Patient Consent

Atif Khan, Sarah Nadi
David R. Cheriton School of Computer Science
University of Waterloo
Ontario, Canada
??, snadi@uwaterloo.ca

***Abstract*—The abstract goes here.**

I. Introduction

With the advance of Information Communication Technologies (ICT), more medical 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. It has been argued that a patient should be aware of all the systems collecting their information, and should be able to specify how this information can be used [1]. 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.

There are many aspects of this problem that need to be solved. First, how can patient consent be captured electronically in an effective way? Second, how can the captured consent policies be represented and processed internally? Finally, how can we define consent policies that protect the patient privacy, but do not compromise their health at the same time? All three problems are very important in this domain. However, in this paper, we focus on the second problem, and briefly touch upon the third.

To address these problems, 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) [2]. We will use the Euler proof mechanism [3] 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. The advantage of using Euler to generate a proof is that in the future, proofs can be validated between different systems when exchanging EHRs. This offers a major improvement over the current industry practice of patient consent management and secondary use of patient information. This paper describes the preliminary effort in this direction where we illustrate the applicability of our idea through a selection of consent policies and situations.

The contributions of this work are as follows:

- A set of consent policies represented in N3 notation. These are expressed as N3 rules which allow or deny access to the specified documents.
- A collection of executable scenarios that show how the consent policies are applied in different situations. A Java application is developed to demonstrate these scenarios.
- Policy conflict detection (We still need more details about this part)

The rest of this paper is organized as follows. Section II provides background information about patient consent, N3 notation, and the Euler engine. Section III describes some of the work that has been done to develop an electronic patient consent system. Section IV explains the different consent policies, and which ones will we be including in our prototype. Section V describes the prototype system developed in this work. It describes how the information flow in the system as well as the policy rules and facts used. This section also mentions the current limitations of the system. Section VI discusses ??, and outlines possible future additions to the system. Finally, Section VII concludes this paper.

II. Background

A. Patient Consent

Background of what patient consent is (accessing records vs consent to an operation for example).

Historically, patient consent was through paper (brief summary of how it went)

B. N3 Notation

Brief summary of N3 notation

C. Euler

Brief summary of how Euler works and how it provides a proof. Mention things like one query per file, and first match only etc.

III. Related Work

Work that addresses patient consent for access of electronic records.

IV. Consent Policies

There are different forms of consent that a patient may choose from. Coiera and Clarke [4] define four general forms of patient consent as follows:

- *General consent*: This is also generally known as "opt-in" which means that the patient agrees that any health care professional may access all of their health data for the purpose of providing care to them.
- *General consent with specific denial(s)*: This means that the patient specifically defines certain exceptions to their general consent policy. These exceptions may be related to particular data or to particular people.
- *General denial with specific consent(s)*: In this case, the patient generally denies access to their data except in specific circumstances. These may include disclosure for specific purposes or to specific people or the disclosure of certain types of information.
- *General denial*: This is the strictest level of consent a patient may have. In this case, the patient denies the use of their information for any future event irrelevant of the circumstances that may occur. This consent policy is also generally known as "opt-out".

Pruski [5] use these four forms of consent while designing their rule-based language for describing patient consent policies. Additionally, Pruski outlines the key requirements that must be taken into consideration while dealing with patient consent. These are expressing who can access the data, the kind and the sensitivity of the data, the period for which a consent policy is valid, the purpose of why the data is being accessed, and what kind of consent is given to the user requesting the data.

In our work, we consider both the four forms of patient consent as well as some of the requirements proposed by Pruski. In our current prototype, we support five types of patient consent policies as follows:

- *opt-in*: As described above, a patient who has an opt-in policy allows any treating doctor to access their information. In our system, we also add other conditions that need to be met such as that the health care professional should be a member of the admitting organization etc. These details will be discussed in Section V.
- *opt-in except for sensitive documents*: In this case, the patient allows access to all their information except for documents that are classified as sensitive. For example, these may include HIV tests or Sexually Transmitted Diseases.
- *opt-in except for certain people*: In this case, the patient allows access to all their information, but specifically denies certain individuals from accessing their data.
- *opt-out*: A patient with an opt-out policy explicitly denies access to all their information regardless of who is trying to access the data or why they are trying to access it.
- *opt-out with emergency override*: In this case, the patient agrees to grant access to their information only if it is an emergency situation.

V. Our System Name

Not sure of this section's title but if we have a name for our system, that would do for the title.

A. Information Flow

Currently, our system assumes that all the information needed is already captured. That is, all information about the patient, their documents as well as their privacy policies. Similarly, we also assume that all the information about the different hospitals, doctors, and nurses is already present. In this sense, we focus on answering the question of whether a doctor or nurse can access a certain document. This is done by loading the facts available and our rule set into Euler, and then querying it to see if a certain doctor or nurse can access a certain document. If access is granted, then we present the user with the proof provided by Euler. If no proof is found, we check if we can find an explicit deny rule for the same actors in the original query. If so, we present the user with the proof of why access has been denied.

PUT SNAPSHOTS HERE

B. Facts in N3 Notation

To test our access policies, we chose a set of facts that can reflect all the situations we wish to test.Figure 1 shows all the facts we use to test our rules. There are four different types of actors: doctors, nurses, hospitals and patients. All hospitals have a "members only" policy where only members of the hospital are authorized to access patient information. Some hospitals enforce a "on shift" only policy where only members that are currently on shift may be able to access any patient information. Doctors and nurses can be members of more than one hospital, but can only be on shift in one hospital at a time. A patient is treated in a hospital, and own documents that reflect their medical information. Some documents are classified as sensitive. Currently, we only classify documents as sensitive or non sensitive (the default). In the future, we may wish to add different types of classifications such that a patient may have more flexibility in specifying which category of documents do they grant access to. Additionally, a patient may be in an emergency situation. The default is that the patient is in a regular episode of care. As indicated in Section IV, we currently support five different types of patient consent policies. These are coded as optin, optinsens, optinexcep, and optout respectively. We assigned the different policies to the patients such that all of our designed access policies can be successfully tested. Appendix A shows the n3 facts file we use to represent the facts shown in Figure 1.

C. Access Policies in N3 Notation

In our current prototype, we have designed the basic set of rules that can later be expanded for more sophisticated rule nesting. The complete rule file can be found in the Appendix B. There are six possible conclusions in our rule set. The two main conclusions are allowing or denying access. However, we need the other rules to reach these conclusions. The following is the list of these four conclusions:

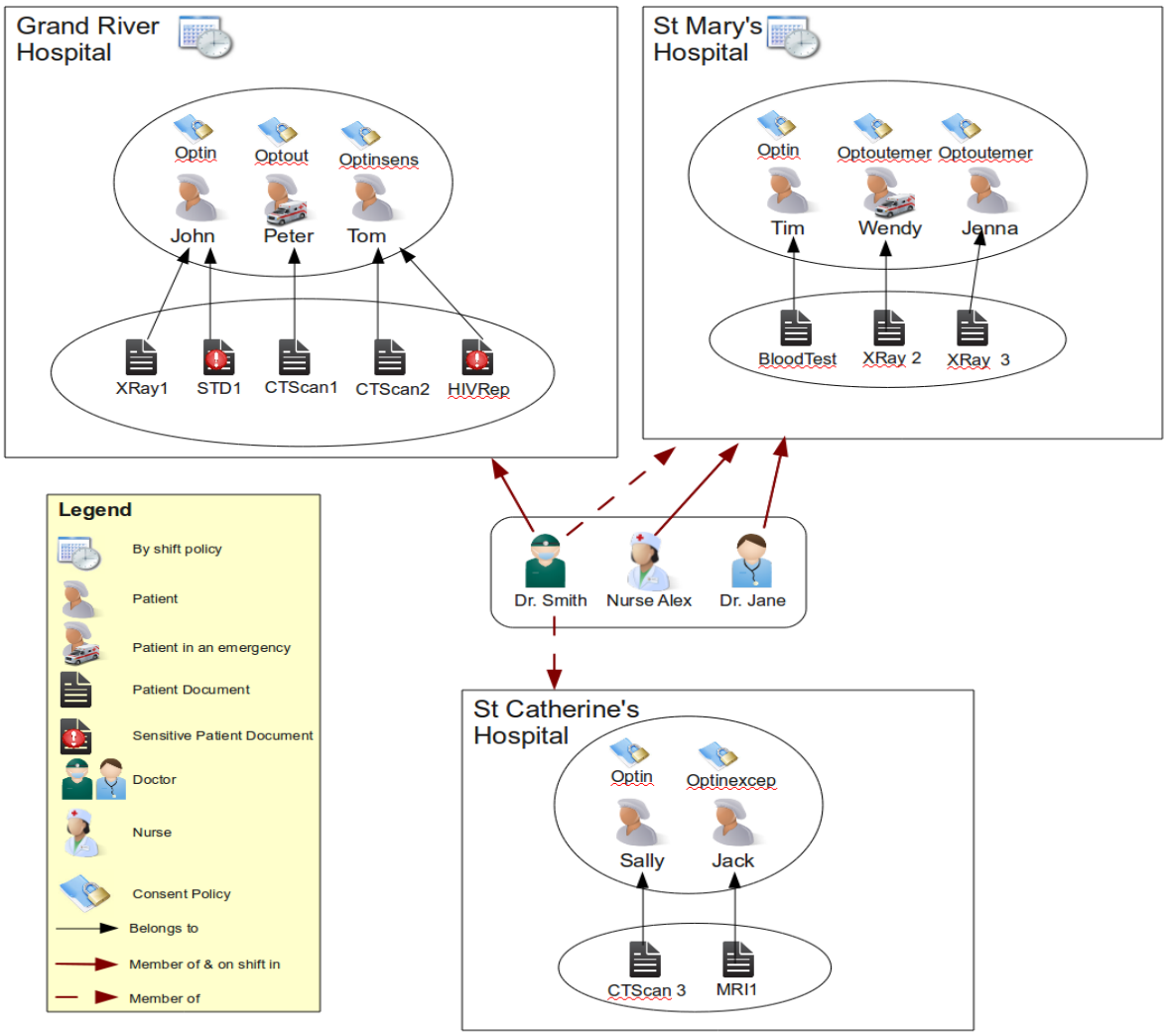

Fig. 1. Tested Facts

- ***possibleaccess***: A person a has possible access to patient p if they are a member of the organization p is treated in. Additionally, if this organization has a by shift policy, then a must be on shift to have possible access.
- ***authenticated***: A person a is authenticated to access a patient p's information if they have possible access to p, and they are treating p. The reason possible access is separated from authentication is that in emergency situations, a non treating doctor might need to access this patient's information. In that case, they still need to satisfy the possible access rule.
- ***access***: A person a is granted access to a document d if one of the following cases is true:
  - a is authenticated to access p's information, d belongs to p, and p has an opt in policy.
  - a has possible access to p's information, d belongs to p, p has an opt out policy with emergency override, and p is in an emergency situation.
  - a is authenticated to access p's information, d belongs to p, p has an opt in policy with exceptions, and a is not one of those exceptions.
  - a is authenticated to access p's information, d belongs to p, p has an opt in policy except for sensitive data, and d is not classified as sensitive.
- ***cannotaccess***: This is the converse of the "possibleaccess" rule. A person a does not have possible access p's information if p is treated in o, but a is not a member of o. Similarly, if they are a member, but are not on shift in an organization that has a by shift policy, then a does not have possible access p as well.
- ***notauthenticated***: This is the opposite of the "authenticated" rule. A person a is authenticated to access p's information, but a does not treat p, then a is not authenticated to access p's information. If a cannot access p's information in the first place according to the previous rule, then a is automatically not authenticated to access p's information.
- ***deny***: A person a is denied access to a document d in

one of the following situations:

- a is authenticated to access p's information, d belongs to p, p has an opt out policy.
- d belongs to p, but a is not authenticated to access p's information.
- a has possible access to p, d belongs to p, p has an opt out policy with emergency override, and the situation is not an emergency.
- a is authenticated to access p's information, d belongs to p, p has an opt in policy except for sensitive information, and d is classified as sensitive.
- a is authenticated to access p's information, d belongs to p, p has an opt in policy with specific denials, and p has explicitly denied a access.

D. Tested Scenarios

Given the above facts, we designed twelve different scenarios to test our different access policies. Table I summarizes these scenarios and an their expected results. In this table, we use plain English to describe the query and facts instead of n3 notation for better illustration. These facts are based on Figure 1. We write the queries in the form of "some person $\rightarrow$ some document" which means that this person is trying to access this document, and we are trying to determine whether we should grant them access or not.

E. Limitations

Describes the current limitations of our system

VI. Discussion and Future Work

can split into two sections if there's a lot of things to discuss

VII. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank Dr. Helen Chen for ...

References

[1] E. Kluge, "Informed consent and the security of the electronic health record (EHR): some policy considerations," *International Journal of Medical Informatics*, vol. 73, no. 3, pp. 229–234, 2004.

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

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

[4] 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.

[5] C. Pruski, "e-crl: A rule-based language for expressing patient electronic consent," *eHealth, Telemedicine, and Social Medicine, International Conference on*, vol. 0, pp. 141–146, 2010.

Appendix A
Facts File

FACTS FILE WILL GO HERE

Appendix B
Rules File

RULES FILE WILL GO HERE

Query	Associated Facts	Expected Results
Dr Smith → XRay1	• Dr Smith is a member of Grand River • Grand River has a by shift policy • Dr Smith is on shift in Grand River • XRay1 belongs to John • John is treated in Grand River • Dr Smith treats John • John has an opt in policy	Dr Smith is granted access
Dr Smith → BloodTest	• Dr Smith is a member of St Mary's • St Mary's has a by shift policy • BloodTest belongs to Tim • Tim is treated in St Mary's • Dr Smith treats Tim • Tim has an opt in policy	Dr Smith is denied access because St Mary's has a by shift policy and he is not currently on shift
Dr Smith → CTScan3	• Dr Smith is a member of St Catherine's • St Catherine's has a members only policy • CTSCan3 belongs to Sally • Dr Smith treats Sally • Sally has an opt in policy	Dr Smith is granted access even though he is not on shift because St Catherin's does not have a by shift only policy
Dr Jane → BloodTest	• Dr Jane is a member of St Mary's • St Mary's has a members only policy • Dr Jane is on shift at St Mary's • BloodTest belongs to Tim • TIm is treated in St Mary's • Dr Smith treats Tim • Tim has an opt in policy	Dr Jane is denied access because she is not treating Tim
Dr Smith → CTScan1	• Dr Smith is a member of Grand River • Grand River has a by shift policy • Dr Smith is on shift in Grand River • CTScan1 belongs to Peter • Peter is treated in Grand River • Dr Smith treats Peter • Peter has an opt out policy	Dr Smith is denied access because Peter has an opt out policy
Dr Jane → XRay2	• Dr Jane is a member of St Mary's • St Mary's has a by shift policy • Dr Jane is on shift in St Mary's • XRay2 belongs to Wendy • Wendy is treated in St Mary's • Dr Jane treats Wendy • Wendy has an opt out with emergency override policy • Wendy is in an emergency situation	Dr Jane is granted access since Wendy is in an emergency
NurseAlex → XRay2	• Nurse Alex is a member of St Mary's • St Mary's has a by shift policy • Nurse Alex is on shift in St Mary's • XRay2 belongs to Wendy • Wendy is treated in St Mary's • Wendy has an opt out policy with emergency override • Wendy is in an emergency situation	Nurse Alex is granted access even though she is not treating Wendy because Wendy is in an emergency
Dr Jane → XRay3	• Dr Jane is a member of St Mary's • St Mary's has a by shift policy • Dr Jane is on shift in St Mary's • XRay3 belongs to Jenna • Dr Jane treats Jenna • Jenna has an opt out policy with emergency override	Dr Jane is denied access because Jenna has an opt out policy with emergency override, and Jenna is not in an emergency
Dr Smith → CTScan2	• Dr Smith is a member of Grand River • Grand River has a by shift policy • Dr Smith is on shift at Grand River • CTScan2 belongs to Tom • Tom is treated in Grand River • Dr Smith treats Tom • Tom has an opt in policy with the exception of sensitive documents	Dr Smith is granted access because CTScan2 is not classified as sensitive
Dr Smith → HIVRep1	• Dr Smith is a member of Grand River • Grand River has a by shift policy • Dr Smith is on shift at Grand River • HIVRep1 belongs to Tom • Tom is treated in Grand River • Dr Smith treats Tom • Tom has an opt in policy with the exception of sensitive documents • HIVRep1 is classified as sensitive	Dr Smith is denied access because Tom has denied access to sensitive documents, and HIVRep1 is classified as sensitive
Dr Smith → STD1	• Dr Smith is a member of Grand River • Grand River has a by shift policy • Dr Smith is on shift at Grand River • STD1 belongs to John • John is treated in Grand River • Dr Smith treats John • John has an opt in policy • STD1 is classified as sensitive	Dr Smith is granted access even though STD1 is sensitive because John has a full opt in policy
Dr Smith → MRI1	• Dr Smith is a member of St Catherine's • St Catherine's has a members only policy • MRI1 belongs to Jack • Jack is treated in St Catherine's • Jack has an opt in policy with specific denials to certain people • Jack has denied access to Dr Smith	Dr Smith is denied access since Jack has explicitly denied him in his policy

TABLE I
SUMMARY OF THE TESTED SCENARIOS