A Prototype of Patient e-Consent in Access Control to Electronic Medical Records

Hong Song[a], Peter Croll[b], Khin Than Win[c]

[a] *PhD Student, School of Information Technology and Computer Science, University of Wollongong, Australia*
[b] *Professor of Software Engineering and Head of School of Information Technology and Computer Science, University of Wollongong, Australia*
[c] *Lecturer in Health Informatics, School of Information Technology and Computer Science, University of Wollongong, Australia*

Abstract

With the development of Electronic Medical Records, there come the new issues on access control over the patient health information. While the ease and speed of electronic data exchange helps people enjoy the benefits of the information age, issues on privacy and security of health information should not be ignored. The authors are researching how to develop a generic model for patient e-Consent mechanism. In order that the generic model is based on sound domain related information, one of the approaches is to review a number of patient e-Consent prototype models as the basis for the development of the generic model. This paper gives an overview of an Electronic Medical Record Prototype with Patient e-Consent mechanism. Using Object-oriented method and UML notation as developing methodology, the prototype model is investigated with a view to its adoption as a part of the generic model.

Keywords:

Patient e-Consent; model; Electronic Medical Records, Access Control

Introduction

From the time of Hippocrates, privacy in medical care has always been important to both patients and the medical profession. However, different countries might deal with patients' health information differently. The publicity of the names of patients with severe acute respiratory syndrome (SARS), especially 'super spreader', in Singapore [1] and the protection of the SARS patient's privacy 'despite an onslaught from hungry media and inquisitive physicians' [2] in O'Bleness Hospital in the United Sates are two examples. In this paper, we would not argue which should come first, patients' privacy or public health interests. While we are expecting the legislations and regulations governing the disclosure of the health data becoming perfect, we at the same time try to work out a solution that how technology could help, in a common-sense balance between the access and control of health data under electronic environment.

Privacy is the basic right of one person. A patient needs to be confident that his health information is handled properly and remains in confidentiality. With the emergence of computerized medical records, patient's personal health information could be transferred easier than ever before. The information could be more readily misappropriated among many people and the likelihood of the unauthorised use of the health information increases. Keeping one's health information in confidentiality is more challengeable under electronic environment.

Despite of the debate on the ownership of the medical records, patients should play some roles in protecting their own health data [3]. Department of health and Ageing of Commonwealth of Australia has supported the Electronic Consent Research and Development project in 2002. The research is to "identify and trial effective mechanisms by which a consumer can record the conditions under which their information is transmitted…" [4] and ensures that it will not affect the access to patient information by clinicians.

In this paper, we will introduce the rationale of e-Consent. We then briefly describe an e-Consent generic model draft. An overview of an Electronic Medical Record prototype with patient e-Consent mechanism, developed by Sybase PowerBuilder, is presented. We then investigate this prototype model to see whether it could act as one of the source domains in the development of the generic model.

Rationale

Effective and efficient data-sharing among the multiple contacts of health professionals within the organization becomes one of the most important reasons to adopt Electronic Medical Records. Access is the ability " to do something with a computer resource (e.g., use, change, or view)" [5]. A system that places fewer access restrictions could be more efficient to use. However, patients might feel unease about the large scale of electronic health data exchange for fear that the people who should not have the right to access could easily access the data. Information should flow freely, however, it should not result in information disclosure that, at least, exceeds the existing control level of paper-based ones. Access control is the means by which the ability of access "is explicitly enabled or restricted in some way (usually through physical and system-based controls)" [5]. Patient Consent in this paper is used to control the access of personal health information [3] and the term e-Consent refers to "consent in the context of electronic health information" [6].

However, it remains great challenges in developing an e-Consent system. CSIRO Commonwealth Scientific &

Industrial Research Organisation worked for The Department of Health and Ageing to explore potential technological solutions that will enable health care consumers to give or withhold consent to the transfer and use of their personal health information. In their Final Analysis Paper, they pointed out there are four key challenges [6]. One challenge is whether the e-Consent mechanism is designed simple enough for consumers to understand and yet sophisticated enough to express complicated consent access rules. The other challenge is that it is likely that embedding routine consent checks on every request for information could impede the clinical work and thus affect the acceptance from healthcare providers. Furthermore, apart from the primary users of the health information, there are also secondary users including researchers, third party payers, legal representatives, employers, and etc. [7] Different stakeholders could have different requirements on e-Consent. How to balance among these stakeholders so that an e-Consent system will be accepted and adopted is another challenge. The e-Consent system should be flexible enough to ensure that a diverse range of viewpoints can be supported.

There are several models proposed for e-Consent mechanism. Among them are from the less restrictive model to the "gatekeeper" model that enforce access restrictions, from the 'opt-in' model that system access to data is only granted where there is consent, to "opt-out" model that system access to data is granted unless specified (denied) in the consent mechanism [8]. The acceptability of different e-Consent models could be different.

The research above has convinced us of the utility and feasibility of developing a generic model for patient e-Consent mechanism. As the medical applications are normally multi-user, multiplatform, and data-intensive, the complexity of e-consent systems increases. High level of abstraction in the generic model could probably improve the process of developing system models. Generic models are models "that are applicable to more than one domain" [9] and they could be parameterisable by the end-users to suit their own needs. However, generic model development of e-Consent mechanism in healthcare area is very new. We are trying to work out a methodology to build the model that later could be applied to develop practical applications.

The approach we are adopting now is to design a very simple generic model for patient e-Consent mechanism according to the research on literature as a starting point. Then we will find and examine some prototype models as source domain models to enhance and complete the model. The current prototype under investigation is eMedical Books, an Electronic Medical Record with e-Consent mechanism. In our next sessions, a description of a patient e-Consent generic model and an overview of the prototype will be presented.

Patient e-Consent Model

Developing a set of design principles could help to minimise the likelihood of unwanted or unexpected behaviours in the system or model design. Researchers are trying to extract from all sources the principles that address both legal requirements and those most frequently expressed by the patients [10]. This paper will not repeat those principles. However, we do find that the e-Consent should be context-based. It should be able to address the issues on *WHO* (Who gives the consent), *WHAT* (What part of data is concerned), *WHOM* (To whom the consent is given), *WHY* (For what purpose the data could be accessed), *WHEN* (The consent could be revoked) and *HOW* (How the consent rules should be expressed).

As a starting point, we develop a simple generic model of patient e-Consent mechanism. Instead of covering all the issues discussed above, it just gives the main classes and a very few of the most important associations between those classes. This simple generic model based on the literature research is used to better understand the process of developing a generic model. It is presented in figure 1, using Unified Modelling Language (UML) and drawn by Rational Rose, a software development tool.

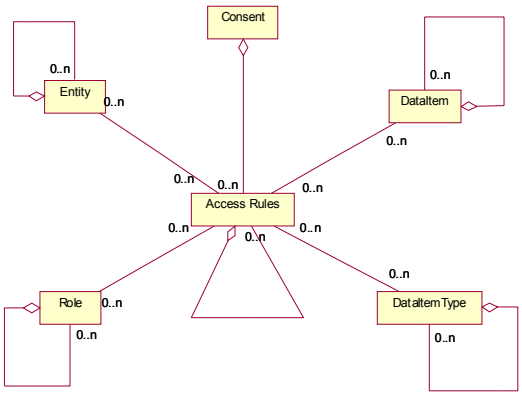

Figure 1: Class Diagram of an e-Consent Model using UML

This model should be the very tip of the iceberg of the main model itself. It could be also used as a reference point against which to decide the approaches to build prototypes. We now summarise the main classes of the model.

Entity: Effector of an activity. An entity could be authorised to access data as an individual, independent of any role he is working under.
Role: The job description. An entity could get the access right based on the role he is playing.
DataItem: The pieces of data.
DataItemType: The types of data, or groups of data. Could be labelled as less sensitive, sensitive, very sensitive. Or could be grouped as Demographic Data, Financial Data or Clinical Data.
Access Rules: Defines the authorisation between the entity (role) and the data.
Consent: Consists of Access Rules.
All the classes support compositions that means the nested consents could be realized.

A Prototype of Patient e-Consent

The Prototype software, named as eMedical Books, was developed by a project group of School of Information Technology and Computer Science of University of Wollongong. The purpose of this project was to clarify issues around security and confidentiality and issues around patient/client confidentiality and consent. It is felt that this prototype could serve as a good source model in the development of the generic model as it adopts the object-oriented develop method and also using UML notation. Therefore it will not be too difficult to demonstrate that this source domain model could be used to amend and complete the generic model. An overview of the prototype is presented in this section.

Aims

- Patient consent can be implemented in electronic medical record systems without compromising the data accessibility.
- Different access levels can be achieved according to the rules of patient consent.

Methods

Development Tools used are Sybase PowerBuilder 8.0 and also make use of Rapid Application Development (RAD) method.

Solution

The result of the prototype software is a basic Electronic Medical Records with the consent security framework. It has three parts. The Client Interface Interaction develops user confidence. The Database Operation copes with data fields and multiple users access. The Security Framework Operations defines access rules (consent).

The Security Framework is 2-Tier. Tier 1 is the Domain-Level Security that defines default access levels. Tier 2 is Patient-Consent Security that defines the consent access rules.

Figure 2 is a Use Case diagram illustrating the 2-Tier Framework based on the UML
standard, using Rational Rose, a software development tool.

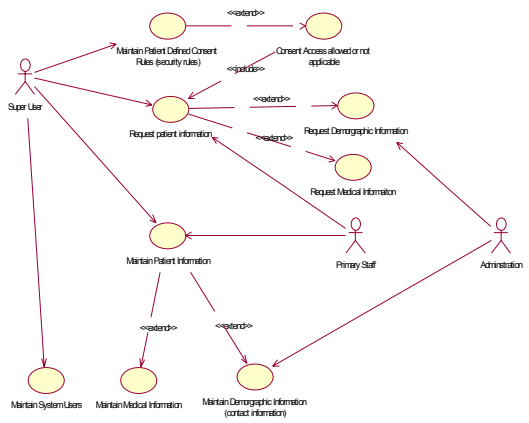

Figure 2: Use Case Diagram of the security Framework of eMedical Books

Domain-Level Security Access Levels

The default access levels are designed as 3 levels: Super User, Primary Staff and Administration. From the Use Case Diagram, we could find the following:

Super User 1) Maintain System Users; 2) Has the full access to System to maintain patient information; 3) Has full access to System to access patient information; 4) Is responsible for maintaining user profiles and record their security rights (access rules).

Primary Staff 1) could maintain patient information; 2) Is the primary subject of Patient-Consent security restrictions and could access to patient data dependent on patient-consent security framework.

Administration 1) has limited functionalities within the System; 2) Is the subject of Patient-Consent security restrictions.

Patient e-Consent

The prototype allows patients to define the access rules for their own health information and allows healthcare professionals to access patient information stored in the Medical Record according to the consent rules set by patients. We now discuss how patient consent is achieved in eMedical Books.

First, the implied consent existed. It adopts an opt-out model that system access to data is granted unless denied in the consent profiles. The default profile has some preset access rules. For example, Administration by default could not access some clinical information.

If the patient wants to define his own access rules, like who can or cannot access which part of his data, he could fill a consent form which he could send the form to the super-user, either by email or in written form. Super-user maintains the user profile by recording the security rights according to the rules defined the patient. Then the data requester would be check against the consent rules.

The default consent profiles are level based: Super User, Primary Staff and Administration. The patient defined consent profiles can also be level based. It can also deny a specific individual to access specific record content. For example, patient could define in his consent access rules that for specific record, it can be accessed by super-user, primary staff, but not Doctor A (who also belongs to primary staff), not Administration.

Discussions

We now have a brief examination on the prototype model to see whether this prototype has the potential to form the basis of a practical solution to the electronic consent question and how it could be used as domain model to enhance the generic model.

Super User, Primary Staff and Administration are recorded as the **ROLE** in the generic model. While a particular individual such as Doctor A is recorded as the **ENTITY** in the generic model. There are also **DataItem**s implemented as different pieces of data like Consultation, Past History, Blood Test etc. **DataItemTypes** in the generic model are implemented as groups of data like Demographic Data and Medical Data. **Access Rules** are implemented as consent security profiles.

In the prototype, the patient initiates the consent. If the patient does not define his own consent access rules, then the default consent is applied, which implies that the patient gives implied consent. The generic model should be improved to accommodate this point.

The prototype has the ability to apply different consent objects (Access Rules) to different parts of data. It also has the ability to modify a consent (Access Rules) to include new unauthorised/authorised users (Entities). It is obvious that in the generic model, the Access Rules define the authorisation between the Entity , Role and DataItem, DataItemType.

The prototype has the ability to revoke a previously existed consent by deleting the relevant consent profiles. The generic model should consider this point and add relevant classes.

The prototype exists the problem that how the consent rules could be recorded in a safer way. The generic model should also be able to facilitate secure transfer of a record to an authorised entity.

Conclusions

We have shown that the patient e-Consent implemented in the prototype is able to perform the access control on the health information. However, the work described in this paper is still in progress. Possible future work needs to reflect the exceptions like emergencies, the therapeutic privilege that "permits a physician t withhold information when disclosure of information poses a significant threat of detriment to the patient" [11], or treatment required by law[11]. Under these situations, the relevant stakeholders might need to access the patient's record even with the explicit denial expression of the patient. How to embedded the override into the system without compromising the patient consent mechanism remains a challenge task. Consequently, the generic model needs to address this point.

Furthermore, the model described in this paper is just a starting point to the development of a generic model for e-Consent mechanism. It must be further formalised and refined so that it could be used in practical applications.

Acknowledgments

Authors would like to thank Corbeski D., Daniels A., Gluseske L., Tancevski N. and Teodorakakos B., for their contribution to the e-Consent Mechanism, e-Medical Books Project.

References

1. Ho, A., *Hospitals own your records, you don't...* in *The Straits Times*. 17 April, 2003: Singapore.
2. Youngstrom, N., *Report on Patient Privacy*. 2003, http://www.aishealth.com/Bnow/042903a.html, retrieved in April 2003
3. Song, H., K.T. Win, and P. Croll. *Patient e-Consent Mechanism: Models and Technologies*. in *7th Annual CollECTeR Conference on Electronic Commerce*. 2002. Melbourne, Australia.
4. *Electronic Consent Research Summary of Final Reports*. November 2002, Primary and Coordinated Care, Health Services Division, Department of Health and Aged Care.
5. *An Introduction to Role-based Access Control*. 1995, NIST/ITL Bulletin, National Institute of Standards and Technology,.
6. O'Keefe, C., et al., *Implementation of Electronic Consent Mechanisms Final Analysis Paper*. 21 August 2002, CSIRO
7. Win, K.T., et al. *Implementing Patient's Consent in Electronic Health Record Systems*. in *7th Annual CollECTeR Conference on Electronic Commerce*. 2002. Melbourne, Australia.
8. Clarke, R., *Consumer Consent in electronic Health Data Exchange Background Paper*. July 2001, Department of Health and Aged Care Acute and Coordinated Care Branch.
9. Jones, M.A.T., *Formal Generic Modelling*. January 1998, Nottingham Trent University.
10. Coiera, E., *The Design and Implementation of Consent in an Electronic Environment*. July 2002, Department of Health and Ageing, Primary and Co-ordinated Care Section.
11. Roach, W.H., *Medical records and the law*. 2nd ed. 1994, Gaithersburg, Md.: Aspen Publication.

Address for correspondence

Hong Song
School of IT and Computer Science
University of Wollongong
Northfields Avenue
NSW 2522
Australia
Tel: 0061 2 4221 5432
Email: hs02@uow.edu.au