CONSENTIR

"A Policy Based Patient Consent & Access Management System"

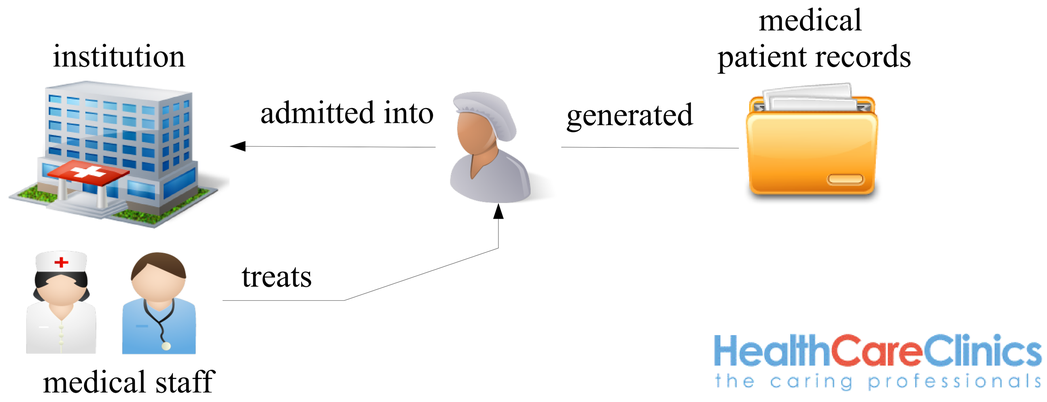
Atif Khan, Sarah Nadi, Ian McKillop, Helen Chen – University of Waterloo

Motivation

Security — How is the patient electronic medical record ***confidentiality*** & ***privacy enforced*** and ***protected*** ?

Access Control — **Who should be provided with:**
1. complete access
2. partial access
3. no access

Information Use — What about ***future & secondary use*** of the stored medical record ?



HealthCareClinics
the caring professionals

I understand that as part of my healthcare, the physicians of HealthCareClinics originates and maintains health records describing my health history, symptoms, examination and test results, diagnosis, treatment and **any plans for future care or treatment**. I understand that this information is utilized to plan my care and treatment, to bill for services provided to me, to communicate with other healthcare providers and other routine healthcare operations such as assessing quality and reviewing competence of healthcare professionals.

HealthCareClinics Notice of Privacy Practices provides specific information and complete description of how my personal information may be used and disclosed. I understand that a copy of the Notice of Privacy Practices is available at the front desk and understand that I have the right to review the notice prior to signing this consent. I understand that HealthCareClinics **reserves the right to change** the Notice of Privacy Practices. Prior to implementation of the revised Notice of Privacy Practices , the revised Notice will be mailed to me if I provide my address below. I understand I have the right to restrict the use and/or disclosure of my personal health information for treatment, payment, or healthcare operations and that HealthCareClinics is **not required to agree to the restrictions requested**. I may revoke this consent at any time in writing except to the extent that HealthCareClinics has already taken action in reliance on my prior consent. This consent is valid until revoked by me in writing.

We may **change our policies** and this notice **at any time** and have those **revised policies apply to all the protected health information** we maintain. If or when we change our notice, we will post the new notice in the office where it can be seen. You can request a paper copy of this notice, or any revised notice, at any time (even if you have allowed us to communicate with you electronically). For more information about this notice or our privacy practices and policies, please contact the person listed at the end of this document.

State of Affairs

Too Generic
- Single generic approach to cover multitude of complex scenarios
- Patient consent is violated more often than it is honoured
- System is not patient consent centric

Lacking
- Semantic understanding of patient consent
- Proof of correctness for the decisions made
- Flexibility to accommodate dynamic roles

Required Characteristics of Electronic Patient Consent

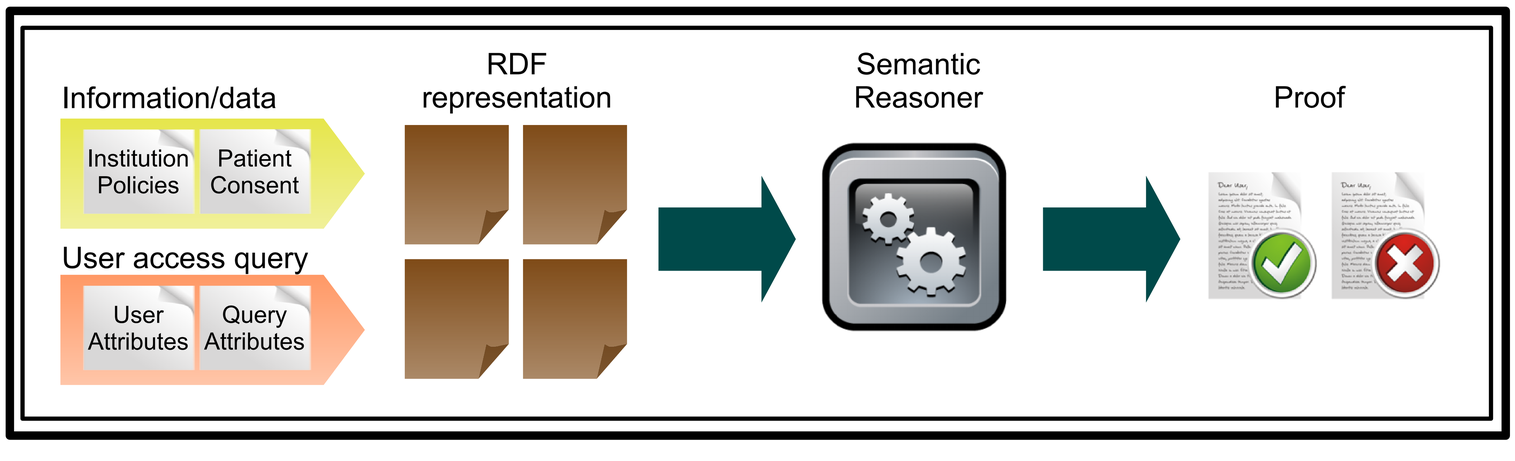
Patients need to be able to control & define:
- Who can access their information
  - generic inclusions to specific exclusions
- When their information can be accessed
  - Privacy & confidentiality a function of need
- What can be accessed
  - complete medical history OR partial medical records

Consentir

1. Attach meaning to information
- All information is represented in RDF (N3) notation
  - Provides meaning to data for machine processing
- Consent and policies are
  - Translated into logical rules
  - Represented by RDF (N3) logic

2. Access based on provable dynamic authorization
- A semantic reasoner to compute access request based on:
  - Patient consent
  - Multi-level policies
  - User attributes

3. Verifiable proof for each access decision
- Third party validation



Supported Policies

Hospital policies
- Members only
- By shift
- Must be treating doctor/nurse (except in emergencies)

Patient consent policies
- Opt in
- Opt in except for sensitive documents
- Opt in except for certain people
- Opt out
- Opt out with emergency override

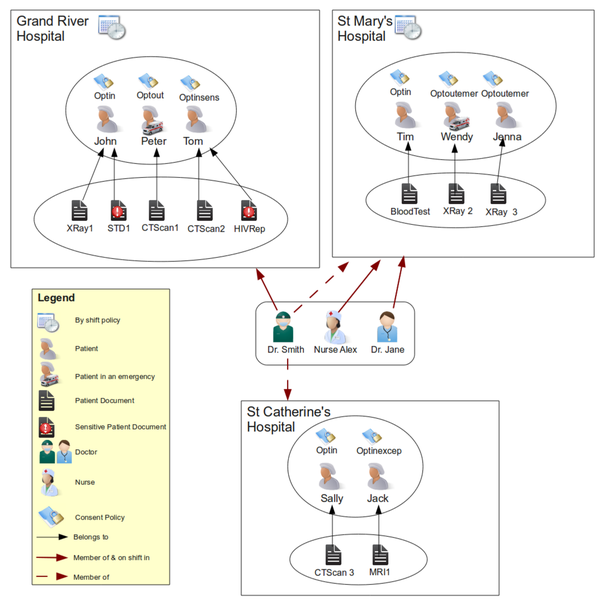
Example Rules

a **has possible access** to p's records
- a member of o & o has a by shift policy & o is on shift & p is treated in o

a **is authenticated to access** p's records
- a has possible access to p's records & a treats p

a **can access** d
- a is authenticated to access p's records & d belongs to p & p has an opt in policy

Setup



Scenarios