Immunological Access Control Model in Distributed Clinical Document Systems

Stephen Chu [a], Mike Mair [b]

[a] *Dept of MSIS, University of Auckland, Auckland, New Zealand*
[b] *Timaru Eye Clinic, Timaru, New Zealand*

Abstract

An aging population and a rapid increase in the prevalence of chronic disease exert great pressure on the healthcare system and accentuate the need for integrated/coordinated healthcare services. Effective information interchange between healthcare providers is considered key to the successful implementation of integrated care. The Clinical document architecture (CDA) has been proposed as the currency for electronic healthcare. It provides an architecture to facilitate effective healthcare information interchange, and an evolution path to the dream of a universal shared electronic record system.

The authors of this paper propose a network of regional systems connected to the Internet using a distributed CDA architecture to facilitate seamless healthcare information access any time, all the time. At each clinical interview, a CDA header and an attestable unit of clinical data are created by the provider system. A detachable CDA Header Object clone will be transmitted to a regional system which maintains a directory of pointers to the CDA headers and documents to support searches by requesters in future.

This model is based on the immunoglobulin molecule as a metaphor. It is a readily implementable architecture for distributed CDA / electronic healthcare record systems. A similar concept was piloted in Finland. Delegates from a number of European countries, USA and Australasia had expressed keen interest in collaborating at international level to further develop and implement these concepts.

Keywords:

Role-based secure access, distributed electronic healthcare records, clinical document architecture

Introduction

The integrated care model has been shown to be highly effective mechanism for coordinating healthcare processes or activities and delivering high quality care/services [6]. Fundamental to the integrated care concept is the effective and efficient interchange of patient information across the healthcare continuum. Evidences from research suggested that effective information sharing among various healthcare providers has been far lower than desirable [2, 3, 4].

The 'cradle to grave' electronic healthcare record (EHR) system is considered the ultimate tool to facilitate seamless information exchange between all stakeholders involved in patient care planning, delivery and monitoring. Given that the development and implementation of integrated EHR systems are still some time away, clinical document exchange presents an immediately implementable solution for improving healthcare provider communications.

The Clinical Document Architecture (CDA) is a document representation and interchange standard developed by the Structured Document Technical Committee (SDTC), one of the technical workgroup of Health Level Seven (HL7). CDA has been proposed as a common currency for electronic healthcare [1]. It addresses the interoperability issues of syntactic and semantic standards.

To fulfill the dream of a universal shared document/EHR system in a distributed environment, technology must be in place to discriminate legitimate from illegitimate attempts to access the document/data. Such techniques must be endlessly customizable to cater for the great diversity of access practices in global healthcare.

The authors of this paper propose a revised version of 'Access Lock' concept, which was initially submitted to Working Group 1 of International Standards Organization Technical Committees on Health Informatics (ISO/TC215 WG1) [7]. It recommends the segregation of CDA into two separate universal healthcare packets, which are called the 'access lock' and 'attestable unit'. This paper discusses the application of the immunological metaphor in the design of 'access locks' for secured access to attestable units stored on distributed CDA based EHR systems.

The Immunological Metaphor

The proposed secured access control is modeled on the 'bi-functional immunoglobulin family of molecules from immunological science [8-10; 15]. In the immune system, a single class of molecule, the immunoglobulin, exhibits bi-functionality in that each molecule has a 'recognition' end and a 'business' end (Figure 1). The 'recognition' end that is highly variable targets antigen, which is usually but not always material foreign to the organism. The 'business' end determines what action the molecule performs when the template match to antigen is made.

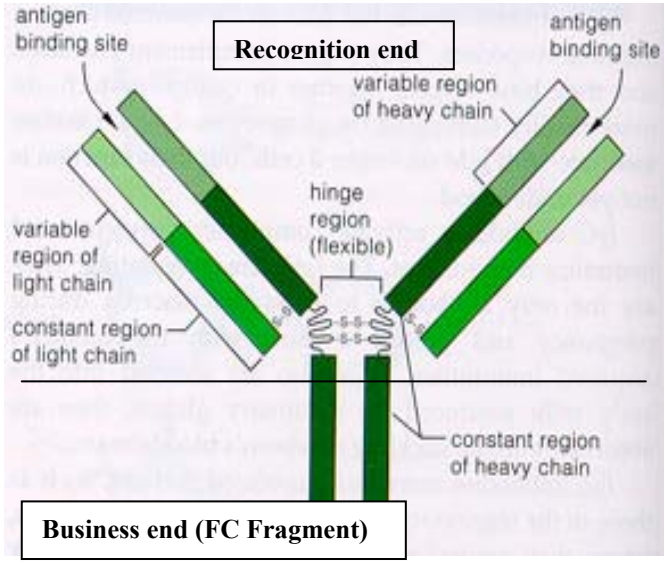

Figure 1. The Immunoglobulin Molecule

The 'recognition' ends can be very specific, and a mechanism exists to generate a limitless supply of different template configurations, to match an equally limitless diversity of antigens (targets). A single design acts as the interface in hugely diverse processes, configured to an endless diversity of targets with great specificity.

The Clinical Document Architecture

The Clinical Document Architecture (CDA) is a document markup standard that specifies the structure and semantics of clinical document for the purpose of exchange [5]. A clinical document contains details about the participants (providers, health organization, and patient), observations (including history, examination and diagnostic tests) and services provided. CDA documents are encoded in eXtensible Markup Language (XML). The documents derive their meaning (including clinical terms used in the document) from the HL7 Reference Information Model (RIM) and uses HL7 Version 3 data types (www.hl7.org). CDA documents can be transmitted in HL7 messages designed to transfer clinical documents.

CDA can be legally authenticated through the use of digital signatures. It also has the advantage of being both human readable and machine processable. The appeal of CDA lies in its ability to meet the document-centric information capturing information, generated during practice of clinicians, as clinical notes in varying formats (highly structured to free text). On the other hand, the syntactic and semantic structures imposed by XML markups makes the document contents processable by computers, thus enabling the clinical notes across documents to be compared.

The CDA Release 2 Ballot document (28 July 2003) defines CDA to be structurally organized into a header and a body [11] (Figure 2) [hppt://www.hl7.org]. The header contains information about the document type, its confidentiality status, the actors of the health event (e.g. the provider who participated in the care, the document creator and the authenticator, the intended recipient), the organization, and the service targets (patient and family). It conveys the context information about the document. The CDA body structures such as sections, paragraphs, tables, and lists provide the 'wrappers' to partition the clinical notes into logical and meaningful compartments, for example, medical history, vital signs, cardiovascular examination, problems, treatment plan, etc. The captions of the 'wrappers' provide the XML markup to tag the various portions of the clinical notes or data so that they can be manipulated and displayed by computers.

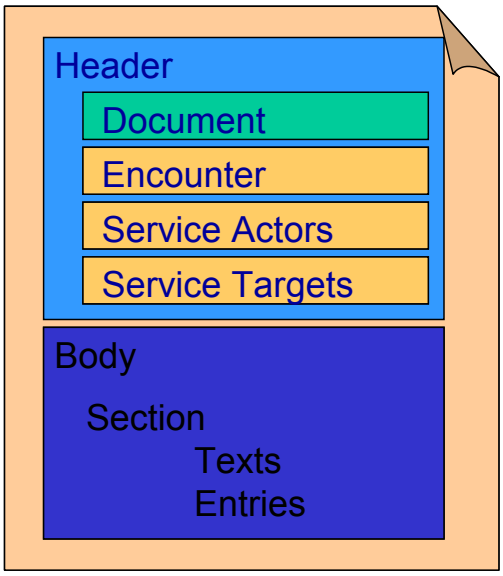

Figure 2. The CDA Architecture

The segregation of CDA into header and body sections makes such structure highly analogous to the 'bi-functional' architecture of the immunoglobulin. The header can be used as the 'recognition' end by a requester to match to a request for a CDA document. This activates the 'access key and lock' mechanism for secured remote access in a distributed environment. The body will function as the parcel of 'attested data'.

The 'Immunoglobulin Metaphor' for Secured CDA Access

The authors' original proposal to ISO/TC215 WG1 [7] recommended that the requester's clinical information system contained a 'request manager' application, which would generate and transmit an 'Access Request' object (ARO). The ARO would carry sufficient information as a request template (e.g. patient ID, information required, requester ID, requester role and request reason). The 'Access Lock' object (ALO) from the target system's 'access controller' application would use information sent from requester ARO to determine whether requested information is available and whether the requester has the right to access the information requested. The 'access lock' concept for the attestable unit was to act as a guard and a pointer to the attestable unit.

The CDA header contains entries for <Author> and <Legal Authenticator>. Both require that the responsible individual has signed a document manually or electronically. While electronic signatures are not part of the CDA header, it does require the acquisition of signature to be documented, via the <signatureCode value="**S**"/> component. However, this does not confer access control. The CDA Release 2 Ballot Document published on 28 July 2003 (P.16) specifies that:

"For communications over public media, cryptographic techniques for source/recipient authentication and secure transport of encapsulated documents may be required, and should be addressed with commercially available tools outside the scope of this standard".

CDA as an integral component of universal shared EHR systems will reside within an increasingly distributed environment. Some CDA will be created and stored in their original systems. Others may be stored in regional systems. The 'Immunoglobulin-metaphor' for access control provides a mechanism to address information access security issues in the distributed environment.

Clinical data are generated and documented during each clinical interview/encounter. Within the CDA application, a CDA document will be created at the end of the interview. The CDA document will provide the source clinical information, which can be accessed by different healthcare provider to support the continual care of the patient in an integrated care environment. Central to the immunological metaphor for access control are a set of objects:

- The ALO and the Detachable CDA Header Object (DCHO)
- The packet of clinical data (Attestable Clinical Data Object, ADO).
- The Request/Search object (RO)

Depending on the configuration of the system, the full copy of the CDA document, or only the DCHO is sent to a regional system. Alternatively, the full CDA object set can be stored on the provider's (original) system. The CDA object set remains within the system hosting the data, along with the audit trail of the 4 WHs (by whom, when, from where or which organization, about who) of instances of access to the data.

The Request Object (RO)

The RO (Figure 3) is generated and dispatched by the provider system, which requests certain clinical information for continual care of a patient. It is routed through the distributed environment in search of the relevant information (Figure 4). This object contains the requester (service actor) ID and role information. It also contains references to the document type (e.g. discharge summary, referral, or progress notes) and data required. To strengthen security of data transmission, dual key cryptography can be employed. The RO can contain a public encryption key and a digital certificate from the requester.

The Detachable CDA Header Object (DCHO)

The DCHO (Figure 3) contains metadata about the clinical document and the clinical event as defined by the CDA standard. It contains information such as the document type, the encounter (including date, time, nature of the event), the provider, the author, legal authenticator of the document, the provider organization, and the patient as the service target. The DCHO uses a set of defined methods to:

- compare the document meta-data information given by the RO with CDA header information stored in regional system to determine whether a match exist between the document required and CDA held at the document store –checkDocInfo() method.
- check that the patient details provided by the RO from the requester match the target patient for whom the CDA header (in the regional server list) was created – checkServiceTarget() method.
- interrogate the CDA Header List stored in the regional server which should hold the Network ID/address of where the original attested CDA data/documents are held - the Provider Organisation that created and stores the data/document, or the regional server itself.
- interrogate the regional system and obtain from it the (Internet) network address of the original system on which the matching full CDA document is stored – getOriginatingOrgNetID(). It is activated when a matching CDA is found and if the CDA is stored on the CDA creator system. If a matching CDA is found on the regional system receiving the request, it will return to the requestor its own network address.

The Access Lock Object (ALO)

The ALO is created at the time the attestable clinical data unit is created. It is stored together with the target data to which its access control properties are applied. The object defines the access privileges/attributes for each piece of clinical data and which healthcare worker (as determined by their roles) is/are allowed access to the data. At the time clinical data are created, the patient can assign their access attribute values; otherwise, 'default' access privilege (as specified by organization/national policy) will be applied. The access privileges can be altered by the patient during subsequent visits. Its matchReq&DataAccessRole() method determines whether the requestor's 'Role for Access' value satisfies that 'Access Control' values previously defined for the requested data (Figure 3).

Confidentiality Attributes for CDA

CDA provides confidentiality codes the values of which will propagate throughout the entire document when applied at the header level. It also provides a context conduction indicator (contextConductionInd) as a mechanism for over-riding confidentiality values defined earlier in the CDA document. Confidentiality code values can be defined by the international standards organization (with local

extensions enabled), which provides attributes for defining data confidentiality along with role-based access rights.

In the ISO paper [7] 'access ontologies' were identified as 'self-defining' sets. We suggest that autonomous culturally derived systems of roles could nevertheless 'connect in' to the confidentiality levels demarcated in the CDA by their 'confidentiality codes'. These might apply to sections within CDAs. Role translation schemas would be necessary at 'realm boundaries' individually customized. However, the mechanism of access control by confidentiality attribute would remain, just defined differently for each user group.

Applying the 'Immunological Metaphor' to Secured CDA Access

The CDA header and body components, together with the Access Lock Object, need to be stored on robust and fault tolerant systems to support 24/7/365 information access demands. For large private practice groups with sufficient technical expertise and financial resources, the CDA components can be stored on the original document creator systems. A copy of the detachable CDA header object is also sent to the regional system to speed up retrieval. For small practices with low technical capability and financial power, storing the all document components on a regional system may be the most desirable (or even the only) option.

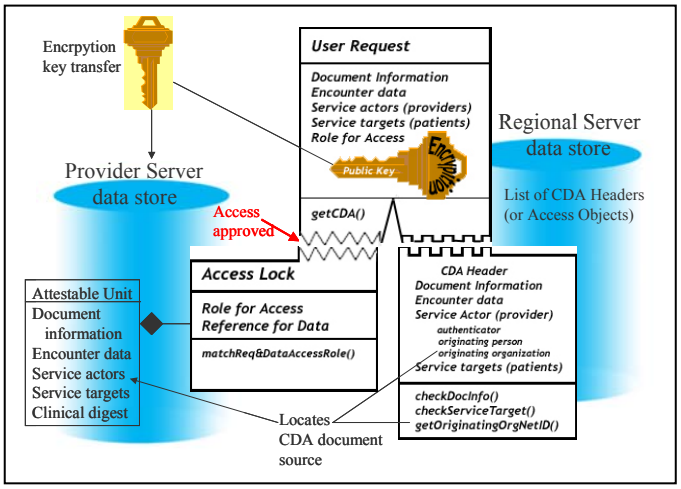

Figure 3. Matching Request to Source CDA

We propose four stages (Figure 3 and 4) for a universal access control mechanism to accompany the CDA as the universal 'attestable unit' of healthcare information:

(1) When a provider requires to access external clinical information sources for continual care of the patient, the provider's application will construct a request or search object which contains information about the target patient, and 'index' of information required, the requester ID and the requester role information. Included in the RO is also the public encryption key and digital certificate from the requester institution.

(2) The RO is automatically routed by the requester application to the nearest regional system, which provides a directory service for searching the relevant documents. Using the information from the RO, the regional system searches through its directory to fine whether there is a match between the request and the copies of detachable CDA Header object stored on the regional server. If a match is not found, the RO will be routed onward to the next neighboring regional system, which will in turn route the request onto the next …….. until a match is found, or eventually, a 'no find' result may be returned if the search effort on all known servers failed to identify a correct match.

(3) When a match is made, including the access role match (Figure 3), the requester gets access to the referent of the stored or virtual CDA. The digital certificate enclosed within the RO envelope authenticates the identity of the requester and the public key he/she sends with the request.

(4) The holder of the CDA data then uses the public key from the requester to encrypt the data, and transmit the requested data across the Internet. The encrypted data can only be deciphered by the requester who holds the private decryption key, thus ensuring the confidentiality and integrity of the transmitted data.

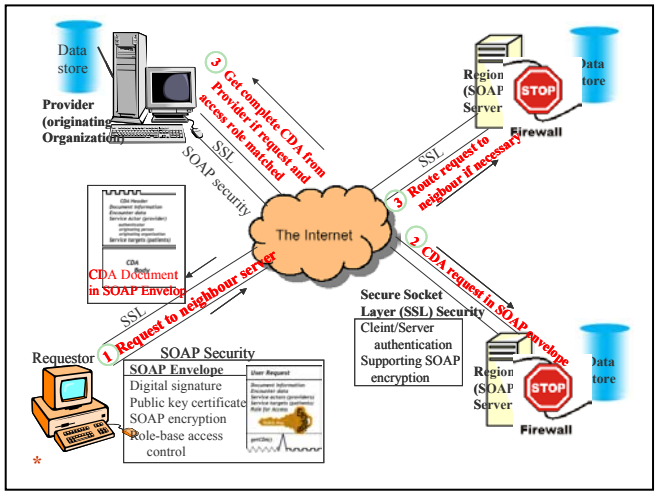

Figure 4. Searching & Transmitting CDA via Internet

This model assumes continuous 'on line' availability of data from participating providers. If any provider opts to adopt intermittent connection mode such as using a dial up approach, a full copy of the CDA will need to be stored at the provider's neighboring regional server to ensure constant availability of the data.

The Internet is a completely open environment. The notion of transmission of sensitive data like clinical documents using the Internet inevitably generates considerable security concerns. It is recommended that all outgoing data from the requester, regional server, and originating organization that created and store the attestable data would be encrypted and enclosed in a SOAP (Simple Object Access Protocol) [12] envelope before transmission. It is also anticipated that transmissions between the requester, the regional servers

and originating organizations would take place over standard secure socket layer (SSL) [13] connections.

The advantage of this approach is that all stakeholders can benefit from secured communication over the Internet. Any node (practice computer or regional server) needs only to know its neighboring node in the distributed architecture.

International and Future Development

Finland proposed and implemented a regional information system in 2001-2002 to service 448 municipalities in 22 health districts [14]. A concept similar to 'detachable' CDA header is proposed and used. During a new health event/encounter, a new package of clinical data is created in the source system together with a CDA header package. The header is then transferred to the regional information system where references to the CDA header and source data are extracted and the reference information inserted into the reference database. The reference information includes patient ID, general description of document contents, encounter date and pointer to the source document. When a request is sent to the regional system for patient data, the system looks up the entry from the list of pointers, and passes the request to the source system, which then generates the whole CDA document 'on the fly'.

CDA will be trialed in New Zealand for distribution of patient discharge summaries and referral requests between care providers. A set of referral enhancement requests has been submitted (in collaboration with Australia) to HL7's Structure Document Technical Committee. They have been included in the CDA Release 2 Ballot Document at the Cleveland meeting in September 2003. The international community has endorsed this concept and. agreed to collaborate to further developing and testing the proposal.

Conclusion

The CDA is proposed as a common currency for electronic healthcare and has been implemented by health care facilities in a number of European countries and USA.

Current trends in globalization and international travels push electronic records towards a distributed architecture. Such architecture will only be accepted by the healthcare industry and consumers if it satisfies two fundamental criteria: seamless and secured information access.

This paper proposes a role-based access control mechanism, digital certificate authentication and public key encryption are considered effective technologies to ensure authorized data access and secured information transmission. Based on the 'bi-functional immunoglobulin' concept, the authors proposed the use of the detachable CDA header enclosed in SOAP envelope and Access Lock objects to provide a secured and authenticated information access model. This ensures secured information access in distributed electronic record environment. The design provides a readily implementable architecture in distributed CDA electronic healthcare record systems.

A similar concept has been tested in Finland with promising results. The international community has agreed to further develop the concepts into wider applications. We hope that the collaborative efforts will lead to a robust, distributed CDA/EHR system that can effectively support continuation of care delivery anywhere around the world.

References

[1] Alschuler L, Dolin B. The clinical document architecture (CDA) framework, Release 1, 2002. (http://www.hl7.org)

[2] Blumenthal D. Quality health care Part 1: What is it? *New England Journal of Medicine*, 1996: 335(15); 1146-1149.

[3] Chassin MR. Quality of health care: Improving the quality of health care, *New England Journal of Medicine*, 1996: 5(14); 1060-1063.

[4] Chu S, Mair M, Hobson C. Developing the Health Event Summary System, in *Proceedings: The New Zealand Health Informatics Conference* August 2002, Auckland, New Zealand.

[5] Dolin RH. Alschuler L. Beebe C. Biron PV. Boyer SL. Essin D. Kimber E. Lincoln T. Mattison JE. The HL7 clinical document architecture, *Journal of the American Medical Informatics Association*, 2001: 8(6); 552-569.

[6] Feachem RGA, Sekhri NK, White KL. Getting more for their dollar: A comparison of the NHS with California's Kaiser Permanente, *British Medical Journal*, 19 January 2002: 324; 135-141.

[7] http://www.health.nsw.gov.au/iasd/imcs/iso-215/areas/atehr2000.pdf

[8] http://www.bmb.psu.edu/courses/bisci004a/immune/immunsys.htm

[9] http://www.liu.edu/cwis/bklyn/acadres/facdev/FacultyProjects/WebClass/microweb/html-files/ChapterH-6.html

[10] http://www.path.cam.ac.uk/~mrc7/mikeimaes.html

[11] http://www.hl7.org/Library/Committees/structure/interimDraft02.zip

[12] http://www.w3.org/TR/SOAP/

[13] http://wp.netscape.com/security/techbriefs/ssl.html

[14] http://www.hl7.de/cdaiw200305/

[15] Male D. *Immunology: An Illustrated Outline*, CV Mosby, 1998.

Author details for correspondence

Stephen Chu, PhD FACS
stephen.chu@auckland.ac.nz

Mike Mair, FRACO
mikemair@eyetech.co.nz