

## **Access Control Models for Clinical and Genetic Information**

**Eduardo B. Fernandez, PhD**

Professor of Computer Science and Engineering, Florida Atlantic University, Boca Raton, FL, USA

**María M. Larrondo Petrie, PhD**

Associate Dean and Professor, College of Engineering, Florida Atlantic University, Boca Raton, FL, USA

### **Abstract**

Remote access to electronic medical information systems facilitates the exchange of patient medical information among doctors, laboratories, pharmacies, insurance providers and medical service providers. The ability to access medical information over the Internet streamlines many health care procedures, such as ordering tests and treatment, communicating test results, billing, insurance authorization and insurance claim processing. With these benefits come an increased potential for misuse of the information and violation of patient privacy, which have prompted many nations to enact laws to ensure security and privacy of patient records. New access control models need to be developed that incorporate the specific security, integrity and privacy requirements of medical and genetic information systems. When building a system that maintains private and sensitive information, security should be forefront in the analysis and design phases of development. We present the requirements, access policies and description for a proposed access control model for medical and genetic information. This model uses object-oriented concepts and patterns.

### **Keywords**

Security Engineering, Medical Information Systems, Access Control, Object-Oriented Modeling, UML/OCL

## **1. Introduction**

Medical information is one of the most sensitive types of information, its misuse could have a very serious effect on an individual's life. In past times this information was collected and stored at physicians' offices and hospitals and relatively few people even knew it existed. In most instances it was not computerized and was protected by its isolation and the ignorance of its existence. All this is fast changing, most or all of the doctor offices use computers, hospitals have large information systems, and a good part of this information is becoming accessible through distributed systems, including the Internet. This means that the number of people that can potentially access information about patients has increased by orders of magnitude. Due to technological advances there is also more information about an individual; for example there is a whole set of genetic information, which was not available a few years ago. This information could affect a person's ability to be hired, his career path, possible promotions, salary, and continued employment.

When building a system that maintains private and sensitive information, security should be forefront in the analysis and design phases of development. We need new access control models that can describe the

specific requirements of medical and genetic information systems. Most of the systems built until now use ad hoc solutions that cannot assure security. We are developing a model that can satisfy those requirements. We discuss the requirements and their effect on the model in the next section, followed by a description of the model. We end with some conclusions.

## 2. Requirements and policies for the model

An access control model suitable for medical records must implement general security policies as well as more specific policies oriented to this type of application. The general security policies that apply to these models, interpreted in this context are:

- It is necessary to apply a “need to know” policy, providing only the information the authorized medical users need for their work and no more.
- Access for the users of this system should be defined by their roles but individual access must also be defined.
- There is a strong emphasis on privacy, which implies a large amount of control by the people about whom we keep information.
- The system should be a closed system, where the lack of an authorization rule implies no access.

To these we can add more specific policies for medical information including:

- Different types of roles have specific access constraints, e.g., patients can see their records and doctors can modify their patients’ information.
- Patients give consent to the use of their records and have the right to be informed of their actual use.
- A doctor or other clinician serves as the record *custodian* and is responsible for the use of the patient record.
- Rights may need to be overridden in exceptional situations.
- Rights may need to be delegated for expediency.
- Records must be accessible for specific time periods.
- Records of patients with genetic or infectious diseases need to be linked to records of their relatives or persons with whom they had contact.

Even more specific policies can be defined; for example, for mental health or infectious diseases. To these policies we must add that the context is a loosely-coupled distributed system, including local area networks as well as the Internet, with applications where records must be frequently exchanged.

From the policies and from the environment where this information is kept we can deduce some requirements for the security model:

*Attribute and credential-based authorization*—In an environment where not all the users that may need access to a document are known in advance, we need to have authorization models that can consider user attributes and credentials to determine access rights.

*Context-dependent access modes*—There are occasions where the standard predefined authorization must be overridden. For example, if a patient is unconscious and needs immediate attention, it is possible that the authorized users of her record may not be present and someone must access the record to decide about treatment. Patients may move around different units of the hospital for tests or treatments and authorization should depend on their location.

*Delegation of rights*—Any authorization model must contain policies on how the rights of a subject are delegated to other subjects. This is especially important in models where privacy is a major objective.

*Temporal restrictions*—Access to patient records depends on time periods. A doctor may have access to a record when the patient is under treatment by this doctor but not after the treatment is finished. He may still retain access to his effect on the treatment but if the patient changes doctors he does not have access to the new additions to the record. This means that the model must be able to apply temporal restrictions.

*Multimedia objects*—Medical records are a combination of text (medicines, treatments, annotations), audio (dictation), and images (X-rays, CAT scans, ultrasound images), as well as other documents related by hypertext links. The model must then include as protection objects all the aspects associated with a record as well as its links to related documents.

*Need for coordinated authentication*—The access control model should be tightly coupled to other aspects such as the authentication model and encryption needs.

*Consideration of different architectural levels*—Enforcement of the security model requires the consideration of all architectural levels. The model must indicate how the enforcement mechanisms at these levels relate to each other.

*Consideration of web standards*—There is a variety of standards that apply to web services and Internet access. These include standards such as WS-Security, SAML, and others. The model should be consistent with these standards in order to be of practical guidance for real systems.

*Compliance with laws protecting security and privacy of health care information*—For example, the Health Insurance Portability and Accountability Act (HIPAA) [hip]. It requires ensuring integrity and confidentiality at all stages of transmission and storage of health care information.

It is clear that no single model can satisfy all these requirements. We need several related models at different abstraction levels. We show here a model that satisfies part of these requirements and that is part of a set of models at different levels of abstraction that can cover all the requirements.

### **3. An access control model for medical information**

We use a hybrid model that combines the access matrix and RBAC models to include aspects such as patient's consent, abnormal (emergency) security access overrides, and ways to relate records. This model is represented using object-oriented diagrams, where authorizations are superimposed on the medical information. We integrate semi-formal and formal specification techniques, combining the Unified Modeling Language (UML) [Rum99] with OCL (Object Constraint Language) [War03], to produce an unambiguous model that is easy to understand. We are also developing a secure methodology to build and configure this type of system. For this, we are adapting and extending our secure systems methodology [Fer04] to suit these types of applications. This methodology makes heavy use of patterns and uses all the architectural levels of the system. The results are being tested on real medical environments, including a hospital and a medical laboratory, having the models and scenarios checked by doctors and nurses.

When building operating systems and other system software, it has long been agreed that security must be an integral part of the design, never an add-on feature or patched as an afterthought. What is not so obvious is that the same principle is valid for general applications, although some authors have indicated this need. Another important aspect is that many models are expressions for security constraints but do not indicate how to enforce these constraints. We believe it is important to provide an abstract architecture to enforce the constraints. Our approach is to develop the appropriate requirements and policies, define an object-oriented model for the security policies, identify patterns in the model, develop

an abstract implementation, test the model and implementation, use the model to create a protection profile, and build a prototype to validate some aspects of the models.

Our work has identified some basic aspects of the proposed model:

*Use of object-oriented models*—Health care records and genetic data contain information that has complex relationships with other information. The object-oriented approach enables us to capture these complex associations in a visual and intuitive manner. Use cases allow us to define role-based access requirements.

*Use of formal constraints*--Using the OCL language we add formality, thus reducing ambiguity while retaining the understandability of the model. The OCL also allows the expression of complex time-sensitive or context-sensitive access rights.

*Consideration of static and dynamic aspects*—An object oriented model includes two types of models: A static model, normally a class diagram, that describes the information and a dynamic model composed of state, collaboration, and activity diagrams, This means that we can describe in our model static and dynamic aspects, including information, states, collaborations, and workflows. In particular, collaboration diagrams are useful to understand a system and to explain the functions to a lay audience.

*Use of different levels of abstraction*—The requirements of the model imply some application-oriented aspects that reflect patient policies. However, some requirements are about architectural aspects, e.g., access control of XML documents. We can build several models at different levels of abstraction, including middleware, DBMS, and operating system aspects [Fer03].

*Use of patterns*—Specific combinations of policies can be defined as patterns. A pattern is a recurrent submodel that describes a solution to a specific problem [Gam94, Sch04]. More complex policies can then be expressed by pattern composition and by adding ad hoc parts.

*Use of implied authorization*—Patient records are logically aggregates of a variety of information, including aspects such as treatments, medications, visits, schedules, and annotations. We have developed policies for the propagation of authorization rules along aggregation hierarchies [Lar90]; we have extended those policies to consider the specific aspects and constraints of this model.

*Content-dependent authorization*--We are investigating two possibilities:

- Extended roles, where the role rights are filtered by content-dependent predicates.
- Attribute-based models, where access depends not only on the subject but also on the satisfaction of assertions including attribute values.

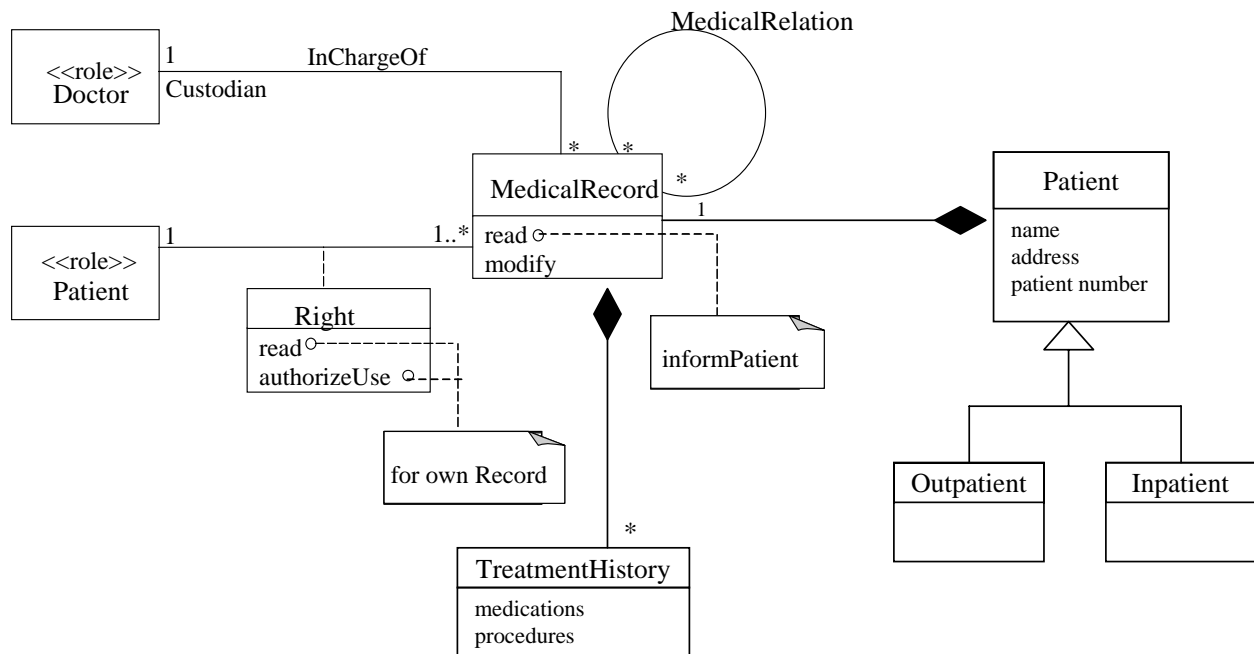
We have started work on the second approach, defining a pattern for access control based on metadata [Pri04]. This will be used in conjunction with the model proposed here.

*Context-dependent authorization*—We are combining our authorization models for databases from [Fer94] with state and workflow conditions.

*Emphasis on privacy*—This appears as having support for specific policies, such as patient control over their records. Another important aspect is to take into account the provisions of the Policies for Privacy Preferences (P3P) [w3c].

*Evaluation of security requests*--When a user sends a request to access information there must be a way to validate the request and decide what information (if any) will be returned to the user. The request is

handled by an abstract reference monitor. The evaluation algorithm must consider both explicit and implicit rules and be reasonably efficient. Starting from a reference monitor pattern [Fer02], we have extended the evaluation algorithms of [Fer94] to this kind of models.



**Figure 1. A model for a patient record.**

Figure 1 shows a first view of the model. This RBAC can be used to define precise access rights to these roles according to a need-to-know policy [Fer97]. A role corresponds to a job or function within a job, or an individual. Rights are assigned to roles, not to each individual. Figure 1 shows how policies are explicitly represented, including:

- A **Patient** role that has the rights to read his own record and authorize the use of this record. Rights are represented in the model as association classes.
- A **Doctor** role showing that a given doctor may act as custodian for a patient record.
- The **Medical Record**, that includes the constraint that any reading of a record must be notified to the corresponding patient.
- Specific medical records may be associated (linked) with other records to describe, for example, family relationships, physical contact, etc.

Because there are a large variety of policy combinations, specific class/association combinations can be described and catalogued in the form of patterns. For example, we could have several models like the one of Figure 1 to represent different combinations of policies. These patterns can be combined to describe more complex sets of policies. They can also be combined with other related aspects such as billing and others. In fact, some of this pattern comes from another pattern, the Patient Treatment pattern of [Sor04].

We are building a catalog of atomic medical security patterns as well as combinations of patterns. We have already developed some patterns for secure patient treatment [Sor04]. For the lower levels, security patterns can be used to define the architecture of the enforcement structure. We have produced several patterns for secure system design.

## 4. Conclusions and future work

We have found that using UML/OCL we can represent complex combinations of medical policies in a precise way that is also convenient for implementation. Patterns for specific combinations of policies, for example for HIPAA use, can be built and catalogued to be used when building secure systems that are HIPAA-compliant. Future work includes development of the lower level models corresponding to distributed architectures that implement and enforce the model. Security is a multilayer problem, one cannot secure just one architectural layer. The lower layers are needed to enforce the application model constraints. Without the enforcement aspect there is not much chance that the model will be used in practice.

## References

- [Epc02] Electronic Privacy Information Center, "Medical Privacy", July 6, 2002.  
<http://www.epic.org/privacy/medical>
- [Fer94] E. B. Fernandez, E. Gudes, and H. Song, "A model for evaluation and administration of security in object-oriented databases", *IEEE Trans. on Knowledge and Database Eng.*, vol. 6, no. 2, April 1994, 275-292.
- [Fer97] E.B. Fernandez and J.C. Hawkins, "Determining Role Rights from Use Cases". *Procs. 2<sup>nd</sup> ACM Workshop on Role-Based Access Control*, ACM 1997, 121-125.  
<http://www.cse.fau.edu/~ed/RBAC.pdf>
- [Fer01] E.B. Fernandez and R. Pan, "A Pattern Language for security models", *Procs. of PLoP 2001*.  
[http://jerry.cs.uiuc.edu/~plop/plop2001/accepted\\_submissions](http://jerry.cs.uiuc.edu/~plop/plop2001/accepted_submissions)
- [Fer04] E.B.Fernandez, "A methodology for secure software design". Accepted for the *Intl. Symposium on Web Services and Applications (ISWS'04)*, Las Vegas, NV, June 21-24, 2004.
- [Gam94] E. Gamma, R. Helm, R. Johnson, J. Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, Boston, Mass., 1994.
- [hip] <http://www.hipaa.org/>
- [Lar90] M. M. Larrondo-Petrie, E. Gudes, H. Song, E. B. Fernandez, "Security Policies in Object-Oriented Databases," in *Database Security III: Status and Prospectus*, D.L. Spooner and C. Landwehr (Eds.), Elsevier Science Pub. (North-Holland) 1990, 257-268.
- [Pri04] T. Priebe, E.B.Fernandez, J.I.Mehlau, E. Masovic, and G. Pernul, "A pattern system for access control " accepted for the *18th. Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Sitges, Spain, July 25-28, 2004.
- [Rum99] J. Rumbaugh, I. Jacobson, and G. Booch. *The Unified Modeling Language Reference Manual*. Addison-Wesley, Boston, Mass., 1999.
- [Sch04] M. Schumacher, E.B.Fernandez, D. Hybertson, and F. Buschmann (Eds.), *Security Patterns*, Wiley 2004 (to appear).
- [Sor04] T. Sorgente, E. B.Fernandez, and M. M. Larrondo-Petrie, "Analysis patterns for patient treatment", submitted for publication.
- [War03] J. Warmer and A. Kleppe, "The Object Constraint Language"(2<sup>nd</sup> Ed.), Addison-Wesley, 2003.
- [W3C] World Wide Web Consortium. <http://www.w3.org>