Patient-Centric Secure-and-Privacy-Preserving Service-Oriented Architecture for Health Information Integration and Exchange

Mahmoud Awad and Larry Kerschberg

Center for Health Information Technology
George Mason University
http://hit.gmu.edu/

Presentation Outline

- Research Motivation
- Research Objectives and Key features
- Architecture
- Discussion
- Conclusion
- Future Work

Research Motivation

Electronic Health Records (EHR) Concerns

1. Privacy
   - HIPAA privacy provisions apply to healthcare providers such as hospitals, physicians and laboratories
   - Companies that aggregate these health records in electronic format such as Google Health, Microsoft HealthVault and Indivo are ***not*** HIPAA-covered entities
   - Online privacy policies established by the companies versus enforceable federal laws

2. Security
   - EHRs aggregated online

3. Ownership
   - Online EHR systems are fully owned by Google, Microsoft, etc. The patient and the individual healthcare providers own portions of the medical records

4. Lack of Standards (Lack of interoperability)
   - Paper-based medical record systems or electronic systems in proprietary format that are hard to integrate

Research Objectives and Key features

- Develop a secure and privacy-preserving Service Oriented Architecture (SOA) for health information integration and exchange
- Health information exchanges have to be approved by the patient
- Avoids centralized online storage of EHRs
- Complete EHRs can be aggregated on-demand using web service requests
- EHR exchanges require:
  - One-time use secure tokens for authentication,
  - Privacy policies to control data elements exchanged,
  - Security policies: role-based and fine-grained security policies
- Use EHR standards for interoperability (Health Level 7 (HL7))

Architecture

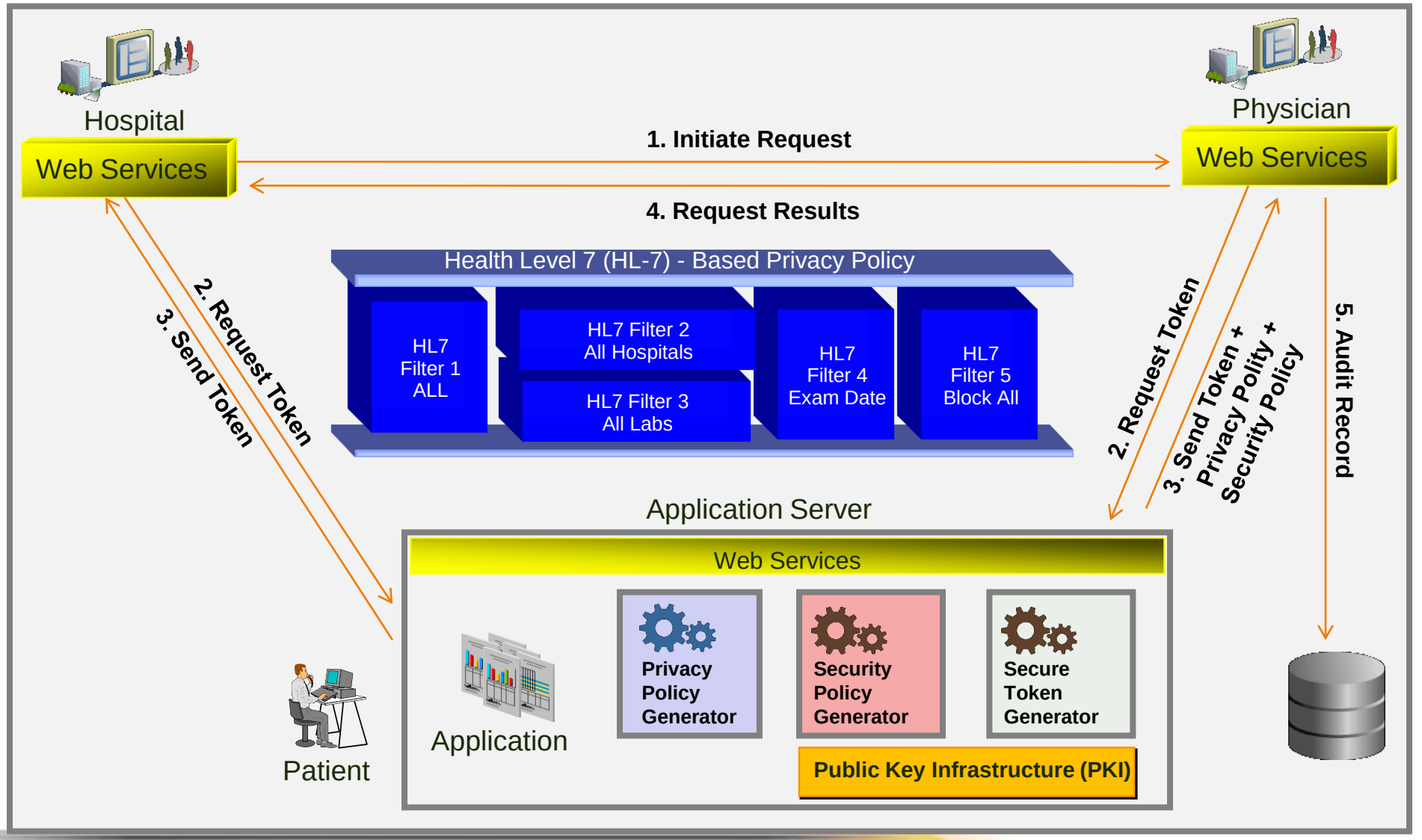
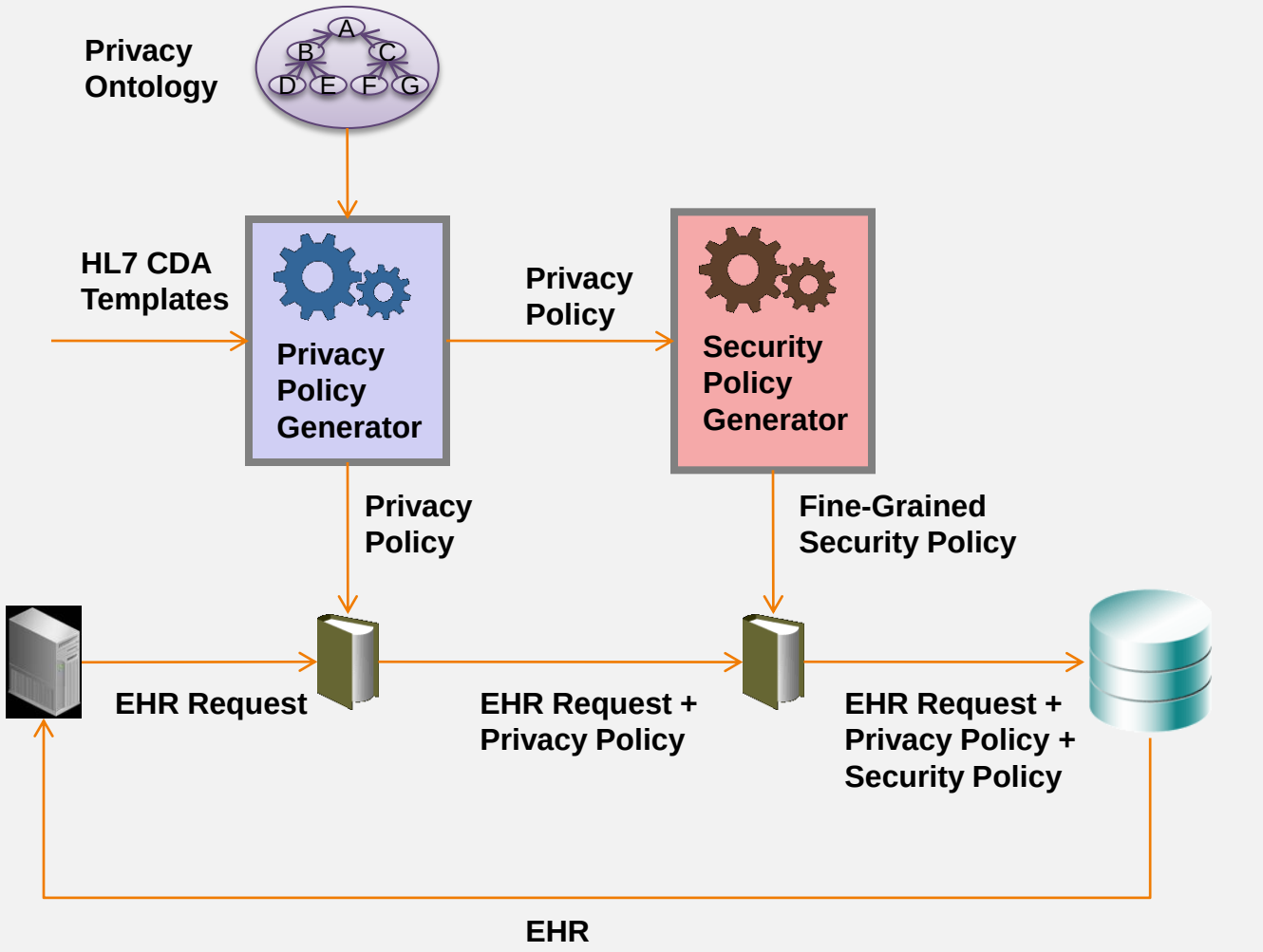


Figure 1: Architecture

Architecture - Continued



Privacy policies affect data structure (which XML elements to include in the EHR)
Security policies affect records retrieved

Figure 2: Privacy and Security Policy Generators

Architecture - Continued

- **Database;** contains fine-grained historical audit trail of all data exchange requests among healthcare providers, which includes additions, modifications and deletions of health record structure or data

- The patient's medical history can be reconstructed using this audit trail but only the patient has privileges to initiate such request

Architecture - Continued

- **Privacy Policy Generator** (PPG) generates privacy policies by defining which data structure elements are allowed to be exchanged between healthcare entities
- The policy itself is represented using HL7 CDA (Clinical Document Architecture) syntax and acts as a filter between a web service and its data store
- Privacy policies can be generated manually or via templates such as Continuity of Care Record (CCR) which is an HL7 constraint

Architecture - Continued

- **Security Policy Generator** (SPG) generates security policies that restrict records retrieved by a database in response to an EHR query
- These security policies enforce fine-grained access

Architecture - Continued

- The architecture offers a clear separation between privacy policies and security policies in order to provide better flexibility in producing and applying the filters and predicates produced by the PPG and SPG respectively
- Privacy filters are applied first to restrict data elements in an XML response (or columns in case of relational tables), then security policies are applied to limit the data element values
- Implementation details depend on the architecture of the medical record system implemented internally at the healthcare providers or health insurance companies
- Systems that use relational database can use fine-grained access control to implement security policies and systems that use XML databases can use XML schemas to validate the XML document produced

Architecture - Continued

- **Secure Token Generator (STG);** Requests for EHR exchange are initiated but not executed until secure tokens are generated by the STG. The tokens are generated using PKI and use a random number to ensure they are used only once

- **Privacy Ontology**; Helps the PPG determine relationships among healthcare providers and between EHR data elements and provides a mapping between the healthcare providers and EHR data elements. Default privacy policy templates are generated using this privacy ontology

Architecture - Continued

- **Privacy Ontology**; (continued) An example of relationships between healthcare providers is all the hospitals and medical practices that use Quest Diagnostics as their diagnostic laboratory testing facility
- This knowledge simplifies the process of generating security policies that would allow lab results to be exchanged between these medical facilities and Quest Diagnostics
- Also, knowing that the patient's primary family physician is a registered practitioner at particular hospital helps establish the level of trust in data exchanges between the physician and various offices within the hospital

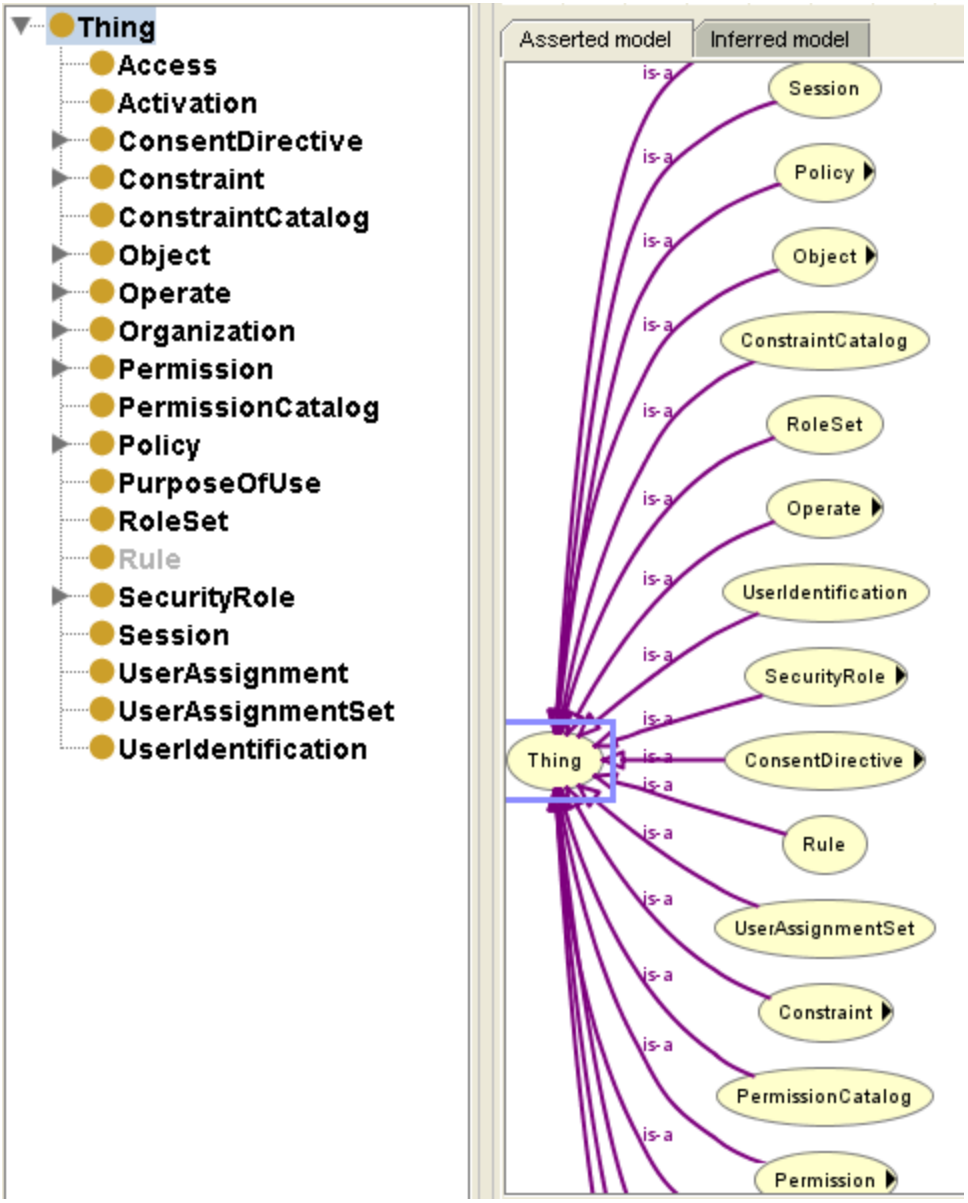


Figure 3: HL7 Privacy and Security Ontology

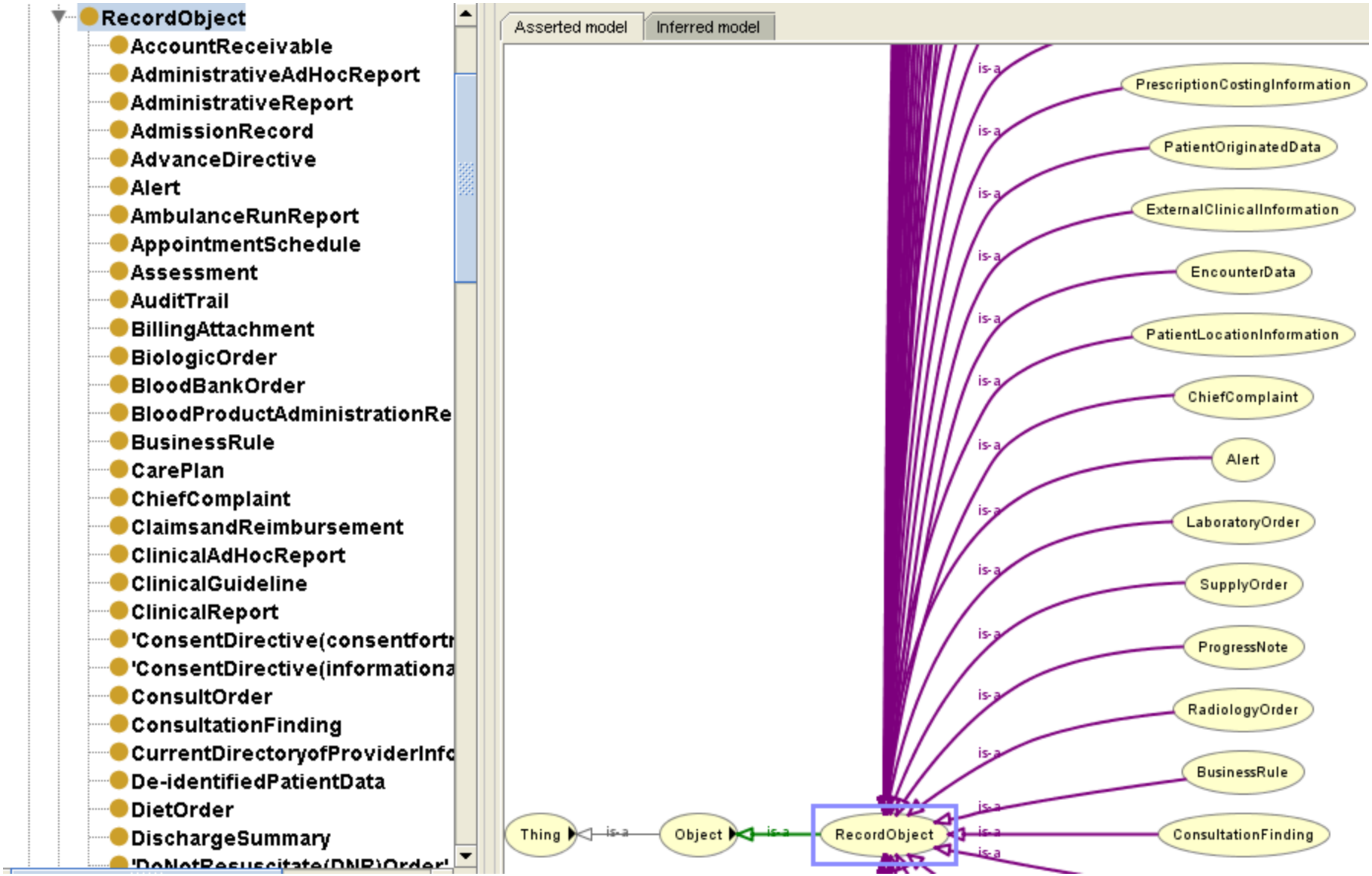


Figure 4: HL7 Privacy and Security Ontology

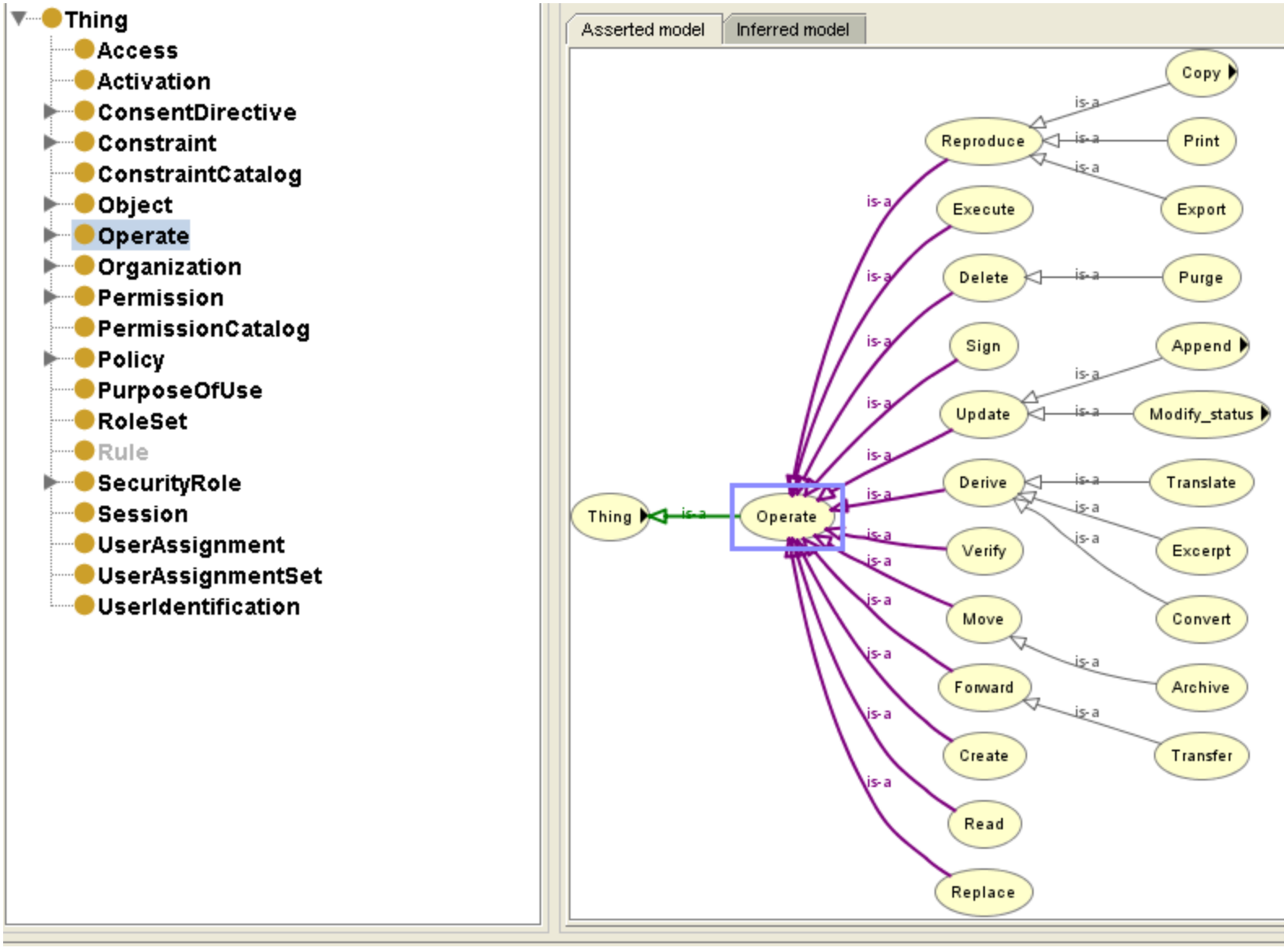


Figure 4: HL7 Privacy and Security Ontology

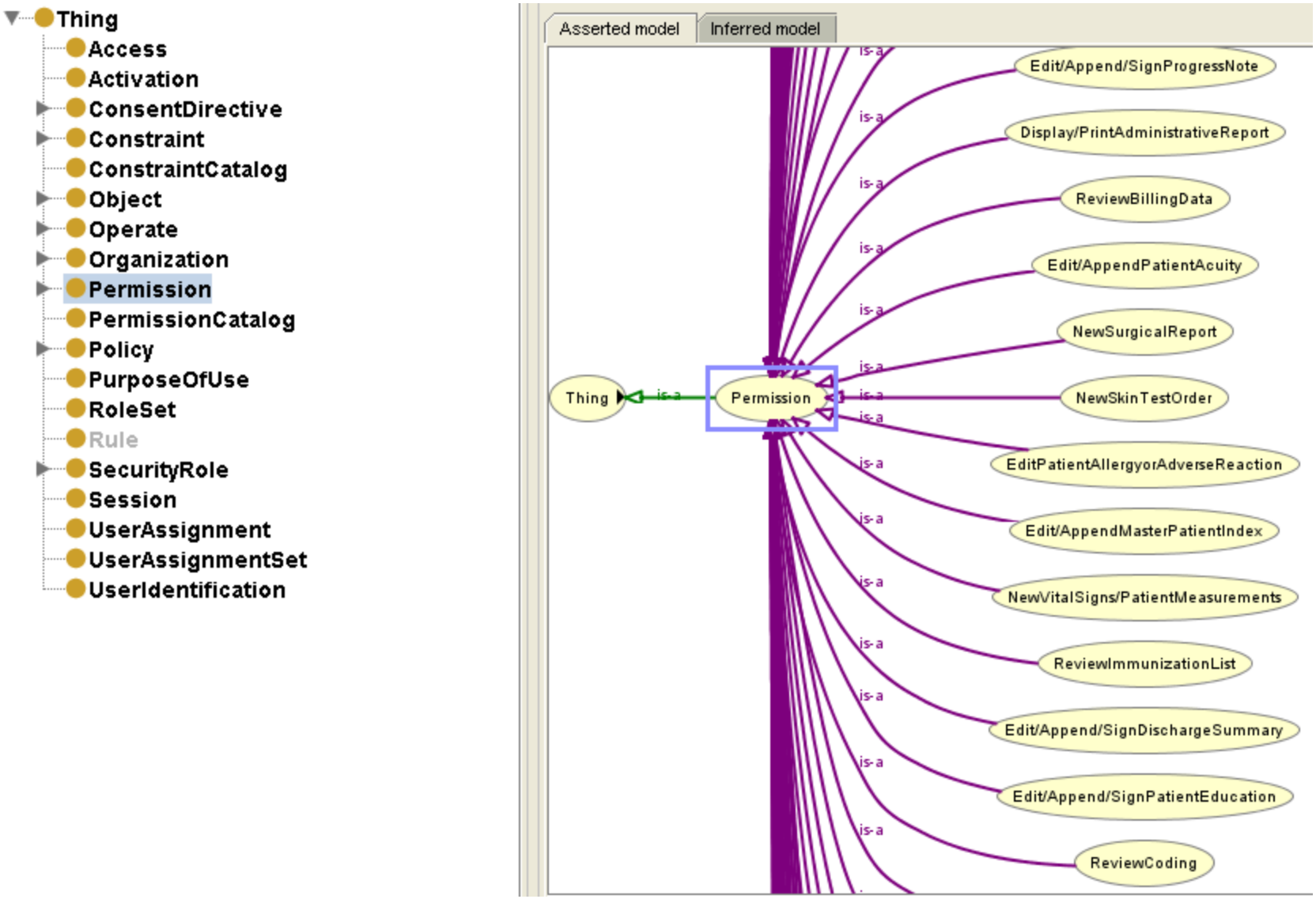


Figure 4: HL7 Privacy and Security Ontology

Architecture - Continued

Applications are used to:

1. Monitor data exchange requests and audit logs;

2. Produce privacy policies and security policies;

3. Query an individual component of the EHR or produce a complete EHR by issuing EHR integration web service requests to all the registered healthcare providers; and

4. Review and correct individual components of the EHR by issuing correction requests to the systems holding the affected record

Discussion

- Any comprehensive solution for EHR integration and exchange has to be technologically feasible but also politically acceptable
- Healthcare providers will always claim ownership of all medical records in their possession, and as long they are HIPAA-compliant, we have to assume that they developed adequate internal security and privacy policies to protect these medical records
- Our proposed solution only requires a web services layer around existing systems while giving patients an active role in the EHR exchange instead of the current practice of providing their healthcare providers with a blank authorization to exchange their EHR with anybody

Discussion - Continued

- Also, fully centralized EHR integration solutions are prone to privacy and security lapses and disruptive hacker attacks such as Denial Of Service (DOS)
- Fully distributed solutions, on the other hand, are prone to data loss if they do not offer proper data redundancy and backup strategies (which is also a concern when the patients decide to purge their medical records)
- Our proposed solution maintains the existing distributed network of systems represented by the healthcare providers but offers a secure method for data integration on demand

Conclusion

- In this paper, we propose a secure and privacy-preserving SOA for health information integration and exchange in which patients are “part owners” of their medical records, have complete ownership of their integrated health information and decide when and how data is modified or exchanged between healthcare providers or insurance companies
- This architecture is different from integrated Electronic Health Record (EHR) such as Google Health and Microsoft HealtVault in that electronic health records are not stored in online databases but instead are aggregated on demand using web service requests
- Web service providers working on behalf of the patients do not keep copies of the complete EHR but instead provide a pass-through service, and would require PKI-based security certificates to initiate health information exchange

Future Work

- Develop adaptors that allow patient-initiated changes to be applied to healthcare provider systems
- Develop generic reusable privacy policy templates using standards such as Continuity of Care Record (CCR) [which acts as an HL7 constaint/filter]
- Expand privacy ontologies to include medical conditions and drug interactions to complement the initial ontology that simply links healtcare providers and EHR data elements

QUESTIONS

QUESTIONS