Flexible Access Control and Traceability of Access in EPR System - the way to patient's assessment and control -

Yasuyuki Hirose [a], Yoshiyuki Sasaki[b], Atsushi Takeda[b], Atsuhiro Kinoshita[b], Shunsuke Minakuchi[b], Naoto Ohbayashi[b], Akira A Fujie [c], Hideo P Togashi [c], Hideki Matsui [c], Shigeru Bito [d]

[a] Medical Informatics, University Hospital, The University of the Ryukyus, Japan
[b] Dental Hospital, Tokyo Medical and Dental University, Japan
[c] Sumitomo Electric Systems Co., Limited, Japan
[d] Seafic Software Corp., Japan

Abstract

Electronic patient record system must grant adequate access right to healthcare practitioners at point-of-care while suppressing inappropriate access, but legacy system design can not satisfy these conflicting requirements. The combination of the three portions, (i) Access Control matrix, (ii) Three Tier Cascading Staff-Group Authoring Model based on Healthcare Party in hospital Model, and (iii) Patient-Doctor Relation and Clinical Situation Model, is able to cover almost all factors for precise role representation and exact access reason clarification for each access in an electronic patient record system. This approach provides the flexible access control environment, avoiding administrative complexity and combination explosion without security breach, because traceability is guaranteed with the clarification of the access reason and the capacity to act in each access by simple few step manipulation. These designs and the environment prepare the way to patient's assessment and control.

Keywords

access reason; capacity to act; traceability of access; peer review; patient's assessment

Introduction

In hospital information system (HIS), or electronic patient record system (EPRS), system account management and access control has three significant parts: security and confidentiality, human resource management, and workflow control.

However, in most HIS, the rigid legacy and tight access control mechanism have prevented to provide both healthcare practitioners and system administrators with smart solutions: **(i)** granting enough access right to healthcare practitioners for flexibly pursuing cure and care jobs at point-of-care while suppressing inappropriate access [1, 2, 3, 4], **(ii)** satisfying time-to-time request of the system setup or its setup changes at point-of-care, and **(iii)** preparing adequate system administration mechanism to system administrators for suppressing the increase of management costs in system account and access control. In addition, **(iv)** patients request to assess the appropriateness of staff accesses of their clinical and social data and information, and desire to control or protect the accesses of hospital staff and researchers [6, 7, 8].

To resolve these problems, system should record the role of operator and access reason in each access, so that each access should be controlled. Some of the roles would be determined by license, degree, department, title and position. However legacy system design has not enough ability to represent care group and access reason. Therefore, the authors have designed a new mechanism and implemented them in the actual EPRS.

Methods

Environments

In Tokyo Medical and Dental University Dental Hospital, the EPRS has been installed and used for past decade, by the clinical staffs themselves directly operating the EPRS at the point-of-care. The EPRS is designed as the browsing platform for the whole data or information, and at the same time, as the operational platform for all order/entry procedures in the integrated HIS.

This HIS has some subsystems and the computer network of the HIS is air-gapped from the campus network or from the Internet. The authentication mechanism is fundamentally homogeneous, and the PC terminal application has an automatic timeout-logoff function.

Design

Healthcare Party in hospital Model

There are at least two kinds of healthcare party in a hospital, one is clinical department and another is care group. They differ from each other at the following points: lifetime length or refresh cycle, dominance of authority [9].

Therefore we distinguish "Care Group class" from the "Department class" in healthcare party model, by granting "Ownership Attribute" to "Care Group class" and preparing "Cost/Profit Distribution Policy class" as an associate class. In other words, a certain staff is "affiliated" to a certain department, and at the same time, she/he is also able to "own" care group(s) in need if she/he has been authorized beforehand, or, she/he is also "affiliated" to care group(s).

In the actual system, affiliation to a department is represented in Access Control Matrix (ACM) and managed by system administrator. On the other hand, ownership or affiliation with care group(s) is represented in another space, Care Group Authoring Area. This implies the possibility that the care group control mechanism works independently from the access control mechanism with ACM.

Cascading Authoring Model

Administrative procedure is designed based on three tier cascading staff-group authoring model. Each tier respectively corresponds to authorization procedure, certifying procedure, and recruiting procedure, in the real world.

In the first tier, a system administrator certifies a "group head certifying person" according to the request and authorization by directors. In the second tier, the "group head certifying person" certifies "group head(s)". And the finally, a "group head" recruits its members from medical staffs inside the department or from other departments [9].

Relation and Situation Model

The information of the "access reasons for patient data" has multi-axial aspects, of course, but for implementation, the method and mechanism for access reason representation should be simple. The patient-doctor relation and clinical situation model is designed to resolve this requirement.

One of the "relations and situations" is recorded as an access reason, and they are classified into the followings [5];

in charge, in charge of pre-examination,
on behalf of, on night shift,
in emergency, for consultation,
as an auditor

Items are pre-set in the system to clarify and specify the "relation and situation" in a clinical scene as the access reason. In addition, this model also contains time parameter, so that valid period or duration can be controlled, when needed [5];

constant	(ex. doctor or care group in charge)
periodical	(ex. anesthetist or ICU staff)
intermittent	(ex. some kinds of therapeutic support)
unsettled	(ex. consultation)

This information is recorded in the access log.

Login sequence and Access Log

When the login-module is booted from a PC terminal, our HIS records "When" and "Where" at first then request account and password. "Who", "what license" and "what department" are recorded consequently, with staff database and ACM [5, 9].

Next, our EPRS is launched, and it requests the clarification of the capacity under which healthcare-party-in-hospital she/he is starting to act, and record it as "what capacity" [9]. Then the EPRS focuses on the target patients.

Before opening a medical chart of a certain patient in EPRS, staff is required to make the declaration on the patient-doctor relation or the clinical situation at the point-of-care as the reason for the access. Needless to say, the EPRS records "Why" and "Whose" [5, 9].

The EPRS also records "Which data and/or information" is accessed, and "What medical action" is performed [5, 9].

Results

Plasticity and Easy Access: for both users and admins

The Relation and Situation model resolves the legacy problem, "could not access although the information was necessary at point-of-care/cure", with simple two step manipulation, and satisfies time-to-time requests. In addition, the combination of "capacity to act" and "access reason" suppresses another legacy problem, "was able to access without appropriate reasons for care/cure or management". (See next sub section)

The Cascading Authoring model based on the Healthcare Party in hospital model avails end users restructuring of care groups without any latency.

System administration work for system administrators have not increased. Their only job is the registration of about a dozen "group head certifying persons".

No Security Breach: Peer Watch and Patient's Assessment

We also prepared the "access audit window" in the EPRS to avoid security breach. This retrieves the access log concerned with the target patient, and displays them, as "doctor X accessed the infection data window of patient Z for the reason of night shift in the capacity of respiratory care unit during eleven pm to midnight at terminal number 99". All of 6W and more are included.

These access histories are always accessible for peer review and the assessment by the patient. Therefore we believe this is very effective in suppressing inappropriate access.

Discussions

Advantages and Limitations

Simplicity and Effectiveness

We believe that the solution should be as simple as possible and cost effective for the implementation of actual system in a large hospital.

Our Solution provides representation of almost all factors of role and reason with easy manipulation, following the time-to-time changes at point-of care with the combination of the three designs, without security breach.

The simplicity and effectiveness is sustained by the clarification of the access reason and the capacity to act in each access.

Necessity of Access Reason and Capacity to Act

Care group or department may determine the role and/or access reason of an operator, in some cases, in some extent. The information about the affiliation with a healthcare party in a hospital would determine the "*role in a hospital*" of a staff. However, it is not enough to determine the exact "reason for access" to a certain patient's data, and it does not always represent the staff "*role to a certain patient*" or the "capacity to act".

In fact, system has no capability to identify the access reason of the operator. Therefore, the declaration of the access reason is essential for peer review and patient assessment.

More discussion about the credibility and reliability of the declaration are described in the previous paper [5].

Coverage

Our designs cover some aspects of security and confidentiality; (i) Security of privacy and Secrecy control, (ii) Balance between the benefit protection of the patient and that of the community in hospital, and (iii) Cost management of the security level control, within the same institution.

They do not cover (iv) Prevention of leakage / theft, and are not regarding the security for hardware/network nor the alternative to security mechanism for hardware/network.

System Audit Tool

Our system holds operator's behavior in the system with his role to a certain patient and access reasons. This means the system has potential power of strong audit-ability, but we have not developed such an analysis tool yet, simply because of the lack of time and money. So we should develop it in the near future.

Comparison with Public Key Infrastructure (PKI)

PKI is able to support secure identification, and also has the ability of representation of several roles. However, PKI would increase administration cost, and has no compliance to time-to-time changes at point-of-care, as same as ACM. In addition, PKI has no ability to represent the exact "reason for access".

The purpose of our models and methods are quite different from PKI, so that PKI is not able to replace our models and methods. At most, ACM may be able to replaced, in our environment.

Patients' Control

During Clinical Procedures

Our system environment has availed the patient's assessment on the hospital staff access to the patient's own data/information. Therefore we have prepared to develop *the module that reflects patient's consent when disclosing clinical data to the concerned*.

This function seems to be theoretically easy to develop. However, we guess there needs to be another innovation in implementation to actual system, to avoid computational over-load arising from multi-axial and multi-layer checking required for access control.

Research Aid

The latest standards and regulations refer the necessity of patient consent when using and disclosing their data and information both for treatment and for clinical research, especially when those data and information can be individually identifiable [6, 7, 8]. The procedure of obtaining such an authorized agreement document may be rather simple. However, *how about the daily procedure of information extraction and disclosing*? And, *how about compliance review procedures*?

It is obvious that the helps is needed from information technology, not only powerful identification technology but also the system design for the reasoning of access and *the tracking capabilities of "access reason" and "capacity to act"*. We authors believe our designs can make some contributions to these aspects.

Conclusions

The combination of the three portions, (i) Access Control matrix, (ii) Three Tier Cascading Staff-Group Authoring Model base on Healthcare Party in hospital Model and, and (iii) Patient-Doctor Relation and Clinical Situation Model, is able to cover almost all factors for precise role representation and exact access reason clarification in each access in a hospital information system.

This approach provides the flexible access control environment, avoiding administrative complexity and combination explosion without security breach. These designs and the environment prepare the way to patient's assessment and control.

Acknowledgments

The primary author thanks Ms. Ruby Tanaka for the thoughtful supports in bringing the manuscript to publication.

References

[1] Bakker AR. Security in Medical Information Systems. In: van Bemmel JH, McCary AT eds. IMIA Yearbook of Medical Informatics. Stuttgart: Schattauer, 1993: 52 - 60.

[2] Brannigan JD. A Framework for "need to know" Authorizations in Medical Computer Systems. Proc 18th Sym Comp App Med Care 1994: 392 - 396.

[3] Safran C, Rind D, Citroen M, Bakker AR, Slack WV, Bleich HL.Protection of confidentiality in the computer-based patient record. MD Comput 1995: 12 (3): 187 - 192.

[4] Barrows R Jr., Clayton PD. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc 1996: 3 (2) : 139 - 148.

[5] Hirose Y. Access Control and System Audit Based on "Patient-Doctor Relation and Clinical Situation" Model. MEDINFO '98 1998: 2: 1151-1155.

[6] CEN. Health informatics - Electronic healthcare record communication - Part 3: Distribution rules. DD ENV 13606-3:2000, May/2000.

[7] US Public Law 104 - 191. Health Insurance Portability and Accountability Act of 1996, Aug/1996.

[8] US Code of Federal Regulations Title 45 Part 160 to 164. Standards for Privacy of Individually Identifiable Health Information, Dec/2000.

[9] Hirose Y, Sasaki Y, Kinoshita A. Human Resource Assignment and Role Representation Mechanism with the "Cascading Staff-Group Authoring" and "Relation / Situation" Model. MEDINFO '2001 2001: 1: 740-744.

Addresses for Correspondence

Prof. Yasuyuki Hirose : hirose@hosp.u-ryukyu.ac.jp
Yoshiyuki Sasaki : sasaki.prev@tmd.ac.jp