Architecture for a Distributed National Electronic Health Record System in Austria

Raimund Vogl1, Florian WOZAKc, Micheal BREUb, Robert PENZa, Thomas SCHA-
BETSBERGERc and Manfred WURZd

1 HITT - health information technologies tirol, Innsbruck, Austria
2 Leopold-Franzens-University Innsbruck, Innsbruck, Austria
3 University of Health Sciences Medical Informatics and Technology, Hall, Austria
4 icoserve Information Technologies, Innsbruck, Austria

Abstract. Quality and efficiency of healthcare services is expected to be improved by the electronic processing and transinstitutional availability of medical data. A prototype architecture based on the IHE-XDS profile is currently being developed aiming at providing a basis for a distributed electronic health record in Austria. Due to legal and organizational requirements specific adaptations to the IHE-XDS profile have been made. In this work the services of the health@net reference architecture are described in details, which have been developed with focus on compliance to both, the IHE-XDS profile and the legal situation in Austria. We expect to gain knowledge about the development of a shared electronic health record using Medical Data Grids as an Open Source reference implementation and how proprietary hospital information systems can be integrated in this environment.

1. Introduction

The electronic processing of medical data which is expected to improve quality and efficiency of health care services [1] will lead to an increasing amount of medical data exchanged across institutional boundaries [2].

The greatest benefit is expected if concise medical data are available for the patient himself as well as for medical institutions involved in the treatment process. Currently transinstitutional data exchange is only partly realized for specific fields. Up to now, and to our best knowledge no systems for a transparent integration of medical data across institutional boundaries have been implemented.

Presently communication among institutions in the healthcare environment is mainly based on directed data flow, implying that the intended receiver has to be known at the very beginning of the communication process. Particularly in a medical context this is very limiting, resulting in multiple transmissions of documents from the producing institution to all the possible recipients.

In this paper we illustrate the development of a network architecture for a patient centered shared electronic health record (SEHR), using a technical infrastructure based on Medical Data GRIDs. The architecture is designed to comply with the cross enterprise document sharing specification (IHE-XDS) and the Austrian federal law for health telematics [3]. The main challenge is to design the architecture in the way to comply

1 Corresponding Author: Dr. Raimund Vogl, HITT – health information technology tirol, Leopoldstrasse 1, A-6020 Innsbruck, Austria. Email: R.Vogl@hitt.at Web: http://www.hitt.at.
with both requirements.

The architecture is designed to be highly scalable and to offer standardized interfaces which simplifies the process of joining for new institutions as much as possible. For this reason an architecture following the blueprint of Medical Data GRIDs seem to be most appropriate. Data GRIDs are usually defined in the following way:

“Data Grid is an emerging technological paradigm for the seamless access, via virtualized middleware, to heterogeneous and distributed ensembles of data storage resources”[4].

A commonly agreed on definition, which takes into account the very specific context in which medical data is treated, is not known to us. Legal and organizational requirements in the medical domain vary vastly for every country. Data handled by a shared electronic health record are specific to a medical domain such as laboratory results or radiological images. Analysis and procession is closely bound to the originating medical domain. These specific requirements demand for adaptation of the data GRID architecture definition. For this paper we propose to extend the original definition as follows:

“Medical Data GRID is an emerging technological paradigm for the seamless access to medical data for a patient centric shared electronic health record with special focus on legal and organizational requisitions of the environment they are operated in, via virtualized middleware, to heterogeneous and distributed ensembles of data storage resources”.

2. Methods

In an initial step functional requirements for a SEHR have been analyzed [5]. According to these requirements the implementation of the architecture was designed.

We apply the SECTET approach [6] to model the functional requirements along with the security requirements of the transinstitutional workflows in a SEHR. The backbone of the SECTET methodology are UML models [7] that specify the workflows between the participating partners. A starting point is the document model that defines the basic objects that are managed and exchanged by the system. In parallel a role model is developed that reflects the permissions and capabilities of the users of the system. These models guide through the elicitation of security requirements

2.1. The Austrian E-Health Initiative

In 2005 the E-Health Initiative (EHI) of the Austrian Federal Ministry for Health and Woman compiled a strategy to organize the development of the health system towards an integrated patient-centered care on a long-term basis [8]. Hereby a major role is played by the electronic health record (EHR; “ELGA” as an acronym for “Elektronische Gesundheitsakte” is the German buzzword) which is a summary of health-related data of an individual, acquired continually from either outpatient or inpatient treatment, and which is filed digitally. This electronic health record should store all these data all one’s life independent of place or time, and should present them demand-oriented to all the persons involved in the medical treatment, including the patient himself.
2.2. The IHE XDS approach

IHE is an initiative by healthcare professionals, institutions and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE integration profiles have improved communication capabilities, are easier to implement, and enable care providers to use information more effectively [9].

The IHE cross enterprise document sharing integration profile (XDS) provides an architectural approach for document sharing in heterogeneous health care environments [10]. The reference architecture proposed by XDS specification is described in Figure 1 (A).

At the Document Source medical documents are produced, which are then stored at the document Repository and made available to the end user (Document Consumer). The document Registry is for indexing and search functions, the Patient Id source provides for unique patient identification.

3. Infrastructure and Network Architecture

The proposals from the Austrian ELGA and e-Health initiative are the foundation for the implementation of the health@net [11] core architecture. Currently our group is implementing an open source prototype architecture based on the IHE XDS specification.

To meet legal and organizational requirements specific for Austria, certain services are to be implemented to adapt the architecture according to the needs. In the following an overview of the most important services of the health@net prototype implementation shown in Figure 1 (B) is outlined.

To ensure greatest possible flexibility and scalability, a distributed approach following the above introduced paradigm of Medical Data GRIDs was chosen. Consistent use of web service technology allows the SEHR interfaces to be designed in a generic way, which simplifies implementation for joining institutions as far as possible.

The core architecture consists of independent services responsible for storing documents and corresponding meta data, security features, unique patient identification and service discovery according to the IHE XDS specification. To guarantee a high level of security beyond the application security covered by role based access control, the entire communication is encrypted using the HTTPS Protocol, digital certificates provide mutual authentication of participating systems and each SOAP message exchanged is digitally signed using Web service security extensions [12].

Core functionality is provided by the three service groups: Document Repository, Document Registry and Patient Id Source.

Medical documents remain stored at the organization where they have been produced in the Document Repository (DR) situated at this organization. Documents are usually provided by the Document Source in a proprietary format (eg. HL7 V2.3 messages, PDF documents, etc...). For this reason incoming documents are converted to the Clinical Document Architecture (CDA) format internally used. The Document Clearing service (DC) is responsible for document conversion and mapping of locally used patient identification to the internally used unique identification.
The Document Registry service provides functionality for document search, per-document access permissions, a link to the physical location at the Document Repository as well as a service discovery unit.

Searches for documents are managed by the Document Meta Data Index (DMDI), which holds search relevant meta data as well as document based access permissions. This service checks each request for a document against the per-document access control lists and if permitted the request is signed. Only in case of a valid signature the Document Repository returns the requested document. The Global Index (GI) is responsible for finding DMDI services that hold document meta data for a specific patient identified by the unique patient ID. The Document Registry provides an Interface for Document Consumers called Access Nodes (AN), which generate queries to the architecture. They are defined as gateways to access the SEHR from external systems.

The Patient Id Source service group provides for unique patient identification across institutional boundaries, independent from patient's nationality. The Austrian legal situation and the fact that a unique patient identification does not exist requires different services, partly provided by the Austrian government to be integrated in the architecture.

The Patient Lookup Index (PLI) is used as interface for other services (mostly DC and AN) to obtain a unique patient identification based on demographic data. Each Austrian citizen is assigned a unique number by a governmental institution called “Zentrales Melderegister” (Central Citizen Registry, shown as ZMR in Figure 1 B). Due to data privacy considerations, this unique citizen Id is not publicly available and must not be recorded by any institution, but a domain specific one-way derivation can be obtained for various sectors of daily live, such as the health care sector. A second way is to take the social insurance number as unique patient identification. Social insurances (shown as HI: Health Insurer in Figure 1 B) provide a service to obtain the insurance number by demographic data such as first name, last name, date of birth, address. This insurance number is not globally unique – it is comprised of a 4-digit sequential number plus the date of birth in 6 digit format – and will be reused after a person is deceased. And can thus only be used as an auxiliary means of identification.
Consequently, a distributed Patient Lookup service (PL) is needed to obtain these identifiers transparently for the underlying architecture. Furthermore this service provides a Patient Id Source for patients without a ZMR identification, especially for non Austrian citizens.

The Austrian federal law for health telematics[3] also requires a central e-Health directory service (shown as EHI in Figure 1 B) to be established until July 2006. At the moment medical data exchange partly makes use of a privately maintained forerunner for this official registry, a central LDAP directory of Austrian physicians known as eVGA (“Elektronisches Verzeichnis der Gesundheitsdienstanbieter”). In the SEHR architecture this directory will be used for role- and context based access control.

Currently two different approaches are being evaluated for services which allow the patient to give fine grained permissions to physicians and institutions which allows them to access specific parts of the record:

1. Distributed services, which manage and enforce access permissions assigned by the patient using roles defined by the e-Health directory.
2. A permission management system based on digital certificates issued for each permitted operation.

Due to the early stage of evaluation this service is not implemented in the first prototype. The privacy of patient related data is temporarily solved in a way that participating institutions are bound by contract to only access data relevant for the specific treatment case. A variety of work flows such as the adding, retrieval, version-save updates of documents and correction of misidentified patients are supported by the architecture. Their detailed description is beyond the scope of this paper.

4. Discussion and outlook

The development of the network architecture follows an iterative approach which we have chosen to gradually adopt the architecture to evolving requirements of the major players. In this article the first prototype implementation is described, which of course lacks certain functionality and implements only simplified security requirements. To guarantee the highest level of data protection for patients, in the initial prototype phase physicians who test the architecture are conscientiously selected and will be bounded by contract to respect the patient's consent. The operators of the architecture commit themselves to prove the adherence to the contract by collecting random samples from logging.

Austrian federal law for health telematics [3] requires a central e-Health directory service to be implemented until July 2006. At the moment medical data exchange partly makes use of a central LDAP directory of Austrian physicians known as eVGA (Elektronisches Verzeichnis der Gesundheitsdienstanbieter). In the SEHR architecture this directory will be used for role- and context based access control.

Though the developed architecture follows the paradigm of Medical Data GRIDs, currently available GRID middleware such as the GLOBUS-Toolkit [13] is not used in this setup. The main reason is that requirements for Medical Data GRIDs as outlined above are currently not satisfactorily covered and only a subset of the provided GRID features would be used.

Nevertheless, the evaluation of the GLOBUS-Toolkit version 4 revealed some use-
ful concepts. Since they mainly rely on open standards defined by the OASIS working group [14] those concepts have been integrated in the architecture.

Our implementation of the architecture follows the IHE XDS specification as closely as possible, nevertheless the Austrian federal law demands for specific modifications of the architecture as described above for patient identification and usage of the central e-Health register. Primarily for the issue of access rights to data, including the incorporation of patient consent, additional specification and design features had to be introduced on top of the IHE profile.

We expect to gain knowledge about the development of a shared electronic health record and how proprietary systems, particularly the clinical information system from the Innsbruck University Hospital can be integrated in this environment. Before the architecture can be used in productive environments technical and organizational issues have to be solved comprising extended security, financing and cooperation with other health care institutions.

Acknowledgements
This work has been funded through the HITT centre of excellence programme supported by the Austrian Ministry for Economy and Work (BMWA) and the Tyrolean Future Endowment Fund (TZS).

References