Compliance-Aware Cross-Organization Medical Record Sharing

Requirements and Case Study

Healthcare services = joint work of many organizations

Data sharing is essential but...

It is **challenging** due to **security**, **privacy** and **business** requirements

**CHINO** Process Definition and Execution

**The CHINO framework elements:**

- **Two categories of data:**
  - Records: detailed and privacy sensitive information
  - Metadata: describes Records
- **Rules:**
  - Access Right Rules: defines access control over Metadata and Records
  - Privacy Filtering Rules: fine-grained data filtering mechanism for XML or HL7 data
- **Data Management Interfaces (DMI):**
  - pushRecord, getRecord, grantRights to manage Records and Metadata
- **Modeling Elements:**
  - BPMN 2.0 elements: supported by the Activiti engine.
  - Custom CHINO BPMN elements: to facilitate access to LLO and interaction with external organizations through DMI.
- **Low Level Operations (LLO):**
  - pushRecord, getRecord, grantRights to access to internal components

**The Process Modeling and Policy Definition Framework**

**The main modeler components are:**

- A: List of all processes
- B: The Modeling framework
- C: List of the Custom CHINO elements
- D: Configuration of the custom elements

**Validation**

- OpenMRS + CHINO integration
- Doctor-consultation module for OpenMRS
- Integrated with CHINO
- 2 sets of processes to demonstrate cross-regulation record sharing.

**User Study**

- Ongoing study with 2 Groups
  - Developers and Business Analysts to understand if it is feasible to model requirements with CHINO.
  - preliminary results are positive
- 2. Privacy Experts: to understand if CHINO process visibility can improve trust

**The CHINO Business Process and Policy Execution Framework**

**from requirements collection to process and policy execution**

1. **Identification of Business Requirements**
   - input: Descriptions of services
   - output: Interactions and Business req.

2. **Identification of Compliance Requirements**
   - input: Compliance requirements
   - output: Security req. and Privacy req.

3. **Definition of Compliance-Aware Data Management Scenarios**
   - input: High-level representation describing the interactions annotated with privacy, security and compliance req.
   - output: Executable compliance-aware business processes and rules.

4. **Definition of Executable Processes and Policies**
   - output: Compliance-aware medical record sharing

**Develop a system to easily share medical records while satisfying security, privacy and business requirements**

**our approach...**

Enable organizations to define their own data management processes and policies that manage their data and share them with others