteren interessanten Informationen.



Stefan Benzschawel

HL7 Luxemburg stellt sich vor

Die kürzlich gegründete „HL7 Luxemburg“ bedankt sich ganz herzlich für die freundliche Aufnahme als neue Affiliation. Eine vorzügliche Starthilfe durch Stefan Sabutsch (HL7 Austria) und Bernd Blobel (HL7 Deutschland) haben wir sehr gerne angenommen. Besonderer Dank gebührt Bernd für die unkomplizierte und herzliche Einbeziehung in die etablierten HL7-Mitteilungen.

HL7 Luxemburg wurde im November 2010 als Verein ohne Gewinnzweck unter Luxemburger Recht registriert. Seit April 2011 ist HL7 Luxemburg eine offizielle HL7 Affiliation.
Die Vereinigung hat ihren Sitz in L-1852 Luxembourg, 2A, rue Kalchesbrück. Die Organe des Vereins sind die Generalversammlung, der Vorstand, der Rechnungsprüfer, die Technischen Komitees und die Arbeitsgruppen.

Gründungspräsident ist Stefan Benzschawel; Stefan ist zudem Projektleiter für eHealth beim öffentlichen Forschungsinstitut CRP Henri-Tudor. Vize-Präsident ist René Krippes; René ist ferner Koordinator der eHealth Projekte im Luxemburger Gesundheitsministerium.

HL7 Luxemburg hat zur Zeit über 20 Mitglieder, darunter die Vereinigung der Luxemburger Kliniken, die Vereinigung der Labore, mobile Pflegedienste, Kliniken, Labore, Pflegeeinrichtungen, die Luxemburger Gesundheitskasse, IT-Beratungsgesellschaften, Forschungseinrichtungen sowie private Mitglieder. Der Gesundheitsminister unterstützt HL7 Luxemburg.

Stefan Benzschawel
Vorsitzender HL7 Luxemburg

www.hl7.lu
Health Level Seven Luxembourg a.s.b.l.
2A, rue Kalchesbrück
1852 Luxembourg
contact@hl7.lu

Die Themen der nächsten Ausgabe sind voraussichtlich:

- **National und International: Übermittlung von Diagnosen in HL7-Version 3**
- **Leitfäden auf der Basis der Clinical Document Architecture (CDA)**
- **Kodes, Kodesysteme und Value Sets**
- **Aktivitäten der Working Group Meetings und des Interoperabilitätsforums**

... und anderes mehr

www.hl7.de · www.hl7.at · www.hl7.ch · www.hl7.lu

Alexander Mense, Stefan Sabutsch

Start des OID-Portals für das österreichische Gesundheitswesen

Nach einer zweijährigen Vorbereitungsphase mit Konzeption, Konsultationsverfahren und Implementierung hat am 1. August 2011 das OID-Portal für das österreichische Gesundheitswesen seinen Betrieb aufgenommen.

Entwicklung

Objekt Identifier (OID) stellen bei der Errichtung von eHealth-Infrastrukturen ein zentrales Basiselement dar. Die im ISO/IEC Standard 9834-1 [ISO/IEC 9834-1] spezifizierten und für Österreich in der ÖNORM A 2642 [ÖNORM A 2642] detaillierten, global eindeutigen und zeitlich unbeschränkten Identifikatoren dienen zur eindeutigen Kennzeichnung von fast allen Objekten im elektronischen Gesundheitsdatenaustausch – so werden z. B. Organisationen, Personen über Codelisten bis hin zu Dokumenten mit Hilfe von OID eindeutig identifiziert. OID spielen in der HL7 CDA-Welt und im Rahmen der Integrationsprofile der IHE eine zentrale Rolle.

Nachdem in einem Beschluss der österreichischen Bundesgesundheitskommission im Jahr 2007 die Verwendung von CDA-Dokumenten und IHE-Profilen als Basiskomponenten bei der Errichtung der österreichischen elektronischen Gesundheitsakte (ELGA) festgelegt wurde, war der Aufbau einer zentralen Verwaltung für OID im österreichischen Gesundheitswesen eine logische Folge und ein weiteres Teilchen auf dem Weg zur österreichischen eHealth-Infrastruktur.

Im Auftrag des österreichischen Ministeriums für Gesundheit wurde 2009 in einer Zusammenarbeit zwischen der HL7-Anwendergruppe Österreich und der Technikum Wien GmbH mit der Konzepterstellung begonnen. In das Konzept sind (neben den normativen Vorgaben) sowohl zu der Zeit aktuelle internationale Entwicklungen (wie z. B. [ISOTC215-NWIP679]) als auch Erfahrungen und Planungen aus Deutschland eingeflossen (besten Dank an dieser Stelle an die Kolleginnen und Kollegen der HL7 Deutschland für die Unterstützung). Nach Abschluss der Erstversion des Konzeptes gab es 2010 ein Konsultationsverfahren in dem alle Stakeholder zu einer Stellungnahme eingeladen wurden und welches in der finalen Version des Konzepts mündete.

Wesentliche Elemente waren:

- Errichtung einer zentralen eHealth-Stammregistrierungsstelle (EHSREG) zur Verwaltung des OID-Unterbaums „eHealth-Austria“ (1.2.40.0.34)
- Regelwerk für Strukturierung und Verwaltung von OID im österreichischen Gesundheitswesen
- Vorgaben für ein nationales OID Repository und OID-Portal

OID-Portal

Ausgehend von der finalen Konzeptversion wurde ein Pflichtenheft für die Umsetzung des OID Repository und dessen öffentlichen Zugang über ein OID-Portal erarbeitet und umgesetzt. Mit 1. August 2011 wurde das OID-Portal auf der zentralen österreichischen Gesundheitsplattform http://www.gesundheit.gv.at im Bereich „Gesundheitssystem“ veröffentlicht.

Das OID-Portal bietet Funktionalitäten für drei verschiedene Benutzergruppen:

- Beantragungs- und Suchfunktionen OID-Anwender
- Selbstverwaltungsfunktionen für Organisationen, die Inhaber einer OID aus dem Unterbaum „eHealth-Austria“ sind
- Administrationsfunktionen für die EHSREG

Über den öffentlich zugänglichen Teil des OID-Portals stehen ein OID-Überblick in Form einer Baumdarstellung sowie eine Suchfunktion zur Verfügung. Des Weiteren können neue OID beantragt oder bestehende OID, welche von anderen Registrierungsstellen wie z. B. der HL7 vergeben wurden und im österreichischen Gesundheitswesen Verwendung finden sollen, gemeldet werden.

Abbildung 1: OID-Portal Baumansicht

Organisationen, die eine OID aus dem „eHealth-Austria“-Baum besitzen, haben die Möglichkeit, in „ihrem“ Unterbaum selbst OID zu vergeben. Zur Verwaltung und Veröffentlichung dieser stellt das OID-Portal in einem geschützten Bereich entsprechende Funktionen zur Verfügung.

Für die österreichische EHSREG ist das OID-Portal die zentrale Verwaltungsplattform für alle OID im österreichischen Gesundheitswesen. Sämtliche benötigte Funktionalitäten wie die Bearbeitung von Anträgen und Meldungen, Neuerfassungen oder Statusänderungen etc. sind in dem Portal abgebildet.

Abbildung 2: Erfassung eines Antrags für eine OID

Schnittstellen

Das OID-Portal wurde in enger Kooperation mit der Entwicklung des österreichischen Gesundheitsdiensteanbieter-Index (GDA-I) erstellt, welcher im letzten Quartal 2011 in Betrieb gehen soll und alle Gesundheitsdiensteanbieter (GDA) Österreichs beinhalten wird. Jeder dieser GDA erhält eine eigene OID aus dem „eHealth-Austria“-Baum, welche von der EHSREG über das OID Repository vergeben wird. Zu diesem Zweck wurde zwischen GDA-I und OID-Portal eine elektronische Schnittstelle implementiert.

Betrieb

Mit der Inbetriebnahme des Portals wurde das finale OID-Konzept zu einer ersten Version der OID-Leitfadens [BMG2011], der den Umgang mit OID im österreichischen Gesundheitswesen vorgibt.

Das OID-Portal befindet sich bis Ende November in einer Pilotphase und wird mit 1. Dezember 2011 den tatsächlichen Echtbetrieb aufnehmen. Das Portal ist unter der Adresse https://www.gesundheit.gv.at/OID_Frontend/ erreichbar.

Alexander Mense, Stefan Sabutsch
HL7-Anwendergruppe Österreich, Eggenberger Allee 11, 8020 Graz (AT)

Referenzen:

- [ISO/IEC 9834-1]
  ISO/IEC 9834-1 Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree, 2009.
- [ÖNORM A 2642]
  ÖNORM A 2642, Informationstechnologie - Kommunikation offener Systeme – Verfahren zur Registrierung von Informationsobjekten in Österreich, 2011.
- [ISOTC215-NWIP679]
  ISO/TC 215 / SC WG3 NWI Proposal 679, ISO/NWIP/TS Health Informatics – Guidance for maintenance of Object Identifiers OID, 2008.
- [BMG2011]
  Österreichisches Bundesministerium für Gesundheit: Leitfaden Object Identifier (OID) für das österreichischen Gesundheitswesen, Version 1.0.0, 2011.
  http://www.gesundheit.gv.at/, 23.09.2011

Peter Seifter

Zwischenbericht des ersten HL7-e-Learning-Kurses in Österreich

Als weitere Aktivität zur Nutzung von Standards im Gesundheitswesen wurde von der HL7-Anwendergruppe Österreich zu Jahresbeginn beschlossen, erstmalig im deutschsprachigen Raum den HL7-e-Learning-Kurs (Global Release 2011) anzubieten. Ziel des Kurses ist die Vermittlung von Konzepten für den Austausch von elektronischen Gesundheitsinformationen um die korrekte Implementierung von Standards (HL7-Standards V2, V3 und CDA) im Gesundheitsbereich zu erleichtern. Damit sollen Applikations- und Software-Entwickler, IT-Consultants, Software-Lieferanten und andere Interessierte angesprochen werden.

Im HL7-e-Learning Kurs lernen die Teilnehmer/innen in 14 aufeinander aufbauenden Themengebiete folgende HL7-Details kennen:

- Überblick über die gebräuchlichsten HL7-Standards
- Standards für semantische Interoperabilität (HL7-Vokabulare: LOINC, Snomed, ...)
- XML- und UML-Repräsentation
- Grundlagen des HL7-V2-Nachrichtenmodells (Nachrichtenbeziehungen, Trigger Events und Nachrichten)
- Z-Segmente und Implementierungsrichtlinien
- HL7-Referenzinformationsmodell V3-RIM
- Grundlagen von HL7-V3-Messaging
- CDA R2 Basis-Architektur
- CDA-Implementierung und Anleitungen

In „Web-based Workshops“ werden geführte Übungen mit praktischen Beispielen („Learning by doing“) abgewickelt. Eine typische Kurseinheit startet mit einer Selbststudium-Session und geht dann in die Lösung praktischer Beispiele über. Der Lernfortschritt wird mit Selbstevaluierungstests laufend überprüft. Zertifizierte Tutoren betreuen die Studierenden während der gesamten Seminardauer und beurteilen den Lernfortschritt zu jeder Kurseinheit. Die Kommunikation der Teilnehmer/innen untereinander als auch mit den Tutoren wird durch Diskussionsforen gesichert.

Im ersten Schritt konnte durch die kooperative Zusammenarbeit mit HL7 Argentina die aktuelle Version des HL7-eLearning-Kurses in die web-basierte e-Learning-Plattform Moodle übernommen werden und mit der Life Long Learning Academy Technikum Wien ein wichtiger Partner mit großer Erfahrung bei Ausbildungen im eHealth-Bereich gewonnen werden. Gemeinsam konnte der erste HL7-e-Learning-Kurs am 16. Mai erfolgreich mit 30 Teilnehmern/innen gestartet werden. Durch die Sommermonate bedingt, wurde der gesamte Kurs in 2 Blöcke mit jeweils 7 Kurseinheiten geteilt. Mittlerweile starten alle Teilnehmer nach der positiven Absolvierung des ersten Blocks mit den fortgeschrittenen Themen in den zweiten Block.

Mit dem erfolgreichen Kursabschluss haben alle Teilnehmer/innen die Möglichkeit ein international anerkanntes Zertifikat zu erwerben und damit ihre Expertise zu stärken.

Besonders erfreulich ist die hohe Beteiligung der Mitglieder der HL7-Anwendergruppe Österreich und das breite Spektrum der Teilnehmer/innen. Die HL7-Anwendergruppe Österreich möchte diese Aktivitäten zukünftig weiter ausbauen und plant aufgrund der aktuellen Nachfrage ein weiteres Kursangebot mit Jahresbeginn 2012.

Dr. Peter Seifter
HL7-Anwendergruppe Österreich,
Eggenberger Allee 11, 8020 Graz (AT)

Thomas Wälti

OID-Portal für eHealth Schweiz

Im Jahr 2010 hat eHealth Suisse, das Koordinationsorgan von Bund und Kantonen, ein OID-Konzept für das Schweizer Gesundheitswesen ausgearbeitet. Dieses Dokument bildet die Grundlage der OID-Registrationsstelle in der Schweiz und beinhaltet alle wesentlichen Konzeptelemente, mit denen ein Inhaber einer OID vertraut sein muss. Grundlage dafür waren die mehrjährigen Erfahrungen von HL7 Schweiz beim Aufbau und Betrieb ihrer Registrationsstelle.

Seit Anfang 2011 verwaltet nun die Stiftung RefData unter http://oid.refdata.ch den OID-Knoten „eHealth-CH; 2.16.756.5.30“ als offizielle Registrationsstelle für eHealth in der Schweiz. In einer gemeinsamen Erklärung begrüßten das Bundesamt für Gesundheit (BAG), die Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (GDK) sowie das Koordinationsorgan Bund-Kantone („eHealth Suisse“) diese Branchenlösung. Sie empfehlen allen Anwendern und Herstellern von IT-Systemen, Objekte und Objektdomänen des Schweizer Gesundheitswesens in Zukunft ausschließlich unter dem OID-Knoten „eHealth-CH“ zu registrieren.

Die Stiftung RefData ist eine nicht profitorientierte Organisation, die das Ziel verfolgt, für die Schweiz volkswirtschaftlich relevante Referenzierungssysteme aufzubauen und zu betreiben. Die einheitliche Registrierung von Objektidentifikatoren vereinfacht den elektronischen Datenaustausch, da keine gesonderten Absprachen zwischen Sender und Empfänger notwendig sind.

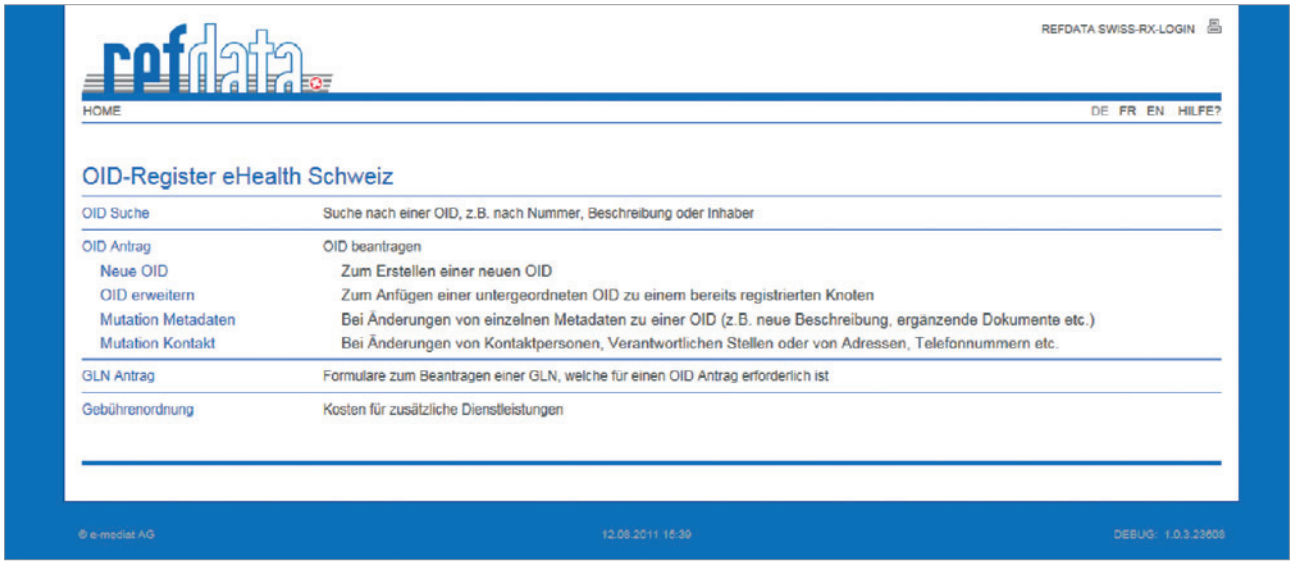
Die operative Verantwortung für den Aufbau und den Betrieb der entsprechenden Stammregistrierungsstelle und für den OID-Knoten hat RefData an e-mediat AG übertragen. Dabei stützt sich e-mediat in ihrer Tätigkeit auf die Erfahrung und Vernetzung von GS1, dem Kompetenzzentrum der Schweizer Wirtschaft für globale Identifikationsstandards und Datenaustausch.

Das OID-Portal bietet alle wesentlichen Funktionen, um eine OID zu suchen, zu beantragen oder zu mutieren. Nach der Aufschaltung der Webapplikation Anfang 2011 erfolgte im Sommer 2011 die Bereitstellung einer aktualisierten Version, die neu auch Webservices anbietet, um die wesentlichen Funktionen auch zwischen Maschine und Maschine ausführen zu können. Ein wesentliches Ziel ist dabei die Interoperabilität zwischen unterschiedlichen Registrationsstellen – zu diesem Zweck berücksichtigen die Webservices den Draft Standard ISO TC 215 - ISO TS 13582 ([1]), wie er in Österreich und Deutschland ebenfalls im Aufbau begriffen ist.

Thomas Wälti
e-mediat, Bern (CH)

Referenzen:

[1] http://wiki.hl7.de/index.php/ISO_TC_215_-_ISO_TS_13582



Stefan Benzschawel

Konzept der eHealth-Plattform für Luxemburg

Im Dezember 2010 ist in Luxemburg ein Gesetz zur Reform der IT-Systeme im Gesundheitswesen in Kraft getreten. Unter anderem wird dort die Bereitstellung eines nationalen, elektronischen Patientendossiers auf einer elektronischen Plattform geregelt. Seit zwei Jahren laufen erste Projekte. Die aktuellen Konzepte sind nach vorheriger Absprache mit dem Luxemburger Datenschutz vor kurzem einer breiten Öffentlichkeit vorgestellt wurden.

Regionale und nationale eHealth-Plattformen werden derzeit vielerorts diskutiert und forciert. HL7 Luxemburg nimmt dieses Thema nun gerne als Anlass, sich der Community der HL7-Mitteilungen vorzustellen und die in Luxemburg geplante eHealth-Plattform im Überblick zu erläutern.

Gleichzeitig möchten wir den Leser um jegliches Feedback bitten. Verbesserungsvorschläge, das Aufzeigen von Ähnlichkeiten zu anderen Projekten bis hin zu eventuellen Anregungen zur Kooperation mit anderen Projekten sind explizit erwünscht. Das Konzept erhebt keinesfalls den Anspruch, neu zu sein. Es werden bekannte Profile des Datenaustauschs und des Informations-Sharing kombiniert mit Pseudonymisierung und zweistufiger Verschlüsselung.

Rahmenbedingungen einer eHealth-Plattform:

Die Vorteile in Luxemburg sind: überschaubare Größe von etwa 500.000 Einwohnern, nur eine gesetzliche Krankenkasse, kurze Wege in der Bürokratie, gelebte Kooperation aller Beteiligten, kein dominantes Marktinteresse großer Healthcare IT Player – mangels zu erwartendem „big business“ und als explizite Zielsetzung das Wohl der Patientinnen und Patienten. Ausgestattet mit diesen guten Vorbedingungen konnte das Gesundheitsministerium zusammen mit dem Forschungszentrum Henri-Tudor und der Krankenhausvereinigung EHL eine Lösung finden, die eine pragmatische Abwägung zwischen Kosten und Nutzen erlaubt, den Schutz der Privatsphäre garantiert und statistische Auswertungen dennoch ermöglicht.

Der Nutzen

Der erste Nutzen einer nationalen eHealth-Plattform und des damit ermöglichten Austauschs relevanter Informationen ist die Verbesserung der Versorgungsqualität und die Reduzierung doppelter, teilweise sehr belastender Untersuchungen.

Weiterhin kann ein Arzt den Patienten im Kontext seiner gesamten Krankengeschichte deutlich besser behandeln. Dies ist ansonsten nur einem langjährigen Hausarzt in dieser Qualität möglich. In Zukunft werden Entscheidungsunterstützende Systeme (Decision Support Systems) basierend auf den Informationen des Patienten-Records den Weg zur personalisierten Medizin ermöglichen.

Neben diesen direkten Vorteilen für den einzelnen Patienten werden statistische Auswertungen von Diagnosen und Behandlungsverläufen zu neuen Erkenntnissen führen, die für die Zukunft die Behandlungsqualität aller Patienten stetig verbessern.

Die Gefahren und deren Eliminierung

Daten bereithalten und Informationen austauschen setzt gegenseitiges Vertrauen voraus, aber es erhöht auch das Risiko von Datenmissbrauch. Der Zugriff von Versicherungen, Banken, Arbeitgebern etc. ist per Gesetz verboten. Dennoch müssen illegale Angriffe auch technisch ausgeschlossen werden. Letzteres Ziel war das zentrale Anliegen beim Design der eHealth-Plattform.

Eckpunkte der eHealth-Plattform

Zur Authentifizierung der Benutzer werden sogenannte Zertifikate eines Trustcenters (gehalten z. B. auf Smartcards) verwendet. Alle Benutzer sind zudem mit ihren jeweiligen Rollen (z. B. als Arzt mit medizinischer Disziplin, als Patient, als Klinik) bei der Plattform registriert. Vom Trustcenter wird somit der Zertifikats-Inhaber als Person oder Institution authentifiziert, während die Benutzerverwaltung der Plattform darauf basierend die Rolle des Zertifikats-Inhabers bezüglich der Plattform hinterlegt hat.

Die Plattform besteht aus zwei unabhängig verwalteten Serverbereichen. Ein Trusted Third Party Provider (TTP) weist den patienten-identifizierenden Daten (Name, Geburtsdatum, Sozialversicherungs-Nummer etc.) zufällig erzeugte Pseudonyme zu. Ein Pseudonymized Medical Information Provider (PMIP) verwaltet, assoziiert zu den Pseudonymen die Metadaten der medizinischen Informationen und die verschlüsselten medizinischen Informationen selbst. PMIP besteht aus einem zentralen Register mit angeschlossenen Repositories.

Legitimierte Benutzer selektieren zuerst den Patienten bei der TTP, dann die gewünschten medizinischen Informationen beim PMIP. Für den Benutzer ist diese Zweiteilung natürlich transparent. Die Selektions-Möglichkeiten beim PMIP sind dabei beschränkt auf die hinterlegten Metadaten (z. B. Laborbefund vom 15. Juli 2011) und den darauf aufgebauten Strukturen des Health-Records. Eine verwendete zweistufige Verschlüsselung erlaubt anschließend die effiziente Umschlüsselung der medizinischen Informationen für den anfragenden Benutzer. Die Zweistufigkeit verhindert die Offenlegung während der Umschlüsselung, bietet also Schutz vor einem illegal agierenden Administrator oder einem Eindringling mit administrativen Rechten.

Bemerkung: Umschlüsselungen sind notwendig, da die potentiellen Nutzer der Daten zum Zeitpunkt der Bereitstellung der Daten noch nicht bekannt sind. Die Weitergabe erfolgt nur aufgrund signierter Anfragen vorher registrierter Benutzer. Strikte Beachtung der hinterlegten Patienten-Zustimmung ist Voraussetzung jeglicher Weitergabe.

Zusammengefasst kann man sagen: Zertifikate und Benutzerverwaltung sichern den Zugang zur Plattform. Pseudonymisierung schützt die Metadaten und erlaubt die Suche nach Patienten auf TTP-Seite und die Suche nach medizinischen Informationen anhand der Metadaten auf PMIP-Seite. Die Verschlüsselung schützt die medizinischen Informationen selbst.

Standards und Profile

Das vorgestellte Plattform-Konzept basiert auf allgemeinen Standards zur Informationsbereitstellung und zum Informationsaustausch zwischen medizinischen und pflegerischen IT-Systemen. Basis ist das IHE XDS-Profil und die verwandten Plattform-Profile XDR, NAV, XCA, XDS-I, die Sicherheitsprofile ATNA, CT, die Benutzeridentifizierungs-Profile XUA, XUA++, Patienten-Identifizierungs-Profile PIX, PAM, PDQ, XCPD.
Das Consent-Management-Profil BPPC geht nicht weit genug. Das Content-Profil XDS-MS wird proprietär erweitert. Andere identifizierte Lücken werden vorerst mittels eines Connectors zwischen den Primärsystemen und der eHealth-Plattform überbrückt.

Nicht so technisch ausgedrückt verwendet die eHealth Plattform ein zentrales Register und mehrere zentrale sowie mehrere dezentrale Repositories. Die aus Sicht der Plattform dezentralen Repositories befinden sich innerhalb der Kliniken (DMZ). Einträge im zentralen Register verweisen dann z. B. in die Kliniken, wo die verschlüsselten Dokumente zu finden sind. Wesentliches Kriterium für den Datenschutz ist die Verschlüsselung aller medizinischen Daten in den Repositories.

Ausblick

Basierend auf dem technischen Plattformkonzept wird ein Prototyp entwickelt, der die technische Machbarkeit demonstriert. Erste Proof-of-Concepts sind bereits erfolgreich abgeschlossen. Ein Anforderungsdokument mit den notwendigen Erweiterungen der IHE-Profile und der besonderen Behandlung von HL7 CDA-Dokumenten ist in Planung. Für eine Übergangszeit werden Connectoren die pragmatische Anbindung der Daten-Provider und der Benutzer an die Plattform ermöglichen. Fernziel ist hier ein konstruktiver Einfluss auf die (vorläufig proprietär) modifizierten Standards und die eventuelle Erweiterung der IHE-Profile. Eine ausführliche Beschreibung der Plattform sowie eine PPT-Präsentation ist auf Anfrage verfügbar (Kontakt: Stefan.Benzschawel@tudor.lu oder Rene.Krippes@ms.etat.lu). Gerne werden wir in einer der nächsten HL7-Mitteilungen mehr Details vorstellen.

Dr. Stefan Benzschawel
Vorsitzender HL7 Luxembourg

Liste der Förderer, korporativen Mitglieder und Ehrenmitglieder HL7-Deutschland

Förderer
- Agfa HealthCare GmbH, Bonn
- Health-Comm GmbH, München

Korporative Mitglieder
- Abbott GmbH & Co KG, Wiesbaden
- Acutronic Medical Systems AG, Hirzel (Schweiz)
- AGH Diagnostics GmbH, Hamburg
- AIS GmbH, Kassel
- Asklepios Kliniken Hamburg GmbH, Hamburg
- astraia software gmbh, München
- atacama Software GmbH, Bremen
- Atelion GmbH, Hamburg
- Avaya Deutschland GmbH, Düsseldorf
- BG-Kliniken Bergmannsheil, Bochum
- bioscientia GmbH, Ingelheim am Rhein
- c.a.r.u.s HMS GmbH, Norderstedt
- C&S Computer und Software GmbH, Augsburg
- CareFusion Germany 234 GmbH, Höchberg
- careon GmbH, Tübingen
- Carestream Health Deutschland GmbH, Aschaffenburg
- Carl Zeiss Medical Software GmbH, München
- Cerner Deutschland GmbH, Idstein
- Charité – Universitätsmedizin Berlin, Berlin
- CHILI GmbH, Heidelberg
- Cibait AG, Bexbach
- CIBS GmbH, Hamburg
- Coach IT GmbH, Kassel
- CoM.MeD GmbH, Barleben
- CoM.MeD GmbH, Dortmund
- COMO Computer & Motion GmbH, Raisdorf
- CompuGroup Beteiligungsgesellschaft mbH, Hattingen
- Computer konkret AG, Falkenstein
- Conworx Technology GmbH, Berlin
- COPRA System GmbH, Sasbachwalden
- CORTEX Software GmbH, Offenburg
- CS Consulting GmbH, Berlin
- cusanus trägergesellschaft trier mbH, Trier
- custo med GmbH, Ottobrunn
- d.velop AG, München
- DATAGROUP GmbH, Pliezhausen
- Deutsche Rentenversicherung Bund, Berlin
- Deutsches Herzzentrum Berlin, Berlin
- Diakonie-Krankenhaus Harz GmbH, Elbingerode
- Diakoniekrankenhaus gGmbH, Rotenburg
- Digital Medics GmbH, Dortmund
- DIMDI, Köln
- DMI GmbH & Co KG, Münster
- Dorner GmbH & Co KG, Müllheim
- DRK Kinderklinik Siegen gGmbH, Siegen
- Dt. Krankenhausgesellschaft e. V., Berlin
- Dt. Rentenversicherung Nordbayern, Bayreuth
- DURIA eG, Düren
- DYNAMED GmbH, Berlin
- e-conmed· GmbH, Löhne
- EMDS AG, Stuttgart
- Evang. Krankenhaus, Berlin
- Evangelisches Krankenhaus, Bielefeld
- Fachhochschule Dortmund, Dortmund
- Fleischhacker GmbH & Co KG, Schwerte
- Fraunhofer ISST, Dortmund
- Fresenius Netcare GmbH, Berlin
- GE Healthcare IT GmbH & Co KG, Dornstadt
- gematik GmbH, Berlin
- Gessner, Berlin
- getemed AG, Teltow
- GLP systems GmbH, Hamburg
- GS4eB UG, Olpe
- Health-Comm GmbH, München
- Heinen + Löwenstein GmbH & Co KG, Bad Ems
- Helios Kliniken GmbH, Berlin
- Hinz – Organisation im Gesundheitswesen, Berlin
- ifasystems AG, Frechen
- IMAGIC Bildverarbeitung AG, Glattbrugg (Schweiz)
- IMESO GmbH, Hüttenberg
- INDAMED GmbH, Schwerin
- INFORM GmbH, Aachen
- Institut für Informatik, Rostock
- InterComponentWare AG, Walldorf
- InterSystems GmbH, Darmstadt
- INVITEC GmbH & Co KG, Duisburg
- ISG Intermed Service GmbH & Co KG, Geesthacht
- iSOFT Health GmbH, Mannheim
- iTech Laux & Schmidt GmbH, Lichtenau-Atteln
- ITZ Medicom GmbH, Willich
- ixmid Software Technologie GmbH, Köln
- JEMYS Medical AG, Jena
- Johanniter Competence Center GmbH, Berlin
- Karl Storz GmbH & Co KG, Tuttlingen
- Kassenärztliche Bundesvereinigung, Berlin
- Klinik Amsee GmbH, Waren/Müritz
- Kliniken Ludwigsburg-Bietigheim gGmbH, Ludwigsburg
- Klinikum Ansbach, Ansbach
- Klinikum Augsburg, Augsburg
- Klinikum der Uni Regensburg, Regensburg
- Klinikum Ingolstadt, Ingolstadt
- Klinikum Nürnberg, Nürnberg
- Klinikum Offenbach GmbH, Offenbach
- Klinikum Oldenburg, Oldenburg
- Klinikum rechts der Isar, München
- Klinikum St. Marien, Amberg
- knowledgepark AG, Neu-Isenburg
- KompAS IT-Service GmbH, Oberursel
- Krankenhaus Bad Cannstadt, Stuttgart
- Krankenhaus Itzehoe, EDV-Abteilung, Itzehoe
- Kreiskrankenhaus Altötting, Altötting

- Kretschmer-Keller GmbH, Leonberg
- KV Nordrhein, IT in der Arztpraxis, Düsseldorf
- Labor Badena AG, Baden (Schweiz)
- laboratoriumsmedizin Köln, Köln
- Leica Microsystems CMS GmbH, Wetzlar
- LIMETEC Biotechnologies GmbH, Bernau
- LMU München, München
- Magrathea Informatik GmbH, Hannover
- Malteser Trägergesellschaft MTG gGmbH, Bonn
- ManaThea GmbH, Regensburg
- Martin-Luther-Universität, Halle
- März Internetwork Services AG, Essen
- MCS Labordatensysteme GmbH & Co KG, Eltville
- MCS Labordatensysteme GmbH & Co KG, Kornwestheim
- MDK Rheinland-Pfalz, Alzey
- Med. Medien Informations GmbH, Neu-Isenburg
- MEDAT GmbH, München
- medatiXX GmbH & Co KG, Bamberg
- medavis GmbH, Karlsruhe
- Mediaform Informationssysteme GmbH, Reinbek
- MedicalCommunications GmbH, Bruchsal
- mediDok Software-Entwicklungs-GmbH, Dossenheim
- MEDISTAR Praxiscomputer GmbH, Hannover
- MediTec GmbH, Bad Salzdetfurth
- Medizinische Hochschule Hannover, Hannover
- Mednovo Medical Software Solutions GmbH, Berlin
- medVISION AG, Unna
- Meierhofer AG, München
- metek, Roetgen
- MICOS GmbH, Oldenburg
- Mollerus, Berg
- NEXUS/DIS GmbH, Frankfurt am Main
- NoemaLife GmbH, Berlin
- OFFIS e. V., Oldenburg
- Olympus Winter & Ibe GmbH, Hamburg
- optimal systems, Berlin
- OSM GmbH, Essen
- Philips Medizin Systeme, Hamburg
- Rhön-Klinikum AG, Bad Neustadt a.d. Saale
- Ringholm bv, Haarlem (Niederlande)
- Roche Diagnostics Deutschland GmbH, Mannheim
- Roeser Medical GmbH, Bochum
- RpDOC Solutions GmbH, Saarbrücken
- RZV Rechenzentrum Volmarstein GmbH, Wetter
- S+T Software Technic GmbH, Paderborn
- Sana IT Services GmbH, Remscheid
- SAP AG, Walldorf
- Schön Kliniken, Prien am Chiemsee
- Schwarzer GmbH, Heilbronn
- seca GmbH & Co KG, Hamburg
- sepp med GmbH, Röttenbach
- SER Healthcare Solutions GmbH, Neustadt
- Siemens AG Medical Solutions, Erlangen
- SLK Kliniken Heilbronn GmbH, Heilbronn
- smart-link GmbH, Bielefeld
- softgate GmbH, Erlangen
- Sorin Group Deutschland GmbH, München
- SQL Projekt AG, Dresden
- St.-Josefs-Hospital Wiesbaden GmbH, Wiesbaden
- Städt. Klinikum München, München
- Städtisches Klinikum Braunschweig, Braunschweig
- STAR Healthcare Management GmbH, Köln
- Steinhart Medizinsysteme GmbH, Vörstetten
- swisslab GmbH, Berlin
- Swissrisk AG, Frankfurt am Main
- Syscomp GmbH, Augsburg
- SysTek EDV Vertriebs GmbH & Co KG, Detmold
- systema Deutschland GmbH, Koblenz
- T-Systems International GmbH, Telemedizin & Telematik, Berlin
- T-Systems International GmbH, Weingarten
- Thieme Compliance GmbH, Erlangen
- TietoEnator Deutschland GmbH, Bochum
- TMF e. V., Berlin
- Unfallkrankenhaus Berlin, Berlin
- Universitäts-Krankenhaus Eppendorf, Hamburg
- Universitätsklinikum Dresden, Dresden
- Universitätsklinikum Düsseldorf, Düsseldorf
- Universitätsklinikum Erlangen, Erlangen
- Universitätsklinikum Essen, Essen
- Universitätsklinikum Gießen, Gießen
- Universitätsklinikum Heidelberg, Heidelberg
- Universitätsklinikum Köln, ZIK IT-Betrieb, Köln
- Universitätsklinikum Marburg, Marburg
- Universitätsklinikum Münster, Münster
- Universitätsklinikum Schleswig-Holstein, Kiel
- Universitätsklinikum Würzburg, Würzburg
- ViewPoint GmbH, Wessling
- VISUS Technology Transfer GmbH, Bochum
- Vitaphone GmbH, Mannheim
- Walter Graphtek GmbH, Lübeck
- Wavelight GmbH, Erlangen
- Zentrum für Telematik im Gesundheitswesen, Bochum
- Zimmer MedizinSysteme GmbH, Neu-Ulm

Ehrenmitglied

- Bernd Mollerus, Berg

Eingeschnürt?

Dann lieber Cloverleaf®!

budgetschonend
transparent
bedienerfreundlich

Health-Comm GmbH

...ein Unternehmen, das seit über 15 Jahren ein beeindruckendes Know-how im Bereich Integration innerhalb des Gesundheitswesens aufgebaut hat.

Mittlerweile werden über 450 Kunden im deutschsprachigen Raum betreut, wobei sich gerade in den letzten beiden Jahren ein überproportionaler Zuwachs verzeichnen lässt. Renommierte Krankenhäuser, Reha-Kliniken und andere Einrichtungen des Gesundheitswesens sowie große Klinikgruppen haben sich nach eingehender Marktsichtung für eine Partnerschaft mit Health-Comm entschieden. Allein in den letzten 18 Monaten sind über 120 neue Anwender hinzugekommen.

Zum einen liegt dies am bewährten Produkt, dem **Kommunikationsserver Cloverleaf®**, zum anderen an der Qualität der realisierten Implementierungsprojekte.

Und was machen Sie?

Health-Comm GmbH
Software für das Gesundheitswesen

www.health-comm.de
info@health-comm.de
Dachauer Str. 11 | D-80335 München
Telefon +49 (0)89-599 88 76-0
Telefax +49 (0)89-599 88 76-11

HL7

HL7

HL7 ANWENDERGRUPPE ÖSTERREICH

HL7 Luxembourg

Wollen Sie Mitglied in der HL7-Benutzergruppe Deutschland, Österreich, Schweiz oder Luxemburg werden?

Informationen finden Sie im Internet unter
www.hl7.de, www.hl7.at, www.hl7.ch, www.hl7.lu