

Design and Implement an Electronic Health Records Platform Based on the Management of the Personal Consent

Yi-Yun Ke, Der-Ming Liou

Institute of Biomedical Informatics, National Yang-Ming University
No.155, Sec. 2, Linong St., Beitou District, Taipei City 112, Taiwan (R.O.C.)

Abstract- The Electronic Health Record (EHR) system is more generally and we should pay more attention on the patient's privacy. The patient's consent is one of the privacy topics. The study focuses on the creating and managing of the patient's consent. The integration of the HL7 standards and the IHE BPPC profile provides the base for the creation of the patient's consent. Establishing the platform offers the patients creating, revoking or updating their consents. Through the platform, they can manage their consents friendly.

I. INTRODUCTION

Due to the advancement of the information technology, the paper-based medical record becomes electronic progressively. The emergence of the Electronic Health Record (EHR) could improve the complex and heavy procedure of the paper-based medical record. The EHR records the information of the patient's health data. The Electronic Health Records and the patient's health and life are close related, so the patients usually have no choice at that status. They have to provide the correct information to the physicians and the information will be recorded in the Electronic Health Record. In contrast to the general personal information, the personal health information is more sensitive information and need more protection ensuring such information is not leaked. Therefore, the security and privacy of the Electronic Health Records is very important.

As a result of the different background and religion environment of individuals, some health records is high level sensitive, such as the record of abortion, the patient doesn't want it to be accessed by non-relevant people. The health status of the individual also may influence the development of the career. The information of the health records may provide the other organization to use, for example, the research organization, the pharmaceutical factory or the insurance company, these organizations interest on the patients' health records. But the patient doesn't like to share their sensitive data to be accessed by the other non-relevant people or the organizations. So, besides the security and privacy of the health records, the patient's volition is also important.

About the EHR, there are several requirements [1]: security, semantic interoperability, author responsibility, audit trail, version control, patient access, and archiving and data retention. About the security requirements of EHR system, Wainer J. et al proposes some opinions [2]. They discuss around four topics: confidentiality, control, integrity and legal value. On the control topic, the patient controls the access right of his or her records. The patient may give the healthcare provider access rights and revoke the permission after treating over.

In the medical field, the security and privacy of the information is quite important topic. Many countries also enact the law related with the security and privacy of the information such as Australia's Privacy Act[3], New Zealand Health Information Privacy Code[4], and Health Insurance Portability and Accountability Act (HIPAA)[5] etc. In 1996, the American Congress passed through the Health Insurance Portability and Accountability Act, HIPAA. HIPAA regulates the security and privacy of the electronic medical information. It acts the standard of the electronic health information exchange between the healthcare providers or between the healthcare providers and insurance companies. HIPAA also interprets when the health information not includes the identity of the individuals, the organizations or the researchers can use the information without the individual's approval.

There are some countries establish the system about the patient's consent, for example, New Zealand[6], Norway[7], or Australia[8] etc. In Australia, the *Healthlink* was established by the NSW (New South Wales) Department of health. The system assists to collect and store the information that come from the individuals and other different healthcare providers. The system sets as the center of accessing and storing and it provides the protection of the security of the data to avoid the non-relevant person accessing and storing the individuals' privacy data. This system also involved the individual's consent.

One of the important standards about e-health is Health Level Seven (HL7) [9]. The Community Based Collaborative Care (CBCC) Work Group of HL7 facilitates development and use of HL7 standards that support and integrate the provision of HHS (health and human services) in community and non-acute care residential settings [10]. The CBCC Work Group is currently focused on some domains; one of the domains is privacy consent directive message format and vocabulary and they implement the project regarding it—CBCC [11]. The related documents in the project website include the domain analysis model, consent directive standard and guide.

Another working group of HL7 is Security Working Group that supports the HL7 mission to create and promote its standards by publishing standards for trustworthy communication among all applications and services in HL7's scope [12]. The project of the Security Working Group is about incorporation of additional RBAC permission vocabulary, Privacy Consents and Constraints.

In addition to the group of HL7, some groups are also interest on the research of the consent. The Healthcare Information Technology Standards Panel (HITSP) sets their

standard about the consent. HITSP Manage Consent Directives Transaction Package illustrates the creation and management of the consent directives. HITSP also use the relative standards of HL7 [13]. Hong Song et al. [14] propose the mechanism about the patient e-Consent. There are some groups interesting on the e-consent research [15][16][17].

The purpose of this paper is hoping to establish the platform of creating the patient’s consent directives. The study refers to the projects of HL7 and the profile of IHE BPPC. The study compares above reference data and integrates them to the better and more useful platform for patients to create their consent directives and then store them into the database.

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

II. MATERIALS AND METHODS

HL7 v3 standard [18] defines the domain analysis model about Composite Privacy Consent Directive Domain. The electronic data consent directives information analysis is included in the document of Composite Privacy Domain Analysis Model. In this document, we focus on the electronic data consent directives information analysis and it describes the structure and attributes of consent directives issued by individuals in the existing privacy policy. The consent directive is expressed using a permission, information category and user role. The related classes, Consenter, ConsentDirective, ConsentRule etc. are included in it. It defines the attributes of above classes.

TABLE 1:

The attribute of the related class

Class	Consent Directive	Consent Rule	Consenter	Operation Type	Role
Attribute	id	sequence	relationship	operation Code	name
	Document Image	Purpose	Digital Signature		structural Role
	Effective Time	obligation Code	signature Recorded		functional Role
	expiration Time	Reason Code	name		

In the CCBC projects [11], some documents are published. In the document of the projects includes the state machine of the data consent directive. It introduces the flow of the data consent directives, the sequence of creating or revoking the consent directives and the message type of the data consent directive.

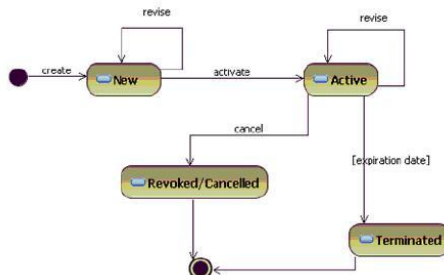


Figure 1: The data consent directive state machine [11]



Figure 2: Manage consent directives interactions [18]

The IHE Basic Patient Privacy Consent (BPPC) [19] profile provides a mechanism can create a basic vocabulary of codes that identity XDS Affinity Domain privacy consent policies with respect to document sharing. The administration of the XDS Affinity Domain will assign each privacy consent policy a unique identifier (or code) for use within the XDS Affinity Domain. The IHE BPPC profile defines the rules of the consent:

- Each patient privacy consent policy will be given a unique identifier (OID) known as a patient privacy consent identifier. The unique identifier is used to label documents published within the XDS Affinity Domain. This label provides the control linkage back to the appropriate patient privacy consent policy.
- Each patient privacy consent policy will have confidentiality codes, for example, the ConfidentialityCode of HL7, “N (normal)”. The ConfidentialityCode can decide the privacy level of the consent policies.

The appendix of the IHE IT Infrastructure Technical Framework is about Privacy Access Policies. In this appendix, privacy consent can be summarized as: “I agree on my personal data being disclosed to some one under specific conditions”. The specific conditions are based on the following:

- Whose data is disclosed?
- Which type of the personal data?
- What type of accessing (normal access, emergency access)?
- What purpose for the data is disclosed?
- The timeframe (period of validity of the consent).

In additional, Song, Win and Croll [14] purpose a model that modified from R.Clarke’s model [20]:

Access to <health data>
 By <one or more (groups of) entities or identities>
 For <one or more purposes >
 In <a context >
 Is [consented/denied]
 By <an identity>
 On behalf of <an identity>
 Valid from <date>
 Expire from <date>

We will use this model and above describe for the base of the consent creating.

This system provides the patient create, revoke or update their consent directives about their personal health records. The patient can create, revoke or update their consent directives through the platform. Through the platform, the consent directives will be stored or removed in/from the consent database. The consent database records the syntax of the consent directives that records in HL7 vocabulary and domain analysis model.

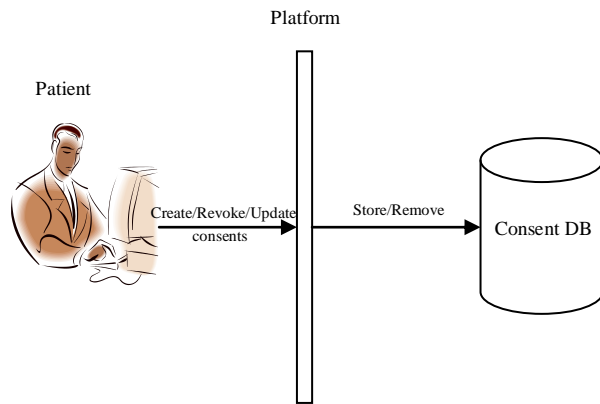


Figure 3: The system architecture

III. EXPECTED RESULTS

System User : Consent Administrator

Name : Tom

ID : A123456789

Create New Consent

Manage Consent

Figure 4: The system picture when the patient using the system

Create New Consent

Allow

Deny

The type of the data

Lab Result

Operation

Access

By whom

Physician

For the Purpose

Healthcare

Effective Period

Year 2010 Month 1 Date 1
 To Year 2010 Month 3 Date 31

Figure 5: The system picture when creating the consent

When the patient wants to decide his/her consent directives of their health records, the system can provide the manner of creating the consent friendly. When the patient creates his/her individual consent, then it stores the consent in the database. The patient also revokes or updates his/her consents through the platform. When the consents are created, these consents need to be managed, so it may need consent directive management system that manger and implement the consents.

The message type of the consent directives will follow the vocabulary of the HL7 defines in the documents of the Composite Privacy Domain Analysis Model [18] and the Composite Privacy Consent Directive [11]. The attributes of the consents may include who can use the data, what data is be consented to use, which purposes of using the data and when the consents are be applied. The ConfidentialityCode of HL7 is used to know the confidential of the data.

IV. CONCLUSION AND DISCUSSION

The IHE is good manner in the healthcare environment. It provides the standard of the health records sharing. When following the standard, the health records can exchange between the organizations. But before the health records exchange, it should create the patient's consent directives prior. The IHE BPPC profile is about the patient privacy consents and the related documents about patient consent are linked. Integration of the IHE BPPC and related documents can be the principle of creating and modifying the patient consent. We use the message type of HL7 and integrate the policies in HL7 and the IHE BPPC and other helpful information to create the system of consent management to provide the people set their consent directives of the health records friendly.

In the emergency condition, the physicians need to know the patient's identity to view his/her health records so that they

can deal with the patient's immediate life threats. In this state, the patient's consent should be ignored. When the patient's consent is ignored, the audit should be started. Audit can log the action of the user during the overriding the patient's consents. In this system, there is no audit function now. We will establish the audit to record the user's action so as to review the user past behalf. The establishment of auditing may follow the IHE Audit Trail and Node Authentication (ATNA) profile. The ATNA profile provides the security measure together with the security policies and procedures for providing patient information confidentiality, data integrity and user accountability.

Another topic we discuss is the policy of different territories. There are much different privacy policies in the different territories, and the patient's consent should be consistent with the policies. When the patient wants to create their personal consents, their consent should not have conflict with the policies of the territory. How to check the consent to not have conflict with the local policies is not easy.

In this study, we want to establish a friendly platform for patients to manage their consents. When the patient creates, revokes or updates their consents through the platform, we will store them into the database. In the future, we will establish this system and hope the audit function will be established. Then, we hope the system will be linked to the system of the privacy by K. Chen and D.W. Wang. When the system links with it, we can evaluate the performance of the system.

REFERENCES

- [1] 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.
- [2] Wainer J, Campos CJ, Salinas MD, Sigulem D, Security requirements for a lifelong electronic health record system: an opinion. *The Open Medical Informatics Journal* 2008, 2, 160-165, 2008.
- [3] Australia's Privacy Act <http://www.privacy.gov.au/>
- [4] New Zealand Health Information Privacy Code <http://www.privacy.org.nz/the-privacy-act-and-codes/>
- [5] United States Department of Health and Human Services, <http://www.hhs.gov/ocr/hipaa/>
- [6] P.A.B.Galpottage and A.C. Norris, Patient consent principles and guidelines for e-consent: a New Zealand perspective, *Health Informatics Journal* vol.11 (1), 2005, pp. 5-18
- [7] V.HEIMLY, Consent-based Access to Core EHR Information: the SUMO-project, *Studies in Health Technology and Informatics*, vol.136, 2008, pp. 431-436.
- [8] *Healthelink* <http://www.healthelink.nsw.gov.au/home>
- [9] HL7 <http://www.hl7.org>
- [10] The Community Based Collaborative Care (CBCC) Work Group <http://www.hl7.org/Special/committees/homehealth/overview.cfm>
- [11] The CBCC project <http://gforge.hl7.org/gf/project/cbcc/>
- [12] The security Work Group <http://www.hl7.org/Special/committees/secure/overview.cfm>
- [13] HITSP/TP30 HITSP Manage Consent Directives Transaction Package http://www.hitsp.org/InteroperabilitySet_Details.aspx?MasterIS=true&InteroperabilityId=365&PrefixAlpha=1&APrefix=IS&PrefixNumeric=12
- [14] H. Song, K. T. Win, and P. Croll, Patient e-consent mechanism: Models and technologies, In *COLLECTeR*, 2002.
- [15] E. Coiera and R. Clarke, e-Consent: the design and implementation of consumer consent mechanisms in an electronic environment, *Journal of the American Medical Informatics Association* vol.11 (4), 2004, pp. 129-140.
- [16] J. Bergmann, O.J. Bott,D.P. Pretschner and R. Haux, An e-consent-based shared EHR system architecture for integrated healthcare networks, *International Journal of Medical Informatics* 76, 2007, pp. 130-136
- [17] Giovanni, Russello, Changyu Dong and Narancker Dulay, Consent-based Workflows for Healthcare Management, *IEEE Workshop on Policies for Distributed Systems and Networks* 2008, pp. 153-161
- [18] HL7 version 3, <http://www.hl7.org/v3ballot/html/welcome/environment/index.htm>
- [19] IHE IT Infrastructure Technical Framework Vol. 1 (ITI TF-1) Integration Profiles-Basic Patient Privacy Consent (BPPC)
- [20] R. Clarke, e-Consent: A Critical Element of Trust in e-Business, *Proceedings of. 15th Bled Electronic Commerce Conference, Bled, Russia*, 2002