Consent-based Electronic Patient Information Exchange

Atif Khan, Ian McKillop and Helen Chen

WATERLOO
CHERITON SCHOOL OF COMPUTER SCIENCE

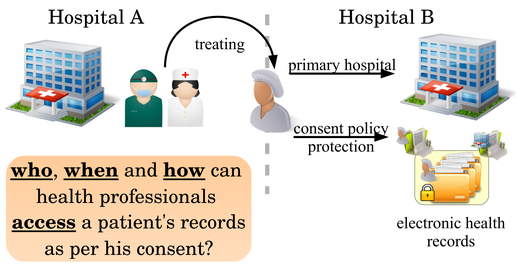
Motivation

Ontario Personal Health Information Protection Act (PHIPA) – 2004

- defines rules that "*health information custodians*" must follow when collecting, using and sharing personal health information

Consent is a complex problem

- representation, management, and enforcement (application & validation)
- institutional privacy & security policies provide additional complexity



who, **when** and **how** can health professionals **access** a patient's records as per his consent?

Our Vision

An information exchange framework

- supporting distributed heterogeneous *health information systems*
- focusing on consent
  along with other privacy & security policies
- creating electronic consent models (*representation*)
- providing access control decision making (*enforcement*)
- auditing for all system-made decisions (*validation*)

Proposed Solution

Semantic policy based access control framework

- explicitly incorporates patient consent
- recognizes multiple interacting policies (consent, institutional security & privacy etc.)

Semantic knowledge representation

- facilitates modelling patient consent and other policies
- information sharing across heterogeneous systems using ontology-based data representation
- allows for automated machine-based processing of policies

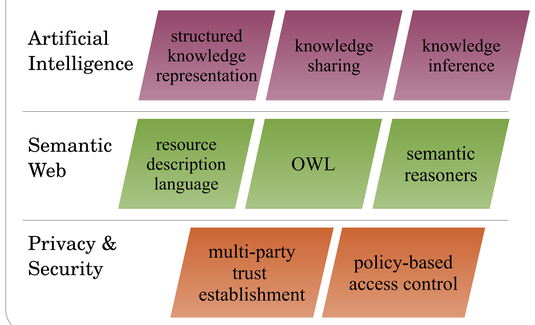
Semantic knowledge inference

- policies can be reasoned with
- inference of knowledge (explicit & implicit)

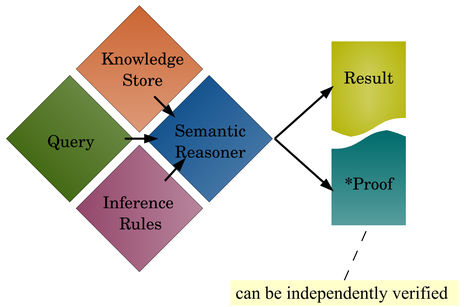
Multi-Agent systems (MAS)

- model healthcare entities as intelligent agents
- model healthcare institutions as MAS

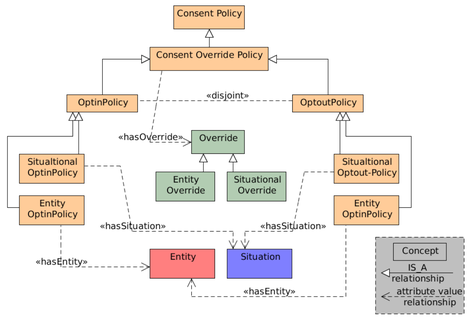
Building Blocks



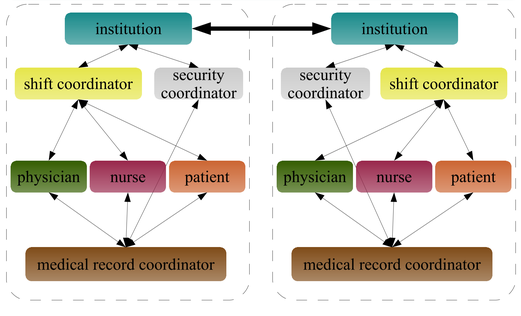
System Components



Semantic Consent Model



Institutional MAS Model



Example: *Semantic Access Control*

knowledge store

:John *a* :Patient; *:hasPolicy* :optin.
:HIV_MR *a* :MedicalRecord; *:belongsTo* :John.
:DrSmith *a* :Physician; *:isTreating* :John.

inference rule

{?P *:haspolicy* :optin.
?MR *:belongsTo* :?P.
?DOC *:isTreating* ?P} ⇒ {?DOC *:hasAccess* ?MR}.

query

_:WHO:hasAccess :HIV_MR.

Semantic Reasoner

proof

{{:John :hasPolicy :optin} *e:evidence* <knowledgebase#_2>.
{:HIV_MR :belongsTo :John} *e:evidence* <knowledgebase#_4>.
{:DrSmith :isTreating :John} *e:evidence* <knowledgebase#_6>} =>

result

{{:DrSmith :**hasAccess** :HIV_MR} *e:evidence* <rules#_1>}.}.

Semantic knowledge representation
all facts are stored in triple format,
therefore a knowledge store is a collection of triples.

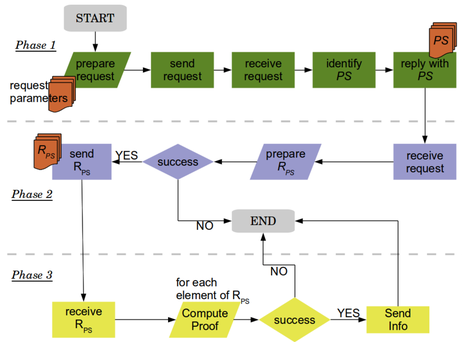
A doctor has access to a medical record
if the doctor is treating the patient
and if the medical record belongs to the patient
and the patient has an optin consent policy

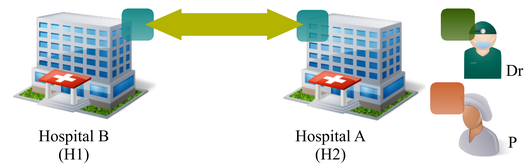
Characteristics of a Semantic Proof
- first order logical proof
- verified by traversing the knowledge graph and applying the inference rules
- provides confidence in the result
- provides auditing capabilities

Information Exchange Protocol

3 Phase protocol

- provides consent enforcement before any information is exchanged



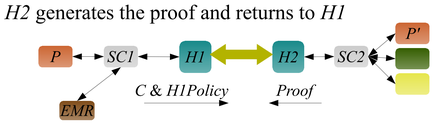


Request for information – Phase 1

- *Dr* request for *P's* medical record from *H1*
- *H2* (institutional agent) propagates the request to *H1*
- *H1* (institutional agent) receives and processes the request

Proof generation – Phase 2

- *H1* identifies protection set *(PS)*
  PS = {patient consent C, H1 privacy & security policies H1Policy}
- *H1* requests *H2* for provable validation of *PS*
  C & H1Policy
- *H2* generates the proof and returns to *H1*



Example scenario

Consent — Opt-out with emergency override

Required Proof:
•confirm that patient is indeed in an emergency situation

Hospital B Policy
- employee has access to patient records
- employee must be treating the patient
- employee must be on shift
- employee must be a physician

Required Proof:
•DR is an employee of the hospital
•DR is treating the patient
•DR is on shift
•DR is a physician

Hospital A Policy
- all hospital employees have access to patient records

Proof validation – Phase 3

- *H1* computes (verifies) the semantic proof
  locally or using a trusted third party proof checker
- Information is exchanged
  upon successful validation of proof (of consent & other policies)

CrySP MITACS AGFA HealthCare