CS898 Project Proposal
Patient Consent via Policy Enforcement
Spring 2010

Atif Khan, Sarah Nadi
University of Waterloo

I. Introduction

With the advance of Information Communication Technologies (ICT), more and more organizations are utilizing electronic systems to capture, manage and use patient related information. The scope of this information varies from organization wide Electronic Medical Records (EMRs) to Electronic Health Records (EHRs) shared between different organizations. Although this improves the effectiveness of information exchange, coordination, and use, it also raises the critical issue of patient consent. Usually, patient information is collected for the primary purpose of providing health care for a specific episode. Any secondary use must be in accordance with patient consent. Ideally, in an electronic system, the system would automatically grant or deny permission to accessing a patient's record according to their specific consent policy. However, it is often difficult, if not impossible, to predict all future-use scenarios and enforce patient consent in an appropriate manner.

To address this problem, we propose building a policy based patient consent management system. The system would utilize (previously captured) patient consent information and various operational policies as input. Each policy will be represented by a set of RDF rules in Notation 3 (N3) [1]. We will use the Euler proof mechanism [2] to compute (a) the result and (b) the proof of the aggregated rules.

Our goal is to demonstrate that various actions on patient information can be protected in a real-time manner by utilizing the policy based consent management. This offers a major improvement over the current industry practise of patient consent management and secondary use of patient information.

A. Assumptions

1) Patient consent is already precaptured and stored in the system: Our project is not concerned with how patient consent can be captured electronically. We assume that this information is already available for our use. We plan to use the four general forms of consent commonly used in the field [3]:

- General Consent (also referred to as the "opt-in" model)
- General consent with specific denial(s)
- General denial with specific consent(s)
- General denial (also referred to as the "opt-out" model)

There are many specifications of these general rules available in the Integrating the Healthcare Initiative (IHE). For example, a specification of the third form could be explicit opt-out, but allowing emergency overrides. Since it is not possible to consider all possible specifications in the scope of this project, due to time constraints, we will consider different policy scenarios as we see appropriate.

B. Policies and facts will be expressed in N3 notation

Privacy policies, patient consent and facts will be expressed in N3 notation. Facts include information such as who belongs to which organization, their schedule information, information about the organization etc.

C. Euler Inference Engine will be used

We will use the Eurler Inference Engine since it accepts N3 notation and can generate a proof for the results of its reasoning.

D. Contributions

1) Ontology of privacy policies expressed in N3 notation: Our first contribution is an ontology of privacy policies expressed in N3 notation. This contribution will provide a basis for future work in this area since N3 is a widely used notation. The ontology will include expressing privacy policies defined in standards such as (IHE) as well as the relationships between them. For example, explicit opt-out is a specialization of opt-out with certain exceptions where the exceptions are an empty set.

2) Policy conflict detection rules: We will define a set of rules that detect conflicting policies. These rules will also be written in N3 notation. For example, if the general opt-in policy and the general opt-out policy both give access to patients' records, then there is something wrong in the policy definitions.

3) A collection of executable scenarios: We will define a set of scenarios that exhaustively test the set of policies included in our project. This includes defining the facts of the scenario in N3 notation, defining the questions that need to be asked in N3 notation, and feeding this information into the Euler engine. The Euler engine then returns the answer to the proposed question along with a proof of how it was obtained. We need to check both the answer and the proof to verify that the policies were indeed applied. Any unexpected behavior will indicate that the policies have not been correctly expressed.

II. Project Deliverables

The project deliverables at the end of the semester are as follows:

1) An ACM style 10 - 12 pages project report describing the following:
   a) A survey of the current techniques followed to implement electronic patient consent systems.
   b) A description of the ontology of privacy policies developed.
   c) A description of the test cases (scenarios) we examined.
2) The developed ontology in N3 notation.
3) Development Code.
4) Class Presentation and Demo.

References

[1] "Notation 3 (n3): A readable RDF syntax," Website, http://www.w3.org/TeamSubmission/n3/.

[2] "Euler proof mechanism," Website, http://eulersharp.sourceforge.net/.

[3] E. Coiera and R. Clarke, "e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment," *Journal of the American Medical Informatics Association*, vol. 11, no. 2, p. 129, 2004.