World Academy of Science, Engineering and Technology
International Journal of Biomedical and Biological Engineering
Vol:4, No:5, 2010

The Study of Managing the Personal Consent in the Electronic Healthcare Environment

Yi-Yun Ko and Der-Ming Liou

Abstract**—**The Electronic Health Record (EHR) system is very general and we should pay more attention to a patient's privacy. The patient's consent is one of the elements when dealing with privacy topics. This study focuses on the creating and managing of patient consent. The integration of the HL7 standards and the IHE BPPC profile provides a base for the creation of patient consent. Establishing the platform offers the patients a way to create, revoke or update their consents. Through this platform, they can manage their consents in an easier manner.

Keywords**—**consent, EHR, HL7, IHE

I. Introduction

DUE to the advancement of information technology, the paper-based medical record progressively becomes electronic. The emergence of the Electronic Health Record (EHR) could improve the complex and heavy procedures when dealing with paper-based medical records. The EHR records the information about the patient's health. The Electronic Health Record and the patient's health and life are closely related. Hence, they have to provide correct information to their physicians, so that the information will be recorded in the Electronic Health Record. In contrast to general personal information, the personal health information is more sensitive information and needs more protection to ensure such information is not leaked. Therefore, the security and privacy of the Electronic Health Record is very important.

As a result of the different backgrounds and religious environments of individuals, some health records are classified as high level sensitive. Such as in the case of abortion records, the patient doesn't want this personal data to be accessed by non-related people. In addition, the health status of the individual may influence the development of their career. The information of the health records may provide other organizational use. For example, it may be used by a research organization, pharmaceutical factory, or insurance company; because these organizations are interested in these patients' health records. But the patient doesn't like to share their sensitive data or let it be accessed by the other non-related people or organizations. So, besides the security and privacy of the health records, the violation of a patient's rights is also important.

The EHR consists of several requirements [1]: security, semantic interoperability, author responsibility, audit trail, version control, patient access, archiving, and data retention. Wainer J. et al proposes some opinions about the security requirements of EHR systems [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 treatment is over.

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

There are some countries that have established systems implementing patient's consent; for example, New Zealand [6], Norway [7], or Australia [8]. In Australia, the Health*elink* was established by the NSW (New South Wales) Department of health. The system assists in collecting and storing the information that comes from the individuals and other different healthcare providers. The system is the center of accessing and storing and it provides protection for the security of the data to avoid non-related people 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 currently focuses on some domains; one of the domains is the privacy consent directive message format and vocabulary and they implemented the project described above [11]. The related

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

Yi-Yun Ko is with the Institute of Biomedical Informatics, National Yang-Ming University, Taiwan (e-mail:kkyiyun@gmail.com).

documents in the project website include the domain analysis model, consent directive standard and guide.

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

In addition to the HL7 group, some groups are also interested in research involving consent. The Healthcare Information Technology Standards Panel (HITSP) set up their standard dealing with consent. HITSP Manage Consent Directives Transaction Package illustrates the creation and management of the consent directives. HITSP also uses the related standards of HL7 [13]. Hong Song et al. [14] proposed a mechanism involving a patient e-Consent, and there are also some groups interested in the e-consent research [15-17].

The purpose of this paper is to establish a platform for creating patient consent directives. This study refers to HL7 and the profile of IHE BPPC projects. The study compared reference data and integrated them into a better and more useful platform for patients to create their consent directives and then stored them into a database.

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

II. Materials and Methods

HL7 v3 standards [18] define the domain analysis model about Composite Privacy Consent Directive Domain. The consent directives are 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 I
The Attributes of the Related Classes

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		functionalRole
	expiration Time	Reason Code	name		

In the CCBC projects [11], the state machine of the data consent directive is illustrated. 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.

The IHE Basic Patient Privacy Consent (BPPC) [19] profile provides a mechanism that 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.

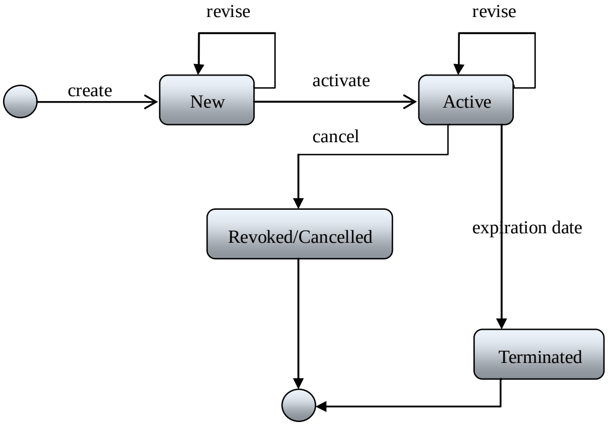


Fig. 1: The data consent directive state machine [11]

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 that my personal data can be disclosed to someone under specific conditions". The specific conditions are based by the following questions:

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

We will use the above description for the base of creating consent.

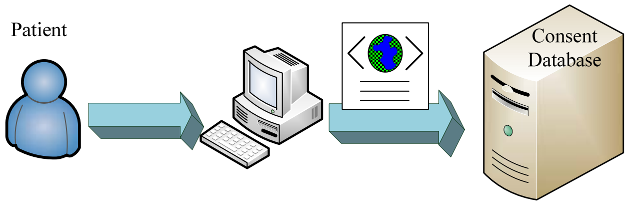


Fig. 2: The system architecture

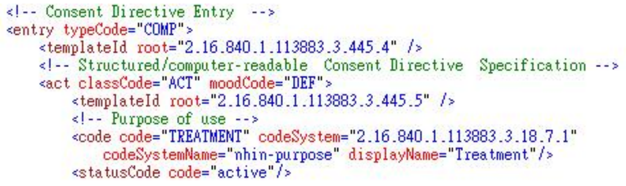
Fig. 2 shows the system architecture. The patient creates his/her consents through the platform. Then, the content of the consent will be translated to the XML format and stored them into the database.

III. Expect Result

In this system, the patient creates, revokes or updates their consent directives about their personal health records. We build a platform that is consistent with the Composite Privacy Consent Directive Domain Analysis Model of HL7 and the IHE BPPC profile.

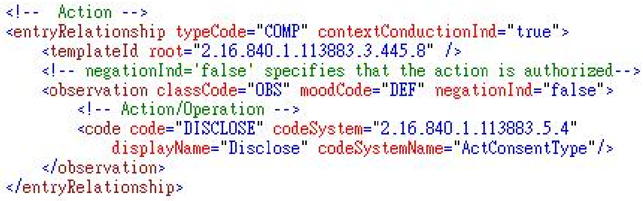
The message type of the consent directives will follow the vocabulary of HL7 that be defined in the documents of the Composite Privacy Domain Analysis Model [18] and the Composite Privacy Consent Directive [11]. We use the attributes and vocabulary defined in the Composite Privacy Domain Analysis Model for the creation of the consent directives. The attributes of the consents may include: who can use the data, what data is be consented to use, what are the purposes of using the data and when the consents are to be applied. The ConfidentialityCode of HL7 is used to classify the confidentiality of the data. These attributes are essential to composing the consent directives.

The patient can manage their consent directives through the platform. Then, the content of the patient’s consent will be translated to the XML format conforming to the Clinical Document Architecture (CDA) and stored into the database. The content of the consent contains the purpose of use, the role and identity of the information recipients, the custodians of the Individually Identifiable Health Information (IIHI), actions/operations, information category, privacy policy and information recipient obligations. The information recipient obligation is about handling the IIHI disclosed. For example, the patient may want the information recipients to dispose of the data after they use it. The example is shown in Fig.3 and Fig.4. Fig.3 shows the CDA example of “Purpose”. It illustrates the purpose of use allowed by the consent directive “TREATMENT”. Fig. 4 shows the CDA example of “ACT”. It illustrates the actions authorized by the consenter in “DISCLOSE”.



```
<!-- Consent Directive Entry  -->
<entry typeCode="COMP">
    <templateId root="2.16.840.1.113883.3.445.4" />
    <!-- Structured/computer-readable  Consent Directive  Specification -->
    <act classCode="ACT" moodCode="DEF">
        <templateId root="2.16.840.1.113883.3.445.5" />
        <!-- Purpose of use -->
        <code code="TREATMENT" codeSystem="2.16.840.1.113883.3.18.7.1"
            codeSystemName="nhin-purpose" displayName="Treatment"/>
        <statusCode code="active"/>
```

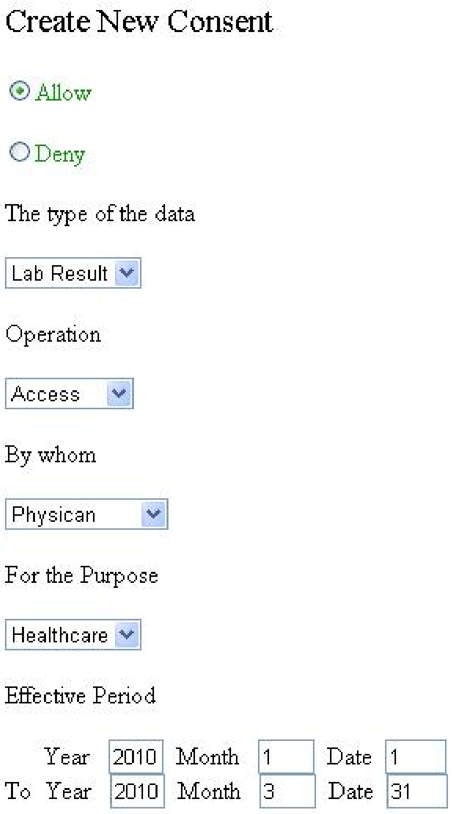
Fig.3: The CDA example of the consent attribute “Purpose”[20]



```
<!--  Action -->
<entryRelationship typeCode="COMP" contextConductionInd="true">
    <templateId root="2.16.840.1.113883.3.445.8" />
    <!-- negationInd='false' specifies that the action is authorized-->
    <observation classCode="OBS" moodCode="DEF" negationInd="false">
        <!-- Action/Operation -->
        <code code="DISCLOSE" codeSystem="2.16.840.1.113883.5.4"
            displayName="Disclose" codeSystemName="ActConsentType"/>
    </observation>
</entryRelationship>
```

Fig. 4: The CDA example of the consent attribute “Act”[20]

Through this platform, the consent directives will be stored or removed in/from the consent database. Fig.5 shows the system picture when creating the consent. The consent also contains the effective period of the consent directive. This is not included in the illustration above.



Create New Consent

● Allow

○ Deny

The type of the data

Lab Result

Operation

Access

By whom

Physican

For the Purpose

Healthcare

Effective Period

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

Fig. 5: The system picture when creating the consent

IV. Conclusion and discussion

IHE is a good way in the healthcare environment. It provides a standard for health record sharing. When following the standard, the health records can be exchanged between organizations. But before the health records are exchanged, it must create the patient’s consent directives prior to use. The IHE BPPC profile is about the patient privacy consent and the related documents about patient consent are linked. Integration of the IHE BPPC and related documents is the principle used for creating and modifying the patient’s consent. We use the HL7 message type and integrate the policies in HL7, the IHE BPPC, and other helpful information to create the system for consent management to provide people with their own set of consent directives for their health records.

The patient can create their consent through our platform. We didn’t consider the security of the platform, so the personal information may be leaked due to the insecure system. In an 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. An audit can log the action of the user when overriding the patient’s consents. In this system, there is no audit function now. We hope establish the audit to record the user’s action so as to review the user’s past behavior. The establishment of auditing may follow the IHE Audit Trail and Node Authentication (ATNA) profile. The

ATNA profile provides a security measure together with security policies and procedures for providing patient information confidentiality, data integrity, and user accountability.

Another topic we discuss is the conflict of the consents. We don't build the mechanism of detecting the conflict of the consent rules. There are much more different privacy policies in the different territories, and the patient's consent should be consistent with the policies. When the patient wants to make their personal consents, their consent should not have conflict with other consent rules or the policies of the territory. How we check the consent to check whether or not there are conflicts with the local policies is not easy.

In this study, we want to establish a friendly platform that is consistent with the Composite Privacy Consent Directive Domain Analysis Model of HL7 and the IHE BPPC profile. The patients can use this platform to manage their consents. When the patient creates, revokes or modifies their consents through the platform, we will store them in our 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 implementing the consents. 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 Informaitcs 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 Naranker 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] Implementation Guide for CDA Release 2.0 Consent Directive DSTU Second Ballot.