Policy and Technical Approaches to Health IT Privacy & Security

Mark Frisse, MD, MSc, MBA
Vanderbilt University

This presentation was made possible by Grant Number HHS 90TR0003/01. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS.
Our panel seeks answers to three questions

• What are the most effective technical and policy tools available for promoting privacy of health information?
• What are the tradeoffs between technical and policy approaches to addressing information privacy in health care?
• How can we maximize the effectiveness of both types of tools?
We are trying something a bit different

To what extent can we model policies in formal ways?
To what extent can we integrate institutional policies with other policies and integrate these into enforceable work flows?
To what extent can such efforts simplify work and reduce unauthorized disclosure?
What is the impact on personnel and on future policy development?
Our goal is to model critical access policies.
Our goal is to model critical access policies

- Health System Requirements
- Health System Information Ontology
- Policy Enforcement Point Design
- Policy Enforcement Point Implementation
- Private Laws and Policies
- Policy Ontology Specification
- Policy Policy Models
- Verified Privacy Policy Logic Code

Specific
Our current work

Build out the state policies (NYU, Dartmouth)
Focus on institutional policies (VU)
Generating code (Drools declarative language)
Apply through generalized use cases
Test the modeling environment
Develop initial list of relationships, ontologies, institutional systems specifications
Focus on the common issues that personnel face – allowing them more time to work on the exceptions
Build a public Web-based environment
Process of authoring

Law
- Federal Privacy Laws (HIPAA, Hitech)
- State level Privacy Laws (PHI disclosures: HIV, substance abuse, mental health, etc.)

Abstracts
- Extract Ontologies from Laws (Persons, Entities, Objects and their relations)
- Extract common patterns in the Laws

Models
- Create Template Models that follow the extracted patterns
- Model the Ontologies
- Combine the Templates and Ontologies to create the Privacy Policy Models

Logic
- Analyze the models using model checking methods for conflicts and entailment
Health Information Exchange (HIE) Policy Workflow

Authoring

- Federal, State, Institutional Privacy Policies
- Policy Authoring / Information Flow Modeling
  - Patterns
  - Semantics
  - System/Actor Models
  - Ontologies
  - Logic or Programming Language
  - Use Cases

Enforcement

- HIE System
- Request Processor/Server
- Enforce. point

- Executable Policy Code
- Use Case Simulation Code

- HIE System Simulator
- Use Case Enactment (Policy Unit Testing)
Visits define steps of the Use case.
- Each steps create new documents that are stored in the specified system.

Requests are evaluated to check whether they violate any policy.
My hypotheses: We might be operating under flawed assumptions

We emphasize state policies (it’s what we have)
We institutional policies; it is difficult and diffuse
We assume minimal granularity (e.g., global “opt out”)
We underestimate the critical role of terms, ontologies, and the need to harmonize these (e.g., roles)
Policy-making meetings operate under the temporary delusion that all policies can be enforced.
We think in terms of organizations (HIE as noun) and less so in terms of actions (HIE as verb).