MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

Interoperability and Security: Design and Development of a Clinical Documents Repository Digitally Signed using CDA Standard

Fernán González Bernaldo de Quirós, Adrián Gómez, Fernando Campos, Jorge Severino, Fernando Plazzotta, Daniel R. Luna

Medical Informatics Department, Hospital Italiano of Buenos Aires, Argentina

Abstract

The amount of institutions with hospital information systems has increased. Different technologies and standards available makes possible to satisfy many information exchange needs. HL7's CDA is a marked-up document standard, which specifies the structure and the semantics of a clinical document. Digital Signature is a tool that guarantees the authorship and integrity of electronic documents. The Hospital Italiano of Buenos Aires, has developed and implemented a CDA documents repository along with the creation of its own PKI infrastructure, obtaining then a trustworthy and unique registry of the medical acts, making possible the access to documents in a format that allows full legibility, also allowing process and later inclusion of this information in other systems or applications, guaranteeing its authorship and integrity.

Keywords:

medical records systems, computerized,
computer security, standards, electronic documents, digital signature

Introduction

The growth of hospital information systems, the information exchange needs and the proliferation of technologies implemented on the Internet, allowed medical documents to be shared and exchanged between organizations, hospitals and healthcare providers [1]. This made possible the development of protocols and methods to assure medical information exchange in a standard format, increasing the possibilities of achieving semantic and syntactic interoperability.

One of the main standards families in health information systems setting is Health Level Seven (HL7). CDA stands for Clinical Documents Architecture and is a markup standard, which specifies the structure and the semantics of a clinical document. The present version is 2.0, is part of version 3 of HL7 standard and describes its semantic content in the Reference Information Model (RIM) [3].

On the other hand, paper documents have traditionally guaranteed its authorship and integrity by handwritten signature. In medical settings physicians records in paper and signs at the end of the chart. Each later registry must be signed, indicating the authorship and responsibility of any modification made from the previous signature.

When it comes to digital charts, the use of simple electronic signatures, like "username and password", does not fulfill all the requirements needed to replace the hand written signature.

Digital signature is a technological tool that guarantees the authorship and integrity of digital documents, giving them the same validity of those signed in paper.

In the present work we will describe the design, development and implementation process of a digitally signed clinical documents repository, created from an electronic health record, using CDA standard and the asymmetric key infrastructure (PKI - Public Key Infrastructure).

Materials and methods

Scenario

The Italian Hospital of Buenos Aires (HIBA) is a tertiary care, teaching and research hospital with a 150 year old history. Since 1998 a full scale HIS has been gradually implemented, including ambulatory Electronic Health Record (EHR), several health informatics standards had been implemented, including HL7, CDA 2.0, ICD-9CM, DRG and ICD10 [4].

Digital Signature legislation in Argentina

In 2001, bill number 25506 of "Digital Signature" was sanctioned, it essentially recognizes the use of digital and electronic signature, and its legal validity, allowing the truthfully identification of individuals making electronic transactions. This way, when a document requires a handwritten signature, that exigency is also satisfied by a digital signature.

This bill also describes in its fifth article the figure of electronic signature as an integrated electronic data set, related in a logical way to other electronic data, used by the signatory like his means of identification, which lacks some of the legal requirements to be considered digital signature [5].

Medical information security

Our project includes as a key issue the development of the security mechanisms needed to operate and maintain a decentralized medical record system, knowing that medical information security is based on five fundamental aspects:

- **Privacy**: medical information cannot be accessed by third parties not related to the attention process.
- **No Disavowal**: references the authorship of the document, only the person who possesses the digital signature is in charge of the generated and saved data.
- **Authenticity**: it refers to the character of authentic of a document, that is to say, that is the original one.
- **Integrity**: related to the previous one, talks about the content of the medical information preventing that it original content is altered.
- **Chronology**: directly related to integrity, allows keeping registry of the date and hour of the creation of the original information, thus giving the data a temporary sequence.

CDA documents creation

The information system of our institution, registers all the medical events generated in the health care process. The clinical document generation begins with the medical encounter or "health care event", for the outpatient setting is the aggregation of all the actions made (medical problems, medical progress notes, orders entered, clinical observations, pharmacologic prescriptions, date and hour).

For in patient and emergency settings, clinical document example is the epicrisis; and, in the case of information generated by ancillary services, each procedure inquired is equivalent to a health care event, reason why it generates a document, using the information made in the report system.

Once the health care event is stored into the clinical data repository (CDR), a web service is in charge of generating a CDA document. This service recovers the medical information recorded from the CDR and creates the document (a XML file). Then the user is asked to validate the information through a confirmation process and the document is digitally signed. This signed documents and its control parameters are stored in file data system.

Digital Signature of medical documents

HIBA took the initiative to create its own PKI by developing an "in house" application that makes possible to lead all the process of creation and administration of public and private keys and digital certificates.

In order to guarantee its integrity and authenticity, a digital document must fulfil three basic characteristics:

- Having a HASH to guarantee the document's integrity.
- Been signed with private and public key system, to guarantee its authorship.
- Having a Time Stamping service, that guarantees document's temporality.

In our project, public and private keys are stored in a cryptographic USB E-Token given to providers and it's asked for its insertion at the moment of the signature. The E-Token is an electronic component with USB (Universal Serial Bus) interface.

When a XML clinical document is created, the application calculates a single HASH value and encrypts it using the private key stored in the E-token. This encrypted file maintains its original information and the digital certificate [6].

The exact moment when the primary load of information happened is one of the most important variants, since the medical document existence at a certain moment in time must be determined in a safe way. We chose to generate a process of time stamping, which stores a digitally signed time registry with the document signed by the user.

Discussion

The summary of providers work, documented in a single XML file, adding Digital and Electronic Signature, provided by the E-token, will allow the creation of a trustworthy and unique registry of the medical acts.

On the other hand, current graphical interfaces, although provide improvements in usability and information visualization, does not correspond with the traditional charts in paper. Traditionally the professionals records their observations and findings in documents and then sign them. The implementation of CDA and Digital/Electronic Signature maintains this sequence.

Conclusion

The implementation of this solution allowed users to access laboratory results, imaging reporting, referral notes, discharge letters, progress notes, diagnoses, procedures and medical prescriptions, in a fully legible format and the possibility of information processing for its later inclusion in other information systems or related health care applications.

Documents visualization was personalized using XSL style sheets being able to render styles, typographies and icons recognized and validated by the institution. A time stamping service (also digitally signed), will allow temporality to this unique registry of medical acts.

CDA standard implementation with the aggregate of digital/electronic signature in an electronic health record is a true challenge, since it entails an important technological

and organizational impact. At this moment we are carrying out a pilot test for the completion of the system and the norms and procedures created to such aim.

References

[1] Muller ML, Uckert F, Burkle T, Prokosch HU. Cross-institutional data exchange using the clinical document architecture (CDA). Int J Med Inform 2005;74(2-4):245-56.

[2] Dolin RH, Alschuler L, Boyer S, Beebe C, Behlen FM, Biron PV, Shabo Shvo A. HL7 Clinical Document Architecture, Release 2. J Am Med Inform Assoc 2006;13(1):30-9.

[3] González Bernaldo de Quirós F, et al. Migración a plataforma web de una Historia Clínica Electrónica. In CBIS'2004 - IX Congresso Brasileiro de Informática em Saúde; 2004; Ribeirão Preto-SP. Brasil

[4] Ley 25506 - Ley de Firma Digital., in Boletín Oficial de la República Argentina. 2001. p. 1.

[5] Imamura, T.D., B. Simon, E., XML Encryption Syntax and Processing. 2002, W3C.

Address for correspondence

Dr. Fernán González Bernaldo de Quirós
Vice-Director Médico Estratégico –
Hospital Italiano de Buenos Aires
Gascón 450 (1181) Buenos Aires, Argentina
fernan.quiros@hospitalitaliano.org.ar