An eConsent-based System Architecture Supporting Cooperation in Integrated Healthcare Networks

Joachim Bergmann, Oliver J Bott, Ina Hoffmann, Dietrich P Pretschner

Technical University of Braunschweig, Braunschweig, Germany

Abstract

Objectives: The economical need for efficient healthcare leads to cooperative shared care networks. A virtual electronic health record is required, which integrates patient related information but reflects the distributed infrastructure and restricts access only to those health professionals involved into the care process. Our work aims on specification and development of a system architecture fulfilling these requirements to be used in concrete regional pilot studies.

Methods: Methodical analysis and specification have been performed in a healthcare network using the formal method and modelling tool MOSAIK-M. The complexity of the application field was reduced by focusing on the scenario of thyroid disease care, which still includes various interdisciplinary cooperation.

Results: Result is an architecture for a secure distributed electronic health record for integrated care networks, specified in terms of a MOSAIK-M-based system model. The architecture proposes business processes, application services, and a sophisticated security concept, providing a platform for distributed document-based, patient-centred, and secure cooperation. A corresponding system prototype has been developed for pilot studies, using advanced application server technologies. The architecture combines a consolidated patient-centred document management with a decentralized system structure without needs for replication management. An eConsent-based approach assures, that access to the distributed health record remains under control of the patient.

Conclusion: The proposed architecture replaces message-based communication approaches, because it implements a virtual health record providing complete and current information. Acceptance of the new communication services depends on compatibility with the clinical routine. Unique and cross-institutional identification of a patient is also a challenge, but will loose significance with establishing common patient cards.

Keywords:
Integrated Health Care Systems; Interdisciplinary Communication; Medical Record Linkage; Computerized Medical Record; Patient Data Privacy

1. Introduction

Economical needs for efficient healthcare in line with quality goals lead to a progressive diversification and specialization of health professions and processes, requiring enhanced communication, coordination, and documentation. Significant problems are well known in various clinical settings (see for instance [1], [2], [3]): the lack of current, complete and timely information, and shortcomings in control and coordination of care processes.
Instantiation of the shared care paradigm in regional healthcare networks is one approach to overcome these problems.

A common approach for building up an efficient communication system for integrated healthcare networks is the replacement of traditional paper-based messaging processes with their electronic equivalents. Pure messaging results in faster communications and may be appropriate for many tasks, but does not lead to an integrated lifelong medical record, because most parts of the record are fragmented and spread over various care providers like in paper-based systems. Advanced information system architectures supporting shared care should provide a patient-centred integrated health record as described in several approaches, e.g. Synapses [4], PICNIC [5], or government initiatives like e-toile [6], the Australian HealthConnect and Canada Health Infoway. These architectures, enabling the authorized health professional to acquire current and complete information nearly whenever needed, require sophisticated security and administration concepts, because many distributed entities are going to provide and request information under different access conditions [7], using various data formats and patient ID schemes. Generally it has to be guaranteed, that access to a patient's medical information is restricted only to health professionals involved into the care process within the required scope [8].

This paper presents an architecture for secure information sharing in integrated healthcare networks addressing the requirements mentioned above.

2. Materials and methods

A methodical analysis has been performed in a healthcare network using MOSAIK-M [9], a framework and tool environment which supports modelling, simulation, and animation of information and communication systems in medicine. A generic process scheme guides projects in producing system models of high quality in terms of correctness, completeness and validity. A meta model defines the modelling language for these models. A UML-based modelling tool allows modelling of organizational structures, applications, and information structures, while processes are expressed with Petri nets. For a better participation of medical staff during modelling and specification phases, the model allows simulation and animation of communication and data processing activities.

The complexity of the analysis was reduced by focusing on the exemplary scenario of thyroid disease care. Thus it was possible to limit the number of communication processes and documents to a manageable amount, while the application field is comprehensive enough to show cooperation between various specialists.

Analysis of the problem domain resulted in an “As is”-model of the current situation of thyroid disease care. Subsequently, the model was transformed into a “To be”-model, which was validated and improved in a workshop with representative participants of the healthcare network. Based on this architecture model, an advanced prototype system was built, which is currently being evaluated in the European funded project INCA (INtelligent Control Assistant for diabetes, www.ist-inca.org) addressing telemedical issues in diabetes care, and in a project supporting the communication between general practitioners and a hospital in a regional setting.

3. Results

Result of analysis and specification is an architecture for distributed information processing in integrated healthcare networks, specified with means of a formal MOSAIK-M model and implemented as an advanced system prototype.
From analysis phase and recent publications, two basic requirements for a system architecture supporting efficient shared care are derived. First, the architecture should support migration from provider-based and isolated information management to consolidated patient-centred documentation [10]. Second, the architecture should reflect the decentralized infrastructure in integrated healthcare networks [6,8]. The proposed concept is intended to merge these apparently oppositional requirements of a consolidated but decentralized information management. It focuses on the virtual integration of distributed documents in order to share information between participating healthcare parties, allowing a health professional’s information system to become part of the Distributed Electronic Health Record (DEHR).

**Patient-oriented clinical document**

Key elements are the *patient-oriented clinical documents* provided by healthcare institutions with respect to the following policy:

- The patient as subject of information recorded in the care process holds the *exploitation rights* to related documents. He is able to monitor, authorize and constrain document usage.
- A health professional providing care for the patient is a *trusted manager* of those documents he creates referring to the patient (stewardship).
- The patient *authorizes* a health professional, who is involved into the care process, to access the shared distributed health record. This authorization includes the right to forward granted privileges, e.g. in case of consultations or laboratory requests.

A clinical document is always assigned to an overall identified patient. This requires a common ID-service like a patient card or a master patient index.

**Contribution, retrieval and messaging in a Distributed Electronic Health Record**

The fundamental concept of a DEHR is, that each clinical document resides where it is originated without copying it to a central server or sending it to a receiver. Fig. 1 shows a simplified configuration of a healthcare network.

---

**Contribution.** The document is processed locally (1) within the Local Repository, until the author or an executive declares it finished and to be of interest for the virtual record. The author signs the current version (2) and subsequently initiates the “publication” process (3), which stores the signed document onto the Publisher (3a) and forwards a characterizing reference to this document (so-called *Document Descriptor*) onto the patient’s Index (3b).

**Retrieval.** Whenever access to a document is required, the client queries its Local Repository (4), which at first processes the query locally and subsequently adds the results from requesting the patient’s index (4a). From this list of Document Descriptors, the health professional decides about relevant documents and subsequently requests them from the related Publisher (5, 5a). The resulting documents can either be exported from the DEHR or viewed with a DEHR viewer, provided from a Catalogue service (not depicted).
Messaging of information about a patient between two care providers, e.g. posting the order for an expert consultation or subsequently sending back the result, can also be seen as access to a document being part of DEHR. Additionally, a message referring to the document has to be transferred, indicating that it has become available.

In order to avoid multiple documentation in DEHR and in the locally used information systems, the Publisher concept allows integrating these legacy information systems (LIS) into DEHR by encapsulating them with a Mounter (see fig. 2).

Fig. 2 – UML model (a) and functionality of a Mounter (b)

Information is processed within the LIS (1), until the health professional “freezes” a specific artefact of the legacy system with a digital signature onto the mounter (2, 2a) and publishes it like a generic document (3, 3a) under a common ID. For retrieval from outside, the mounter checks the authorisation of a query, maps the common ID-space into the LIS domain and forwards the resulting request to the LIS (not depicted). If the LIS allows to lock a document or a well-defined information unit as finished and invariant, the mounter only has to store a signature (S) instead of a whole document, with which integrity and authorship of the information unit are ensured.

Electronic consent

Since accessing medical documents in a DEHR is not limited to the health professional’s own repository, the architecture has to ensure, that a query to the virtual record is permitted by the patient. Thus an eConsent-concept [11] is introduced, which electronically reproduces the contract between patient and health professional. The patient creates a digital certificate, referring to a health professional and including access privileges and a validity period:

\[
eConsent^{p, h} := (p, h, v, R)
\]

given patient p, health professional h, validity period v, and set of privileges R.

This certificate is always sent with a request and authorizes its owner to attend the distributed health record according to granted access privileges. To cover the case of consultation, a health professional is granted a non-transferable privilege to forward the eConsent to a further expert. This new eConsent represents a contract between the primary health professional and the expert to be consulted. It includes the original consent of the patient to prove the health professional’s legitimation concerning patient p:

\[
eConsent^{h, h'} := (h, h', eConsent^{p, h}, v', R')
\]

given health professionals h and h’, validity period v’ covered by v, and privileges \( R' \subseteq R \).

This concept implies a public key infrastructure (PKI) including equipment for creating qualified digital signatures.

Health professional authorization

Whenever a health professional requests a document, he has to authenticate to the remote service with an end-to-end-security challenge/response process, based on health
The remote service checks the identity of the user and of the following transferred credentials:

- an eConsent object representing the patient’s consent, and
- an attribute certificate, which is stored on the health professional card and represents the user’s roles within the healthcare system. This certificate is supposed to be issued by the German association of CHI physicians in the near future.

After verification of the credentials against a Trusted Third Party, the service processes the request. Due to end-to-end authentication and the attribute certificates, there is no need for a common authentication service or a central repository of users and roles.

**Proof of concept: trial system V-Net Med**

The trial system V-Net Med (Virtual Medical Network) was developed to prove the architecture in pilot studies. Apache Web Services with SOAP messages are used, allowing flexible deployment and implementation-independent client systems. Clinical information is recorded in HL7 CDA Release 1 documents [13] and wrapped with a digital signature following the PKCS#7 Cryptographic Message Syntax Standard. “Black-box” documents containing any kind of information (e.g. PDF) are supported.

Although Apache's SSL connectivity with client authentication is used exclusively, the system operates through a VPN to enhance security. For digital signature, a commercially available qualified signature card (T-Systems PKS SigG card) is used.

**4. Discussion and Conclusion**

The requirement of a consolidated patient-centred documentation can be achieved by virtual integration of documents, where the unique and cross-institutional identification of a patient is done with the help of a patient card. The requirement of distributed management of information is achieved with publication services, providing documents directly from the source system (or from an outsourced storage node, if continuous availability cannot be guaranteed due to network configuration). This respects an author’s properties of the information he has recorded, whereas a sophisticated security concept grants access only to the health professionals involved into the care process. The patient is always able to control and restrict the access to the shared record. Granting privileges derived from the original contract between patient and health professional allows a health professional to consult an expert and thus forward a constrained authorisation. The architecture provides a vision similar to a Health Bank [10, 14], with the patient deciding about the locations of his document collections (the indexes) and probably many institutions competing for his trust.

On the other side, some challenges currently constrain deployment of the proposed architecture. First, publication services have to guarantee high availability to provide a reliable shared record, which requires an advanced and probably expensive infrastructure within the healthcare network. Second, a common identification infrastructure has to be established. This could be achieved either by a patient card or a person identification service, which maps several ID domains together. Third, acceptance of the new communication services depends on a transparent fitting into clinical routine without disarranging well-working processes.

New architectures supporting cross-institutional cooperation are more and more requested from the increasing number of healthcare networks. A trend towards national platforms providing common services for integration of distributed information can be found in several countries. The report of the CEN/ISSS e-Health Standardization Focus Group [15] determines the necessity of coordinating these approaches and recommends a Europe-wide
eHealth interoperability platform. There is a growing market for a new type of software connecting healthcare systems together. But concerning interoperability between legacy systems, not even the problem of interoperability on a functional level is currently solved. For instance, OMG’s healthcare interoperability specifications are not widely used and the OASIS standards from the eBusiness field are recently being explored by medical informatics. The HL7 Clinical Document Architecture provides a helpful common syntax for information exchange in the presented project. But semantic interoperability remains a major issue. CDA Release 2 with its templates and Reference Information Model is an important step in this direction, as well as the two model approach (archetype and reference model) recently introduced into the CEN EN 13606 revision.

5. References


Address for correspondence

Dipl.-Inform. Joachim Bergmann, Technical University of Braunschweig, Institute for Medical Informatics Muehlenpfordstr. 23, D-38106 Braunschweig, Germany, J.Bergmann@mi.tu-bs.de

www.mi.tu-bs.de

*Section 13: Public Health Informatics, Clinical Trials*