Unlocking the Power
of Health Information

HEALTH LEVEL SEVEN

HL7(tm) (c) 2009 Health Level Seven(tm), Inc. All Rights Reserved.
HL7 and Health Level Seven are registered trademarks of Health Level Seven, Inc. Reg. U.S. Pat & TM

Healthcare IT Security: Domain Analysis Model Version 1 Release 1

Security
Work Group

Custodian Work Group:
http://www.hl7.org/workgroups/security
Custodian Work Group eMail: security@lists.hl7.org
Co-chairs: Mike Davis, Bernd Bloebel, Glen Marshall
Modeling Facilitator: Serafina Versaggi, Ioana Singureanu

November 23, 2009

Document URL:

Table of Contents:

Introduction

This model contains the analysis of security system policies required to support the needs of healthcare organizations. The model is intended to support the reuse of security standards in order to enforce access control policies required by jurisdictional and organizational privacy policies as well as individual clients consent directives. It focuses on the information required to support the authorization and access control use cases detailed in Appendix A of this document.

The requirements are based on the need for future systems to provide electronic interoperability standards to exchange individually identifiable health information and enforce privacy policies and consent directive using a variety of robust security infrastructure components.

The emergence of Electronic Health Record Systems and the wide use of electronic and/or personal health records requires that medical information be protected from abuse and unauthorized disclosure. Currently national and state/province legislation, regulations, and/or privacy policies are already in place to protect individuals from the misuse of their identifiable health information. In addition to privacy, healthcare organizations must meet a variety of access control policies to ensure the proper use of their computer systems. Therefore this domain analysis is intended to identify the information and system behaviors required to optimize the use of security standards and technology in healthcare. It includes ISO/TS 22600 Privilege Management and Access Control (PMAC), ASTM E1986 - 98(2005) Standard Guide for Information Access Privileges to Health Information, ANSI/INCITS 359-2004 Information Technology - Role Based Access Control, OASIS SAML and XACML Profiles, and HL7 RBAC Engineering concepts.

Domain Analysis Model

A Domain Analysis Model (DAM) is an abstract representation of a subject area of interest to provide a generic representation of a class of system or capability and suggest a set of approaches to implementation. In HL7 a DAM is complete enough to enable the development of downstream platform-independent models: HL7 RIM-based information and services models. A DAM may also be used to constrain other standards for use in healthcare (e.g. to constraint access control markup standards). The process used to create a DAM is documented in the HL7 Development Framework.

Therefore, the analysis model described here is the result of analyzing stakeholder requirements regarding enforcing access control policies regarding the privacy of health records (e.g. organizational policies, consent directives) in a digital world. The requirements are based on the need for next generation systems to provide electronic interoperability standards to automatically enforce access control and authorization policies specific to health IT and healthcare interoperability. Based on the stakeholders use cases, the analysis has revealed the conceptual information structures and system interactions required to support the access control needs of healthcare organizations.

The applicability of this DAM is limited to the requirements identified in Appendix A – Security Use Cases.

Document Changes

Initial Version, Release 1, Version 1, Informative

Authors

Co-chairs:
Bernd Bloebel, HL7 Germany, bernd.blobel@klinik.uni-regensburg.de
Mike Davis, U.S. Department of Veterans Affairs, mike.davis@va.gov
Glen Marshall, Grok-A-Lot, LLC, glen@grok-a-lot.com

Contributors:
Kathleen Connor, Microsoft Corporation, kathleen.connor@microsoft.com
Richard Thoreson, SAMHSA, Richard.Thoreson@samhsa.hhs.gov
Steve Connolly, Apelon, sconnolly@apelon.com

Modeling Facilitator, Contributor:
Ioana Singureanu, Eversolve LLC, ioana@eversolve.com

Publishing Facilitator:
Serafina Versaggi, Eversolve, LLC, serafina@eversolve.com

Glossary of Terms

See Security Glossary HL7 2008(c), Version 3

Electronic Health Record (EHR)

An electronic record (not a computer system) of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization.
Source: National Alliance for Health Information Technology (NAHIT)

Individually Identifiable Health Information (IIHI)

For the purposes of this document, IIHI refers to health data that is transmitted by or maintained in electronic media or any other form or medium that can be uniquely associated with an individual. The use of this term is without respect to any jurisdiction. For example, this type of personal health information is specified in Standards for Privacy of Individually Identifiable Health Information - 45 CFR Parts 160 and 164.

1. Security Policy structure used to represent Privacy Policies

The following section describes the classes and associations required to evaluate electronic privacy policies and consumer consent directives.

The following diagram describes the elements of a security policy from a jurisdiction or organizational standpoint. These policies apply to electronic records rather than paper-based system. They are intended to exchange privacy policy information in a platform-independent, semantically interoperable, and standard-based way.

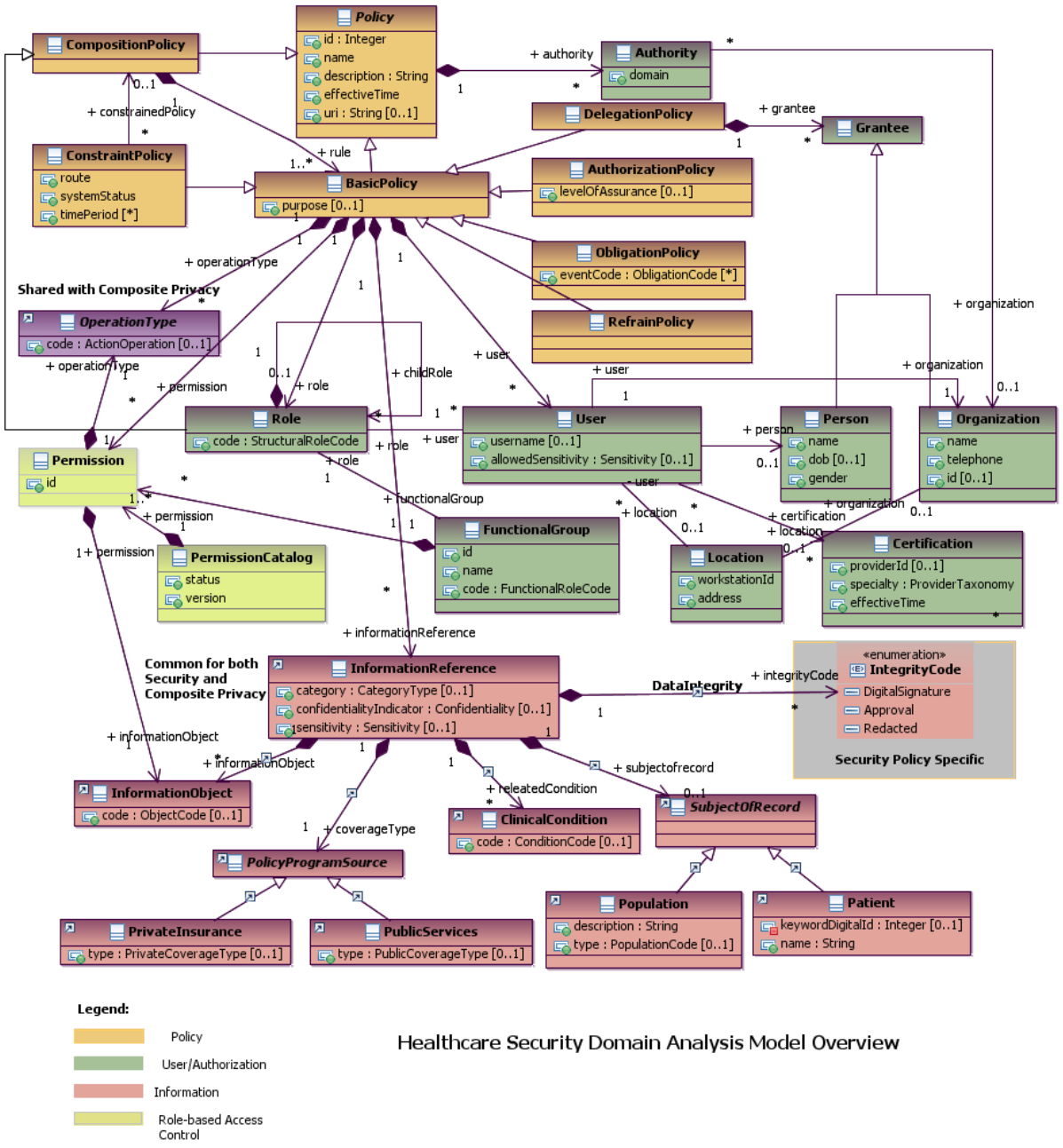

Figure 1: Security Policy Overview Diagram

The following diagram describes the information required to specify authorize healthcare users. The classes described here represent the subset of the overall information model that is required to support the use case.

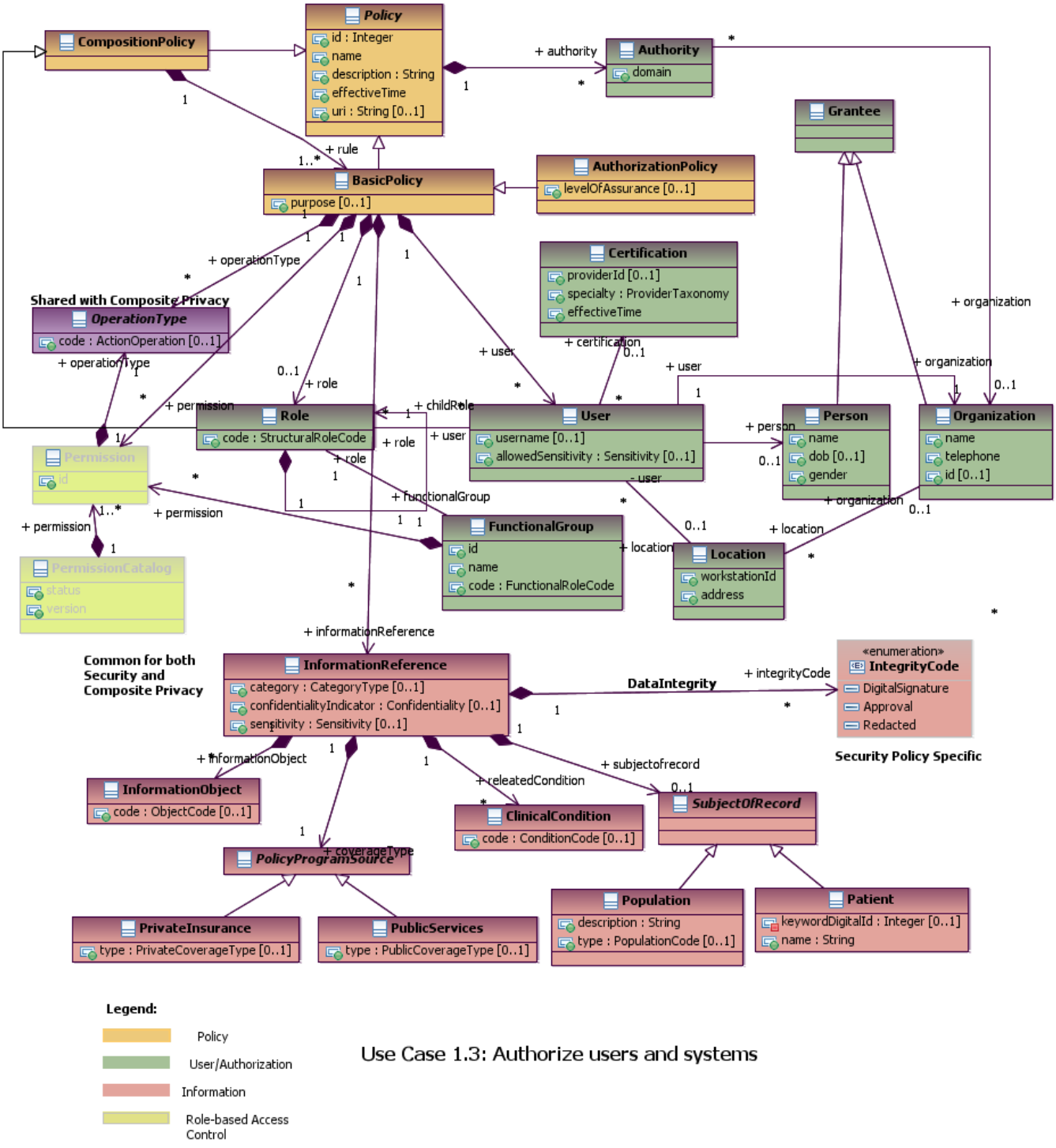

Figure 2: Use Case 1.3 - Authorize users and systems

The following diagram summarizes the classes and associations required to represent the policies involved in supporting the evaluation of privacy policies and consent directive.

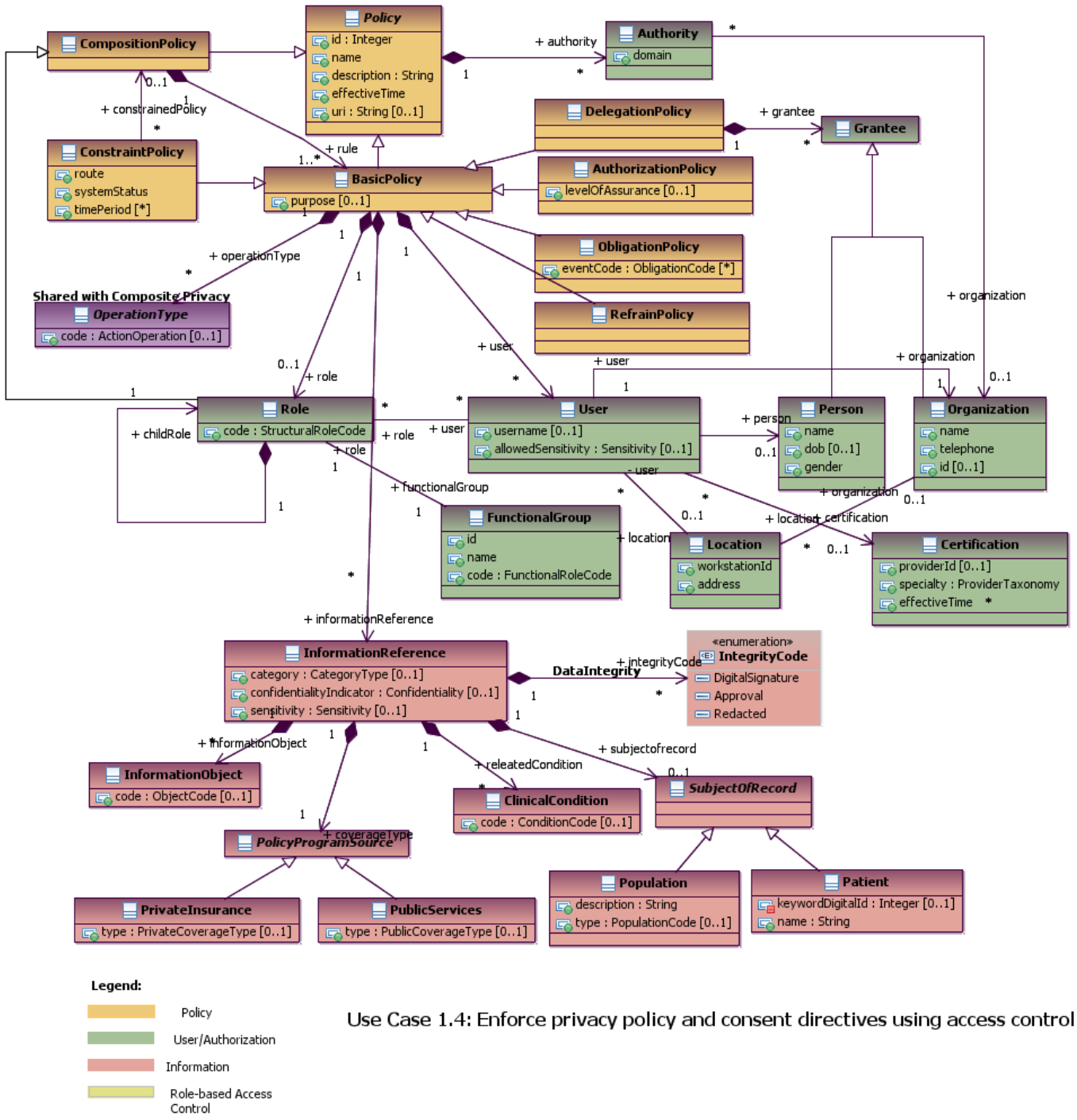

Figure 3: Use Case 1.4 - Enforce privacy policy and consent directives using access control

The following diagram contains the classes required to support the information exchanged during the process of resolving policies applicable to a specific request. Note that the classes required to support the permission catalog interoperability are not relevant for this use case.

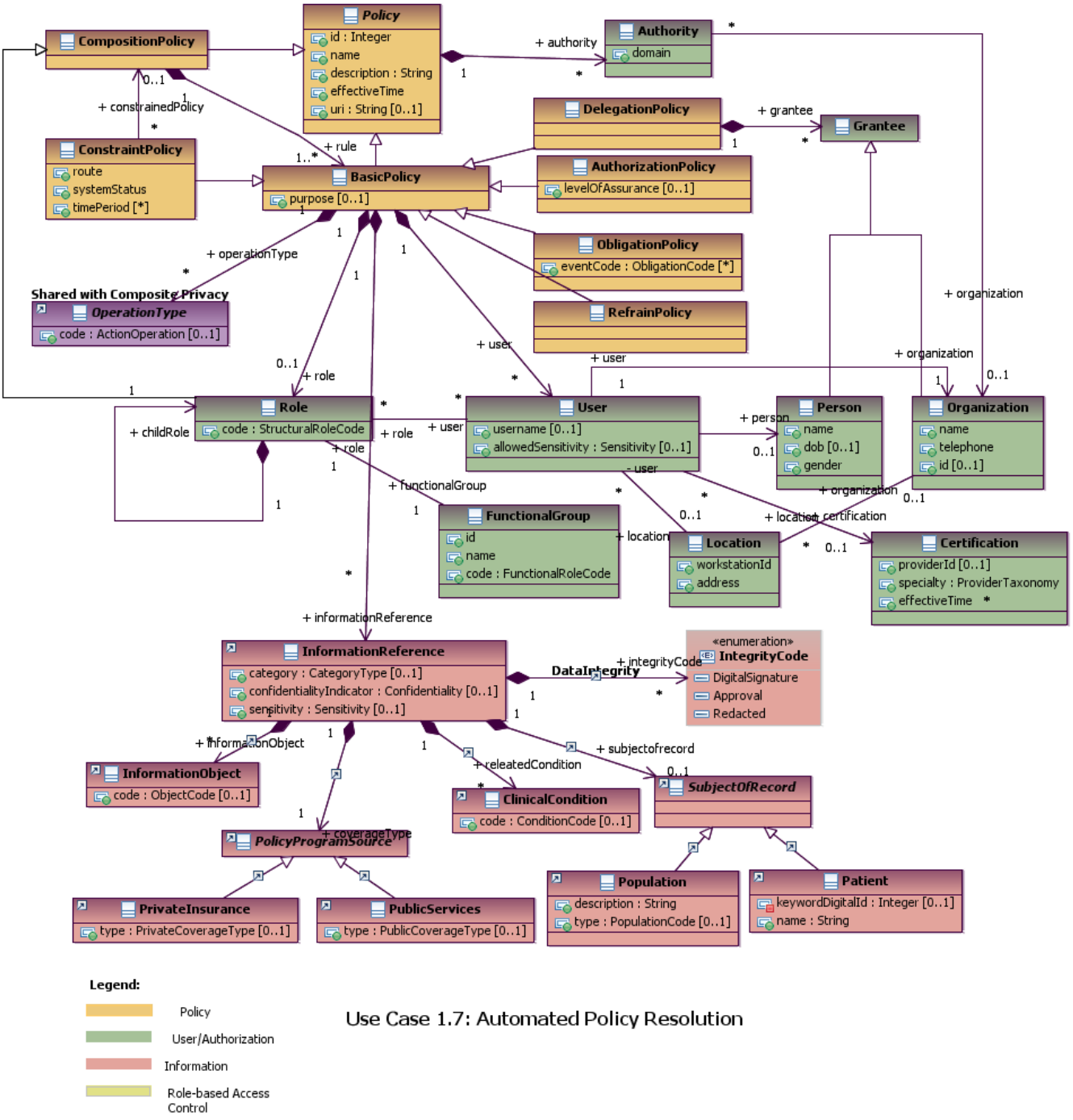

Figure 4: Use Case 1.7 - Automated Policy Resolution

The following diagram describes the classes required to specify the policies and consent directives negotiated by a patient with a healthcare organization where they wish to receive healthcare services. This use case requires the same information structure but applies to a different purpose: to describe the policies including a patient consent directive. A consent directive may consist of a ConstraintPolicy instance including instances of a Refrain and Obligation policies.

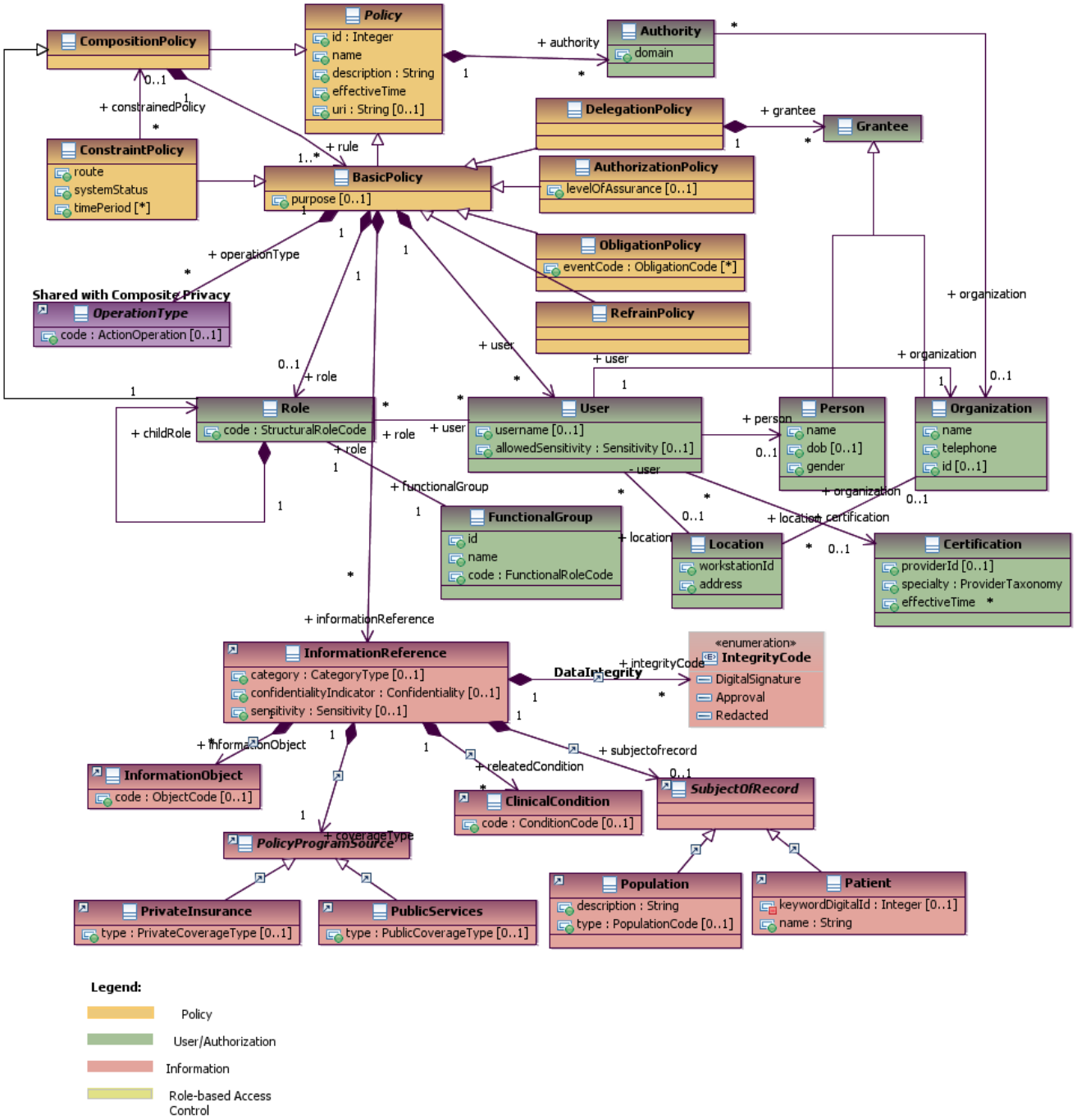

Figure 5: Use Case 1.8 - Negotiate Privacy Policy

Authority

This class is used to describe the authority that issues a specific policy. This typically, is a role played by an organization but it may also be jurisdictional authority (e.g. governmental agency).

Attribute	Notes
domain	The registered domain name of the healthcare organization that issues a specific privacy policy, used to uniquely identify the Authority.

AuthorizationPolicy

This class is used to describe an authorization policy that may be exchanged across domains. This class is a specialization of a basic policy and it inherits all its attributes. It also defines an additional attribute:

Attribute	Notes
levelOfAssurance [0..1]	Level of Assurance (LoA) refers to the degree of certainty that (1) a resource owner has that a person's physical self has been adequately verified before credentials are issued by a registration authority, and (2) a user indeed owns the credentials they are subsequently presenting to access the resource. The requirements for the level of certainty at both ends of that set of transactions should be driven by a risk assessment based on the value of the resources being protected. LoA is relevant to authentication, authorization, and access control in an SOA environment. Relevant references: • InCommon Credential Assessment Profile r0.3 • NIST 800-63: Electronic Authentication Guideline • NIST 800-53: Recommended Security Controls for Federal Information Systems Access may only be granted when authentication mechanisms of at least a given strength are used. That is indicated using the Level of Assurance.

BasicPolicy

This is the base class for a variety of policy types. It extends the abstract Policy class and provides additional attributes. This class may be used to instantiate specific policies.

Open Issue: For consistence with ISO/TS 22600 Privilege Management and Access Control, this model contains two base classes for a concrete policy. Based on future harmonization with ISO/TS 22600 this class may be combined with its abstract parent class “Policy”.

BasicPolicy a specialization of the abstract Policy class and thus it inherits all its attributes. It also defines an additional attribute:

Attribute	Notes
purpose [0..1]	This attribute is used to specify the purpose to permit a specific type of action/operation according to the policy. The vocabulary analysis section provides additional illustrative values for the concept embodied by this attribute.

Certification

A user's certifications may affect their access to specific IIHI for a patient. Healthcare providers are certified to provide specific services or use specific healthcare devices. This class deals specifically with professional certifications that may affect a user's privileges in a healthcare organization.

Attribute	Notes
providerId [0..1]	A unique identifier for the user requesting access to a client's IIHI.
specialty ProviderTaxonomy	A unique code describing a provider's specialty of practice. Multiple code sets exist to describe provider specialties, one of which is the US HIPAA ProviderTaxonomy code set.
effectiveTime	The time period during which the user's certification is valid.

CompositionPolicy

This class is the main/focal class for electronic privacy policies. It contains a set of basic policies that work together to enforce a privacy policy, organizational standard operating procedure, or a consent directive. Its basic characteristic is that it contains other policies.

ConstraintPolicy

A constraint policy is intended to constrain an existing policy. For example ConstraintPolicy instance may be used to represent a consent directive that sets specific "constraints" on a default organizational policy regarding substance abuse data (e.g., 42CFR Part2).

Attribute	Notes
route	Access to IIHI may only be granted for a specified route of access. For example, access is restricted to emergencies when the patient is unable to grant consent.
systemStatus	An access may be granted only for a particular ACI when the system has a particular status, for example during a disaster recovery
timePeriod [0..*]	An access may be allowed only during specific time periods of the day (e.g. 9 am to 5 pm).

DelegationPolicy

A delegation policy is intended to delegate access rights to a specific individual or organization.

FunctionalGroup

This class is used to specify the functional role of a user of a computer system. This role defines the way in which

Functional Roles can be grouped according to their authorization to access IIHI and perform various operations on health care information. E.g., A health care provider in Organization A is authorized to access IIHI from Organization B (when Organization A & B have entered into a trusted relationship), when that provider is associated with the Functional Group whose permissions grant access per that FunctionalRole.

Attribute	Notes
id	The unique identifier for the Functional Group in which the user's membership is asserted.
name	The functional role name used to associate groups of permissions for convenience in assigning to users.
code FunctionalUserCode	This code provides additional clarification regarding the type of role that may be used for specific types of users.

Grantee

This class is used to identify the choice of grantee - the person or organization - of a specific delegation policy.

Location

Access may be granted only to initiators on specific end-systems, workstations or terminals, or only to initiators in a specific physical location.

Attribute	Notes
workstationId	Unique identifier describing the mainframe terminal or personal computer used to access IIHI.
address	A unique number associated with a host that identifies it to other hosts during network transactions.

ObligationPolicy

An obligation policy may be used to specify additional privacy preferences specified by a client/patient. An obligation policy may be specified in addition to a ConstraintPolicy to describe full a patient's access control preferences. The obligation may be used to indicate that the receiver of an information object may not be allowed to redisclose it or persist indefinitely.

Attribute	Notes
eventCode ObligationCode [0..*]	This attribute identifies the action required before completing the step in the workflow. In this model we assume it is coded concept (ObligationCode) but in today's implementations it's primarily and ad-hoc rule reference (e.g. the name of a DB stored procedure) and thus it is not interoperable across organizations. An obligation may be associated with the release of an object. For example it may require a signature. This information is passed as rule for an application to enforce. In other cases it may require that audit record be created.

Permission

This class corresponds to a Role-based Access Control (RBAC) permission consistent with HL7 RBAC. It specifies an information object and action/operation allowed on that object.

Attribute	Notes
id	A unique identifier describing the approval to perform an operation on one or more RBAC-protected objects. Format for the identifier is: P = Code for O**p**eration 0000 = numeric identifier Examples: P1002 = CREATE; P1003 = READ; P1004 = UPDATE

PermissionCatalog

The permission catalog specifies a set of standard permissions.

Attribute	Notes
status	Indicates the current status – draft, active, inactive, suspended, etc.
version	This attribute identifies the version of the RBAC Permission Catalog from which the Permissions are derived.

Policy

This is the abstract class from which the concrete policy classes in this model are derived and instantiated. It specifies the properties reused by all policies. This class is abstract and thus it cannot be instantiated as a security policy for healthcare.

RefrainPolicy

A refrain policy is used to indicate that a specific action is prohibited based on specific access control attributes (e.g. purpose, information type, user role, etc.). It is a specialization of "Basic Policy" class. It does not have any additional attributes but implies a different behavior.

Role

This class is used to specify the role of a user of a computer system. It represents a job function within the context of an organization and specifies the capabilities that are available to the user assigned to that role. In accordance with ISO/TS 22600 PMAC, a role is itself a type of policy since it specifies the authorization policies.

Attribute	Notes
code StructuralRoleCode	Identifier of hierarchical group in which membership is asserted, for example, organizational position. Structural roles provide authorizations on objects at a global level without regard to internal details (ASTM E2595). Examples include authorization to participate in a session, connect authorization to a database, authorization to participate in an order workflow, or connection to a protected uniform resource locator (URL). A structural role applies to the business process task as a group.

User

This class is used to describe the properties of an individual who uses an information system.

Attribute	Notes
username [0..1]	The login identifier associated with a person using an information system used to access IIHI.
allowedSensitivity [0..1]	Coded attribute that describes the level sensitivity of the IIHI that the user may access or use. Sensitivity is a characteristic of a resource which implies its value or importance.

2. Use Case Analysis

The following section provides an analysis of use cases in scope for this analysis model. The complete description of the use cases is provided in Appendix A.

The notation described in Fig. 6 is used to identify the conceptual users of the systems and the systems required to support the use cases. The user activates the use cases. However, one system may also use the capabilities supported by another system.

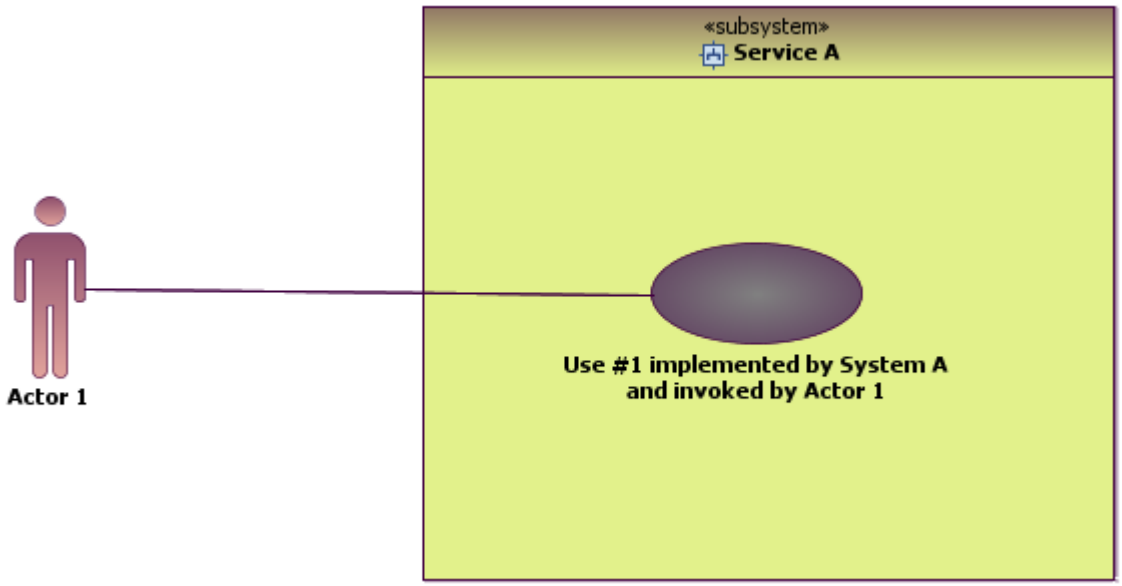

Figure 6: Use Case Analysis Notation

The use case analysis diagram in Fig. 7 identifies the business actors and systems that are required to support the use cases detailed in this specification. Each actor and system represents, conceptually, a set of users and information system.

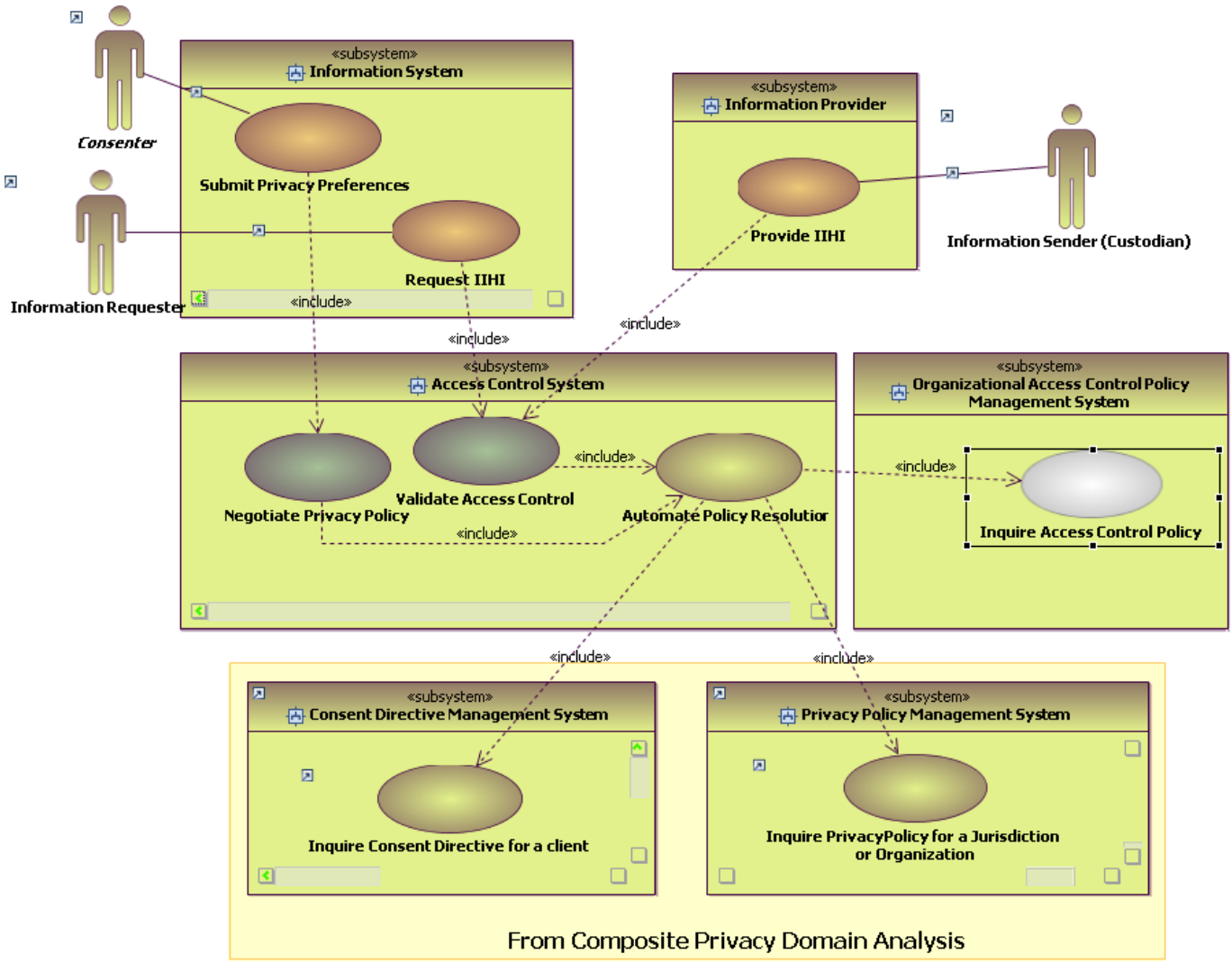

Figure 7: Use Case Analysis

The systems described in Fig. 7 illustrate the security implemented by all the systems required to enforce authorization and access control policies (e.g. Access Control System). As seen here the Access Control system is responsible for Implementing the “Negotiation Privacy Policy” and “Validate Access Control”. These use cases depend on “Automate Policy Resolution” and “Inquire Access Control Policy”. Conceptually each organization will provide a policy information point system like the one represented in this model by the “Organizational Access Control Policy Management System”. In order to automate the resolution of access control policies the Access Control System requires access to patients’ consent directive and privacy policy definitions. These definitions are provided by the systems identified during the analysis of consent directives and privacy policies and documented in the Composite Privacy Domain Analysis Model (see References).

Analysis of Systems

The use case analysis identified several conceptual systems that implement specific capabilities required to support the business use cases. The following system description summarizes the operations supported by each system along with the operation parameter. The parameters are expressed using the classes and enumerations identified in the information analysis section.

Access Control System

This system represents a conceptual access control system that evaluates and supports the enforcement of access control polices - including privacy and consent directives.

Operation	Notes	Parameters
evaluatePrivacyPreferences()	This operation and similar operations taking a variety of input parameters based on the criteria specified in the information model is intended to be used by an information system to evaluate the privacy preferences asserted by a consenter/patient.	**ConsentDirective** [in] **preferences** This parameter specifies the client's consent issued upon the completion of the policy negotiation.
resolvePolicies() CompositionPolicy	This operation represents the ability of the access control system to organize and prioritize applicable access control policies based on the criteria provided by the information requester.	**BasicPolicy** [in] **policy** This parameter specifies the policies that need to be resolved. **CompositionPolicy** [return] **resolvedPolicy** The return value specifies the combined/resolved policy set.
validatePolicy()	This operation represents the basic capability of an access control system to evaluate a policy to allow or deny the action requested.	

Organizational Access Control Policy Management System

This system stores the access control policies that are managed by an organization to ensure the proper use of its computer systems and healthcare information.

Operation	Notes	Parameters
getAccessControlPolicy()	This operation is used to inquire for the access control policies applicable in a specific context.	

Information Provider

This conceptual system represents any system that responds to requests for information from other systems and provides only that information allowed to be disclosed according to access control polices.

Operation	Notes	Parameters
requestInformation() InformationArtifact	This operation is invoked by when a user requests information from the system that stores/manages IIHI.	**ObjectCode** [in] **objectType** The document or information object type request **PurposeCode** [in] **purposeOfUse** This parameter specifies the purpose of use asserted by the information requester. **StructuralRoleCode** [in] **structuralRole** The structural role of the user who initiated the request. **FunctionalUserCode** [in] **functionalRole** The functional role of the user who initiated the request. **InformationArtifact** [return] **requestedInfo** The information artifacts that match the criteria as specified by the policy. If the systems use rights management then the information may be encrypted and a license is issued.

Information System

This subsystem conceptually represents any system that may be used by a provider that requires information from a system within the same domain or remote.

Operation	Notes	Parameters
addConsent()	This operation is used by a consenter or clerk to add a specific consent directive based upon the successful negotiation between a client and the healthcare organization.	**ConsentDirective** [in] **consent** This parameter specifies the client's consent issued upon the completion of the policy negotiation.

Operation	Notes	Parameters
requestInformation() InformationArtifact	This operation is invoked when a user requests information from the system. If the information requested is available remotely this system will request the information from the remote information provider.	**ObjectCode** [in] **objectType** The document or information object type request **FunctionalUserCode** [in] **functionalRole** The functional role of the user who initiated the request. **StructuralRoleCode** [in] **structuralRole** The structural role of the user who initiated the request. **InformationArtifact** [return] **requestedInfo** The information artifacts that match the criteria as specified by the policy. If the systems use rights management then the information may be encrypted and a license is issued. **PurposeCode** [in] **purposeOfUse** This parameter specifies the purpose of use asserted by the information requester.
submitPrivacyPreferences()	This operation is used by the consenter or a clerk acting as their proxy to propose a set of privacy preferences that may or may not be based on a valid privacy policy. The provider organization may negotiate with the client prior to accepting the proposed privacy preferences.	**ConsentDirective** [in] **preferences** This parameter specifies the client's consent issued upon the completion of the policy negotiation.

Use Case Elaborations

The following sequence diagrams illustrate how the various information systems have to interact in order to support the requirements documented in the use cases. The diagrams use UML Sequence Diagram notation to show the flow of information over time from the top to the bottom of the diagram. Each interaction is associated with a sequence number.

Negotiate Policies

This collaboration is an elaboration of the "Negotiate Privacy Policy" use case as detailed in "Use Case 1.9".

The collaboration involves all the system types identified in this analysis model. The following diagram illustrates the interactions required to negotiate and agree upon a specific set of privacy preferences. As seen here the end use initiates the negotiation by supplying a set of privacy preferences. Depending on applicable organization and privacy policies the Access Control System resolves whether the preferences are enforceable or not and responds with a counterproposal. If the user accepts it, then the user issues an authorization policy.

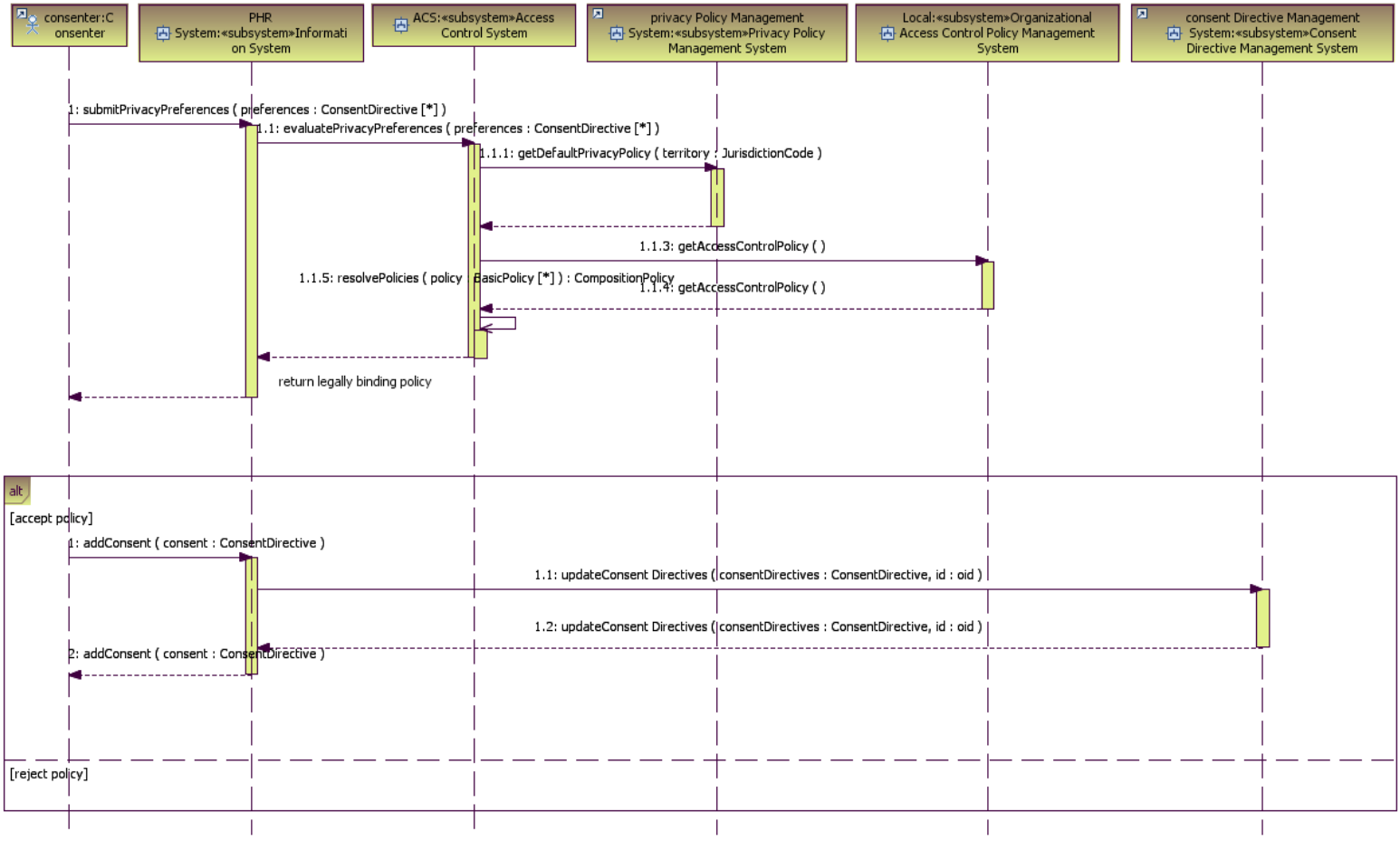

Figure 8: Negotiate Policies

Validate Access Control

This collaboration is an elaboration of the use case - "Validate Access Control" based on "Use Case 1.4: Enforce privacy policy and consent directives use access control" and revolves around the Access Control System.

The following diagram illustrates the interactions required to validate an access request. The information is requested using several request parameters (.e.g. information requests, roles, purpose of use, etc.) and the expected response represents the matching information according privacy and organization access control policies.

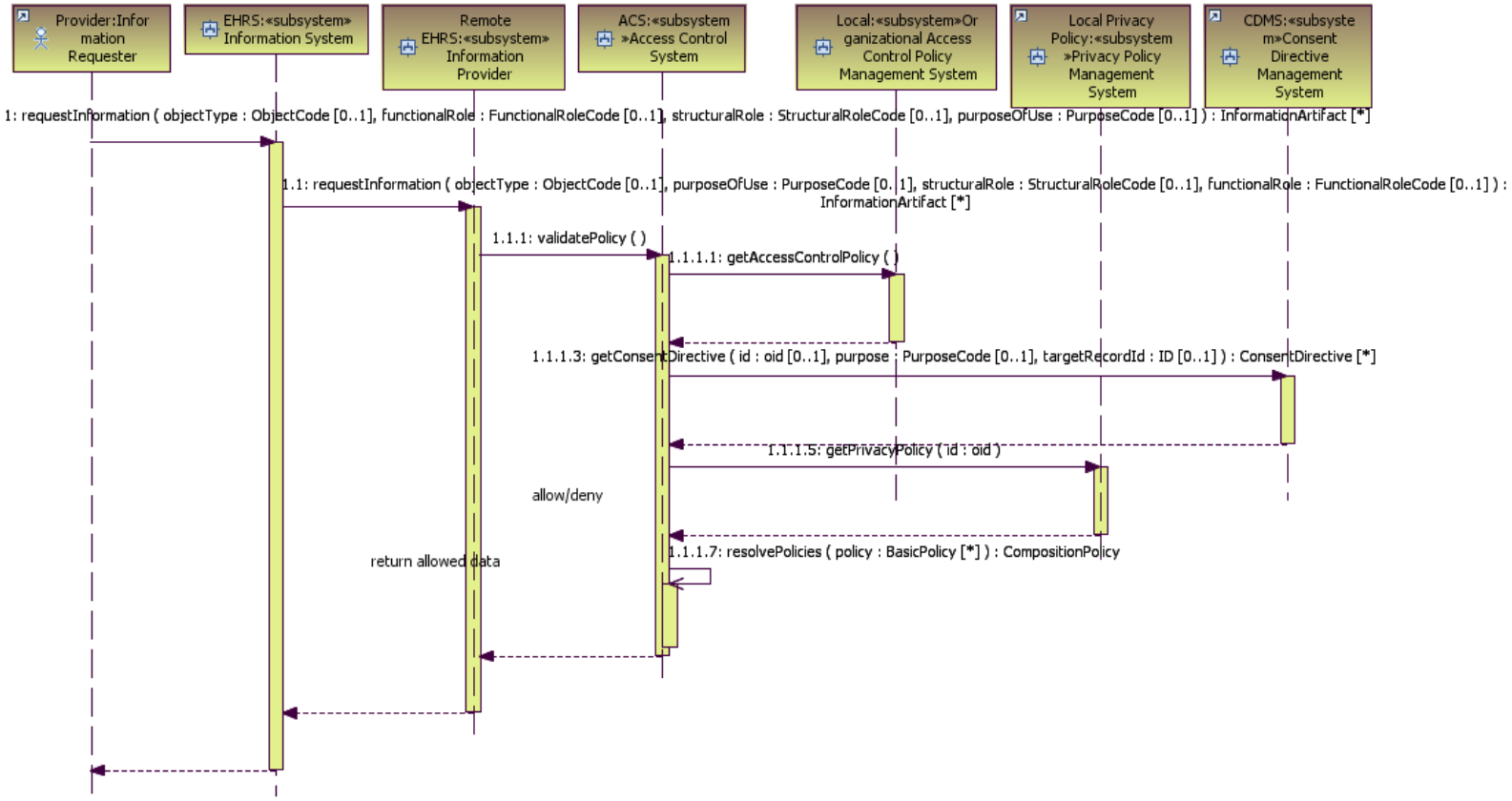

Figure 9: Validate Access Control

3. Vocabulary Analysis

The following section describes an analysis of the controlled vocabulary required to support the access control and authorization requirements of healthcare organizations.

> **Note** that the enumerations in this section list only example codes and are not expected to be used by implementers "as is".

The following diagram shows the value sets required to support the requirements for interoperable policies across healthcare organizations. The diagram identifies a significant number of common concepts that are common in order to support privacy and access control and authorization enforcement.

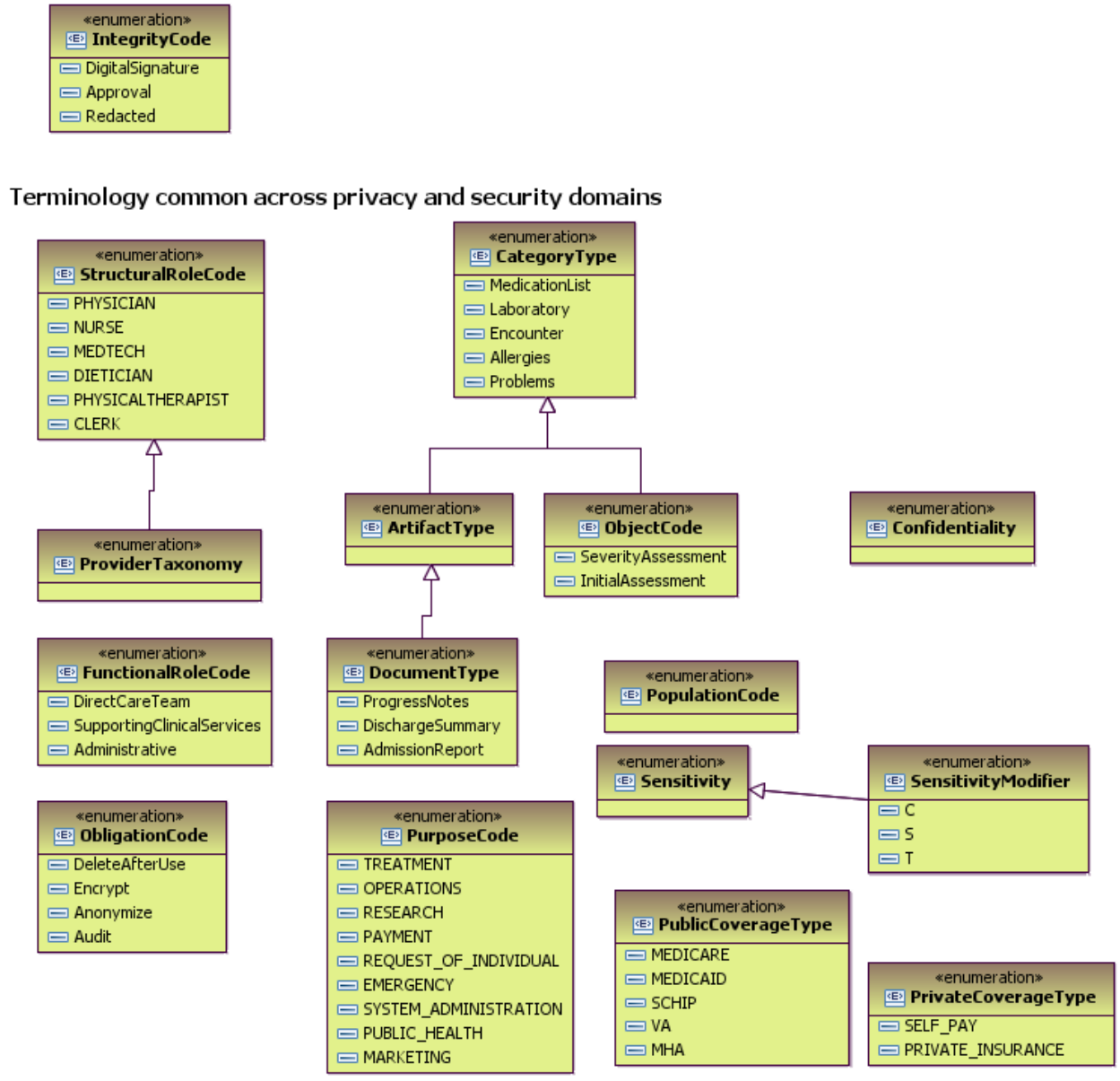

Figure 10: Vocabulary required for Security DAM

IntegrityCode

This vocabulary concept is used to describe the values that may be assigned to the integrity attribute of a user or an information artifact. This is an explicit coded concept for security policies but it typically implied in privacy policies or consumer consent directives.

Note: the following are example code used to illustrate the concept of data integrity as it applies to healthcare IT solutions.

Codes	Notes
DigitalSignature IntegrityCode	Indicates that the data requires a digital signature from a provider to be considered intact.
Approval IntegrityCode	Indicates that a data element must be officially "approved". This only an example integrity code
Redacted IntegrityCode	Indicates that the patient redacted the information

References

HL7 Composite Privacy Consent Directive Domain Analysis Model – DSTU September 2009

Appendix A – Security Use Cases

Authorize users and systems

This use cases is based on **"IN1.3 Authorize users and systems"** function in *EHR Functional Model - Infrastructure*. "Manage the sets of access control permissions granted to entities that use an EHR-S (EHR-S Users). Enable EHR-S security administrators to grant authorizations to users, for roles, and within contexts. A combination of these authorization categories may be applied to control access to EHR-S functions or data within an EHR-S, including at the application or the operating system level.

EHR-S Users are authorized to use the components of an EHR-S according to their identity, role, work-assignment, location and/or the patient's present condition and the EHR-S User's scope of practice within a legal jurisdiction.

- User based authorization refers to the permissions granted or denied based on the identity of an individual. An example of User based authorization is a patient defined denial of access to all or part of a record to a particular party for privacy related reasons. Another user based authorization is for a tele-monitor device or robotic access to an EHR-S for prescribed directions and other input.
- Role based authorization refers to the responsibility or function performed in a particular operation or process. Example roles include: an application or device (tele-monitor or robotic); or a nurse, dietician, administrator, legal guardian, and auditor.
- Context-based Authorization is defined by ISO 10181-3 Technical Framework for Access Control Standard as security relevant properties of the context in which an access request occurs, explicitly time, location, route of access, and quality of authentication. For example, an EHR-S might only allow supervising providers' context authorization to attest to entries proposed by residents under their supervision. In addition to the ISO standard, context authorization for an EHR-S is extended to satisfy special circumstances such as, work assignment, patient consents and authorizations, or other healthcare-related factors. A context-based example is a patient-granted authorization to a specific third party for a limited period to view specific EHR records. Another example is a right granted for a limited period to view those, and only those, EHR records connected to a specific topic of investigation."

Pre-conditions

- Authenticate users and systems in Domains A and B.
- Both organizations (Domain A and B) have agreed on the functional roles that may be exchanged and the meaning of the permissions carried by the functional roles.

Basic Scenarios

1. RBAC Authorization Use Cases

Actors

- Domain A Information Requester - Radiologist, Nurse, Physician, Pharmacist, etc.
- Domain B Policy Enforcement Point (Verifier PEP)
- Domain B Policy Information Point (Verifier PIP)
- Domain B Policy Decision Point (Verifier PDP)
- Domain B Policy Administration Point (Verifier AP)
- Domain B Service Provider

Enforce privacy policy and consent directives using access control

This use cases is based on **IN.1.3 "Entity Access Control"** function in *EHR Functional Model - Infrastructure*.
"Verify and enforce access control to all EHR-S components, EHR information and functions for end-users, applications, sites, etc., to prevent unauthorized use of a resource.
Description: Entity Access Control is a fundamental function of an EHR-S. To ensure that access is controlled, an EHRS must perform authentication and authorization of users or applications for any operation that requires it and enforce the system and information access rules that have been defined."

Pre-conditions

- Organizational and Jurisdictional Privacy Policies provide specific rules regarding the use, disclosure, or update of Individually Identifiable Health Information (IIHI)
- Patients have the option to authorize the disclosure of their information (e.g. IIHI) that meets specific criteria.
- Two Domains exist [Domain A (Security Domain A) and Domain B (Security Domain B)] as separate entities each with a set of subjects, their information objects, and a common security policy (NIST Special Publication 800-33).
- A trust relationship exists between Domain A (Security Domain A) and Domain B (Security Domain B).
- Both organizations have agreed to use the Cross Enterprise Security and Privacy Authorization (XSPA) Security Assertion Markup Language (SAML) Profile.
- Both organizations have agreed on the functional roles that may be exchanged and the meaning of the permissions carried by the functional roles
- The patient has created a patient consent directive in Domain B to deny access to their medical record to all radiologists under normal treatment circumstances. The patient's consent directive allows access to their medical record to radiologists under emergency treatment circumstances.

Basic Scenarios

Purpose of Use: Permit Patient Consent

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Radiologist
    - Functional Role: None
    - Obligations: None
    - Domain A Policy: Radiologist may make external requests for patient information at Domain B.
    - Domain B Policy: Grant radiologist access for treatment.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to deny access for radiologists for all purpose of use other than emergency access.
- Scenario: The radiologist in Domain A asserts the purpose of use as Emergency Treatment and then requests the patient's medical record in Domain B.
- Result: The radiologist's access to the patient's medical record is granted by asserting the purpose of use as emergency treatment

Purpose of Use: Deny Local Policy

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Physician
    - Functional Role: None

    - Obligations: None
    - Domain A Policy: Physicians may make external requests for patient information at Domain B.
    - Domain B Policy: Grant Physician access for treatment.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to grant access for purpose of use of emergency access. Requests made under all other purposes of use are denied.
- Scenario: While on an out-of-town business trip, the patient develops a slight fever and cough and determines they may have an infection and goes to the local urgent care center in Domain A. A healthcare provider sees the patient. During the discussion the patient states that they recently had a physical and that some blood work was done at Domain B. The provider believes these results might contain information valuable to this encounter. Since there is an existing trust relationship between Domain A and Domain B, the Domain A provider is able to assert the role of physician. The Domain B policy permits access to physicians for treatment purposes however the patient has generated a consent directive at Domain B that states that Domain A clinicians may access their information only in the event of an emergency. The provider will attempt to access the patient's medical record at Domain B by performing a cross-enterprise lookup of the patient's medical record.
- Result: The provider is denied access and cannot view the patient's medical record based on patient consent directive stating that Domain A clinicians may access their information only in the event of an emergency

Purpose of Use: Deny Patient Consent Directive

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Radiologist
    - Functional Role: None
    - Obligations: None
    - Domain A Policy: Radiologist may make external requests for patient information at Domain B.
    - Domain B Policy: Grant Radiologist access for treatment.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to deny access for radiologists for all purpose of use.
- Scenario: During the patient's visit at the urgent care center in Domain A, the patient mentions to the provider that the patient's knee has been sore and swollen. The provider writes a radiology order for a standard series on the patient's knee. The radiologist performs the procedure and prepares his findings. The radiologist is concerned over some abnormal findings and feels it necessary to review the patient's clinical history. The radiologist attempts to access the patient's medical record at Domain B.
- Result: The Radiologist is denied access to patient's medical record per the patient consent directive to deny access for radiologists for all purpose of use.

Information Masking Scenario 1 - Patient Consent Directive Denies

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Physician
    - Functional Role: None
    - Obligations: Mask Medication Information
    - Domain A Policy: Physicians may make external requests for patient information at Domain B.
    - Domain B Policy: Grant Physician access for treatment.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to grant general access to patient's medical records but deny access to patient's medication history to all but pharmacists.

- Scenario: While on an out-of-town business trip the patient experiences pain in their knee, from a pre-existing condition. The patient goes to the local urgent care center in Domain A. A healthcare provider sees the patient. During the patient's visit at the urgent care center, the patient indicates to the provider that they have received treatment for the pain in their knee at Domain B. The provider attempts to view the patient's medical record at Domain B to review the treatment given and determine what medications the patient has been given.
- Result: The physician is able to see the patient's medical record at Domain B but is denied access to the patient's medication history as a result of the patient consent directive at Domain B to deny access to the patient's medication history to all but pharmacists.

Information Masking Scenario 2 - Patient Consent Directive Permits

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Pharmacist
    - Functional Role: None
    - Obligations: Mask Medication Information
    - Domain A Policy: Pharmacists may make external requests for patient information at Domain B.
    - Domain B Policy: Grant Pharmacists access for treatment.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to grant general access to patient's medical records but, deny access to patient's **medication history to all but pharmacists.
- Scenario: While on an out-of-town business trip the patient experiences pain in their knee, from a pre-existing condition. The patient goes to the local urgent care center in Domain A. A healthcare provider sees the patient. During the patient's visit at the urgent care center, the provider prescribes pain medication for the patient's sore knee, and sends the patient to local pharmacy to pick it up. The pharmacist attempts to check for drug-to-drug interactions by accessing the patient's medication record at Domain B.
- Result: The pharmacist is able to see the patient's medical record complete with the patient's medication history as a result of the patient consent directive at Domain B to deny access to the patient's medication history to all but pharmacists.

Functional Role Access Control: Permit

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Nurse
    - Functional Role: Nurse
    - Obligations: None
    - Domain A Policy: Nurse may make external requests for patient information at Domain B.
    - Domain B Policy: Grant Nurse access to patient record for treatment as per functional role and required permissions.
- Scenario: The patient, while on an out-of-town business trip, develops a slight fever and cough. The patient determines they may have an infection and goes to the local urgent care center. The Provider sees the patient. During the discussion the patient informs the provider of a recent physical and that some blood work was done at Domain B. The provider believes these results might contain information valuable to this encounter and asks the nurse to document the results of the blood work from Domain B. Since an existing trust relationship exists between Domain A and Domain B, the nurse will attempt to access the patient's medical record at Domain B by performing a cross-enterprise lookup of the patient's medical record.
- Result: The nurse has the required functional role and is granted access to view the patient's medical record.

Functional Role Access Control: Deny

- Policy Environment
    - Model: Extranet
    - Purpose of Use: Treatment
    - Structural Role: Nurse
    - Functional Role: None
    - Obligations: None
    - Domain A Policy: Nurse may make external requests for patient information at Domain B.
    - Domain B Policy: Grant Nurse access to patient record for treatment as per functional role.
- Scenario: The patient, while on an out-of-town business trip, develops a slight fever and cough. The patient determines they may have an infection and goes to the local urgent care center. The Provider sees the patient. During the discussion the patient informs the provider of a recent physical and that some blood work was done at Domain B. The provider believes these results might contain information valuable to this encounter and asks the nurse to document the results of the blood work from Domain B. Since an existing trust relationship exists between Domain A and Domain B, the nurse will attempt to access the patient's medical record at Domain B by performing a cross-enterprise lookup of the patient's medical record.
- Result: The nurse does have the required functional role and is denied access to view the patient's medical record.

Structured Role Access Control - Permit

Structural roles provide authorizations on objects at a global level without regard to internal details (ASTM E2595). Examples include authorization to participate in a session, connect authorization to a database, authorization to participate in an order workflow, or connection to a protected uniform resource locator (URL). A structural role applies to the business process task as a group. The use cases below will use structural role access permissions to health information based on ASTM E1986 as part of the authorization process.

- Policy Environment
    - Purpose of Use: Treatment
    - Domain A Policy: Licensed clinicians may make requests for patient information including information located at Domain B.
    - Domain B Policy: The structural role of "Physician" is required for cross-domain access to Domain B EHR data objects under the purpose of use of "Treatment".
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to grant unrestricted access to all health information to properly authorized clinicians for the purposes of use of "Treatment" (opt-in w/o restriction).
- Scenario: The patient, while on an out-of-town business trip, develops a slight fever and cough. The patient determines they may have an infection and goes to the local urgent care center. The Provider sees the patient. During the discussion the patient informs the provider of a recent physical and blood work done at Domain B. The provider believes these results might contain information valuable to this encounter. The provider, in the role of physician, performs a cross-enterprise lookup of the patient's medical record, finds the patient, and then makes a request for the physical and blood work. Since the policy for these objects requires structural role of physician, the request is allowed and the Domain B Service Provider provides information in its response.
- Result: The provider is able to access and view the patient's medical record.

Structured Role Access Control - Deny

- Policy Environment
    - Purpose of Use: Treatment
    - Domain A Policy: Physicians may make external requests for patient information including information located at Domain B.

    - Domain B Policy: The Physician role is allowed to make requests under the purpose of use of "Treatment" at Domain B for specific EHR data objects.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to grant unrestricted access to all health information to properly authorized clinicians for the purposes of use of "Treatment" (opt-in w/o restriction).
- Scenario: The patient, while on an out-of-town business trip, develops a slight fever and cough. The patient determines they may have an infection and goes to the local urgent care center. The Provider sees the patient. During the discussion the patient informs the provider of a recent physical and that some blood work was done at Domain B. The provider believes these results might contain information valuable to this encounter. The provider does not have access to a computer. The provider asks the nurse, to login to system and perform a cross-enterprise look up of the patient's medical record.
- Result: The nurse is denied access to patient's medical record at Domain B based on the policy at Domain B to grant access to physicians and to deny access to all others.

Structural Role Access Control – Patient Denies

- Policy Environment
    - Purpose of Use: Treatment
    - Domain A Policy: Pharmacists may make external requests for patient information at Domain B.
    - Domain B Policy: The structural role of licensed clinician is required to make requests under the purpose of use of "Treatment" at Domain B for specific EHR data objects.
    - Domain B Privacy Policy: The Domain B privacy policy (per the patient consent directive) is to grant access to all structural roles except pharmacists for the purposes of use of "Treatment".
- Scenario: The patient, while on an out-of-town business trip, develops a slight fever and cough. The patient determines they may have an infection and goes to the local urgent care center. The Provider sees the patient. During the discussion the patient informs the provider of a recent physical and that some blood work was done at Domain B. The provider believes these results might contain information valuable to this encounter. The provider attempts to access the patient's medical record at Domain B by performing a cross-enterprise lookup of patient's medical record. The provider notes a change needs to be made on one of the patient's prescriptions, notifies the onsite pharmacy of the change, and sends the patient to pick it up. The Pharmacists attempts to check for drug-to-drug interactions by accessing the patient's record at Domain B.
- Result: The pharmacist's access to the patient's medical record is denied based on a patient consent directive denying access to Domain B information by Domain A pharmacists under purpose of use of Treatment.

Note: Even though the patient has given consent for the pharmacist at Domain A to make the request, the pre-established Domain B policy dominates under the principal that each domain is responsible for enforcing its own policies. In this case, the patient will need to modify the Domain B consent directive. Note: The result does not preclude Domain A from issuing the prescription; it is only that the drug interaction check will not be possible. Note: The physician can still access the patient's Domain B medications. Assuming the patient allows, the Domain B pharmacist can then access the medications from the Domain B repository.

Actors

- Domain A Information Requester - Radiologist, Nurse, Physician, Pharmacist, etc.
- Domain B Policy Enforcement Point (Verifier PEP)
- Domain B Policy Information Point (Verifier PIP)
- Domain B Policy Decision Point (Verifier PDP)
- Domain B Policy Administration Point (Verifier AP)
- Domain B Service Provider

Automated Policy Resolution

This use case illustrates an example of how an automated system would use structured negotiation for resolving and enforcing privacy policies and rules under normal treatment conditions. An important facet of this use case is the system's ability to change a user's access privileges automatically based on a series of pre-set conditions.

Pre-conditions

Jurisdictional and organizational authority has developed privacy policies that cover patient information at Sunnybrook Hospital. These policies comply with all applicable laws and mandates of the hospital and also allow patients to register their privacy preferences through consent directives. Patient preferences fit within the guidelines provided by the hospital policies so as not to conflict with these policies.
Hospital policy allows patients to indicate which individuals, who may normally have access to their records, they wish to block from accessing their medical records.

- Hospital authorities have implemented privacy policies that comply with jurisdictional and organizational mandates for patient privacy.
- Hospital authorities have provided the means for patients to register their own personal preferences for privacy.

Basic Scenario

Sam Jones has been provided with a form to register his privacy preferences. He indicates that he does not want Dr. Bob to access his records. Sunnybrook Hospital has a rule that provides access to all patient records to treating physicians. Mr. Jones is alerted to this rule when he enters his preferences and agrees to it. Dr. Bob is not Mr. Jones' primary physician and so is not granted access to Mr. Jones' record on a regular basis.
During the course of normal treatment it is necessary for Dr. Bob to access Mr. Jones' medical record. Dr. Bob indicates to the system that he is in the role of Mr. Jones' treating physician. The system grants Dr. Bob access to Mr. Jones' medical record automatically without requiring an override condition.

Post-Conditions

All jurisdictional and organizational policies are complied with and no consent directive has been changed without the stakeholders' previous consent. At such a time as Dr. Bob is no longer Mr. Jones' treating physician, he will no longer have access to Mr. Jones' medical record.

Negotiate Privacy Policy

This use case describes a how a manual process, unstructured negotiation, can be used to resolve conflicts between jurisdictional and organizational privacy policies and the patient's preferences under normal treatment conditions. This use case covers the consent to access information and not necessarily the consent for treatment.
The unstructured negotiation process is used at decision points in the system where decision options are either not known or require further elaboration before the decision can be made.

Pre-conditions

Jurisdictional and organizational authority has developed privacy policies that cover patient information at Sunnybrook Hospital. These policies comply with all applicable laws and mandates of the hospital and also allow patients to register their privacy preferences through consent directives. Not all patient preferences fit within the guidelines provided by the hospital policies creating conflict with these policies. These situations will require unstructured negotiation in order to resolve the conflict.
Hospital policy allows patients to indicate which individuals, who may normally have access to their records, that they wish to block from accessing their medical records.

- Hospital authorities have implemented privacy policies that comply with jurisdictional and organizational mandates for patient privacy.

- Hospital authorities have provided the means for patients to register their own personal preferences for privacy.

Basic Scenario

Sam Jones has been provided with a form to register his privacy preferences. He indicates that he does not want Dr. Bob to access his records. Sunnybrook Hospital has a rule that provides access to all patient records to treating physicians. Mr. Jones is alerted to this rule when he enters his preferences. Although Dr. Bob is not Mr. Jones' primary physician, there may be occasions when Dr. Bob would be granted access to Mr. Jones' medical record.
Mr. Jones does not agree to the policy and does not sign the consent form. Because the hospital cannot provide service to Mr. Jones without a signed consent form, a privacy officer at the hospital is alerted to this and contacts Mr. Jones.
The privacy officer explains the situation to Mr. Jones and explains the different options that are available and their consequences. Mr. Jones either selects an option that he is comfortable with or suggests an alternative option. The privacy officer then complies with Mr. Jones' decision or evaluates the alternative option. This process continues until a mutually satisfactory option is reached.

Post-Conditions

All jurisdictional policies are complied with and neither organizational policy nor consent directive has been changed without the stakeholders' knowledge. One possible resolution to the conflict could be that the hospital and patient have not come to an agreement and the patient has decided to seek healthcare services at another hospital.