Access and Usage Control Requirements for Patient Controlled Record Type of Healthcare Information System

Annanda Thavymony Rath and Jean-Noël Colin
PReCISE Research Center, Faculty of Computer Science, University of Namur, Belgium
{*rta*}*@info.fundp.ac.be*,{*jean-noel.colin*}*@fundp.ac.be*

Keywords: access control requirement, e-health, usage control requirement, patient controlled record

Abstract: This paper addresses the issue of access and usage control requirements in healthcare information system. Our work aims at identifying the access and usage control requirements for a particular healthcare information system where patients have pivotal right to grant or deny access to their health records. We term this system "Patient Controlled Record type of Healthcare Information System or PCRHIS". It is worth noting that the requirements, presented in this paper, are the results of our studies from both user's requirements and legal issues (based on 95/46/EC Directive) under the scope of Walloon Healthcare Network (WHN). The WHN project aims at providing an electronic healthcare facility for patients in Walloon region, Belgium, that joins all healthcare institutions, clinics, and physicians and allows sharing of patients' health records when needed. The main contribution of this work is that, with these requirements as a reference, one can identify an appropriate access and usage control model. This applies not only to the proposed system under the scope of WHN project but also to any system that has similar model.

1 Introduction

Access control (Vincent C. Hu et al., 2006) is about defining and enforcing the rules to ensure that only authorized users get access to resources in a system while usage control (Alexander Pretschner et al., 2008) refers to the actions taken after data is granted access. From the data protection point of view, especially sensitive private data, the enforcement of the two controlling steps is necessary.

Concerning access control requirement, it is about the required attributes to form the rules that need to be enforced before data is granted access while usage requirement is about the required attributes to form the rules applied after data is granted access. The study of access control requirements in e-health is not new, some researches (Annanda RATH and Jean-Noël Colin, 2012b) (Rostad and Lillian, 2008)(Andre Reyneke et al., 2003)(Rostad et al., 2006) (Alhaqbani Bandar and Fidge Colin, 2008) (DocuLiv EPR, 2003) (Rostad and Lillian, 2008) have been contributed in this aspect; however, they focused on e-health in general and particularly, system with a central control of access policy while our focus is on patient controlled record type of healthcare information system (PCRHIS), a system where the control on access policy is decentralized to patients.

As more and more people are interested in privacy protection and get to know the risk that they may have concerning their private health records (Annanda RATH and Jean-Noël Colin, 2012a), they increasingly willing to have more level of control over their health record. This leads to the emerge of the concept of Privacy Preference and personal-control (HL7 PHR, 2011). A good example of such system (similar in concept) is the HL7 Personal Health Record (HL7 PHR, 2011). However, HL7 PHR system allows only patient to play with their unofficial health record. This means that the official record still works under the HL7 EHR (Electronic Health Record) system. The big question about HL7 PHR is how much data and what type of data (health information) should be made available for patient? How to ensure the transparency between the official data under HL7 EHR and unofficial data under HL7 PHR. It seems that HL7 PHR poses more questions for health record management.

To minimize the data management problem as appeared in HL7 PHR and to maximize the right of the patient in controlling their health record, in our work, we intend to create a patient controlled-record healthcare information system that provides a full control to patient. In our proposed system, patient can define different policy for different type of user they consent.

Concerning usage control requirement, to the best

of our knowledge, although usage control has a significant affect on security in protecting patient's record, there is no research so far in e-health, which focuses on this aspect. Most of the researches focus on the access control. This may be because of the feasibility study or the believe that usage control is just the extended-access control. But in our view, we should separate the two processes clearly cause they require different method for handling, hence, different control requirements.

The rest of the paper is organized as follows. We provide the background in Section 2. Section 3 presents the user and data requirements. Section 4 talks about the access control requirements while Section 5 presents usage control requirements. Section 6 is the discussion and we conclude in Section 7.

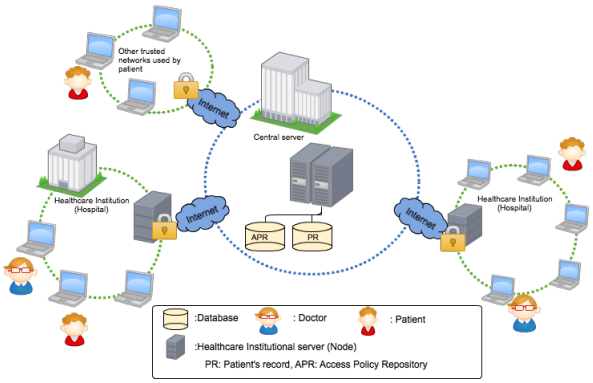

Figure 1: Simplified Schema of PCRHIS

2 Background

PCRHIS Architecture: As illustrated in Figure 1, PCRHIS is a network of health institutions such as hospitals, and clinics, but also of physicians, that aims at supporting the exchange of patient's medical record between healthcare professionals, in a timely and secure way. Two types of data are actually stored centrally: access and usage policy defined by patient and optionally patient's medical record. In addition, PCRHIS also manages in a central way the access and usage permissions that apply to the various pieces of data it manages. Permissions are managed by patient himself/herself, by his/her legal representative (guardian), or by a trusted-person. In general, PCRHIS central server is in charge of the overall authorization process; it receives the requests from the nodes, checks them against the applicable access policy (as defined by the patient) and returns the requested information. Then requested information is viewed at client (or requester's device) where the control of information usage is taken place.

Requirements Elicitation: The data requirements we identified in next section result from the study of practical documents for treatment procedure in different healthcare institutions, clinics, and hospitals in French speaking region in Belgium under the Walloon Healthcare Network Project. The user requirements were identified based on two sources of information. First, we studied the practical data processing procedures at different healthcare institutions under the WHN project. Second, we studied the EU directive concerning the processing of sensitive private data, particularly, the 95/46/EC Directive (EU-directive, 1995). For Access and usage control, the requirements were captured based on two important sources of information, access and usage policies of the existed healthcare institutions in Walloon region and the 95/46/EC Directive.

3 User and data requirements

In this section, we present different types of users who are supposed to involve in processing of patient's data (or record) and different types of data considered to be sensitive.

3.1 Patient Data

Two types of patient's data are considered to be sensitive: administrative and treatment data. Administrative data is any data related to the administrative work including patient personal information. The treatment data is any data related to the treatment of the patient. Treatment data is categorized further into sub-categories, as presented below.

"Treatment report" is a report of treatment containing the information such as patient personal data, type of illness, location, people involved, time, and duration of the treatment. "Summary treatment result" is a short report describing the result of the treatment. It can be a success operation, fail, or follow-up. "Conclusion on state of patient health" describes the condition or state of the patient's health after the operation or treatment. This type of report is generally generated by a doctor who leads the treatment or a consented-doctor. "Prescription" describes the types of drug that patient needs to consume and also the instruction on when and how to consume it. "Follow-up report", for some illnesses, after treatment, follow-up report is required. It allows doctor to follow the health condition of patient.

3.2 Type of user

In our study, we identified users by considering two different circumstances. First, we consider a normal situation where patient is able to exercise his/her rights. Second, we consider a situation where patient loses his/her ability to exercise his/her rights physically or morally, for instance, in case patient becomes disabled. Following our study, we identified

six groups of users who can access patient's record either directly or indirectly. Those are: Patient, Healthcare professional, Legal-representative (or guardian), Trusted-person, Administrative-personnel, and IT-Technical-personnel.

"Patient": the physical person who is the owner of the health records. "Healthcare professional": people who work at the healthcare institution and are possibly responsible for the treatment of patient. These people are classified into sub-groups depending on their skill or domain of expertise that ranges from generalist-doctor, specialist-doctor, to nurse or pharmacist. "Guardian": people closed to patient who can legally represent patient in case he/she can not exercise his/her rights. "Trusted-person": is a user or group of users, defined explicitly by patient, who can decide on behalf of patient when patient is in situation where he/she can not exercise his/her rights physically or morally. "Administrative-personnel": people who are responsible for the administrative work concerning the patient treatment at healthcare institution. "IT-Technical-personnel": people who are responsible for maintaining the IT-infrastructure to ensure the proper functioning of the e-health system.

4 Access control requirements

In this section, we present the access control requirements in PCRHIS. We classify access control requirements into different categories ranging from action restriction to system requirement. The detail information is illustrated in Figure 2.

"Action restriction" is about the possible actions that can be used in processing patient's data. Those actions are: "print", "copy/transfer", "read/write/display", "delete", and "execute".

"Constraints: Temporal and Spatial", "temporal access" is the time related constraint. "Spatial access" is the constraint based on geographical location. For example, the policy that prohibits every access from hospital "B" to hospital "C".

"Least privilege principle", in order for users to do their job correctly, it is essential that concerned users have the correct permissions allowing them to gain access to the information they require. However, these permissions should not allow users to gain access to information that is not meant for them. Least privileges allow us to ensure that there is no security gap for user to intrude patient's record.

"Permission transfer (delegation)" is important to ensure the smooth management process in case the responsible person is on mission and is not able to exercise his/her rights. In PCRHIS, it is also required for permission or rights transfer. For instance, patient delegates their rights to guardian and trusted-person in case patient is not able to exercise his/her rights. There are three types of delegation: patient to guardian, patient to trusted-person, patient to healthcare professional.

"Obligations" refers to the duty for user to fulfill before or after access is granted. For example, notification of access to patient for traceability purpose.

"Purposes of access" allows patient to determine precisely the access rights to content. It also contributes in sharping the access control decision on the requested content. There are six types of purpose: Normal, Critical, Emergency, Personal archive, Research, and Statistic.

"System Requirements", there are three important requirements: "Interoperability" (because we address the data processing problem in distributed and heterogeneous environment), "Simplicity and User friendliness" (as patient is the one who administrates the access policy. Thus, a simple system is required), and "Performance" (a very good system performance is required because in some case a fast decision is required, for instance, emergency case).

5 Usage control requirements

In this section, we discuss the usage control requirements applied to PCRHIS, ranging from usage restrictions to action requirements, the detail is illustrated in Figure 3.

"Usage Restriction" defines the circumstances under which the content can be viewed and also under which content can not be viewed. "Action restriction" refers to the allowed or not allowed actions to perform on patient's record.

"Temporal usage restriction" is the time related usage refers to time within which user is allowed to view patient's record. "Spatial usage restriction" refers to the place/location where data is allowed to view, particularly, when data is moved out of its original location. "Data viewing" refers to the number of times allowed to view data after it is liberated or the number of devices allowed to view data, for instance, allowing to view data two times.

"Usage purposes" is one of the most important constraint that ensures patient's record being used is in the right direction. It is important to note that usage purpose should be continuously controlled during usage session. Based on our analysis, six types of purpose are identified, the same as that of access purposes: normal, critical, emergency, personal archive, research, and statistic.

"Obligations" refers to any duty that needs to be performed by requester or system during the usage session (before, during, or after the use of patient's record). For example, a "delete" action is required to be performed after the usage license is expired while "notify" needs to be performed before and after the

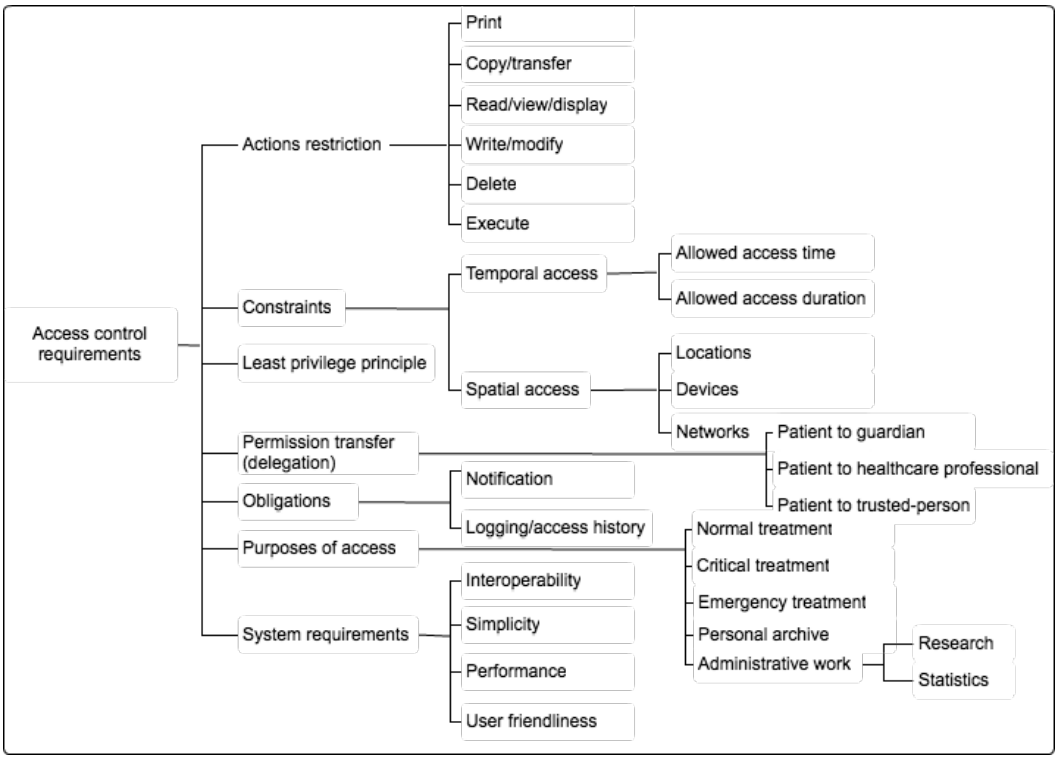

Figure 2: Classification of different requirements for access control ranging from actions restriction to system requirements.

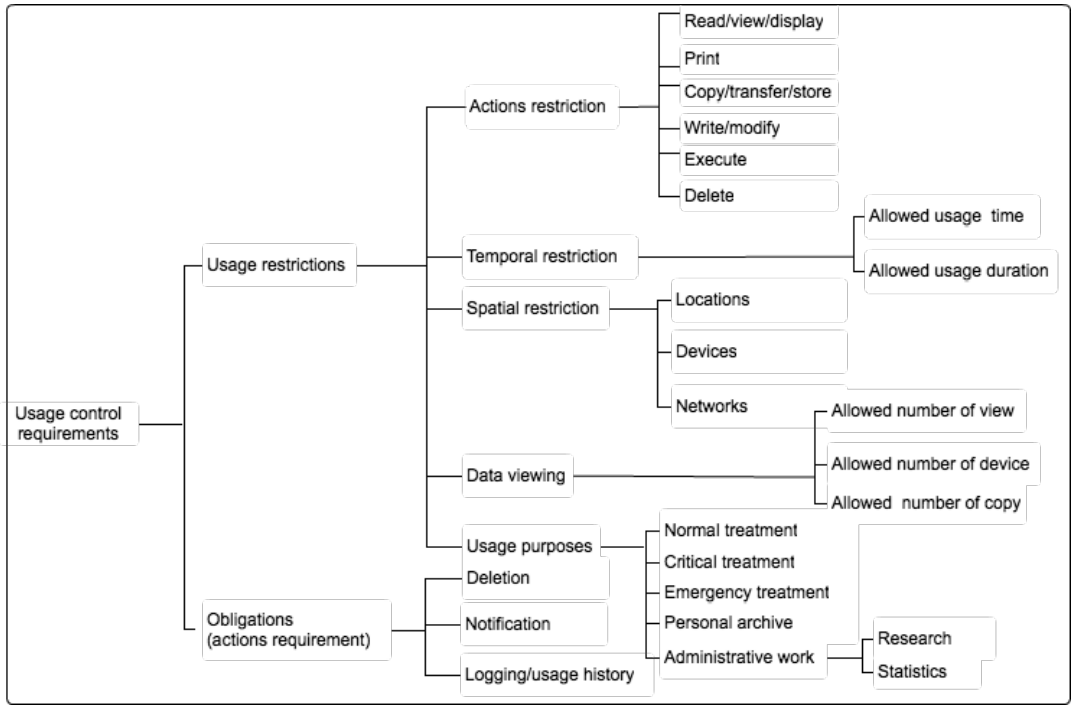

Figure 3: Classification of different requirements for usage control differentiates between usage restrictions and Obligations (actions requirement).

use of data. Here are the possible obligations required in usage control applied to PCRHIS: “Deletion and store ”, “notification”, and “logging”.

6 Discussion

In this section, we discuss the issues that can be raised when patient is given fully the rights to administrate and control the access and usage policy. In system where access control is based on rule/policy, it is required for rule/policy creator to have the knowledge on how rule works and to be beware of what they are doing and the consequence of doing so. In health information system, particularly in our proposed system, it is understood that it is not possible to make an assumption that all patients have sufficient computer skill or knowledge and can operate or set rule by themselves. Thus, to solve this problem, we propose to use three possible groups of users as presented below for rule creation and validation.

1) Patient: they can set up the rule through policy administration point by themselves without the support from healthcare professional or other people such as their trusted-person or guardian, but if the problem occurs, for instance, patient mistakenly defines a rule that is not like what he/she wishes, it is the responsibility of patient themselves.

2) Patient's trusted-person and guardian: as mentioned in the requirements in previous section, it is required for a patient to assign their trusted-person and/or guardian to represent them in case patient can not exercise their rights. Those person can help patient in setting up and validating the rule if patient wishes to do so.

3) Healthcare professional: healthcare professional can also help patient to set the rule on their behalf, but patient's consent written in paper is required in this case. This entity may be the most trusted entity in the system in term of knowledge.

Although those three entities may be sufficient to solve the raising problem, we still need other mechanism to make sure that the data is safe for at least a minimum required security as defined in law. To fix the problem, a default access and usage policy is required. This means that policy creator can set up their own preference policy, if not the default policy is applied.

7 Conclusion and future work

In this paper, we identified different types of users and data applied to PCRHIS. We also identified access and usage control requirements for the addressing system. It is important to note that although this work links primarily to the WHN project, its result can be applied to any other system that has a similar model. Our future work includes a thorough study of the access and usage control models, then the construction of the configurable access and usage control system based on the requirements presented in this paper.

REFERENCES

Alexander Pretschner, Manuel Hilty, Florian Sch, Christian Schaefer, and Thomas Walter (2008). Usage control enforcement: Present and future. *IEEE Security and Privacy*, 6:44–53.

Alhaqbani Bandar and Fidge Colin (2008). Access control requirements for processing electronic health records. In *Proceedings of the 2007 international conference on Business process management*, BPM'07, pages 371–382, Berlin, Heidelberg. Springer-Verlag.

Andre Reyneke, Reinhardt A. Botha, and Stephen Perelson (2003). Access control requirements for content management systems. *Department of Computer Science, School of IT, University of Pretoria, South Africa*.

Annanda RATH and Jean-Noël Colin (2012a). Analogue attacks in e-health: Issues and solutions. CeHPSA - 2012 : 2nd IEEE International Workshop on Consumer eHealth Platforms, Services and Applications (CeHPSA)(accepted but unpublished).

Annanda RATH and Jean-Noël Colin (2012b). Patient privacy preservation: P-RBAC vs OrBAC in patient controlled records type of centralized healthcare information system. case study of walloon healthcare network, belgium. *The Fourth International Conference on eHealth, Telemedicine, and Social Medicine eTELEMED 2012*, 4:111–118.

DocuLiv EPR (2003). *DocuLive EPR: A hospital Electronic health record system developed by Siemens Medical Systems Norway*. http://www.siemens.com/entry/cc/en/, latest access: July 2011.

EUdirective (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. https://www.cdt.org/privacy/eudirective/EU %Directive%.htmlHD%NM%1. Latest access: March 2012.

HL7 PHR (2011). *Health Level International Seven*. http://www.hl7.org. Latest access: July 2012.

Rostad and Lillian (2008). An initial model and a discussion of access control in patient controlled health records. In *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, pages 935–942, Washington, DC, USA. IEEE Computer Society.

Rostad, Lillian, and Edsberg Ole (2006). A study of access control requirements for healthcare systems based on audit trails from access logs. In *Proceedings of the 22nd Annual Computer Security Applications Conference*, pages 175–186, Washington, DC, USA. IEEE Computer Society.

Vincent C. Hu, David F. Ferraiolo, and D. Rick Kuhn (2006). Assessment of access control system. *National Institute of Standards and Technology*.