DOI 10.1007/s10916-009-9266-9

ORIGINAL PAPER

Application of Portable CDA for Secure Clinical-document Exchange

Kuo-Hsuan Huang · Sung-Huai Hsieh · Yuan-Jen Chang · Feipei Lai · Sheau-Ling Hsieh · Hsiu-Hui Lee

Received: 14 November 2008 / Accepted: 12 February 2009 / Published online: 25 February 2009

Abstract Health Level Seven (HL7) organization published the Clinical Document Architecture (CDA) for exchanging documents among heterogeneous systems and improving medical quality based on the design method in CDA. In practice, although the HL7 organization tried to make medical messages exchangeable, it is still hard to exchange medical messages. There are many issues when two hospitals want to exchange clinical documents, such as patient privacy, network security, budget, and the strategies of the hospital. In this article, we propose a method for the exchange and sharing of clinical documents in an offline model based on the CDA—the Portable CDA. This allows the physician to retrieve the patient's medical record stored in a portal device, but not through the Internet in real time. The security and privacy of CDA data will also be considered.

Keywords Health level seven · Clinical document architecture · Privacy · Information protection

Introduction

Even within a city, a patient may go to different hospitals, and the personal medical records are distributed across each hospital. Medical errors can be avoided if the related medical information of the patient can be retrieved correctly and efficiently. Therefore the effective communication and availability of medical information among hospitals is an important issue. In recent years, there have been a lot of researches on different architectures for sharing medical records based on Internet technologies [1–3]. In order to reuse the sharable information, many medical standards are proposed for the smooth exchange of electronic medical records following the specific standards.

Health Level Seven (HL7) organization has worked hard to provide a comprehensive framework for the exchange and sharing of clinical information (such as discharge summaries and progress notes). Clinical Document Architecture (CDA), Release 1, became an American National Standards Institute (ANSI)—approved HL7 standard in 2000 and CDA Release 2 in 2005 [4]. The HL7 standard clearly defines the style of the exchanged information. According to CDA R2, CDA documents use the Extensible Markup Language (XML) format [5] for a wide variety of applications. XML is a flexible text format that is

K.-H. Huang (✉)
Department of Computer Science and Engineering,
Tatung University,
Taipei, Taiwan
e-mail: kuohsuan1225@gmail.com

S.-H. Hsieh · F. Lai
Information Systems Office, National Taiwan University Hospital,
Taipei, Taiwan

S.-H. Hsieh · Y.-J. Chang · F. Lai · H.-H. Lee
Department of Computer Science and Information Engineering,
National Taiwan University,
Taipei, Taiwan

F. Lai
Department of Electrical Engineering,
National Taiwan University,
Taipei, Taiwan

F. Lai
Graduate Institute of Biomedical Electronics and Bioinformatics,
National Taiwan University,
Taipei, Taiwan

S.-L. Hsieh
Network and Computer Centre, National Chiao Tung University,
Hsin Chu, Taiwan

straightforward to use over the Internet and hence many applications have been previously published with it [6–8].

Although HL7 organization tries to make medical messages exchangeable, it is still hard in practice to exchange medical messages. There are many issues when two hospitals want to exchange medical data using HL7 messages, such as patient privacy, network security, budget, and the strategies of the hospital. Therefore in this paper we advance a new concept—Portable CDA—that is a portable storage for the CDA content, just like Universal Serial Bus (USB) storage. It provides an offline model to store the patient's medical record, which can be a carry-on and allows for faster reading of vital medical information in real time. Even if the Internet is unavailable, the information can still be retrieved [9, 10]. In addition, in order to prevent personal medical information exchange and sharing in the process was illegal access or malicious tampering, the proposed approach applies encryption techniques and digital signatures to achieve confidentiality, authenticity, and integrity of the exchanged medical data.

This paper gives a new view on the usage of the CDA. First we will discuss why we chose the HL7 V3 and CDA standard, as well as some features of these two standards. The next section describes why and how to use the Portable CDA, along with its requirements and functions. Finally, we give a conclusion about the Portable CDA structure and discuss directions for future work. Possible new and useful technologies to enhance our design are also covered.

Background

The HL7 mission is to provide standards for the exchange, management and integration of data that supports clinical patient care and the management, delivery and evaluation of healthcare services. Specifically, it is to create flexible, cost-effective approaches, standards, guidelines, methodologies, and related services for interoperability between healthcare information systems [11].

HL7 V3 improves the Version 2 process and its outcomes. HL7 V3 adopts an Object Oriented (OO) approach using Unified Modeling Language (UML) principles, so it can be represented graphically using the UML style. Here we focus on the HL7 V3 Reference Information Model (RIM) because it is the basic structure of the CDA. RIM is used to express the information content, which consists of six important classes: Act, Participation, Entity, Role, ActRelationship, and RoleLink. These are defined as follows:

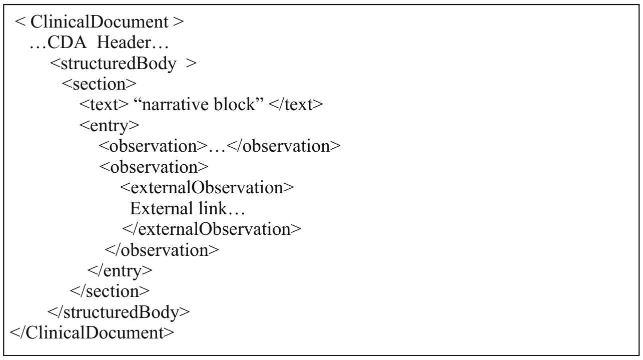
- Act: Actions that are executed and must be documented as health care is managed and provided.
- Participation: The information of an Act, such as who performed it and where it was done.
- Entity: The actual person or organization that takes part in an Act.
- Role: Illustrates the roles that entities play in the Act.
- ActRelationship: Shows the relationship between two Acts.
- RoleLink: Represents a dependency between two Roles.

A CDA document uses the XML schema to wrap contents. The whole content is wrapped by <ClinicalDocument> and inside it are a header and a body. The header contains the document information and the authentication of the entities in this CDA document. For example, <custodian> represents the organization that is in charge of maintaining the document; <legalAuthenticator> represents a participant who has legally authenticated the document; and <recordTarget> represents the medical record that this document belongs to. The body can be a structured body using <structuredBody> or an unstructured body using <NonXMLBody>. An unstructured body is used to wrap existing non-XML documents.

A structured body has one or more <section>, which can be nested or not. One of the important schemas in <section> is <text>. <text> is a narrative block which contains the human readable content of the meaning of the section. This schema is important because it can only have <text> content in a <section>, so the <text> content is not null. There are none or more <entry> in a <section> which are used to encode the content in the <text>. Each <entry> has one or more clinical statement schemas inside, such as <Observation>, <SubstanceAdministration>, <Supply>, or <Procedure>. The clinical statement schemas store the coded contents provided for computer processing. Sections and clinical statement schemas have many attributes inside, such as classCode, moodCode, statusCode, and so on.

A CDA document also offers external reference, such as another CDA document, hyperlink, sounds, images, multimedia, and so on. It may be contained under <externalObservation>. This way, the medical record can be made more complete. Figure 1 shows a simple sample of the content of the CDA document [4].

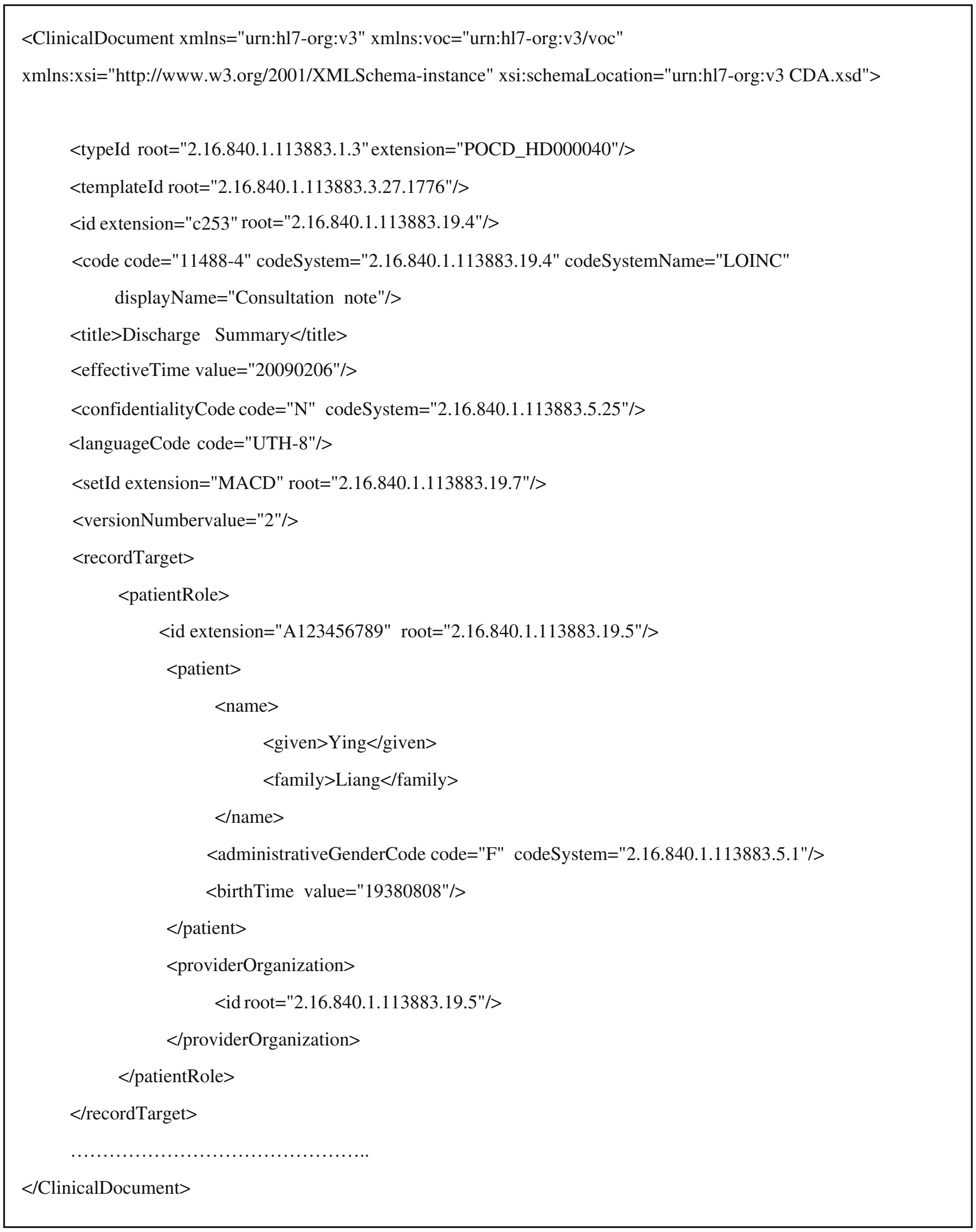
It deserves to be mentioned that the CDA can have code systems. We can use well-known code systems such as the Systemized Nomenclature of Medicine Clinical Terms (SNOMED CT) [12], Logical Observation Identifiers Names and Codes (LOINC) [13], International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM), and so on. These code systems can improve the consistency of the information and accelerate computer processing to enhance the interoperability.



```
< ClinicalDocument >
  …CDA  Header…
     <structuredBody  >
       <section>
          <text> “narrative block” </text>
          <entry>
             <observation>…</observation>
             <observation>
                <externalObservation>
                  External link…
                </externalObservation>
             </observation>
          </entry>
       </section>
     </structuredBody>
</ClinicalDocument>
```

Fig. 1 A simple sample of the CDA document

It is an important concern to achieve confidentiality, authenticity and integrity while the clinical document is being exchanged [14–16]. Confidentiality can prevent the data from being disclosed maliciously and maintain the patient’s privacy. Authenticity ensures the validity of the original data. Integrity avoids deliberate modification of the data, resulting in unnecessary medical errors. Adopting the proper cryptographic technique can deliver the security requirements. In relation to data confidentiality, encryption is the most common method to protect the information by making it unreadable while storing and transmitting the exchangeable clinical document. Accordingly, encryption is a suitable method to provide infor-



```
<ClinicalDocument xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/voc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:hl7-org:v3 CDA.xsd">

    <typeId  root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>
    <templateId root="2.16.840.1.113883.3.27.1776"/>
    <id extension="c253" root="2.16.840.1.113883.19.4"/>
    <code code="11488-4" codeSystem="2.16.840.1.113883.19.4" codeSystemName="LOINC"
        displayName="Consultation  note"/>
    <title>Discharge   Summary</title>
    <effectiveTime value="20090206"/>
    <confidentialityCode code="N"  codeSystem="2.16.840.1.113883.5.25"/>
    <languageCode  code="UTH-8"/>
    <setId extension="MACD" root="2.16.840.1.113883.19.7"/>
    <versionNumbervalue="2"/>
    <recordTarget>
        <patientRole>
            <id extension="A123456789"  root="2.16.840.1.113883.19.5"/>
            <patient>
                <name>
                    <given>Ying</given>
                    <family>Liang</family>
                </name>
                <administrativeGenderCode code="F"  codeSystem="2.16.840.1.113883.5.1"/>
                <birthTime  value="19380808"/>
            </patient>
            <providerOrganization>
                <id root="2.16.840.1.113883.19.5"/>
            </providerOrganization>
        </patientRole>
    </recordTarget>
    ………………………………………..
</ClinicalDocument>
```

Fig. 2 A snapshot of a CDA document of the discharge summary

mation security and prevent unauthorized disclosure based on controlling the decryption key. The Advanced Encryption Standard (AES), providing vastly superior security and good throughput, is a significant symmetric cryptosystem recently developed [17]. Snyder et al. [18] advises that adoption of AES with 256-bit keys will provide the necessary security, but also that the influence of the workflow in hospital should be minimized.

In respect to data authenticity and integrity, the physician uses the private key to sign a clinical document, and anyone can use the corresponding public key to verify the signature. Because the private key is unique and known only to the physician, the authenticity of the signed clinical document is guaranteed. If a clinical document is digitally signed, any change in the document will invalidate the signature. This ensures the completeness of data. The

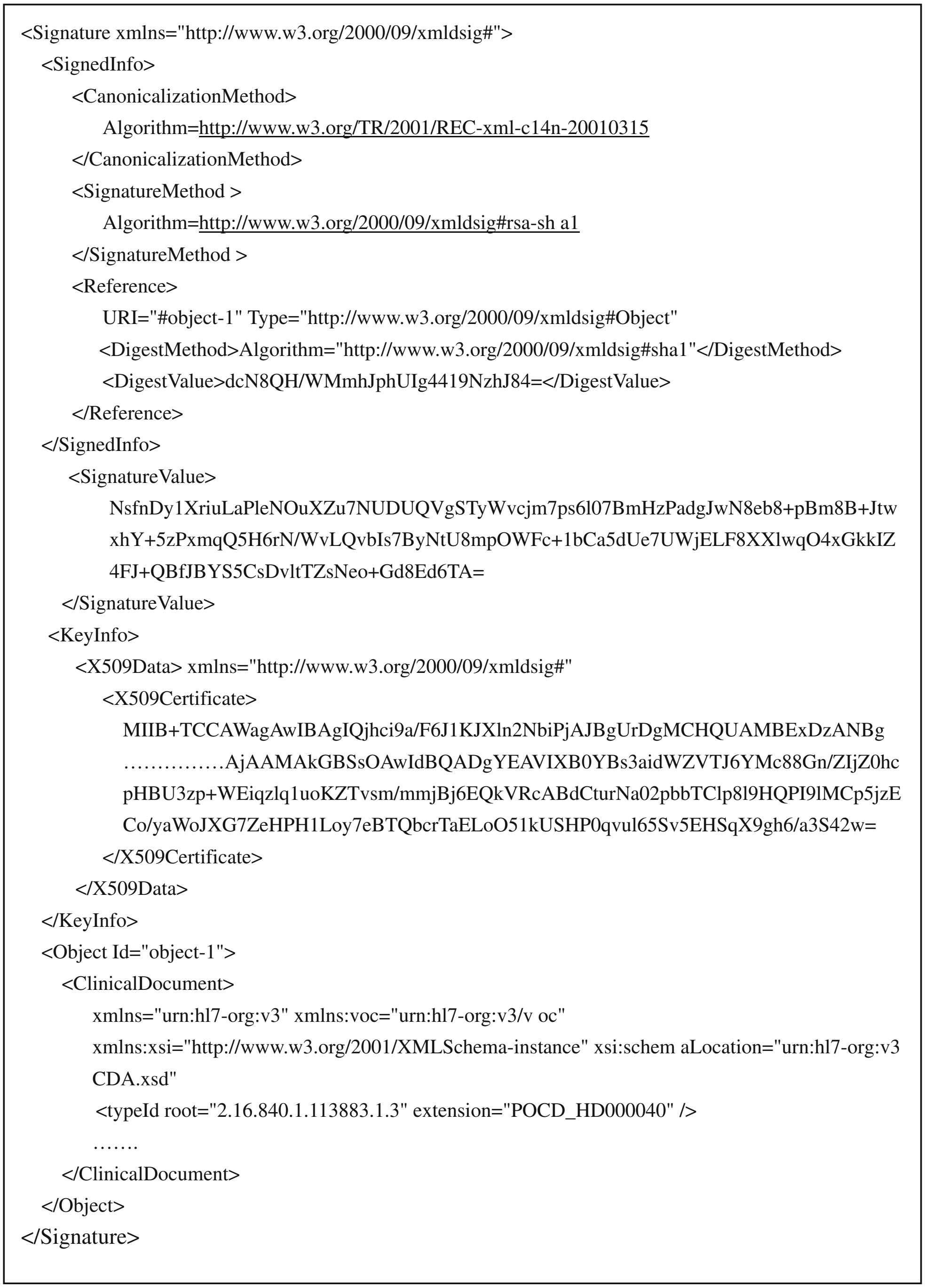


Fig. 3 A Signed CDA document

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
     <CanonicalizationMethod>
        Algorithm=http://www.w3.org/TR/2001/REC-xml-c14n-20010315
     </CanonicalizationMethod>
     <SignatureMethod >
        Algorithm=http://www.w3.org/2000/09/xmldsig#rsa-sh a1
     </SignatureMethod >
     <Reference>
        URI="#object-1" Type="http://www.w3.org/2000/09/xmldsig#Object"
        <DigestMethod>Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"</DigestMethod>
        <DigestValue>dcN8QH/WMmhJphUIg4419NzhJ84=</DigestValue>
     </Reference>
  </SignedInfo>
     <SignatureValue>
         NsfnDy1XriuLaPleNOuXZu7NUDUQVgSTyWvcjm7ps6l07BmHzPadgJwN8eb8+pBm8B+Jtw
         xhY+5zPxmqQ5H6rN/WvLQvbIs7ByNtU8mpOWFc+1bCa5dUe7UWjELF8XXlwqO4xGkkIZ
         4FJ+QBfJBYS5CsDvltTZsNeo+Gd8Ed6TA=
    </SignatureValue>
   <KeyInfo>
      <X509Data> xmlns="http://www.w3.org/2000/09/xmldsig#"
         <X509Certificate>
           MIIB+TCCAWagAwIBAgIQjhci9a/F6J1KJXln2NbiPjAJBgUrDgMCHQUAMBExDzANBg
           ……………AjAAMAkGBSsOAwIdBQADgYEAVIXB0YBs3aidWZVTJ6YMc88Gn/ZIjZ0hc
           pHBU3zp+WEiqzlq1uoKZTvsm/mmjBj6EQkVRcABdCturNa02pbbTClp8l9HQPI9lMCp5jzE
           Co/yaWoJXG7ZeHPH1Loy7eBTQbcrTaELoO51kUSHP0qvul65Sv5EHSqX9gh6/a3S42w=
         </X509Certificate>
      </X509Data>
  </KeyInfo>
  <Object Id="object-1">
    <ClinicalDocument>
       xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/v oc"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schem aLocation="urn:hl7-org:v3
       CDA.xsd"
        <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040" />
       …….
    </ClinicalDocument>
  </Object>
</Signature>
```

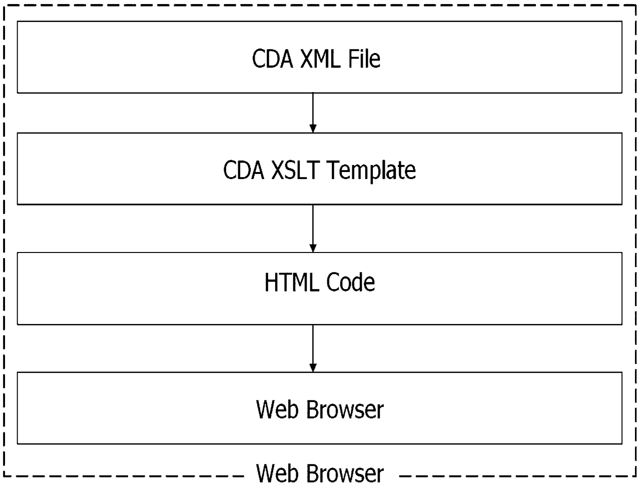


Fig. 4 Approach for displaying a CDA-based XML file

algorithms of digital signature include RSA, DSA and ECDSA [19].

Portable CDA

This section introduces the architecture of Portable CDA, which provides an efficiently, securable and sharable clinical document. A portable device, like a USB flash device, characterizes the advantages of a bigger capacity while being lightweight, removable, and possesses fast access time. Therefore, we adopted this device to implement the proposed architecture of Portable CDA to store and exchange clinical documents. In order to assure the authenticity, integrity and confidentiality of the clinical document, the stored documents need to be signed and encrypted by an authorized person. The smart card [20] is the tool used to implement the digital signature and encryption. The Portable CDA should provide the functions below:

(1) **Importing/exporting a CDA file**: A new CDA XML file can be added into the Portable CDA or an existing CDA XML file exported from it.

(2) **Read the CDA content**: The Portable CDA has the ability of an XML browser. The eXtensible Stylesheet Language (XSL) template is used to transform CDA XML files into the HyperText Markup Language (HTML) format. A web browser core is then used to view the clinical documents.

(3) **Viewing the medical images and multimedia files**: The Digital Imaging and Communications in Medicine (DICOM) standard is a well-known standard that the Portable CDA should include. There are also some simple graphics and multimedia files in CDA document that the Portable CDA must have the ability to open.

(4) **Sorting**: CDA documents in the Portable CDA can be sorted by date, by department, by disease name, and so on. This makes it convenient to view all the CDA documents.

(5) **Encryption**: The files stored in the portable device need to be encrypted properly to protect the information. No one can read the content of the file unless they are authorized.

(6) **The limits of authority**: All CDA documents are kept encrypted to prevent unauthorized disclosure. However, patients can handle the decryption key to control the protected information to maintain their personal privacy.

(7) **Digital signature**: To assure that the CDA document is not modified arbitrarily so that its validity can be verified, the CDA document needs to be signed by legitimate medical staff and a digital signature generated.

(8) **Emergency access:** When a patient is in a narcose or critical situation, they can not decrypt the protected CDA documents. It is necessary to have a mechanism for medical staff to obtain the decryption key and access the CDA document stored in the portable device.

We use the CDA standard and the hospital information system database to produce a CDA document. We query the medical record from the database by using a HL7 message, and combine the data and the CDA format to output the CDA document. Here we use the discharge summary as an example of generating the CDA XML file. The discharge summary is an important part of the medical record that is often created by a hospital. It records many kinds of items, such as patient information, brief history, laboratory results, discharge status, medications, and so on. Figure 2 is a snapshot of a CDA document of the discharge summary. We can see the embedded coded content inside it.

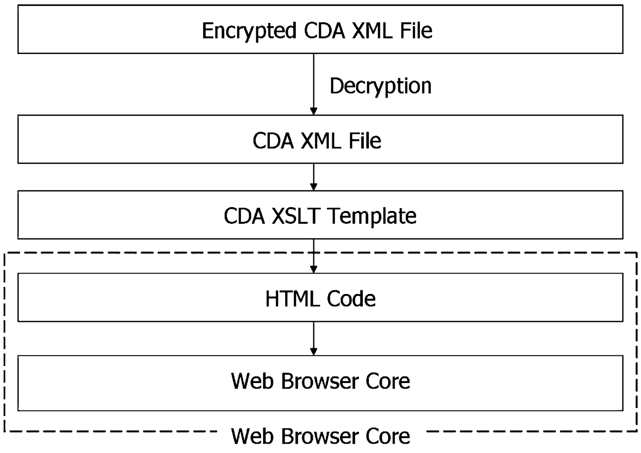
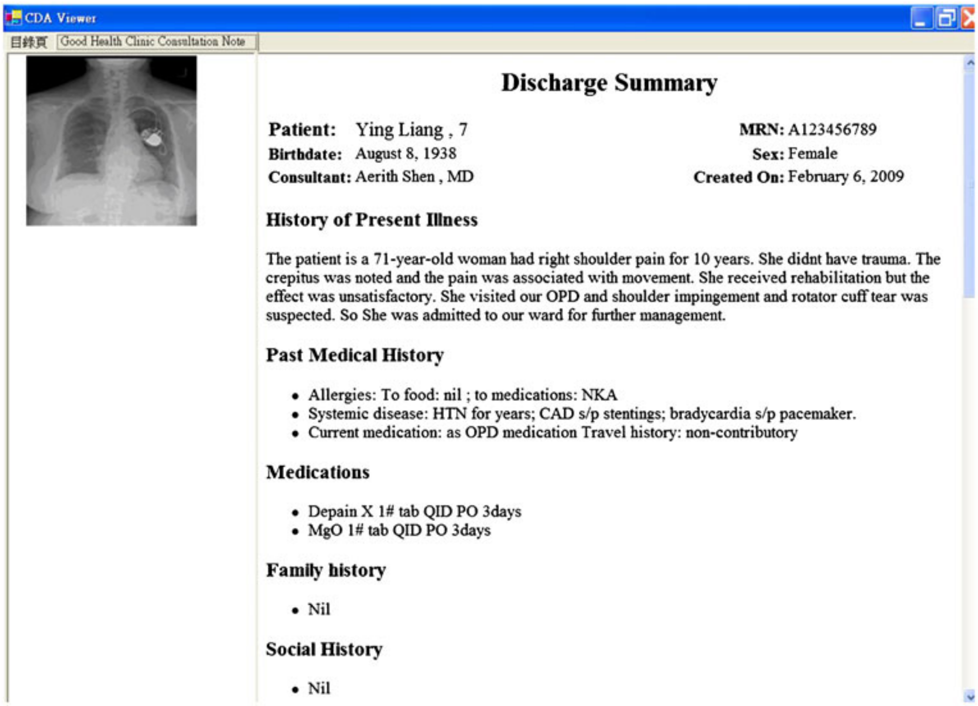


Fig. 5 Approach of Portable CDA to display CDA-based XML files



Discharge Summary

Patient: Ying Liang , 7
Birthdate: August 8, 1938
Consultant: Aerith Shen , MD

MRN: A123456789
Sex: Female
Created On: February 6, 2009

History of Present Illness

The patient is a 71-year-old woman had right shoulder pain for 10 years. She didnt have trauma. The crepitus was noted and the pain was associated with movement. She received rehabilitation but the effect was unsatisfactory. She visited our OPD and shoulder impingement and rotator cuff tear was suspected. So She was admitted to our ward for further management.

Past Medical History

- Allergies: To food: nil ; to medications: NKA
- Systemic disease: HTN for years; CAD s/p stentings; bradycardia s/p pacemaker.
- Current medication: as OPD medication Travel history: non-contributory

Medications

- Depain X 1# tab QID PO 3days
- MgO 1# tab QID PO 3days

Family history

- Nil

Social History

- Nil

Fig. 6 Realistic CDA viewer

The title text is in the <title> tag, the generated date is in the "value" property of the <effectiveTime> tag, the language code is in the "code" property of the <languageCode> tag, and so on.

Figure 3 shows a signed CDA document. All signed content and the information of the signature are wrapped by the <Signature> tag. <SignedInfo> records the information of the signature. <CanonicalizationMethod> points out the processing method before performing signature calculations which is recorded in the algorithm attribute. The algorithm attribute of the <SignatureMethod> tag records the position where can find the definition of the signature algorithm. <Reference> records the reference position of the signed content and its type information. There are two tags inside <Reference>. <DigestMethod> records the position where can find the definition of the digest algorithm. <DigestValue> stores the value of the digest algorithm. <SignatureValue> records the value of the digital signature. It is always encoded using base64. <KeyInfo> contains the public key information of the digital signature. <X509Data> represent this document sign with X.509 certificate and inside this tag are all information about the X.509 certificate. <X509Certificate> is containing a base64-encoded certificate value. Inside the <Object> tag is the original content which needs to be signed. We can find the corresponding relationship between the ID attribute and the URI attribute of the <Reference> tag by comparing its value.

A basic approach to display CDA-based XML files is shown in Fig. 4. Because CDA documents are of XML formation, we can use Extensible Stylesheet Language Transformations (XSLT) [21] to transform XML to a general web site format. XSLT is a World Wide Web Consortium (W3C) Recommendation. XSLT is used to transform an XML document into another XML document, or into another type of document that is recognized by a browser, like HTML and Extensible HyperText Markup Language (XHTML). We transform an XML document into

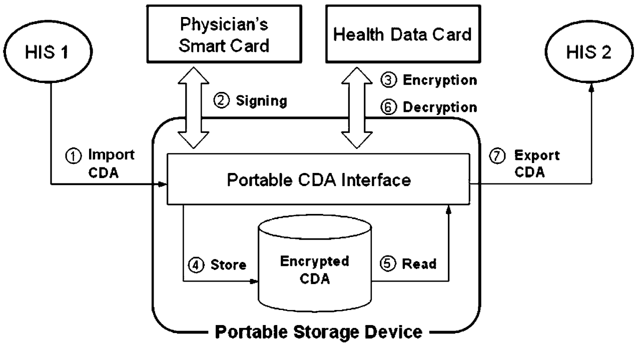


Fig. 7 Exchange flow of the clinical documents by Portable CDA

an HTML format that the browser can recognize so that the content inside the XML document can be displayed.

In this case, we have an XSL file to store the displayed style of a CDA XML document. When the browser reads a CDA XML file, it will automatically determine the corresponding XSL file which is recorded in the XML file and transform the XML document into HTML format. All these actions are done automatically by the browser.

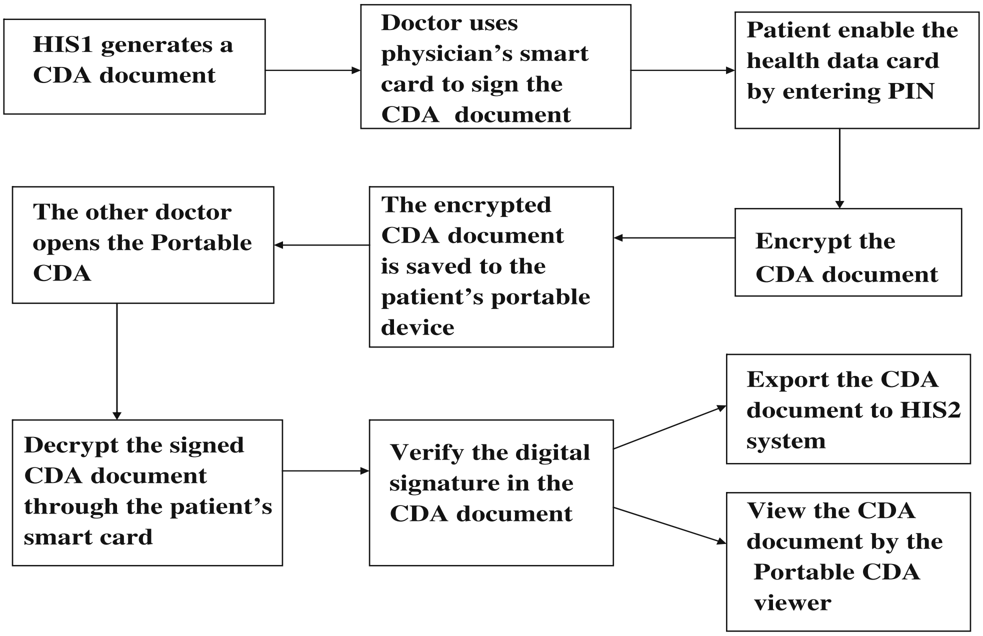
However, the Portable CDA cannot display CDA-based XML files using this basic approach. This is because CDA-based XML files that are stored in the portable storage are encrypted; hence the contents are not recognizable to the web browser. In order to solve this problem, the Portable CDA adopts a new approach as shown in Fig. 5. The decryption and transformation work is done by the Portable CDA. The Portable CDA will then open a blank web page and insert all the transformed contents into the blank web page. Finally, we use a web browser core to open the web page to see the correct contents and display style.

The proposed prototype of CDA viewer is shown in Fig. 6. The right side is the content of discharge summary and the left side is the image list which stores images embedded in the CDA document. The reason why we put those embedded images in the image list left side is that all of our files are encrypted. The right side is a web browser core. When a CDA document has an external image link, the web browser core will directly open the image. It will fail to open the image because our images all are encrypted. The method we used is to find the external image links and decrypt them first when opening the CDA file. Then we remove these links form the showing content and put these images into the image list left side. If we want to see the real size of images, we can double click the image which we want to see. It will pop up a new window to show the real size of the image.

In the proposed Portable CDA, the doctor has a physician's smart card that stores the private key for signing clinical documents. Each patient has to register at the governmental healthcare office to obtain a health data card in order to become eligible for the healthcare services provided by the healthcare provider. The office generates a secret key for the patient and stores the patient's identification information as well as the secret key in the healthcare office database and on the patient's health data card, and then gives the card to the applicant. The patient's health data card is used to encrypt CDA documents and to enforce rules-based access control to a patient's CDA documents.

A general exchange flow of the clinical documents by Portable CDA is shown in Fig. 7, and the Information flow across different HIS is presented in Fig. 8. The doctor uses a physician's smart card to sign the CDA document after the hospital information system (HIS) transfers the medical record to CDA format. To encrypt the signed CDA document, the patient must enable the health data card by entering his or her Personal Identification Number (PIN). The enabled card will encrypt the CDA document. Then, the encrypted CDA document is saved to the patient's portable device. When the patient goes to another hospital, the encrypted CDA document is decrypted using their personal health data card. The doctor reads the CDA document with the

Fig. 8 Information flow across different HIS


HIS1 generates a CDA document
Doctor uses physician's smart card to sign the CDA document
Patient enable the health data card by entering PIN
Encrypt the CDA document
The encrypted CDA document is saved to the patient's portable device
The other doctor opens the Portable CDA
Decrypt the signed CDA document through the patient's smart card
Verify the digital signature in the CDA document
Export the CDA document to HIS2 system
View the CDA document by the Portable CDA viewer

viewer provided by the Portable CDA. It also can be output as a CDA-based XML file. The HIS system can fetch the individual items mapped in data tab.

If the patient is in a state of narcosis and cannot perform the decryption, the doctor can apply for and get the secret key from the governmental healthcare office to decrypt the encrypted CDA document.

Conclusion and discussion

Despite the rapid development of the World Wide Web, people still cannot access the Internet everywhere. The computer is more pervasive than the Internet, so the Portable CDA is useful today. Furthermore, even if two hospitals are inter-connected, there are still a lot of difficulties, such as the strategies of the hospital and legal requirements. If these two hospitals are located in different countries, the exchange of the clinical documents is even more cumbersome. It may depend on the friendship and the laws of the two countries. If we use the Portable CDA, we just need to consider whether or not the hospital has a computer.

The Portable CDA can also be a lifelong personal health record. The American Society for Testing and Materials (ASTM) International Continuity of Care Record (CCR) [22] is also a standard of data exchange. ASTM International defines the CCR as a "summary of the patient's health status (e.g. problems, medications, allergies) and basic information about insurance, advance directives, care documentation, and care plan recommendations" [23]. Clinicians have participated in the creation of the CCR, so its forms and contents are those that clinicians actually want. The CCR focuses on the items that need to be preserved and displayed when saving a lifelong care record. It is very useful for physicians when diagnosing patients because the CCR has saved items which physicians want to see.

HL7 announced in November 2005 that it was creating an implementation guide for expressing the CCR data set in the CDA [23]. In February 2007, HL7 announced that the Continuity of Care Document (CCD) had passed HL7 balloting and is endorsed by the Healthcare Information Technology Standards Panel (HITSP) as the harmonized format for the exchange of clinical information including patient demographics, medications and allergies [24].

The CCR has defined all the necessary items for the exchange of clinical information, so the CCR architecture may overlap the CDA templates. Although the CCR and the CDA are different standards, the CCR also uses XML format to make it easy to exchange. It gives the opportunity to change the CCR architecture to the CDA templates. If this is successful, we can benefit by reducing the manpower needed to develop such similar templates and to enhance the usage of the CDA.

Reference

1. Yu, W. D., Chekhanovskiy, M. A., An electronic health record content protection system using smart card and PRM™. *In Proceedings of the 9th International Conference on e-Health Networking, Application and Services*, (pp. 11–18), 2007.
2. McGuire, M.R.: Incorporating an EPR system with a universal patient record. J. Med. Syst. **30**, 259–267 (2006). doi:10.1007/s10916-005-9007-7
3. Maglogiannis, I., Delakouridis, C., Kazatzopoulos, L.: Enabling collaborative medical diagnosis over the internet via peer-to-peer distribution of electronic health records. J. Med. Syst. **30**, 107–116 (2006). doi:10.1007/s10916-005-7984-1
4. Dolin, R.H., Alschuler, L., Boyer, S., Beebe, C., Behlen, F.M., Biron, P.V., Shabo, A.: HL7 Clinical document architecture, Release 2. J. Am. Med. Inform. Assoc. **13**(1), 30–39 (2006). doi:10.1197/jamia.M1888
5. Extensible Markup Language (XML) 1.0 (Second Edition) W3C Recommendation 6 October 2000. Available from: http://www.w3.org/TR/2000/REC-xml-20001006
6. Marcheschi, P., Mazzarisi, A., Dalmiani, S., Benassi, A., New standards for cardiology report and data communication: an experience with HL7 CDA release 2 and EbXML. *Comput. Cardiol*. 383–386, 2005. doi:10.1109/CIC.2005.1588117
7. Bilykh, I., Jahnke, J. H., McCallum, G., Price, M., *Using the clinical document architecture as open data exchange format for interfacing EMRs with clinical decision support systems. In Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, (pp. 855–860), 2006.
8. Kim, H. S., Tran, T., Cho, H., A Clinical Document Architecture (CDA) to generate clinical documents within a hospital information system for E-Healthcare services. *In Proceedings of the 6th IEEE International Conference on Computer and Information Technology*, (pp. 254–254). 2006.
9. Chan, A.T.S., Cao, J., Chan, H., Young, G.: A web-enabled framework for smart card application in health services. Commun. ACM. **44**(9), 77–82 (2001). doi:10.1145/383694.383710
10. Kardaas, G., Tunali, E.T.: Design and implementation of a smart card based healthcare information system. Comput. Methods Programs Biomed. **81**, 66–78 (2006)
11. Health Level Seven, Inc., HL7 V3 Guide. HL7 Version 3 Interoperability Standards, Normative Edition, 2006.
12. SNOMED Clinical Terms, College of American pathologists.: Available from: http://www.snomed.org/. Accessed Jan 2007.
13. Logical Observation Identifiers Names and Codes (LOINC): Available from: http://www.loinc.org/. Accessed Jan 2007.
14. Win, K.T., Susilo, W., Mu, Y.: Personal health record systems and their security protection. J. Med. Syst. **30**, 309–315 (2006). doi:10.1007/s10916-006-9019-y
15. Gritzalis, D., Lambrinoudakis, C.: A security architecture for interconnecting health information systems. Int. J. Med. Inform. **73**, 305–309 (2004). doi:10.1016/j.ijmedinf.2003.12.011
16. Win, K.T.: A review of security of electronic health records. Health Inf. Manage. J. **34**(1), 13–18 (2005)
17. 17 FIPS PUB 197, Advanced encryption standard. Federal Information Processing Standards Publications, US Dept. of Commerce/N.I.S.T., Nov. 2001.
18. Snyder, A. M., Weaver, A. C., *The E-Logistics of securing distributed medical data. In Proceedings of the IEEE International Conference on Industrial Informatics*, (pp. 207–216), 2003.
19. Adams, C., Lloyd, S., *Understanding the public-key infrastructure: concepts, standards, and deployment considerations. New Riders*, 1st edition 1999.

20. Zoreda, J.L., Oton, J.M.: Smart cards. Artech House, Norwood, MA (1994)
21. Transformations, X. S. L., (XSLT) Version 1.0 W3C Recommendation 16 November 1999. Available from: http://www.w3.org/TR/xslt. Accessed Jan 2007.
22. ASTM WK4363 Draft Standard Specification for the Continuity of Care Record: Version 1. ASTM International, 2004.
23. Ferranti, J. M., Musser, R. C., Kawamoto, K., Hammmond, W. E., The clinical document architecture and the continuity of care record: a critical analysis. *J. Am. Med. Inform. Assoc*. 13(3), 2006. doi:10.1197/jamia.M1963
24. HL7 Continuity of Care Document: a Healthcare IT Interoperability Standard, is Approved. Available form: http://www.hl7.org/documentcenter/public/pressreleases/20070212.pdf. Accessed Jun 2007.