Exploring Complexity in Health: An Interdisciplinary Systems Approach
A. Hoerbst et al. (Eds.)

Security and Privacy in a DACS

Jaime DELGADO[a,b,1], Silvia LLORENTE[a,b], Martí PÀMIES[b] and Josep VILALTA[b]
[a] *Distributed Multimedia Applications Group (DMAG),*
Computer Architecture Dept. (DAC), Universitat Politècnica de Catalunya (UPC)
[b] *Clinical Document Engineering (CDE)*

Abstract. The management of electronic health records (EHR), in general, and clinical documents, in particular, is becoming a key issue in the daily work of Healthcare Organizations (HO). The need for providing secure and private access to, and storage for, clinical documents together with the need for HO to interoperate, raises a number of issues difficult to solve. Many systems are in place to manage EHR and documents. Some of these Healthcare Information Systems (HIS) follow standards in their document structure and communications protocols, but many do not. In fact, they are mostly proprietary and do not interoperate. Our proposal to solve the current situation is the use of a DACS (Document Archiving and Communication System) for providing security, privacy and standardized access to clinical documents.

Keywords. Security, Privacy, DACS, eHealth

1. Introduction

When Healthcare Organizations (HO) want to provide an easy, flexible, interoperable, secure and private storage and access to clinical information, a number of issues need to be solved. To achieve interoperability, HIS should use software that supports standards, such as HL7 CDA (also ISO 27932) [1] [2]; this will help in improving the interaction inside and between organizations.

When patients move from one hospital to another, or when healthcare professionals work in different points of care, there is a need to access to patients' information from as many different devices as possible. In addition, patients' privacy must be taken into account, which could imply the convenience of defining flexible privacy rules to guarantee it. Besides having secure and controlled access, clinical information should be also stored in a secure way.

A PACS (Picture Archiving and Communication System) is a technology for the storage, retrieval, management, distribution and presentation of medical images. Therefore, a Document Archiving and Communication System (DACS) wants to be the equivalent to PACS for medical documents. In this way, it can help in fulfilling security and interoperability requirements for clinical documents. [3] describes an example of an initial DACS that implements a use case of CDA level 1 using external files. Our approach however aims to go a step further, providing a DACS that uses up to HL7 CDA level 5 documents to store medical information. In this way, interoperability between different HO will be easier to achieve.

[1] Corresponding Author: jaime.delgado@ac.upc.edu

The use of these and other HL7 (and non-HL7) standards allows us to provide a Vendor Neutral Archive (VNA) system for the secure storage of clinical documents. Standards facilitate integration of the DACS with the HIS being used in HO and with other DACS (from other organizations) when required.

The rest of this paper describes the complete functionality of our DACS supporting HL7 CDA, the connection with existing HIS and the applications for performing complex queries over documents in the DACS.

2. Methods

The DACS is the central component of our system. Its final aim is to provide digital archiving services, including custody, and access to structured clinical documents in a secure and confidential manner, using the only globally accepted standard in this regard, HL7 CDA (ISO/HL7 27932) [1]. It can consist on one isolated DACS installation, acting as an autonomous software component, or on a federation of several DACS, allowing their interoperability.

Figure 1 shows DACS main technical components: web portal, server and databases. All these components can be installed in the Cloud or On site. The DACS can be accessed via a Web Portal and via a Web Services API, always after positive User Authentication. Users can use different devices (laptop, smartphone, …) to gain access to DACS features.

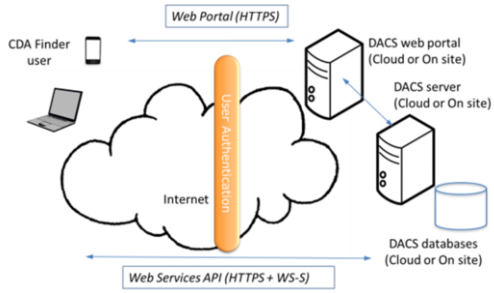


Figure 1. DACS architecture and services.

As described in section 2, a HIS can upload documents to the DACS using HL7 RLUS (Retrieve, Locate, and Update Service) [4] or IHE-XDS (Cross-Enterprise Document Sharing) [5]. These clinical documents, which have to follow the HL7 CDA structure, are stored into the DACS database that allows users' access with the Finder.

The DACS architecture is completely distributed, using Web Services (WS) and WS-Security to add standard security. On the other hand, it follows IHE ATNA (Audit Trail and Node Authentication) [4] to manage traceability. It is also worth noting that access to the clinical data is controlled by means of XACML (eXtensible Access Control Markup Language) privacy rules [6] and SAML (Security Assertion Markup Language) security tokens [7], returning only the authorized results, based on the rules and conditions (for instance, time period) defined. Regarding privacy and security, one can define rules based on roles (defined in HL7 V3 Personal Management Domain) [2], at the smallest but practical granularity level as possible. The most common rules are defined as templates, to facilitate its use. Some ideas on access control to medical information using XACML and SAML were already described in [7].

The DACS does not substitute but complements current HIS functionality. DACS allows HIS focusing on document creation (and features like beds/schedule/rooms handling) whilst it manages document storage, custody and sharing. In this way, it is possible to obtain better interoperability and to perform complex queries that provide alerts and advanced knowledge based on the stored documents. As an example, our DACS can create temporal series of lab results or spirography devices, automatic summaries of immunizations and vaccines, as well as allergy summaries and treatment interactions. Moreover, it is a very convenient platform for documentary tracking of Clinical Trials to evaluate health status of patients based on the applied treatments and the published reports.

3. Results

Clinical documents may pass through several stages before and after being stored into the DACS. In this section, we describe the lifecycle of a clinical document, since its creation by the Healthcare Professional in a point of care, through its storage into the DACS and, afterwards, to its querying using different kinds of applications (web, mobile, etc.) from different locations (for instance, in an emergency scenario), as already described in section 1. The result of the search may vary depending on the privacy rules defined over the documents stored and the role of the user performing the query. As an example, a nurse and a family doctor will have access to some medical information whilst a specialty doctor may have only access to the clinical information related with her specialty or the clinical documents she has created [7].

Figure 2 shows the complete infrastructure of an HO with its own HIS, which wants to take profit from DACS functionality.

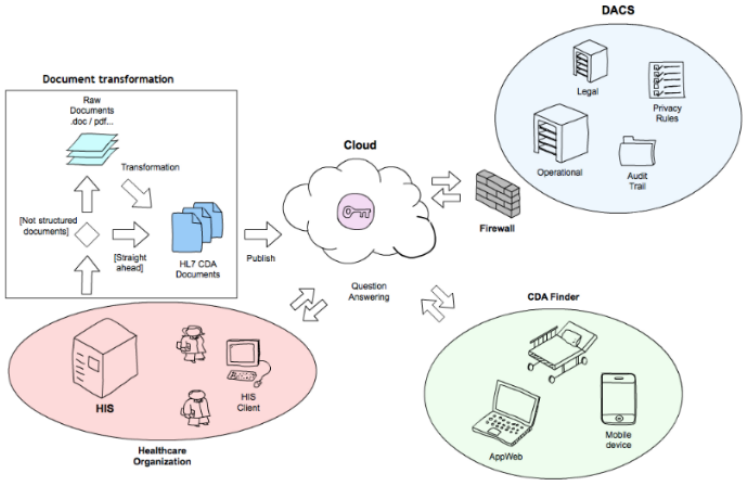


Figure 2. General infrastructure for storing medical information using DACS and HIS.

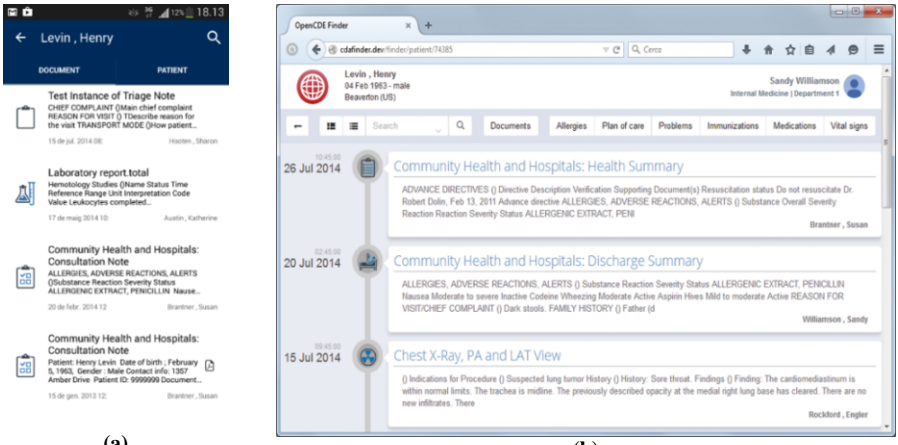
First, non-structured documents in doc, pdf or any other HIS exporting format have to be converted into HL7 CDA documents. The complexity of this transformation process depends on how they are originally structured. In the case of non-structured documents, templates are useful to improve structuring. The easiest case is when the HIS already exports HL7 CDA structured documents, so no transformation (or little one) is

required. When the documents follow the HL7 CDA structure, they can be directly published into the DACS. This transformation part is represented in the Document Transformation phase in Figure 2.

Only authorized users can operate over DACS. Documents are stored into two different repositories inside the DACS. One is the Legal repository that cannot be modified. It proves when the document was created, by which user, and that it has not been modified since then. Then, there is the Operational one, which is optimized to respond to complex queries in an efficient way, considering the Privacy Rules governing the documents. Finally, an Audit Trail module is in charge of auditing and storing operations.

Once documents are stored into DACS repositories, they can be queried from the HIS or, the normal case, from the Finder, which is a specific client application implemented in both web and mobile versions allowing the easy and powerful query and classification of clinical documents.

Figure 3 shows an example of how clinical information is presented using the CDA finder, both in mobile app (Figure 3a) and web (Figure 3b) versions. This is the view for a doctor, who can access his patients' clinical information. The icons represent the kind of information, such as lab results, x-ray images, different kinds of notes, summaries, etc. In particular, Figure 3b shows the Time Series Line of clinical documents, but other views are possible, like the List View, the Structured Clinical Document View, which shows the composition of several documents according to the sections appearing in them, or the Non-structured body pdf, when no structure document exists for a particular document.



(a) (b)

Figure 3. CDA Finder app and web versions.

4. Discussion

The privacy rules defined in DACS are very powerful to control access to medical documents for primary care. However, these rules may not have the same application for secondary care and some privacy problems could arise.

The storage of clinical information in a structured way opens the door to a new set of search services based on the correlation of different parameters (medical conditions,

drugs, etc.) to find out better ways of patient care based on experiences. For instance, one could try to find if a particular drug was well tolerated by patients with a specific illness and then look for the patients that were prescribed this treatment to review their medical records. On the other hand, this search power could be a double-edged sword in terms of privacy protection of the patients, as this correlation may show information about patients to persons that are not authorized by privacy rules, because it is not their medical specialty or any other reason. Therefore, it is critical to properly anonymize medical data when medical information is used for research, finding a compromise between privacy protection and medical advance thanks to the structured knowledge.

Once the privacy protection objective is achieved, using anonymization or other techniques, the use of Business Intelligence or even Big Data processing to find hidden relationships between medical conditions, allergies, patient age range and medical treatments, could become the strongest point of DACS structured information storage.

5. Conclusions and future work

In this paper, we have proposed the secure storage and query of HL7 CDA structured documents using a DACS (Document Archiving and Communication System). The use of XACML privacy policies and SAML security tokens guarantees preservation of patient's privacy when healthcare professionals access to clinical information. Moreover, insertion of documents into DACS repositories is also supported by standards, thanks to the use of RLUS or IHE-XDS.

One of our most relevant contributions is a new way of accessing clinical documents, allowing complex queries not currently supported by HIS. The Finder (web and app versions) allows taking the maximum benefit from this query power.

It is planned to implement Business Intelligence operations over DACS repositories in order to be able to perform studies on illness correlation, drug's effects over medical conditions, etc.

Our solution, OpenCDE [8], improves the patient's quality of life through effective sharing of clinical information among HO, professionals and patients [9], allowing reduction of bad practice and improvement in wait times for care, disease management, care quality and timely access to clinical information and results. Finally, it is worth mentioning the fact that different DACS can be interconnected without the need of having all documents in a central node.

References

[1] ISO/HL7 27932:2009, Data Exchange Standards – HL7 Clinical Document Architecture, Release 2, 2009.
[2] HL7 International, http://www.hl7.org/, 2016.
[3] Y. Matsumura et al, A Scheme for Assuring Lifelong Readability in Computer Based Medical Records, Volume 160: MEDINFO 2010, 91–95, IOS Press, The Netherlands, 2010.
[4] IHE (Integrating the Healthcare Enterprise), http://www.ihe.net/, 2016.
[5] VICO & PYMMA, http://vico.org/MeusPOSTERS/Posters%20IHE/ATNA/IHE_ATNA.pdf, 2016.
[6] OASIS (Org. for the Advancement of Structured Info. Standards), https://www.oasis-open.org/, 2016.
[7] J. Delgado, S. Llorente, Privacy provision in eHealth using external services, Volume 210: Digital Healthcare Empowering Europeans, 823–827, IOS Press, The Netherlands, 2015.
[8] Clinical Document Engineering, http://www.clinicaldocumentengineering.com/en, 2016.
[9] J. Delgado et al, Mejora de la interoperabilidad con un DACS: El caso Salud de la Mujer Dexeus (in Spanish), XIX Congreso Nacional de Informática de la Salud, Inforsalud 2016, Madrid, 2016.