A Collaborative Environment for Formalizing Privacy Policies in Health Care
Andras Nadas, Tihamer Levendovszky, Laszlo Juracz, Janos Sztipanovits, Mark E. Frisse, Ann J. Olsen

Privacy Policies, HIEs and ACOs

Privacy Policies:
- Federal (HIPAA, HITECH, Omnibus)
- State (Mental Health, Genetics, STD, HIV, etc.)
- Institutional (Notice of Privacy Practices, IRBs, etc.)
- Patient Preferences (Opt-out)
- Increased punishment for privacy violation
- Increased risk aversion of institutional policy makers

Health Information Exchanges (HIEs):
- Increased adoption of EHRs
- Pressure for more affordable care
- Move towards coordinated care
- Accountable Care Organizations (ACOs)
- More pressure for sharing health information
- Conflicts with risk aversion

Develop an engineering method that provides the right provisions to enable functioning HIEs of all size.

Policy Forge Architecture

Policy Forge Workflow

1. Recognize the common patterns used in the textual policy descriptions. These patterns will form the templates in PATRN.
2. Compile the object and actors of the policies and organize them into ontologies.
3. Formal policy models are composed from the templates and ontologies.
4. Using the semantic anchors, the formal policy models can be translated for analysis or enforcement.

Reasoning Framework using Formula

- A system for modeling with logic
- Generic; not specifically designed to model software.
- Specifications are written as “open-world” logic programs.
- FORMULA 2.0 can verify, synthesize, transform, compile and check models all with logic
- Z3 SMT Solver

Templates and Semantic Anchoring

- Patterns:
  - <structure> || <ontology> || <logic>
- Example: SUBJECT allowed to perform OPERATION on OBJECT given that CONSTRAINTS are met
- SUBJECT, OPERATION and OBJECT are derived by ontologies
- ACCESS CONDITIONS are defined with first order logic expressions
- RESTRICTIONS are defined with the other logic constructs.

Policy Formalization Problem

- Policies
  - Policy Formation is complex...
  - How to understand legal domain, context and language
  - How to understand formal domain, context and language...
  - But feasible for a small set of policies and experimentation 1,2

- Federal, State, Institutional Privacy Policies

- Federal Policies
- State Policies
- Inst. Policies

Policy Exchange/Artifact Sharing

- Templates
- Ontologies
- Policies and Sets
- Scenarios
- Taxonomic search

Sharing  Collaboration

Projects

Screenhots

- Ontologies represent the formal knowledge base.
- Documents from the library can be annotated by ontology terms.
- Words and expressions from the text can be used to create elements in an ontology.
- Ontologies can be imported from standards (HL7 and joint-il).

- Uses imported templates as the language.
- Multiple languages can coexist and can be combined if their representation and semantics enables it.
- We prefer graphical languages but textual languages will also be supported (as long as they are formal and meets environmental constraints.)

Use Cases are simple clinical workflows represented on a timeline.
- Concentrates on data flows between systems and accesses by users.
- The dataflow is check to conform to a selected set of policies.
- The policy set is also checked for internal consistency.

- Policy Text Tools
- Policy Modeling Tools
- Policy Modeling Tools
- Generator Tools

- HIS, HIE, ACO etc.

Highly Scalable Cloud Infrastructure

User Management

Collaboration Tools

Trust Management

Infrastructure Management

Vulcan Forge

1. Combines the object and actors of the policies and organize them into ontologies.
2. Compile the object and actors of the policies and organize them into ontologies.
3. Formal policy models are composed from the templates and ontologies.
4. Using the semantic anchors, the formal policy models can be translated for analysis or enforcement.

- Z3 SMT Solver
- Opens World Reasoning:
  - Facts and Rules
- Open World Queries:
  - PFO: Find a closure of the program by ground facts where a goal is satisfied. E.g. “Is document of accessible by x?”
  - PIF: Partially close P with facts F and remove “new” marking from all associated data types. E.g. Can x access any documents?
- Term Algebraic Data Types
- Formula adds data types to logic programming
- Data types are “algebraic”, i.e. they are functions that create data
- A data constructor always constructs the same value when provided the same arguments
- Two values are the same if and only if they were constructed by the same constructor with the same arguments.