Assuring Privacy of Medical Records in an Open Collaborative Environment - A Case Study of Walloon Region's eHealth Platform

Syed Naqvi, Gautier Dallons, Arnaud Michot, and Christophe Ponsard

Centre of Excellence in Information and Communication Technologies, Belgium
{syed.naqvi,gautier.dallons,arnaud.michot,christophe.ponsard}@cetic.be

Abstract. In many European countries, elderly citizens constitute a growing part of the population. In some countries like Belgium, it is expected to be as high as one third of the population by 2060. Non-traditional high-tech healthcare solutions are therefore indispensable to cope with the shortage of medical and paramedical staff in the future. In this context, several eHealth projects are launched to modernise the public healthcare system and to address the challenges of declining active workforce in the medical domain. The Walloon Region of Belgium is sponsoring an eHealth Platform for the deployment of internet-based technologies for monitoring of patients and exchange of medical records between hospitals and general practitioners. In this paper, we provide an overview of this eHealth platform and report on-going design activities on managing privacy-sensitive medical data by using a context-aware access control model.

Keywords: eHealth, medical records privacy, access control, open collaborative environments, medical ethics.

1 Introduction

Provision of adequate healthcare services to the increasing elderly population in the coming decades has emerged as a great challenge for the policy makers and healthcare professionals. The current ageing trends depict significant increase in the proportion of elderly population worldwide [1]. The situation in Walloon region of Belgium is not different than the rest of the world. According to the estimation of the Belgian National Statistical Institute, the elderly citizens of Walloon region will constitute almost a third of its population by the early second half of the current century [2]. In order to cope with the resulting demographic realities especially the declining active workforce in the medical domain, several technology-based healthcare projects are launched in the country so as to modernise the public healthcare system. In the same context, Walloon regional government is sponsoring an eHealth Platform *Les TIC au Service des Patients* (ICT for Patient Care) for the deployment of internet-based technologies for monitoring of patients and exchange of medical records between hospitals and general practitioners [3]. This paper provides an overview of this platform and

M. Bezzi et al. (Eds.): Privacy and Identity, IFIP AICT 320, pp. 146–159, 2010.

elaborates our work on managing privacy-sensitive medical data over the eHealth platform by using a context-aware access control model.

The set of legal requirements for collecting, storing, and processing of human data is provided in the section 2. Salient features of the eHealth platform are described in the section 3. Section 4 presents a pragmatic analysis of different access control models and evaluation of their suitability for assuring privacy of medical records in the specific context of the eHealth platform. This analysis yields that OrBAC (Organisation-based Access Control) model [4] is the most suitable for deriving access control decisions. The strength of the OrBAC model is therefore highlighted through a real life scenario in the section 5 where access to a patient's medical record is presented in different situations such as a routine visit to general practitioner, medical treatment at a different clinic, and emergency situations. Those also include potential conflict situations and show how to reason in such a situation both at an abstract level (at design time, using model-checking technology) and at a concrete level (at run-time and instance level). This scenario is deployed on an existing OrBAC engine. We show that organisation-based access control policy assures privacy of digital records by granting access to various actors of the eHealth ecosystem. A number of limitations about the design of scalable set of rules are also highlighted.

2 Legal Requirements for Medical Records Confidentiality

Regulations on the processing of personal data assure the legally enforceable rights for data subjects and obligations for those who process personal data. They also set forth penalties for offenders. This legal coverage spans any information (including health related information) concerning an identified or identifiable person. It is extremely important for the technology-based healthcare solutions to fully comply with these regulations as any shortcomings in the design and/or development phases may lead to legal prosecutions.

2.1 European Union Directive 95/46/EC

This directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data [5] sets the foundations of confidentiality as fundamental principles applicable to all forms of electronic communications. Among others, it imposes conditions of *transparency*, *legitimacy* and *proportionality* for the processing of personal data.

Article 29 Data Protection Working Party. This article defines *working party* on the protection of individuals with regard to the processing of personal data; and recommends specific legislation in member states to regulate the electronic records.

European Union directives are legal bindings on Member States. Their adoption on the Member State level is required for their transposition into national

legislation. Following sub-section describes the Belgian law that implements European directive 95/46/EC.

2.2 Belgian Law of 11 December 1998 on Privacy Protection

Article 22 of the Belgian Constitution already guarantees the right of privacy and private communications. Belgium promulgated its Data Protection Act in 1992 to regulate the processing and use of personal information. This legislation was subsequently modified to make it coherent with the European directive 95/46/EC. The definition of *processing* is extended in the new law so as to enlarge the scope of its application to determine the possible processing of special categories of data and to reinforce data subjects' rights.

The collection, storing, and processing of data over the eHealth Platform requires strict adherence to these legislations. The project consortium includes interdisciplinary experts of IT laws to assure the compliance of legal and regulatory issues. Two main requirements are emerging from this law:

1. The access must be compliant with the finality of the collected private data
2. The collected data must be proportional to the finality

Concretely, it means that the access must be as restrictive as possible depending on the access finality. So, the access context has to be considered in order to determine the finality. The context has a direct impact on rights.

3 Walloon Region's eHealth Platform

Walloon region's eHealth Platform *Les TIC au Service des Patients* (ICT for Patient Care) is an ambitious project that aims to deploy state of the art telemedicine technologies and to advance the existing scientific endeavours to better address the imminent future needs of secure distance healthcare systems. First demonstrator of this platform is planned for the first trimester of 2010 whereas the final prototype of this platform is anticipated for 2012. The salient features of this platform include:

- Multi-platforms and multi-modal interfaces and tailored to users' needs. This research area will explore and develop adaptive human machine interfaces. These interfaces will be adaptive to the context of their use and patient's profile.
- Tangible interface adapted to special users. A new mode of interaction with tangible communicating objects will be studied.
- Inference and composition of services. Different types of mechanisms for services composition will be studied, analyzed and enhanced to meet the needs of the eHealth services.
- Communication protocol for medical equipment. Standard communication protocol for the medical equipment will be defined.

- Security Model for medical data. Technical solutions necessary to ensure the protection of personal data such as medical data will be examined.
- Services certification model. The ways and means of ensuring the overall safety of the platform will be investigated.
- Data mining and integration of medical data. Necessary mechanisms will be developed to achieve interoperability of medical data.
- Review of legal constraints. Analysis of legal constraints on data protection and compliance requirements will be conducted.

Figure 1 gives an overview of the various stakeholders of the eHealth platform. The eHealth project aims to provide medical care to different kinds of elderly patients at home. Initially there are three groups of direct beneficiaries of this project. However, this platform can be easily adapted for other types of

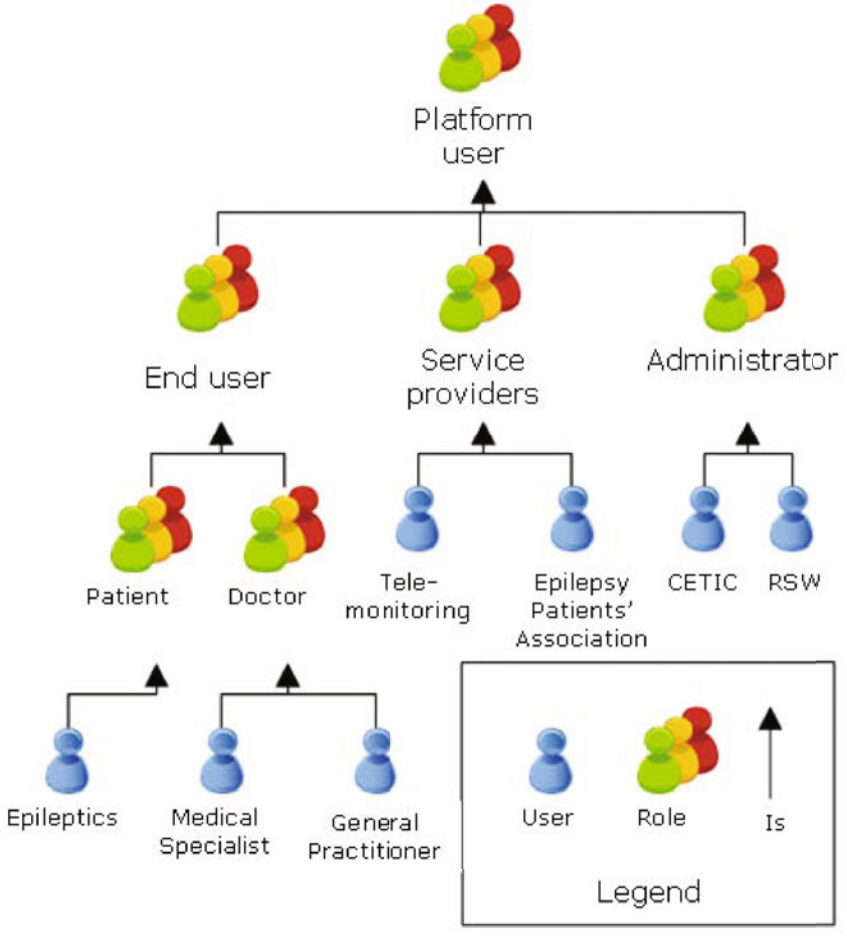

Fig. 1. eHealth Platform

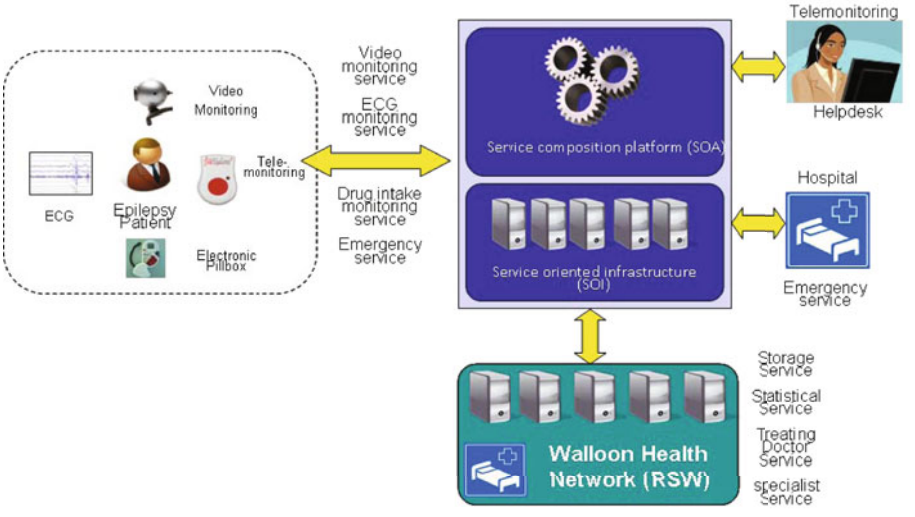

Fig. 2. eHealth Infrastructure

diseases/patients that require distance medical care at their homes. The current beneficiaries of the eHealth platform are:

- Elderly citizens
- Epilepsy patients
- Parkinson patients

Figure 2 highlights the fundamental architectural components of the eHealth platform. This platform will ensure patient care at home through its monitoring of various medical parameters and will provide prevention and adequate intervention on the basis of available medical information of the patient in care. The data generator (such as hospitals) will be responsible for data protection; however they will not be accountable for the security architecture of the platform. The delegation of the security will be bound by the contractual agreements among the participants of the platform in accordance with the compliance to the existing privacy laws. This platform will also ensure better coordination among medical actors (e.g. general practitioners, specialists, laboratories, etc.) paramedics (nurses, physiotherapists, pharmacists, etc.) and nonmedical (dieticians, remote health monitoring companies, etc.) who play specific roles in the management of the patient at home. This eHealth platform will also enable Walloon region's technological SMEs to develop and test new products and services through eHealth pilot scenarios and then at a larger scale by using this platform.

4 State of the Art

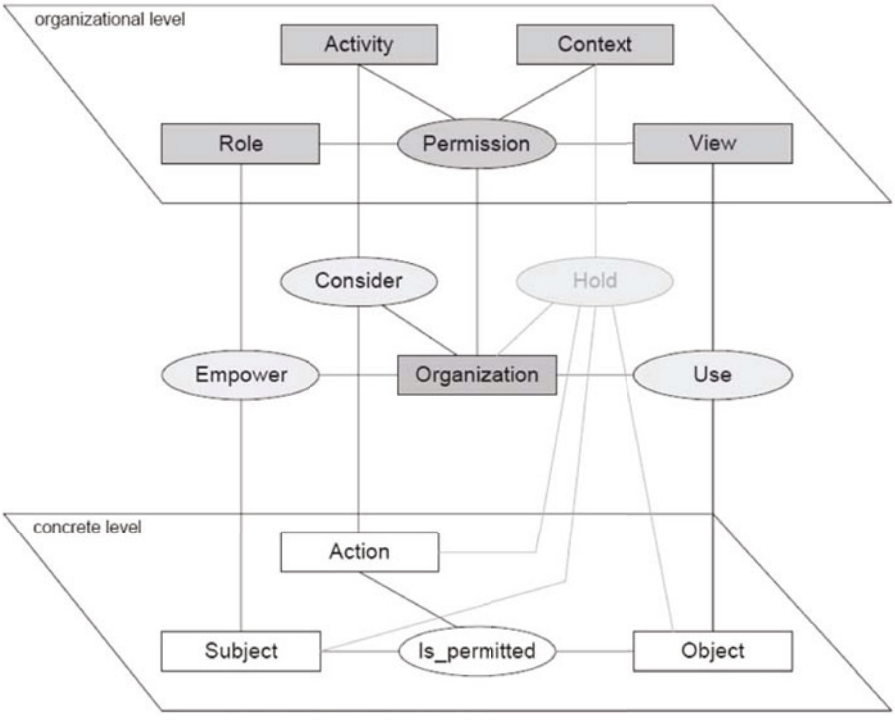

Fig. 3. The OrBAC Model (taken from [16])

4.1 Access Control Models

Access control models are often classified into two broad categories namely Discretionary Access Control (DAC) [6] and Mandatory Access Control (MAC) [7]. Some common implementations of these models include *access control lists (ACLs)* that are considered as the most common mechanism for implementing DAC policies [8]; *Bell-La Padula model* [9] that focuses on data confidentiality and access to classified information; *Chinese wall security policy* [10] that keeps information from one client separated from persons or teams which are working on projects or tasks for a competitor of first client; and *Role-based Access Control (RBAC)* [11].

RBAC is increasingly becoming the de facto access control model for highly scalable networked systems due to its simplified management of authorisation with flexibility in specifying and enforcing enterprise-specific security policies. In the RBAC model, access permissions are administratively associated with roles, and users are administratively made members of appropriate roles. Roles can be granted new permissions as new applications and actions are incorporated, and permissions can be revoked from roles as needed.

We use OrBAC for deriving access control decisions as it allows security policy definition independent of its implementation details by introducing an abstract level [4]. The granularity of the policy definition is at the organisation level and therefore abstraction is done via the organisation. Another interesting feature of OrBAC compared to other models is its capacity to express permissions and prohibitions relative to some context (temporal, spatial, user-declared, prerequisite, provisional)[12]. This model is the only one making it possible to implement requirements emerging from privacy law. Indeed, it allows dynamic right depending on access context. The OrBAC model provides abstraction to the classical access control entities (such as Subject, Action and Object) into organisational entities (such as Role, Activity and View). Therefore OrBAC is a unified access control model that integrates role-based, activity-based and view-based access controls.

Access controls models have been widely formalised in order to perform verification and validation of their expected properties [13]. Some specific work was devoted to the OrBAC model. In [14], OrBAC is formalised in the description logic language with default and exception ALde. In [15], the OrBAC model is translated in Event-B using refinement steps: the first step captures the abstract part of the security policy, the second step introduces OrBAC subjects, actions and objects, and a third step for additional constraints not expressed in OrBAC, allowing to go beyond the limits of the model to cope with increasingly complex security policies.

4.2 Some Related European Projects

OLDES: Older people's e-Services at home. The OLDES project aims to offer new technological solutions to improve the quality of life of older people, through the development of a very low cost and easy to use entertainment and health care platform. OLDES is creating an infrastructure of channels. The project is considering three main categories for care:

1. entertainment and companionship;
2. clinical monitoring;
3. domestic monitoring.

The first category does not correspond with the objectives of the eHealth project; however, the last two categories are inline with the eHealth objectives. We participate in the OLDES project as a consortium member; and the experience gained through this project is a valuable asset for our participation in the eHealth platform.

EPSOS: European Patients Smart Open Services. The EPSOS project is a large scale pilot project with the goal of establishing an interoperable environment for electronic exchange of health information. EPSOS is not a development project in its own right rather it is an implementation quest that aims to facilitate the existing national solutions to communicate with each other enabling secure access to patient health information, particularly with respect to basic patient summaries and ePrescriptions between different European healthcare systems.

EPSOS has the potential of providing an established framework for the integration of our eHealth platform into a European eHealthcare infrastructure where medical records can be securely accessed for treating a Walloon resident travelling abroad or seeking expert opinion of nonlocal medical expert for a medical case study.

CALLIOPE: Call for Interoperability. The Calliope is a European thematic network for eHealth interoperability that aims to create an open forum to support the implementation of interoperable eHealth infrastructures and services across Europe. The network is focusing on a defined set of *Priority Areas* and is already collaborating with the EPSOS project. It is therefore as significant for our eHealth platform as the EPSOS project is.

5 Designing the Access Control Model

5.1 Experimentation Scenario

This scenario illustrates dynamic rights depending on the access finality and context. Figure 4 gives an overview of the case study conceptual model.

- As a general rule, doctors only have access to their speciality if they take care of the patient except in specific contexts.
- In consultations, only physicians who are responsible have access to the relevant part of the record (a cardiologist, the cardiac record, etc.)

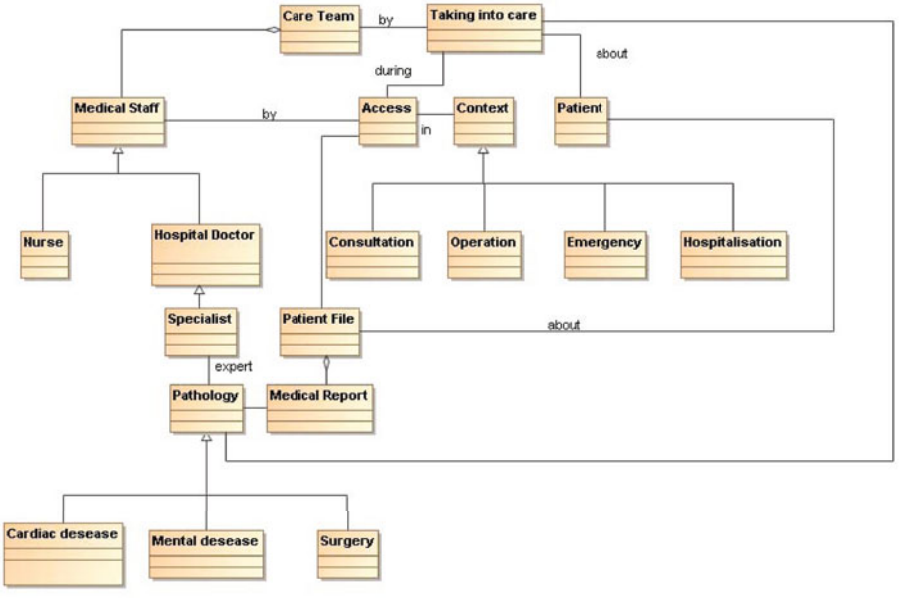

Fig. 4. Conceptual model of the case study

– In operations, the entire care team (including nurses) has access to the record except psychiatric records.
– In any emergency, the whole support team has access to everything.
– In the hospital, only doctors directly involved have access to the entire medical record, except the psychiatric parts.

The invariants, which must be satisfied during the life of the system implementing this scenario, are:

– All medical staff have access to health records in emergency situations.
– The psychiatric record is accessible only to the psychiatrist who takes care of the patient except in an emergency situation.
– The nurses never have access to medical records except in emergency situations or in the operating theatre where doctors are already present.
– Only the doctor who is treating a patient has access to the patient's medical records (partial or total depending on the situation).

5.2 MotOrBAC Implementation

The use case example scenario is implemented by using MotOrBAC [17] as the experimentation engine. The access control policy is expressed in OrBAC. The policy rules are implemented by using separation of constraints and hierarchies. The policy rules contains subjects (medical and paramedical staff); objects (patients records); and actions (read, write).

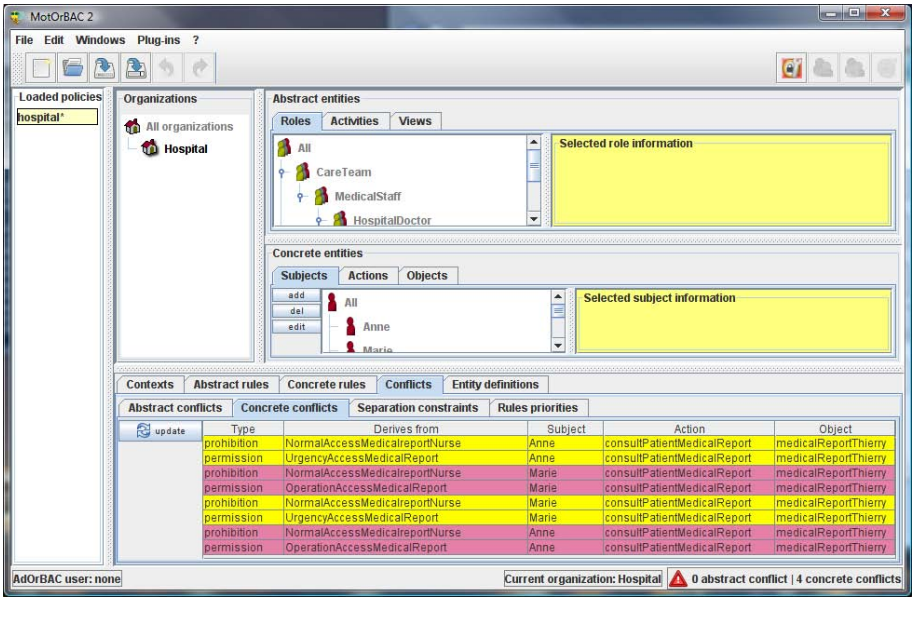

Fig. 5. Implementation of use case scenario in MotOrBAC

MotOrBAC engine identifies the conflicts among the policy rules. In our use case scenario these conflicts are mainly raised due to the expression of both positive and negative privileges in the same set of policy rules. Managing such conflict at the abstract level is advised because it reduces the occurrence of conflict to be dealt with at the concrete level. It will reduce the need of adding several resolution rules at a concrete level which can make the model difficult to maintain in the long term, i.e. when the number of instances grows.

In order to produce an OrBAC model with no or well-identified conflict, we defined a conflict detection and resolution process based on a model formalisation and checks using Alloy.

5.3 Conflict Detection

A conflict occurs when a subject is both permitted and prohibited to carry out a specific action on a particular object in the same context of an organisation. It is especially critical to detect and resolve conflicts at design time to ensure that the behaviour of the policy is adequate. For instance, to ensure that in an emergency situation, medical staff will have access to the necessary information such as surgical information that is not accessible to them in other contexts.

MotOrBAC distinguishes between abstract and concrete conflicts. Abstract conflicts occur between rules, while concrete conflicts involve concrete instances and reflect a concrete situation where the abstract conflict will occur, with reference to particular instances of subjects, objects, roles, context, etc. MotOrBAC is also able to detect abstract conflicts through syntactic analysis, by examining the permission obligation and prohibition of each rule. Abstract conflicts can be made concrete through SAT-solving, through tools such as Alloy [18].

The following model snippet shows a partial formalisation of the medical domain.

```
sig Pathology{}                  // pathology

abstract sig MedicalStaff{}      // medical staff
sig GP, Nurse extends MedicalStaff {}
sig Specialist extends MedicalStaff {
    pathology:Pathology
}
sig Surgeon extends Specialist{}

abstract sig Context{            // context
    team: set MedicalStaff,
    patient: Patient
}
sig Consultation, Emergency extends Context{}

sig Record {}                    // medical records
sig Patient{                     // patient information
    file:Pathology -> lone Record
}
```

```
sig OrbacRule {                    // OrBAC rule
   staff:MedicalStaff,
   patient:Patient,
   context:Context,
   records: set Record
}
```

Some contextual rules are formalised here after for an access in a consultation context and in an emergency context. Additionally, it is also stated that nurses normally have no access.

```
// consultation: only GP or Specialist
fact consultation_staff {
    all c:Consultation, s:c.team | s in GP || s in Specialist
}

// all medical staff have access in emergency situation
fact emergency {
    all c:Emergency, s:MedicalStaff | s in c.team =>
        (one rule:OrbacRule | rule.staff=s && rule.patient=c.patient
                && rule.context=c && rule.records=ran[c.patient.file])
}

// nurse has no access to medical file
fact nurse {
    all n:Nurse | no rule:OrbacRule | rule.context=Consultation && n in rule.staff
}
```

The following consistency check on the model can be run using the tool and will fail to find any model instance due to a conflict. By relaxing the predicate, it appears that the problem is related to the presence of nurse in the team. Actually, in the above formalisation nurses are not allowed to access any patient information.

```
// access in Operation context
pred surgery(p:Patient, c:Operation){
    c.patient=p && some s:Surgeon| s in c.team && some n:Nurse| n in c.team
}
// running the related check
run surgery for 5 but 1 Patient, 1 Operation, 1 Context
```

5.4 Conflict Resolution

Once a conflict is detected, several resolution techniques can be applied:

- OrBAC supports the notion of priority, to denote that one rule has higher importance than another one, and that the later one might be violated in a situation where these two rules conflict with each other.
- Another technique is to weaken one of the conflicting rules to ensure that the precondition of the rule cannot be true at the same time

– The last one is to ensure that the situation that makes the rule conflicting cannot occur, typically by modifying other parts of the model. For instance, one could imagine forbidding administrative staff and medical staff to intersect in order to prevent a conflict between a privacy protecting rule against administrative staff and a medical rule giving access to data to medical staff [19].

To solve the abovementioned conflict, we apply the weakening by explicitly allowing nurse to access in the *Operation* context. The corrected formalisation is the following.

```
fact nurse {
    all n:Nurse | no rule:OrbacRule |  n in rule.staff && rule.context=Consultation
}
```

5.5 Resulting OrBAC Model

OrBAC rules can be directly inferred from the previous model. Some representative rules are the following:

– *Prohibition* $NormalAccessMedicalreportNurse$ for role=$Nurse$, activity=$ConsultMedicalReport$, context=$defaultContext$
– *Permission* $OperationAccessMedicalReport$ for role=$Nurse$, activity=$ConsultMedicalReport$, context=$Operation$
– *Permission* $ConsultationAccessMedicalReport$ for role=$HospitalDoctor$, activity=$ConsultMedicalReport$, context=$Consultation$

The resulting model can then easily be deployed. We can also encode it in the MotOrBAC tool to check about the conflicts at concrete level.

6 Conclusions and Perspectives

Technology-based healthcare solutions such as telemedicine have already been striving for some comprehensible solutions for assuring the privacy of personal data due to the fact that any breach of personal data privacy inflicts irreversible consequences. The emerging technology-based public healthcare systems offer the promising feature of ensuring needful healthcare facilities to the population especially to the increasing proportion of society's elderly population. However, these systems have to be equipped with the adequate security features that can provide privacy assurances to comply with legal obligations.

The eHealth project of the Walloon region of Belgium is an ambitious initiative that aims to address the growing needs of contemporary healthcare practices. In this paper, we presented our proposed solution for assuring privacy of medical records in an internet-based open environment that can handle both routine medical practices and emergency situations.

The current use case scenario does not analyse the privacy concerns of electronic prescribing; however, it is an important area that requires thoughtful consideration especially to assure secure interoperability of the eHealth medical

records with its counterparts in other countries/regions. We also plan to work out the security requirements for assuring overall privacy in the advent of integrating the eHealth platform into a European or into some other international Healthcare infrastructure (such as Health-Grid). We also need to investigate the privacy concerns associated with the use of smart devices in the eHealth platform. The security and privacy concerns are exacerbated when these gadgets are deployed in the open networking architectures. The term *internet of things* is recently coined for this paradigm. Our future directions include research on privacy assurance solutions for the eHealth platform composed over the internet of things.

Acknowledgment

The work presented in this paper is carried out in the context of an eHealth project of the Walloon Region, supported by the FEDER - European Union and the Walloon Region under the terms defined in the Convention ECV12020022296F. Part of the underlying research has also received funding from the European Union's seventh framework programme (FP7 2007-2013) Project RESERVOIR under grant agreement number 215605.

References

1. Kinsella, K., He, W.: An Aging World: 2008 - Int. Population Reports (P95/09-01) (June 2009)
2. Belgian National Statistical Institute, `http://www.statbel.fgov.be`
3. Réseau Santé Wallon, `http://www.reseausantewallon.be`
4. Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C., Trouessin, G.: Organization Based Access Control. In: Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Como, Italia (June 2003)
5. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, CELEX number 31995L0046, Official Journal L 281, November 23, pp. 0031 - 0050 (1995)
6. Lampson, B.W.: Protection. ACM SIGOPS Operating System Review 8(1), 18–24 (1974)
7. United States Department of Defense, Trusted Computer System Evaluation Criteria (TCSEC), Deaprtment of Defense Standard CSC-STD-00l-83 (August 1983)
8. Ferraiolo, D., Kuhn, D.R., Hu, V.C.: Assessment of Access Control Systems, Technical Report NISTIR 7316, National Institute of Standards and Technology, US Department of Commerce (2006)
9. Bell, D.E., La Padula, L.J.: Secure Computer Systems: Mathematical Foundations, MITRE Corporation Technical Report (1973)
10. Brewer, D.F.C., Nash, M.J.: The Chinese Wall Security Policy. In: IEEE Symposium on Security and Privacy, pp. 206–214 (1989)
11. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer 29(2), 38–47 (1996)

12. Cuppens, F., Cuppens-Boulahia, N.: Modeling contextual security policies. International Journal of Information Security (IJIS) 7(4) (August 2008)
13. Habib, L., Jaume, M., Morisset, C.: Formal definition and comparison of access control models. Journal of Information Assurance and Security (JIAS), Special Issue on Access Control and Protocols 4(4) , 372–381 (2009)
14. Boustia, N., Mokhtari, A.: Representation and Reasoning on ORBAC: Description Logic with Defaults and Exceptions Approach. In: Proceedings of the 2008 Third international Conference on Availability, Reliability and Security (March 2008)
15. Benaïssa, N., Méry, D.: Proof-based design patterns, final report of the RIMEL project (ANR-06-SETI-015) (August 2008)
16. Miege, A.: Definition d'un environnement formel d'expression de politiques de securite. Modele Or-BAC et extensions' PhD Dissertation in IT Security, Networks and Computer Science Department of ENST Paris (2005)
17. MotOrBAC: An open source implementation of the OrBAC model, `http://motorbac.sourceforge.net`
18. Jackson, D.: Software Abstractions Logic, Language, and Analysis. MIT Press, Cambridge (2006)
19. van Lamsweerde, A., Darimont, R., Letier, E.: Managing Conflicts in Goal-Driven Requirements Engineering. IEEE Transactions on Software Engineering, Special Issue on Managing Inconsistency in Software Development, 908–926 (November 1998)