Flexible Access to Patient Data through e-Consent

Haridimos Kondylakis
FORTH-ICS
N. Plastira 100, Vassilika
Vouton, Crete, Greece
kondylak@ics.forth.gr

Giorgos Flouris
FORTH-ICS
N. Plastira 100, Vassilika
Vouton, Crete, Greece
fgeo@ics.forth.gr

Irini Fundulaki
FORTH-ICS
N. Plastira 100, Vassilika
Vouton, Crete, Greece
fundul@ics.forth.gr

Vassilis Papakonstantinou
FORTH-ICS
N. Plastira 100, Vassilika
Vouton, Crete, Greece
papv@ics.forth.gr

Manolis Tsiknakis
FORTH-ICS
N. Plastira 100, Vassilika
Vouton, Crete, Greece
tsiknaki@ics.forth.gr

ABSTRACT

The advances in healthcare and information technology are shifting more and more the ownership of data from medical institutions and doctors to individual citizens. However, since the medical information of an individual is confidential, the only basis for sharing it, is through prior informed consent which will regulate access to his private healthcare data. This paper highlights challenges investigated in three EU research projects and presents a solution utilizing *novel access control mechanisms* to ensure the selective exposure of the patients' sensitive information thereby empowering them. Our solution can efficiently support the entire lifecycle of consent such as withdrawal, activation, deletion or update. Moreover it responds to complex and different scenarios in which the patient can define *complicated* and *dynamic access control policies* at different granularity levels. In this paper we propose a Personal Health Record (PHR) system, accessible through desktop and mobile devices, that explores the efficient access regulation to information according to the *consent forms* provided by the patients.

1. INTRODUCTION

A recent report by the eHealth Task Force entitled *"Redesigning health in Europe for 2020"*[1] focuses on how to achieve a vision of *affordable*, *less intrusive* and *more personalized* care, ultimately, increasing the quality of life as well as lowering mortality. Such a vision depends on the application of ICT, the use of data and requires a radical redesign of health to meet these challenges. The starting point for such a redesign, as identified by the report, is *enacting individual ownership of personal health data*. The adopted theme is *"my data, my decisions"*. Individuals are the owners and controllers of their own health data, they can manage their data with their personal devices, and have the right to *make decisions on who can access the data and to be informed about how it will be used*. This principle is outlined in EU law but is *rarely fully implemented in health systems*.

In parallel, a second main driver for change is currently taking place under the term *"liberate the data"*. The secondary use of care data for research, quality assurance and patient safety is still rarely supported and the main barriers to this are the lack of interoperability, common standards and terminologies. Large amounts of data are currently stored in different silos within health and social care systems. If this data is released in an appropriate manner respecting the patients' privacy and used effectively it could transform the way that care is provided.

This paper focuses on current research activities within three EU research projects (iManageCancer[2], EURECA[3], p-Medicine[4]) which are currently trying to enable individuals who are the owners and controllers of their own health data, with the right to make decisions over access to their data and to be informed about how it will be used by third parties. More specifically, the scenario that we envisage is that the patients' data are stored in some repository, upon which several data consumers (such as doctors, nurses, funding organizations, insurance companies etc.) would require access for different purposes. In such a setting, we explore how to enforce appropriate *access control* to the patients' data, given the *electronic consent* forms that are provided by the patients. At the same time a key requirement is to support the release of the data from different silos throughout the healthcare system and to connect them to the vibrant digital environment for health information which is expected to transform the landscape of healthcare. Our approach relies on the RDF data model [3] that promotes the interoperability among e-health systems among others and has the following benefits:

[1] http://goo.gl/wyIZhO

[2] http://imanagecancer.eu/
[3] http://eurecaproject.eu/
[4] http://p-medicine.eu/

- It provides an appropriate access control enforcement mechanism, that essentially filters the data shown to a data consumer, depending on who the consumer is, his current role, the purpose of access, and the access rights imposed by the consent form(s) for the patient's data as specified by the patient herself.
- It allows partial release of personal health information at different granularity levels. The patient can avoid the low-level detail but is also capable of defining fine grained access control to his/her information.
- Instead of defining explicitly the roles that may have (or not) access to the information, access privilege to entire hierarchies of roles can be used.
- It manages the entire lifecycle of consent such as consent withdrawal, activation, and deletion. It handles updates on information efficiently and effectively without requiring each time e-consent redefinition. In addition, it can handle emergency situations and provides an auditing mechanism to ensure proper system usage.

Providing patients with *consent management* offers a dual benefit: first of all there is the direct empowerment aspect of controlling one's own data; and second, it facilitates interaction with patients in order to ask for new consent for a different purpose, both increasing efficiency and involving the patient actively.

The rest of this paper is structured as follows: In Section 2 we give example healthcare scenarios that show the complexity of the problem. Section 3 focuses on the access control approach that we propose for implementing the patient consent forms. In Section 4 we present other approaches that try to resolve similar problems and finally Section 5 concludes the paper and presents directions for future work.

2. SCENARIOS, CHALLENGES AND REQUIREMENTS

In this section, we give some example scenarios that highlight the complexity of providing selective access to patients' health record and analyze the challenges that must be addressed. Section 3 presents in detail our approach for addressing these challenges.

Let us consider a patient, named Alice, who moves to another city, or decides to visit a new General Practitioner (GP). The GP would require access to Alice's medical history, which consists of several medical tests and reports by various healthcare professionals. All required information is stored in Alice's PHR account and the GP would greatly benefit if he could have direct access to Alice's data. To perform this, Alice must give permission to the doctor to access her medical record through a consent form.

According to the EU Data Protection Directive [6] *the data subject's consent shall mean any freely given specific and informed indication of his wishes by which a data subject signifies his agreement to personal data relating to him being processed.* Furthermore, according to the same directive, the patient's personal data may only be accessed if she has given her consent for a well-defined access purpose ("least privilege"); data subjects may withdraw their consent at any time ("right to be forgotten").

In addition, the PHR system should offer a simple web-based interface that allows her to access her personal records from everywhere, using her computer, or her smartphone, requiring no special software or hardware. This web interface should provide basic functionality for Alice to easily create and manage e-consent forms. Such consent forms would allow her to give or withdraw ("right to be forgotten") consent for specific part(s) of the dataset to specific data consumers (users/roles) and for a specific purpose. Moreover, Alice should be able to monitor the access requests by different data consumers (in this case, the GP), allowing her to review who is requesting the access, the purpose of the request, and which data is requested and accessed and when. This will allow her to easily decide whether access should be granted, and fill in the corresponding e-consent form. Management functionalities for the consent forms would be useful in this respect; for example, Alice may decide to change a consent form or she may want to withdraw or delete saved consent forms and to re-activate withdrawn consents. In addition, an auditing mechanism should record each access to one's medical information to ensure that only authorized accesses are actually realized.

Assume now that Alice is updating her PHR. New entries should be checked against existing consent forms so that Alice can review whether these forms address in a satisfying manner the newly added information. Note that an update could cause other items to be accessible due to correlations in the data. For example, assume that Alice has created a consent form through which she accepts to release to a research trial her tumor type if and only if the stage of her tumor is greater or equal to T3. After a future treatment, if the cancer is in recession (cancer stage different than T3), the information that was previously accessible for the specified role and purpose should not be accessible anymore. On the other hand, irrelevant data and consent forms should not be affected by a change in the data. The PHR system should ensure that the identification of relevant and non-relevant consent forms and data, as well as the access control enforcement should be efficient.

Now, suppose that, Alice has a car accident and sustains minor injuries. The emergency response team reaches the accident location and starts treating Alice. For the treatment, the paramedic requires Alice's consent to access her medical history to get information about her allergies and any serious conditions that she already may have and could interfere with the provided emergency treatment. However, Alice is unconscious, and cannot provide the required consent. To support this case, Alice's PHR should provide a basic medical data set which can be accessed only in emergency situations. So, the necessary access control mechanisms should be in place specifying not only the user or role that should have access to the information, but also the purpose and the situation in which they apply. Auditing will be a measure to prevent data misuse in this case.

Besides defining explicitly that specific roles have access or not to information, hierarchies of roles could also be used. For example, Alice could decide that all Emergency Medical

Responders (EMRs) have access to her information. Since a Paramedic is a specialization of an EMR all paramedics have also access to her information.

From the aforementioned examples, it becomes obvious that specifying a set of authorization policies which capture all the details required to enforce correctly an individual's decisions about consent is a very complex task and should also adhere to the existing legislations. Although work has been done to address the problem of automatically resolving conflicts [11], it is not possible to completely automate the decision since in the specific case of the healthcare scenarios humans are also involved. To complicate matters further, contextual information needs to be captured to identify the purpose of the access being requested. Serious consequences might arise if the security administrator does not record correctly all these details in the policy specification. And although the social workflows of the scenarios described in this section are not yet fully in place and some aspects require further exploration, we expect that the situation will soon change. To this direction, in this paper, we explore the technological mechanisms that should be fully in place when this happens.

3. ACCESS CONTROL MECHANISM

Annotation models are simple and straightforward, but cause efficiency problems when dealing with dynamic information, because any change in the dataset would affect some of the implicit annotations, but there is no way to know which ones (or how). Thus, a change in the dataset would require the re-computation of all annotation labels to make sure that the access labels of all triples are correct. The same is true if a change in the access control policy happens (which could be as simple as the introduction/ withdrawal of a consent form in our scenario, or as complex as a legislation change that causes massive changes in the accessibility rights of medical data).

In our setting, both the data itself and the related accessibility information are dynamic, especially given the fact that any patient can at any given time submit (or withdraw) a consent form that changes the access rights to her information. Thus, we chose an abstract access control model, described in [9], which has better computational properties in the presence of dynamic information. In this subsection we give a brief introduction to this model, without entering into too many technical details, as the focus of this paper is on the application of the model in a patient-managed medical data repository; further details on the technical aspects can be found in [9].

Unlike standard annotation models, abstract access control models are based on the idea that the accessibility of each data item (triple) is not pre-computed; instead, each data item is associated with an access label, which is essentially an abstract algebraic expression that encodes how the label should be computed (rather than the result of this computation). Thus, in abstract access control models, the access control annotation is an algebraic expression, rather than a simple access label (value). These algebraic expressions are constructed using abstract tokens and abstract operators.

Abstract tokens are explicitly assigned to the data items by the knowledge curator, and determine the "chunks" of data that need protection: two data items with the same token are necessarily protected under the same access control scheme. All triples associated with the same abstract token are assumed to be of the same "nature", as far as accessibility is concerned. Abstract operators are applied in cases where the accessibility of a triple is somehow related to the accessibility of other triples, e.g., in the case of inference described above. Essentially, abstract operators "compose" access tokens into more complex algebraic expressions [9].

To identify the accessibility of a given triple, we first compute its abstract label using the abstract token(s) explicitly assigned by the curator (if any) along with any implicit labels (resulting from inference). The final algebraic expression does not, in itself, tell us whether a triple is accessible or not for a given user/role and purpose; to determine that, we need to associate each token with a specific (concrete) value, and each abstract operator with a specific (concrete) algebraic operator. This is the done via the concrete policy, which is a set of definitions determining how abstract tokens and operators should be interpreted (i.e., translated into concrete ones), and allows the computation of the actual accessibility of the triple under question. To allow different accessibility schemes, a different concrete policy per user/role and purpose is defined.

In our example scenario, when Alice submits an e-Consent form (either an explicit one, or a default one), behind the scenes, a new concrete policy is defined for the specified user/role and purpose. Moreover, Alice can also specify the granularity of the information she is sharing; for example, she can allow only the tumor type to be accessed but not more specific details about it. This is done by specifying the appropriate condition under which an algebraic expression is evaluated to an accessible or inaccessible value. When a patient wants to refine the granularity of data access this is handled by simply defining correctly the concrete policy and more specifically the condition under which an algebraic expression is evaluated to an accessible or inaccessible value. This happens without involving the patient in the definition of low-level algebraic expressions. These are automatically generated as the patient selects the necessary information level from the hierarchy of the data currently available.

If Alice later decides to change or withdraw her consent, such an update would normally result in the costly re-computation of access control annotations for all triples in standard access control enforcement approaches. However, our technique avoids that by using abstract access control models which persist; the only thing that changes is the way that the algebraic expression is interpreted (when the accessibility of the corresponding triple is computed - which is done at query time). Similarly, when Alice adds new data or updates her existing data, there is no need to re-compute the access labels of all triples and recheck all applicable consents; algebraic expressions allows us to determine which triples are affected by the change, and how, essentially limiting re-computation to the part of the data that is indeed affected.

4. RELATED WORK

In the literature, there have been proposed several approaches for regulating access to data. There are role-based, team-based, attribute-based, content-based, scenario-based, situation-aware, context-aware, and context sensitive access control methods (see [14] and [4] for an overview). However, only some of these approaches have been implemented for healthcare scenarios [4]-[15], a few of them consider the problem in distributed and dynamic scenarios [7] whereas a small number of approaches propose models adherent to healthcare standards [14], [2], [5], [8]. In all these systems the notion of e-consent is integrated with the policy decision mechanism.

Other approaches focus on the notion of e-consent. For instance, Russello et al. [12] propose to capture the notion of consent through the use of medical workflows and to integrate it with Ponder2 authorization policies. However, there is no automatic mechanism for managing the lifecycle of consent, such as consent withdrawal, activation or deletion. In another work, Asghar and Russello [1] suggest a mechanism for managing the consent lifecycle. They introduce a notion of very expressive consent represented as a consent policy. However, they assume that a data subject defines solely his/her consent policies; unfortunately, such a solution may not be acceptable because data subjects may not be able to understand low-level policy details. The same limitations with complicated preferences can be also found in the EnCoRe (http://www.encore-project.info) UK research project. In a follow-up work of Asghar and Russello, called ACTORS [10], a goal-driven approach is presented to glue together and manage authorization policies that aim at handling user consent in a specific context. The authors simplify the specification of authorization policies when these are treated as a program sequence towards a specific goal. By using such Teleo-Reactive programs a security administrator can capture more naturally the security requirements. However, we believe that both administrator and usual user preferences should be considered when dealing with patient data. Wuyts et al. [13] use the XAXML policy language. However, the attributes defined a priori may not be sufficient to capture consent since the latter might involve multiple different conditions and exceptions. Other approaches [1] try to overcome this issue, by considering consent as an authorization policy; however, other problems appear in these cases. For example, these approaches require users to specify low-level details, a normal user may not be aware of at the time of policy creation. Second, there is no automatic mechanism for managing the consent life-cycle.

Given the fact that patient information is distributed across different sources, it is required that she should manage her different consent forms in a unified and consistent manner. Our approach succeeds in collecting all patient data in a PHR and then managing his/her consents in a unified consistent manner.

5. CONCLUSIONS

This paper presents an approach for e-consent implemented on top of a PHR system. Our approach promotes interoperability among different e-health systems and allows partial release of personal health information at different levels of granularity. The rules generated continue to work when new knowledge is entered in the system or to knowledge inferred by existing data. The system efficiently supports different and complex scenarios in which the user can define complicated and dynamic access control policies. For future work we plan to optimize the system implementation and to evaluate its usability with real patients. In addition, we expect more complex use-cases to appear, which might dictate changes in the approach. It becomes obvious that informed consent is an important topic and several challenging issues remain to be investigated in the near future.

6. ACKNOWLEDGMENTS

This work was partially supported by the iManageCancer (H2020-643529), the p-Medicine (FP7-270089) and the EURECA (FP7-288048) EU projects.

7. REFERENCES

[1] R. G. Asghar, M.R. Flexible and dynamic consent capturing. In *iNetSeC*, 2011.

[2] B. Blobel. Trustworthiness in distributed Electronic Healthcare Records - basis of shared care. *Computer Security Applications Conference*, 17, 2001.

[3] D. Booth, C. Dowling, E. Fry, S. Huff, and J. Mandel. RDF as a Universal Healthcare Exchange Language. SEMTECH Panel, 2013.

[4] A. Ferreira, R. Cruz-Correia, L. Antunes, and D. Chadwick. Access control: how can it improve patients' healthcare? *Studies in Health Techn. and Informatics*, 127, 2007.

[5] P. Hung. Towards a privacy access control model for e-healthcare services. In *PST*, 2005.

[6] N. Iheanyi. Legal and ethical issues in integrating and sharing databases for translational medical research within the EU. In *BIBE*, 2012.

[7] J. J. Hu and A. Weaver. A Dynamic, context-aware security infrastructure for distributed healthcare applications. In *Workshop on Pervasive Privacy Security, Privacy, and Trust*, 2004.

[8] W. Jih, S. Cheng, Y. Hsu, and T. Tsai. Context-aware access control on pervasive healthcare. In *MAM*, 2005.

[9] V. Papakonstantinou, M. Michou, I. Fundulaki, G. Flouris, and G. Antoniou. Access control for RDF graphs using abstract models. In *SACMAT*, 2012.

[10] A. M. Rizwan. ACTORS: A Goal-Driven Approach for Capturing and Managing Consent in e-Health Systems. In *POLICY*, 2012.

[11] G. Russello, C. Dong, and N. Dulay. Authorisation and conflict resolution for hierarchical domains. In *POLICY*, 2007.

[12] G. Russello, C. Dong, and N. Dulay. Consent-based workflows for healthcare management. In *POLICY*, 2008.

[13] K. Wuyts, R. Scandariato, G. Verhenneman, and W. Joosen. Integrating patient consent in e-health access control. *IJSSE*, 2(2):1–24, 2011.

[14] M. H. Yarmand, K. Sartipi, and D. G. Down. Behavior-Based Access Control for Distributed Healthcare Systems. *Journal of Computer Security*, 21(1):1–39, 2013.

[15] L. Zhang, G. J. Ahn, and B. Chu. A role-based delegation framework for healthcare information systems. In *SACMAT*, 2002.