MEDINFO 2010
C. Safran et al. (Eds.)
IOS Press, 2010

doi:10.3233/978-1-60750-588-4-889

Implementation of a Secure and Interoperable Generic e-Health Infrastructure for Shared Electronic Health Records based on IHE Integration Profiles

Thomas Schabetsberger[a,*], Florian Wozak[a,*], Basel Katt[b], Richard Mair[a], Bernhard Hirsch[a], Alexander Hörbst[c]

[a] *ITH icoserve technology for health care GmbH, Innsbruck, Austria*
[b] *University of Innsbruck, Innsbruck, Austria*
[c] *University for Health Sciences, Medical Informatics and Technology, Hall, Austria*
[*] *These authors contributed equally to this paper.*

Abstract

Introduction: The ubiquitous availability of medical or care data for authorized clinicians and nurses is expected to increase quality while reducing costs in the health care sector. The standardized, distributed provision of medical or care data is capable to support the vision of patient centered shared electronic health records (SEHRs). A main contribution to cross-institutional data exchange is provided by Integrating the Healthcare Enterprise (IHE). However, holistic implementations of IHE based eHealth infrastructures for SEHRs are currently rare and security and privacy regulations are not fully covered by existing IHE Integration Profiles. This work aims to point out our experiences and lessons learned from five years of development and the implementation of IHE compliant products.

Methods: Cross-Enterprise Document Sharing (XDS) describes the base components for exchanging medical or care data. A unique patient Identification is described by the Patient Identifier Cross-referencing (PIX) and the Patient Demographics Query (PDQ) Integration Profile. All interactions are logged in an "Audit Record Repository" deployed once per Affinity Domain and defined in the Audit Trail and Node Authentication (ATNA) Integration Profile.

Results: Based on the IHE Integration Profile XDS and other Integration Profiles high-level components for eHealth infrastructures and applications, supporting a holistic, secure concept and, based on these concepts, software products for a technical cooperative care infrastructure, has been developed. The products are practically evaluated in a project for setting up an IHE XDS Affinity Domain in the Austrian district of Tyrol and a number of lessons have been learned.

Keywords

Medical records, Medical record linkage, Data security

Introduction

The ubiquitous availability of medical or care data for authorized clinicians and nurses in a timely manner and in appropriate representation is expected to increase quality while reducing costs in the health care sector [1-3].

Currently health care institutions are experiencing a transformation in cross-institutional data exchange from proprietary solutions, mainly for point-to-point communication of selected medical data, towards a standardized provision of various document types including (radiological) images and multimedia content as virtual electronic patient records [4].

The standardized, distributed provision of medical or care data is capable to support the vision of patient centered shared electronic health records (SEHRs) [4]. As an extension to the exchange of medical or care data between health care providers, the patients with SEHRs are empowered to add content to their records (i.e. self assessments, medical diaries), to view audit events and to define security policies, as well as to access their own medical or care data [4, 6].

A main contribution to cross-institutional data exchange is provided by Integrating the Healthcare Enterprise (IHE), an international initiative which aims to support interoperability by widely accepted international standards such as Web services, HL7 and DICOM. Common workflows for standard-based sharing of clinical data are compiled as so called IHE Integration Profiles [7]. IHE Integration Profiles represent building blocks for the realization of holistic e-Health infrastructures (and other common clinical processes) in a broad sense [8].

Holistic implementations of IHE based eHealth infrastructures for SEHRs are currently rare and broad experience is missing. Apart from missing practical experiences with the implementation also the IHE frameworks shows some weaknesses. IHE describes the technical interoperability between systems of several vendors well, but does not focus on additionally required organizational interactions. Security and privacy requirements are only covered on a basic level by existing IHE Integration Profiles.

However, the importance of privacy aspects seems to vary between different nations in a European but also in a worldwide scope. This may have to do with historical events and possible data misusages in the past. Such strong privacy expectations in several regions require slight extensions of standardized IHE Integration Profiles.

Therefore our work aims at the identification and description of gaps between theory and practical experiences in implementing IHE Integration Profiles by pointing out our experiences and lessons learned from five years of development of IHE compliant products for the realization of a SEHR in Tyrol, the western part of Austria.

Methods

In order to ensure the highest possible degree of interoperability with other vendor's systems an IHE compliant architecture is a strict requirement. The design of the architecture followed standardized software engineering processes [9] incorporating architectural paradigms predetermined by the following IHE Integration Profiles relevant for SEHRs:

Cross-Enterprise Document Sharing (XDS) describes the base components for exchanging medical or care data between different institutions participating in an organizational framework called "Affinity Domain". XDS defines "Repositories" as data storage units which can reside locally in the institutions where data is produced. "Registries", deployed once per Affinity Domain, hold metadata about documents stored in the Repositories.

Registries serve as index services which allow predefined queries to find documents. Services used for registering Documents are called "Source" and services for retrieving documents "Consumer".

A unique patient Identification is described by the Patient Identifier Cross-referencing (PIX) and the Patient Demographics Query (PDQ) Integration Profile. The first allows mapping of locally used patient Identifiers to a unique Identifier per Affinity Domain, the latter provides services for identification of patients based on their demographic data.

As traceability of interactions is a key requirement for extended privacy aspects all interactions are logged in an "Audit Record Repository" deployed once per Affinity Domain and defined in the Audit Trail and Node Authentication (ATNA) Integration Profile. ATNA furthermore defines the use of Transport Layer Security (TLS) for encrypted communication and mutual authentication of services based on client certificates.

Apart from the use of IHE Integration Profiles the successful implementation of an e-Health infrastructure is also dependent on the fulfillment of a variety of other elements. To guarantee a high level of quality modern principles of software engineering were applied and intense testing was carried out through the whole process of development.

In order to assure compliance to IHE Integration Profile the software products has to be periodically tested at so-called Connect–a–thons, where different vendors are able to test and prove interoperability of their product with other vendor's software based on IHE Profiles. The products developed successfully took part in 4 Connect–a–thons.

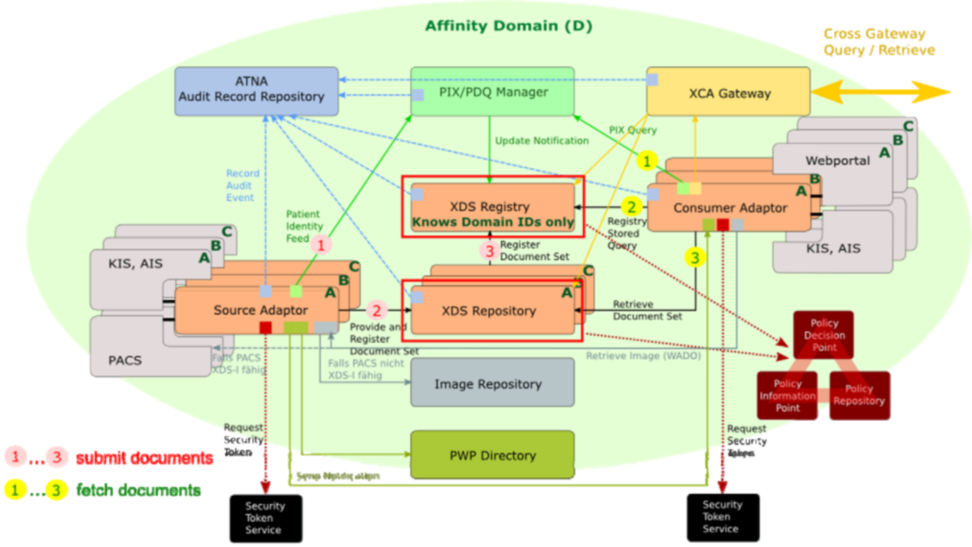

Figure 1 - Overview of sense Architecture based on several IHE Integration Profiles. Actors are depicted as boxes and Transactions as lines.

Results

Development of IHE compliant products

General considerations

Interoperability is required to support trans–institutional clinical data exchange in the context of SEHRs [10].

IHE describes the above mentioned building blocks for standardized e-Health infrastructures as so-called "Actors" and their interactions as so-called "Transactions". The IT-Infrastructure Technical Framework of IHE facilitates distributed data storage and also distributed index services. One of the main advantages is that medical or care data can reside in the institution, where they have been produced, and can be accessed by other institutions, provided that access rights are sufficient.

Based on the IHE Integration Profile XDS high-level components for eHealth infrastructures and applications, supporting a holistic concept for cooperative care, has been developed. Originally this development started five years ago as a research project [5] of universities in cooperation with industrial partners.

System Architecture for e-Health infrastructure

The software products are designed as modular components incorporating the Service-Oriented-Architecture (SOA) approach using Web service technology. Figure 1 shows an illustration of the architecture. The product family is called "sense® – smart eHealth solutions" owned by ITH icoserve technology for health care GmbH [11], which is a subsidiary company of a regional hospital holding company and Siemens. The products are available worldwide.

Workflow for transmission of documents

Workflow for registration of documents (cf. Figure 1, red numbers): Documents are submitted from the Clinical Information System (CIS) to the sense Source Adaptor which triggers the following IHE Transactions for (1) Adding patient identification to PIX/PDQ, (2) submitting the document to the Repository and (3) submitting metadata to the Registry.

Workflow for retrieval of documents (cf. Figure 1, green numbers): Documents are retrieved from the sense Consumer Adaptor which triggers the following IHE Transactions for (1) obtaining patient Identification, (2) querying the Registry and (3) retrieving the document from the Repository.

Java-based Web services offer a high degree of flexibility in implementation while supporting interoperability, as required by IHE, with other vendor's products, independent from platforms and programming languages. Therefore Apache Tomcat and Axis2 have been selected as application server and Web service runtime environment. For the sharing of clinical documents highly configurable services are deployed locally (sense® Localnodes) in health care institutions as well as centrally (sense® Communitynodes), operated for example by a large hospital, forming the XDS Affinity Domain as described above. Localnodes provide XDS Repositories as data storage and adaptors for the connection of existing, proprietary systems such as Clinical Information Systems (CIS) or GP's systems. Communitynodes provide XDS Registries as index services, a PIX/PDQ master patient index for unique patient identification and an ATNA audit record repository for central storage of audit events.

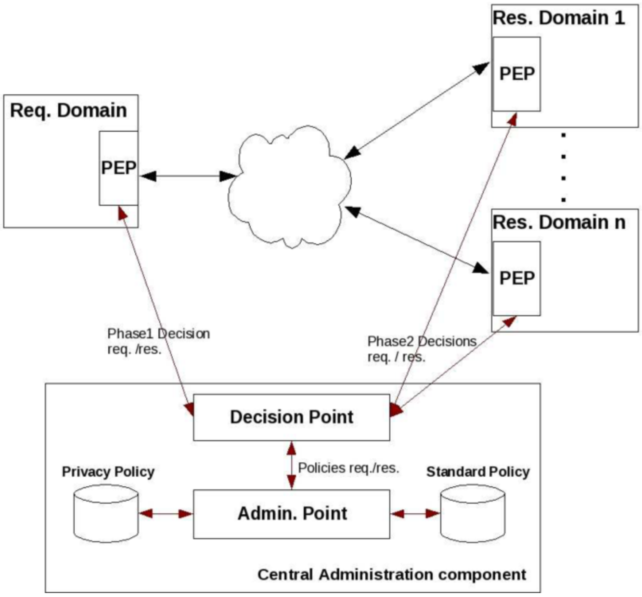

Figure 2 – Design of the security architecture

Security Concept

The sharing of patient data requires a sophisticated security concept reaching from Transport Layer Security (TLS) to provide authenticated and encrypted data exchange on Network Layer as well as an advanced authorization framework based on the Security Assertion Markup Language (SAML) [12] and extensible Access Control Markup Language (XACML) [13] on the application layer, which – in future – should empower the patient to decide who may access his health information.

The security concept [14] tackles privacy and access control in IHE systems from two perspectives: a Policy and an Enforcement. Two types of policies were defined: standard and privacy policies. While standard policies represent data security regulations in Austria, privacy policies enable – in future – citizens to define their own personal preferences and conditions. From the enforcement point of view, two phases' enforcement and decision making process was defined (cf. Figure 2). The difference between the two phases is the granularity. In the first phase the whole patient's record is considered as one virtual object and the enforcement is done at the requesting side. In the second phase a finer granular decisions can be taken for each part of the patient's record. Due to the fact that the parts of a patient's record are stored in different domains, the enforcement in this phase is done at the responding side, i.e. affinity domains that store parts of the requested record.

Implementation of a SEHR in Tyrol

Based on these components in the Austrian district of Tyrol a virtual electronic patient record with capability to future extension to a shared electronic health record has been set up.

Tyrol is located in the western part of Austria, with alpine topography. It has approx. 750.000 citizens, 12 hospitals with together approx. 4000 beds and 2.000 physicians (in- and outpatient).

Prior and during the implementation, a couple of important lessons have been learned, which are of interest to other similar projects:

- The financing and the assignment for projects related to e-Health is one of the most difficult tasks. The benefits are mostly in the public economics and less in the business economics. This means that public bodies are the main beneficiaries. This leads to the fact, that health care institutions are often not the buyers of such systems and are not willing to invest in such solutions.
- In general, the benefits of e-Health (infrastructures or applications like SEHRs) are not easy to verify. Big saving potentials with regard to macroeconomics are regularly published [1]. But health professionals do mostly not think in big numbers but in small steps assisting their personal work. Therefore it's very difficult to create acceptance amongst health professionals.
- In Tyrol, several independent health care providers requested in common a standardized e-Health infrastructure to improve cooperation. This common appearance at public bodies got the ball (for assignments) rolling.
- After assignments a working group for common coordination, consisting of all participating health care institutions has been established.
- The introduction of standards for medical document formats or metadata was one of the most labor intensive steps. With currently available technology such as CDA, a very fine–grained structure can be applied to clinical data. Structuring of clinical data influences the workflow of data capturing. This is an organizational rather than a technical challenge as health professionals must be motivated to switch from flexible free text to a rigid framework for data capturing.
- Austrian data protection regulations require a 2-level access control mechanism. The fist level requires that a current treatment relationship exists between physician and patient. The second level requires consent of the patient. In the consent document restrictions can be applied for institutions, departments, document type and time range. Level 1 is covered by a service, provided by the operators of the so called "e-card" (Austrian health insurance card). Level 2 requires extensions to the XDS Document Registry and an organizational framework.
- In order to support patient-controlled restrictions as described above, new queries had to be added to the Document Registry which allow filtering particularly for institutions and departments. Level 2 restrictions are currently not evaluated technically. Physicians querying for documents have to obey the patient's restrictions when setting search criteria in the user interface. In order to assure that those restrictions are actually applied all queries are logged to the ARR. Health care professionals participating in the SEHR have to obligate themselves to respect the patient's consent and to store the consent document paper-based or electronically. Furthermore health care professionals have to agree to periodic inspections of consent documents with the aim to prove that issued queries, logged in the ARR, match the consent of the patient given in the consent document. However in future versions of the software the patient's consent will be covered by access control policies.
- Early usability evaluation revealed that a seamless integration of the SEHR application in the Clinical Information System (CIS) or the GP's system is vital for end-user acceptance. A web portal solution is only the second-best choice. The concept of the sense Source and Consumer Adaptor proved to be important to facilitate the development effort for those systems as complex IHE transactions and the handling security validations is covered by the Adaptor services.
- Operating the SEHR in a dedicated physical network, strictly separated from the Internet improves security and therewith also end-user acceptance.
- Although IHE dramatically improves interoperability between different systems, test effort remains high.

This seems to be rather caused by semantic then by technical issues.

- End-user and system administrator training is a key factor for success and acceptance of SEHRs. The challenge is to create awareness of the sensitivity of retrieved data, which implies that restrictions issued by patients in the consent document have to be strictly obeyed.
- A professional project management from acquisition to routine operation of a SEHR is a vital success factor. E-Health projects are complex and risky as there are many players involved with partly distinct interests, level of technical understanding and organizational objections. Advanced project and also conflict management skill is required to reach the goal. However this is a time-consuming process.

Discussion and Outlook

IHE Integration Profiles leave details open for implementation, which is, from the economic point of view, expected to support the market. Technically this might lead to slightly different interpretation of the specification, which may prevent successful communication between different systems.

The concept of IHE is interoperability testing and not certification. This means that systems attested conformity to an Integration Profile can be further developed. This “snapshot” approach allows vendors to further modify and improve their systems even after conformity has been attested, which furthermore allows modifications carried out during the Connect–a–thon to be stabilized to a mature system. We however would like to create awareness that changes to a successfully tested system might lead to side effects that can, in the worst case, break interoperability.

Particularly the upcoming seamless integration of the security concept shows that especially in the health care sector technical challenges can be solved rather easy in comparison to organizational challenges such as a nation-wide role definition for medical personnel or such as required changes in medical or care workflows.

Interoperability between computer systems in health care seems to be adequately solvable using state-of-the-art technology such as Java and Web services. Semantic interoperability which should provide for identical, language independent interpretation of the submitted content is expected to remain one of the major challenges for the next years.

References

[1] Stroetmann KA, Jones T, Dobrev A, Stroetmann VM. eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites. Loxembourg: Office for Official Publikations of the European Communities; 2006.

[2] Haux R, Ammenwerth E, Herzog W, Knaup P. Health care in the information society. A prognosis for the year 2013. Int J Med Inf. 2002 Nov;66(1-3):3–21. 22341698 1386-5056 Journal Article.

[3] Van Bemmel JH. Toward a virtual electronic patient record. MD Comput. 1999 Nov-Dec;16(6):20–1. 0724-6811 (Print) Journal Article.

[4] Waegemann CP. The five levels of electronic health records. MD Com-put. 1996 May-Jun;13(3):199–203. 0724-6811 (Print) Letter.

[5] Schabetsberger T, Ammenwerth E, Andreatta S, Gratl G, Haux R, Lechleitner G, et al. From a paper-based transmission of discharge summaries to electronic communication in health care regions. Int J Med Inform. 2006 Mar-Apr;75(3-4):209–15. 1386-5056 (Print) Journal Article.

[6] Ramsaroop P, Ball MJ. The ”Bank of Health A Model for More Useful Patient Health Records. MDComputing. 2000;(July/August 2000):45–48.

[7] Wozak F, Ammenwerth E, Horbst A, Sogner P, Mair R, Schabetsberger T. IHE based interoperability - benefits and challenges. Stud Health Technol Inform. 2008;136:771–776.

[8] Integrating the Healthcare Enterprise. 2009. Available from: http://www.ihe.net/About/

[9] Sommerville I. Software Engineering. 8th ed. Edingburgh, England: Pearson Education Limited; 2006.

[10] Kalra D. Electronic health record standards. Methods Inf Med. 2006;45 Suppl 1:136–144.

[11] ITH icoserve technologies for healthcare GmbH. 2009. Available from: http://www.ith-icoserve.com

[12] Security Assertion Markup Language (SAML). 2009. Available from: http://saml.xml.org/saml-specifications

[13] eXtensible Access Control Markup Language (XACML). Available from: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#technical

[14] Katt B, Breu R, Hafner M, Schabetsberger T, Mair R, Wozak F. Privacy and Access Control for IHE-based Systems. Proceedings of E-Health 2008: Electronic Healthcare, First International Conference, eHealth 2008, London, UK, September 8-9, 2008. Revised Selected Papers. P. 145-153. ISBN 978-3-642-00412-4.

Address for correspondence

DDr. Thomas Schabetsberger, thomas.schabetsberger@ith-icoserve.com, ITH icoserve technology for healthcare GmbH, 6020 Innsbruck, Innrain 98a, Austria.