



## The Process of Policy Authoring of Patient-controlled Privacy Preferences



*Thomas Trojer, Basel Katt, Ruth Breu,  
Thomas Schabetsberger, Richard Mair*  
e-Health 2011, Malaga, Spain, 22.11.2011

# Outline

- **Problem statement**
  - Privacy considerations for SEHR  
(Shared electronic health-records)
- **Policy authoring**
  - A usability-supporting perspective
  - Process activities
  - Use-case within IHE  
(Integrating the Healthcare Enterprises)
- **Research project**
  - Ongoing and future work

## Problem Statement | Privacy considerations for SEHR

- (Data) privacy is a personal concern and can therefore only be understood individually
  - This concern is present if data allows identification of an individual
  - The right on information self-determination comes by implication
  - E.g., Directive 95/46/EC of the EU defines control of data by identifyees
- In the context of Shared Electronic Health Records (SEHR)
  - Highly sensitive data regarding ones privacy, so why share at all?
  - Since sharing of (electronic) health data is important ...
    - ... from a economical perspective
    - ... from a viewpoint of effectiveness of medical treatment

## Problem Statement | Privacy considerations for SEHR

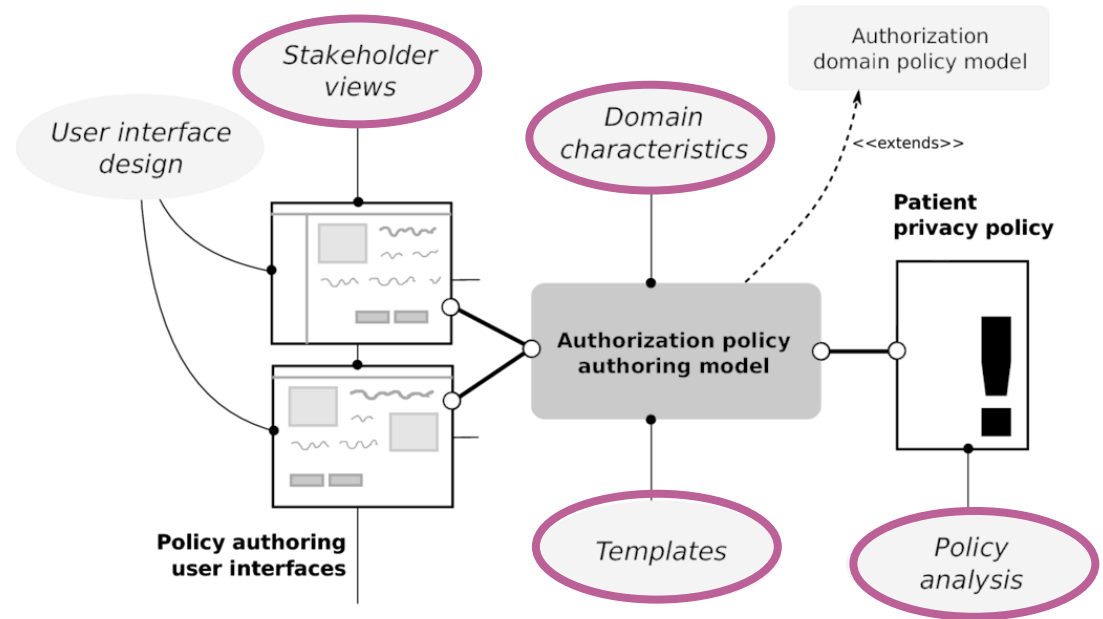
- What can typical privacy concerns look like?
  - Who has access to/accessed what documents of mine?
  - Why does someone have access to my health data, what is the purpose?
  - Does the system reflect the trust I have in certain medical practitioners?
  - Is it possible to hide data I don't want to be visible in my health record?

Solution: **Enable citizens/patients to express individual privacy concerns**

- What are the tools required to express privacy?
  - Access control is a way to enforce privacy
  - Authorization policies are therefore a way to declare privacy statements
  - Ordinary citizen/patient (i.e. user) is not a privacy/security expert
  - ... nor is she/he fully familiar with the health-care domain

# Policy Authoring | A usability-supporting perspective

- User-interface design
  - Not considered for now, but of course part of usability considerations
  - Usability in a broad sense, will be evaluated to guide the development
- Focus is on usability supporting factors, which are directly related to the authoring of privacy policies
  - Views for stakeholder roles
  - Authoring templates
  - Domain characteristics
  - Policy analysis



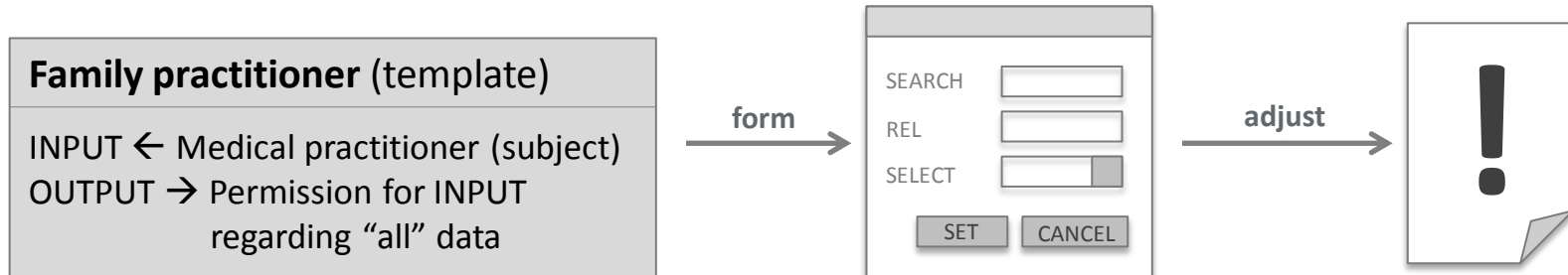
# Policy Authoring | A usability-supporting perspective

- Stakeholder views
  - Initial case study to be published at ACM IHI 2012
  - Different stakeholder views for
    - Medical practitioner without a patient attending, e.g., creating new health records or protecting these if critical
    - Medical practitioner participating in a medical treatment of the patient, e.g., creating medical referrals, accessing medical data for viewing
    - Patient managing her/his health record, e.g., as part of home self-care or data protection
  - From stakeholder views to authoring templates, by analyzing privacy-related issues ...

# Policy Authoring | A usability-supporting perspective

- (Authoring) Templates

- Templates are pre-defined forms to process a subset of the authorization domain policy model
- Templates entitle and define a user action, which leads to adjustments of the corresponding privacy policy
- Examples of templates are forms to define
  - Referrals, family practitioner, self-protection, ...



# Policy Authoring | A usability-supporting perspective

- **Domain characteristics**

- Mostly integration aspects of policy authoring tools are related to the retrieval of domain data
- The challenge is the connection of sources of domain data
- Decision to do integration based on IHE proposals as,
  - The Austrian eHealth initiative (ELGA) suggests implementation of IHE profiles
  - Our partner ITH-icoserve for healthcare technology is a certified implementer
- The following relevant domain-related entities were identified:
  - Patient, i.e. UIDs, corresponding health records, related practitioners, ...
  - Medical data, i.e. record IDs, record types, related stakeholders, ...
  - Health-care provider, i.e. working roles, UIDs, ...
  - Health-care work processes, i.e. record type – role mapping, purpose, relationships, needs-to-know aspects, ...

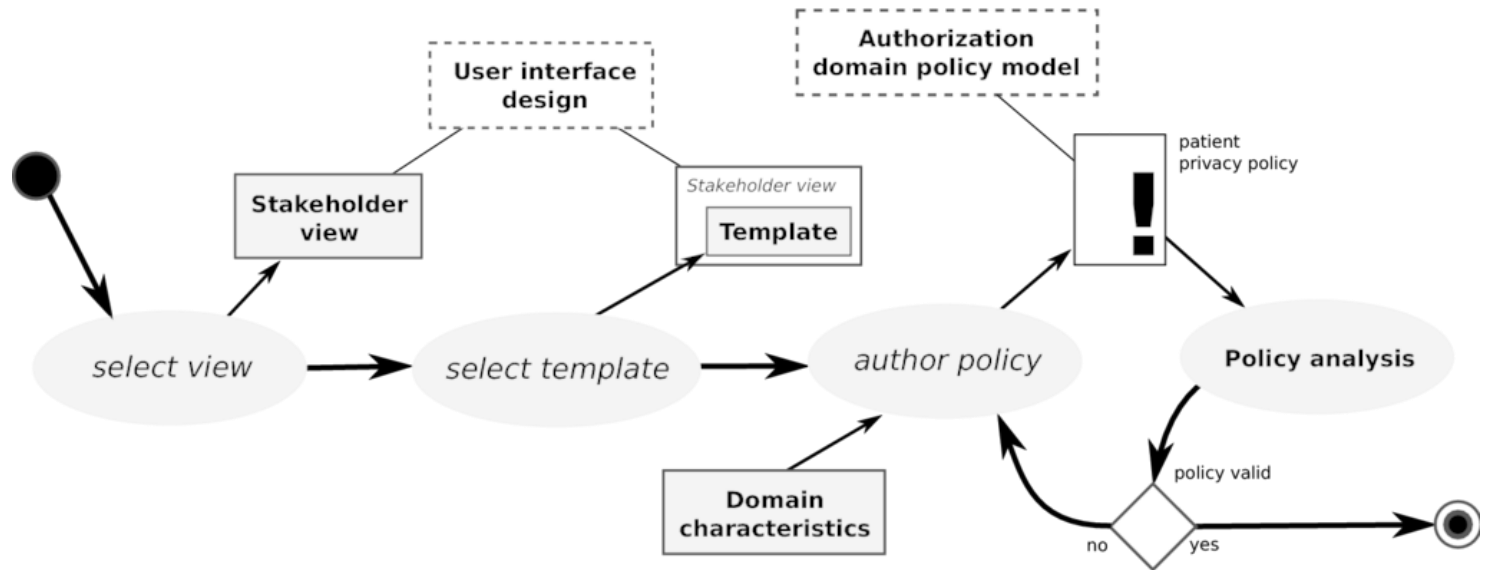
# Policy Authoring | A usability-supporting perspective

- **Domain characteristics**
  - The following IHE-defined profiles to be implemented were identified:
    - **XDS** (Cross-enterprise document sharing)
      - XDS patient identity source to get local patient information
      - XDS document registry and repository to get (meta-)data of health records
      - Part of medical data and health-care work processes domain-related data
    - **PIX** (Patient identifier cross-referencing) and **PDQ** (Patient data query)
      - Unified (i.e. national) patient identifier
      - Part of patient domain-related data
    - **HPD** (Healthcare provider directory) and **PWP** (Personnel white pages)
      - Provider meta-data, e.g. working roles and credentials
      - Part of health-care provider domain-related data

# Policy Authoring | A usability-supporting perspective

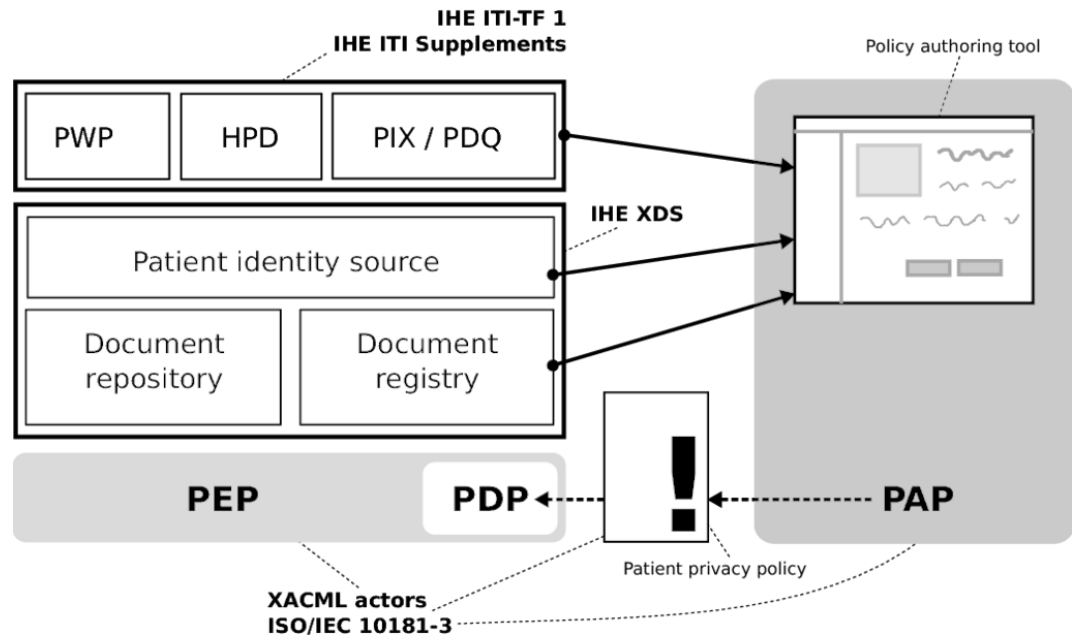
- **Policy analysis**
  - Recurring task activated when policy adjustments are performed
  - Conflict or redundancy detection between policies
    - E.g. modality conflicts render policy decision outcomes undecidable
    - E.g. dominated policies can be removed to simplify the overall management
  - Constraint checks
    - Especially domain-aware constraint checks, e.g., privacy warning if no personal relationship (via a medical record or a treatment) can be detected between a patient and a medical practitioner
    - In a case study we considered privacy as a concept related to personal relationships and needs-to-know aspects between patient, practitioner and medical data
  - Helps to **understand** implications of a policy and to **resolve conflicts** as valuable feedback can be provided to the patient policy author

# Policy Authoring | Process activities



1. **Selection of a view** according to the stakeholder role to make ...
2. ... **authoring templates** accessible for being chosen.
3. **Authoring** of a privacy policy involves domain characteristics and leads to ...
4. ... a (preliminary) patient privacy policy which is **analyzed** regarding potential conflicts or privacy risks
5. The deployment of the policy ends the process

# Policy Authoring | Use-case within IHE



- Policy authoring by integrating IHE-based data sources
- Policy maintenance and enforcement via XACML infrastructure (eXensible Access Control Markup Language, based on ISO/IEC 10181-3 actors)
- IHE IT-Infrastructure elements provided by our industry partner

## Our Research Project | What are we doing and has been done?

- Case study regarding stakeholder templates
  - Interviews have to follow to cover more templates, if necessary
- Development of an authoring tool prototype
  - Implements some templates for the patient-stakeholder view
  - Domain-aware policy analysis is performed
  - Generates and deploys XACML policies if settings are valid
- Successfully integration of the prototype into IHE XDS
  - Service-based document registry and repository is used
  - Patient-identifiers are retrieved



**That's it ... Thanks for listening ...**

Questions and comments are much appreciated!

Also, if you're interested in anything,  
please don't hesitate to contact me via

*[thomas.trojer@uibk.ac.at](mailto:thomas.trojer@uibk.ac.at)*