International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:3, No:6, 2009

The implementation of IHE ATNA for the EHR system

Sheng-Chi Tseng, Der-Ming Liou

***Abstract*—**The health record in the Electronic Health Record (EHR) system is more sensitive than demographic. It raises the important issue for the EHR requirement in privacy, security, audit trail, patient access, and archiving and data retention. The studies about the EHR system security are deficient. The aim of this study is to build a security environment for the EHR system by Integrating the Healthcare Enterprise (IHE) Audit Trail and Node Authentication Security (ATNA) profile. The CDAs can be access in a secure EHR environment.

***Keywords*—** IHE ATNA, EHR security.

I. Introduction

THE appearance of the Electronic Health Record (EHR) had improved the heavy and complicated procedure of paper-based medical record. For providing better healthcare, the concept of clinical data exchange is appeared. The best solution for clinical data exchange is to build a life-long EHR system. However, EHR systems also raise the important issue of the health record confidentiality and patient's privacy. The records need better protection because of the health records are more sensitive than demographic. But few physicians agree with the developing of EHR system because of the efficiency, financial, quality, liability and safety are not clear [1].

There are several EHR requirements [2]: security, semantic interoperability, author responsibility, audit trail, version control, patient access, and archiving and data retention. The requirements reveal that it is more important in security and privacy than getting the required health records. According to the study of David C. Kaelbers [3], there were 12% of healthcare system related literatures (the sample size is equal to 100) cited the security and privacy references in National Library of Medicine Pubmed database. But there was 0% of articles really specialized conferring the secure layer issues of health record. The studies about the EHR system security are still deficient.

There are some subjects should be discussed when the EHR system serves. The privacy and security issues are associate with authentication, auditing and should be compliance with relational legislations [4]. Some of studies discuss the access right of health records [5]. To protect patient's privacy, the health record should be seen by those who are authorized physicians that provide the patients consultants. The authentication mechanism is also needed. The authentication confirms the users are the register in the system. To both provide health record sharing services with privacy and security is a challenge [6]. The Health Insurance Portability and Accountability Act (HIPAA)[7] was enacted by the U.S. Congress in 1996. HIPAA provisions address that everyone has the right to access his or her health records. HIPAA also address the security of the health data. For reaching the purpose, the health record systems should be located at a private, security and trusted environment [8]. Although HIPAA describes individuals owns rights to their health record particular, but it does not define the related regulation for health record service providers. It is a big secret worry.

In addition to HIPPA, there are EHR related legislations in Taiwan. According to the No.603, Judical Yuan interpretation the Judicies of Consitutional Court in 2005[9], although the privacy right is not explicit list in the constitution, the privacy right is still the in need of basic rights on the strength of preserving complete majesty and subjectivity. Besides, Computer-Processed Personal Data Protection Law [10] defines health record as a category of personal data. There are some main principles lists in Table.I bring the EHR related lawmaking in Taiwan into practice.

TABLE I
MAIN PRINCIPLES FOR PROTECT PATIENT SAFETY AND PRIVACY

	Definitions
1.	There should be securing software and hardware used by the health record system.
2.	There are clear rules for authority and control mechanism when accessing, adding or deleting, consulting, reproducing and maintain electronic health record. The time and content should be merged into the record for preserving.
3.	The digital signature should be approbation and publication by the central competent authority. It should be attached a time stamp by the central competent authority.
4.	The operator who takes down the health record should add a digital signature with the year, month and day clearly. It attaches and connects with the health record, too.
5.	If there is any modified health record, it should be state the digital signature of the modifier and the date.
6.	The health record deletion process is an inhibition.
7.	There should be a standard operation procedure for staff operating, maintaining, system altering, and audit controlling.

Integrating the Healthcare Enterprise (IHE) recommends the architecture for integrating the information systems in the

DerMing Liou is with the Institute of Biomedical Informatics, National Yang-Ming University, Taipei, Taiwan (phone: 886-2-28267187; e-mail: dmliou@ ym.edu.tw).

Sheng-Chi Tseng is with the Institute of Biomedical Informatics, National Yang-Ming University, Taipei, Taiwan. (e-mail:g39623007@ym.edu.tw).

healthcare environment [11] with the information technology infrastructure and other relevance fields of the healthcare industry. IHE integrates standards into profiles [12]-[15] for encouraging the development of healthcare record exchange technologies.

The IHE Audit Trail and Node Authentication Security (ATNA) profile is an integration profile that establishes security measures. The security measures are together with the security policies and procedures for providing patient information confidentiality, data integrity and user accountability. There are a time server, two secure node grouped with any IHE actor, a secure node grouped with Protected Health Information (PHI) applications, and an audit trail repository in the ATNA concept (see Fig.1).

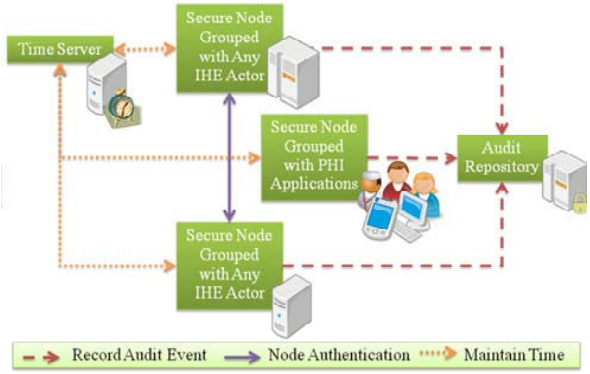

Fig. 1 Audit Trail and Node Authentication Diagram

TABLE II
AUDIT MESSAGES DEFINED BY ATNA

Attributes	Definitions
Status	The status of the operation. Completed, error, or pending
StartTime	The date and start time of the operation <day mmm dd hr:mn:sec GMT –05:00 yyyy>
CompletionTime	The completion date and time of the operation. Forma <day mmm dd hr:mn:sec GMT –05:00 yyyy>
Message	Includes all of the possible information about the operation.
LogLevel	The logging level. For example, Information, Warning, Error, etc.

The basis requirement of ATNA profile is the bi-directional certificate-based node authentication for connections between IHE actors. The authentication confirms the user/network. The authorized user/network can access the required resource in the other system without any interrupt.

The secure node is an application on a system which is complying with ATNA requirement. They can create, access, update, and delete PHI. The secure node grouped with any IHE actor may be implementing with other IHE profiles, for instance, the Cross-enterprise Document Sharing profile (XDS) or Patient Identifier Cross-referencing Integration profile (PIX). All secure nodes synchronize the system time with the time server.

The secure nodes have to audit system events, and send the audit logs into the audit trail repository. The audit trail is the Record Audit Event transaction in the Information Technology Infrastructure Technical Framework (ITI-TF).the ITI-TF had defined the most of the audit trail methods. The Record-Audit-Event audits who the user is, when and where the user does access the system, and which health record does the user access or modify. The IHE ATNA profile had defined the specific attributes for audit messages (see Table. II). The formats of audit messages are in accordance with the RFC-3881 schema, DICOM Supplement 95, HL7, and ITI-TF. The audit trial can be used to illustrate the interaction between systems. The last step of the audit trail is sending the audit trail logs into the audit trail repository. The audit trail repository stores log files and puts log files together for user looking up.

The IHE ATNA seems very helpful when the EHR system developing. The patients register the EHR system, and then go to the clinic for the examination and treatment. But there is a practical condition may break the rules, the emergency procedure. Once the outpatient comes to the emergency department, the physicians will examine and treat the outpatient first. There is the possible the patients' demographics are unknown. Although the EHR system functions for the emergency situations are not enough, the EHR system still play an important role in the emergency department. The emergency procedures are collaborative, complex, and fast works[16]. The existing of the system does help the emergence department workers decrease their burden. Thus, the emergency procedure in the secure EHR system is another important issue[2].

The aim of the study is to build a security environment for the EHR system by IHE ATNA profile. The healthcare owner and the authorized users can access the healthcare data. Only the physicians of the authorized users can alter the healthcare data. The emergency procedure is considered in the study. The study specific discuss the emergency situation with the EHR system.

In the second section of the paper will provide some related concepts, then present the methods used in the study. The third section will describe the expected results, and discuss the study in the conclusions.

II. Materials and Methods

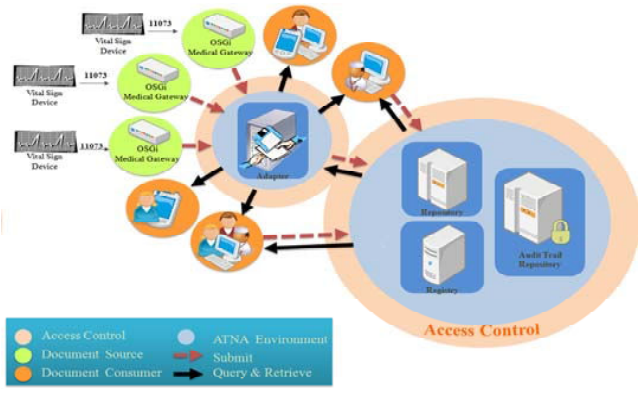

Fig. 2 The whole picture of the study

A. The EHR system

There is an EHR system which built in the study. The EHR system is based on the IHE XDS profile. The IHE XDS profile provides a standards-based specification for sharing clinical record between healthcare enterprises in the form of documents. It facilitates the registration, distribution and access across health enterprises of patient electronic health records. There are a document source, a document repository, a document registry, a patient identity source, and a document consumer in the XDS diagram (see Fig.3).

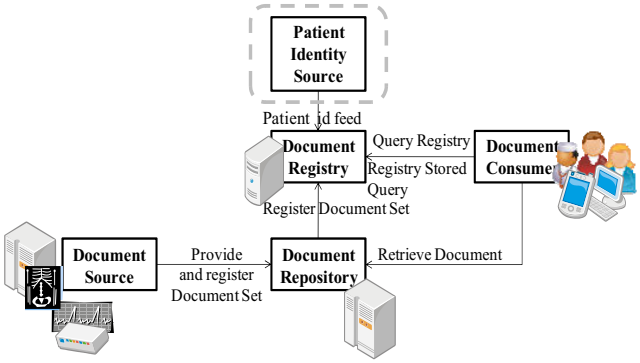

Fig.3 Cross-Enterprise Document Sharing Diagram

The registry (document registry) and repository (document repository) are implemented by National Institute of Standards and Technology (NIST) registry and repository.The registry will point out where the queried healthcare data is. Health Level 7(HL7) v3 Clinical Document Architecture (CDA) is used here as the format of health data. The repository assigns the uniform resource identifier (URI) to documents for subsequent retrieval by a Document Consumer. CDAs are stored in the repository. The document sources are the medical devices and the EHR system. The document sources provide the document Set to the document repository, and register document set in the document registry. Document consumers are the healthcare related applications. The study implements an EHR system interface as the document consumer. Users (such as the physician and patient) can query the registry to get the metadata of the CDAs and retrieve documents from the repository.

The Open Health Framework (OHF) Bridge is used here as the tool to submit, query, and retrieve documents. There are a lot of institutes devoted to the healthcare information standard [17]-[19]. Some of the institutes are devoted to the technique support services platform [11], such as Eclipse Open Health Framework (OHF) and OpenEHR [20]. They share their application development experiences to the healthcare industry by project. OHF is an extensible framework. There are many web services components in the OHF framework, includes the related healthcare standards, data structures, encryption, and the tools for developing the healthcare system. It is an open source framework for the healthcare area [21]. The purpose of OHF is to provide technology and services helping healthcare application platform (electronic medical record system, medical device, etc.) development. The framework can be applied in different electronic health record system. The OHF Bridge is built as the adapter to get the vital signs from the healthcare devices. It also provides querying and retrieving CDAs without the adapter.

B. The secure EHR system environment

For developing a secure environment for the EHR system, the IHE ATNA profile is applied in the study. The manners to reach the ATNA goals list in Table. III.

TABLE III
THE GOALS OF IHE ATNA PROFILE

Goals	Manners
User Accountability	Audit trail
PHI[a] transactions	Centralized audit record repository , access control , and PHI data integrity
Secure node access	TLS
Authentication failures.	Centralized audit record repository and PHI data integrity

[a]PHI = Protected health information
[b]TLS= Transport layer security

1) Audit trail

The audit result is consisting of audit messages and node authentication logs. All transactions within the systems are record in audit trails. There are three message types of audit messages, query, import and export, stand for query, import and export the Protected Health Information (PHI). The OHF ATNA related packages are used for composing the audit messages in the study. The DICOM supplement 95, HL7 vocabulary and IHE extensions are integrated with the source code provide by the OHF ATNA related packages. Thus there is no need to spend lots of time to understand the definitions of the standard message format. Dekker, M. A.C. et al [8] considered that it is better to do the audit actions after the system events have happened. After each system event happened, the system will produce an audit message.

The last process in the IHE ATNA profile is to send audit results in to the audit trail repository. IBM audit trail repository is used to collect the audit trails. This IBM audit trail repository is serves in the Open Health Tools (OHT) project.

2) Node authentication

ATNA specifies that there is a certificate connection between actors. And both actors can know the other one's certificate is valid or not. It also mandates using transport layer security (TLS) as the transmission standard for all communications between secure nodes as a means of the authority.

Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. The connections are populated in the configuration of each node. The TLS is used in the study.

There are 64% people consider it is very important to keep an access control card in the secure mechanism. The primary users of the EHR system are patients, and their healthcare providers. The Taiwan citizen digital certificate is used as the tools for user login in the study. The Taiwan citizen digital certificate is issued by the Taiwan Interior Ministry Certificate Authority.

There is a required process for TLS plug-in with the X.509 certificates, and the data format should match Java Key store (JKS).

The ATNA profile requires only local user authentication. The profile allows each secure node to use the access control technology of its choice to authenticate users. The Role-based access control (RBAC) is the basis of the access control to the system. The users carry out the permissions (privileges) by playing one or more roles. The owner assigns a user as the agent. The agent has the same rights as the owner has. The RBAC is completed with the Taiwan jurisdictions.

C. The emergence situation

To afford the emergency and fast procedures in the emergency department, the adaption of the patient consents are required. The access control mechanism does not really work in the emergency procedure. If the patient already has his CDA stored in the repository, then there was already a consent agreement prepared to be signed via the patient's citizen digital certificate. The consent agreement will be effective in a period of time. After the end of the effective time, the CDA owner should be sign again to allow emergency physician query. If the agreement is with the patient's digital signature, once the patients come to the emergency department and the user's identification can be identified, the emergency treatment doctor can view the patient's CDA. If the patient's identification is unknown, the physician submits a new CDA for the outpatient is allowed.

III. Expected results

Once the patient comes to the hospital at the first time, he should register in the EHR system. He will receive a consents agreement after register. The physician can submit the patient's CDA into the repository via the EHR system. The CDA owner and authorized user using the Taiwan citizen digital certificates to identified their identification. After that, they can query the metadata of the CDA via the registry. They also can query the registry to retrieve CDA from the repository. There is an exception when run into the emergency procedure. The access control mechanism is not work in the emergency time. If the outpatient of the emergency department had signed the consents agreement, the physician is allowed to view the patient's CDA. Otherwise, the physician creates new CDA for the outpatient. The EHR system, the registry and the repository communicate with TLS. All the system events, PHI transactions, and authentication results are record in audit trail messages after the time the events had happened.

IV. Conclusion and discussion

The IHE framework is a great solution to the healthcare environment. There are many profiles to provide the guides to build a complete healthcare system environment for data exchange. The IHE XDS and ATNA profiles are applied in the study. When developing the IHE-completed environment by the IHE profiles, the researcher realized the advantage when using standard. No matter HL7 CDA or IHE profiles, they all provide a clear solution for the researchers to do their studies.

The work of the study is still working. A friendly audit trail not only saves the audit results, but also provides audit results views. The administrator of the repository can view the audit events with a user interface. The audit results arrange to further analysis. It helps administrator the find out the unusual events. But we just use the audit repository only for saving those audit results. The study will implement the audit trail repository in the future work. Because of the lacking the knowledge of encryption algorithms, the data encryption did not discuss in the study. The related encryption algorithms are out of the scope.

The OHF framework did not update anymore. There is a new project called OHT which provides more than OHF. The OHT project is derived from the OHF project. The OHT project gathers more specialists to work for the health information system environment. The IHE ATNA related classes are much different between OHF and OHT. The author of the study is familiar with the OHT ATNA related classes. Thus audit functions are built with the OHF project. The experience of the study will transplant with OHT soon.

Each citizen has his own identification card in Taiwan. There is no need to build a patient identifier cross-reference. The Taiwan citizen digital certificate is the identification card for Taiwanese on the internet. It issued by the Taiwan Interior Ministry Certificate Authority. The uses of the Taiwan citizen digital certificate should be applied especially. Taiwanese can play a part in many public affairs. There is also a National Health Insurance Identification card (NHI IC) which can identify the identification. The NHI IC is used when Taiwanese visit the encounter. There are demographic, some of mediation data, and some health related data in the card. Both citizen digital certificate and NHI IC card can identify individuals. The citizen digital certificate used here rather than the NHI IC because of the citizen digital certificate can sign the document and the data in the certificate is simpler. There is an ideas derived from the study is to add a new filed to the certificate. The field records the consents agreement for the emergence procedure. Thus it is faster to do the emergency procedure.

Acknowledgment

It is a great appreciation to Information and Communications Research Laboratories, Industrial Technology Research Institute of Taiwan for funding this research project, and the excellent research assistances by Dr. Mei-Lien Pan, Ms. Yi-Ting Chou and Tai-Ling Tsai.

References

[1] D. A. Ludwick and J. Doucette, "Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries," *International Journal of Medical Informatics,* vol. 78, pp. 22-31, 2009.

[2] H. van der Linden, D. Kalra, A. Hasman, and J. Talmon, "Inter-organizational future proof EHR systems: A review of the security and privacy related issues," *International Journal of Medical Informatics,* vol. 78, pp. 141-160, 2009.

[3] J. A. Kaelber DC, Johnston D, Middleton B, Bates DW., "A research agenda for personal health records (PHRs)," *J Am Med Inform Assoc,* vol. 15, pp. 729-36. Epub 2008 Aug 28., Nov-Dec 2008.

[4] "Supporting Multi-State Collaboration on Privacy and Security to Foster Health IT and Health Information Exchange," p. 871., 2008.

[5] "Access Control and Data Integrity in Medical Records," *Pediatrics,* vol. 98, p. 538, 1996.
[6] P. E. Kaelber DC, "The Value of Personal Health Record (PHR) Systems," pp. 343-7., 2008.
[7] "United States Deparment of Health and Human Services."
[8] A. Atreja, S. M. Gordon, D. A. Pollock, R. N. Olmsted, and P. J. Brennan, "Opportunities and challenges in utilizing electronic health records for infection surveillance, prevention, and control," *American Journal of Infection Control,* vol. 36, pp. S37-S46, 2008.
[9] "No.603, Judical Yuan interpretationthe , Judicies of Consitutional Court in 2005."
[10] "行政院主計處電腦處理個人資料保護法."
[11] "Free and open source enabling technologies for patient-centric, guideline-based clinical decision support: a survey," *Yearb Med Inform,* pp. 74-86, 2007.
[12] "IHE IT Infrastructure Technical Framework Volume 1 (ITI TF-1) Integration Profiles."
[13] "IHE IT Infrastructure Technical Framework Supplement 2004-2005 Audit Trail and Node Authentication Profile (ATNA)."
[14] "IHE Cross-enterprise Document Sharing for Imaging."
[15] "IHE Infrastructure Profile Overview," 2006.
[16] C. P. Nemeth, R. I. Cook, and R. L. Wears, "Studying the Technical Work of Emergency Care," *Annals of Emergency Medicine,* vol. 50, pp. 384-386, 2007.
[17] "HL7."
[18] J. Choe and S. K. Yoo, "Web-based secure access from multiple patient repositories," *International Journal of Medical Informatics,* vol. 77, pp. 242-248, 2008.
[19] "European Comittee for Standardization."
[20] G. Goth, "Global Information Health Networks Get a Boost," *IEEE Distributed Systems Online,* vol. 7, p. 4, 2006.
[21] e. Lodewijk Bos, Inc, L. Roa, K. Yogesan, Andy Marsh, *Medical and Care Compunetics 3*: IOS Press, 2006.