Federal Health Architecture Program

Federal Health Information Model (FHIM)

SecurityAndPrivacy Model

Publishing Facilitator: Ioana Singureanu, Eversolve/SAMHSA

October 8th, 2010

TABLE OF CONTENTS:

LIST OF FIGURES:

SecurityAndPrivacy

The HL7 DAM contains two subclasses to illustrate the type of security/privacy policies that are inherent from the healthcare payment source. Those two subclasses are examples of many potential kinds of policies, and would be 'fleshed out' in the terminology referenced by the code.

This class may need to be replaced by existing EHR concepts such as 'Problem' or 'Diagnosis'

The HL7 DAM several subtypes, including Access, Collection, Disclosure, and Use. These subclasses may be handled in the taxonomy referenced by the Code

SecurityandPrivacyDomain

_SecurityAndPrivacy

Noted differences between this model and the HL7 Security and Privacy DAM: a) The DAM has SecurityRole as a subtype of CompositePolicy. We made it an association instead. Then, because both BasicPolicy and CompositePolicy have associations to SecurityRole, we moved the association to Policy, which is the common supertype of both BasicPolicy and CompositePolicy. b) The DAM models JurisdictionalOrganization and ProviderOrganization as subtypes of Authority. Indeed, ProviderOrganization is also a subtype of Grantee (multiple-inheritance). In the FHIM, ProviderOrganization and JurisidictionalOrganization are existing stand-alone concepts. So we changed the inheritance relationship to association relationships. c) The DAM models Patient and Population as subtypes of SubjectOfRecord. In the FHIM, Patient and Population are existing stand-alone concepts. So we changed the inheritance relationship to association relationships. Need to better understand the PrivateInsurance and PublicServices classes. These appear to mimic E/E/COB classes, but the purpose for these is unclear. HL7 already has an exhaustive list of coverage types. Should OrganizationalProvider be an Entity rather than a Role?

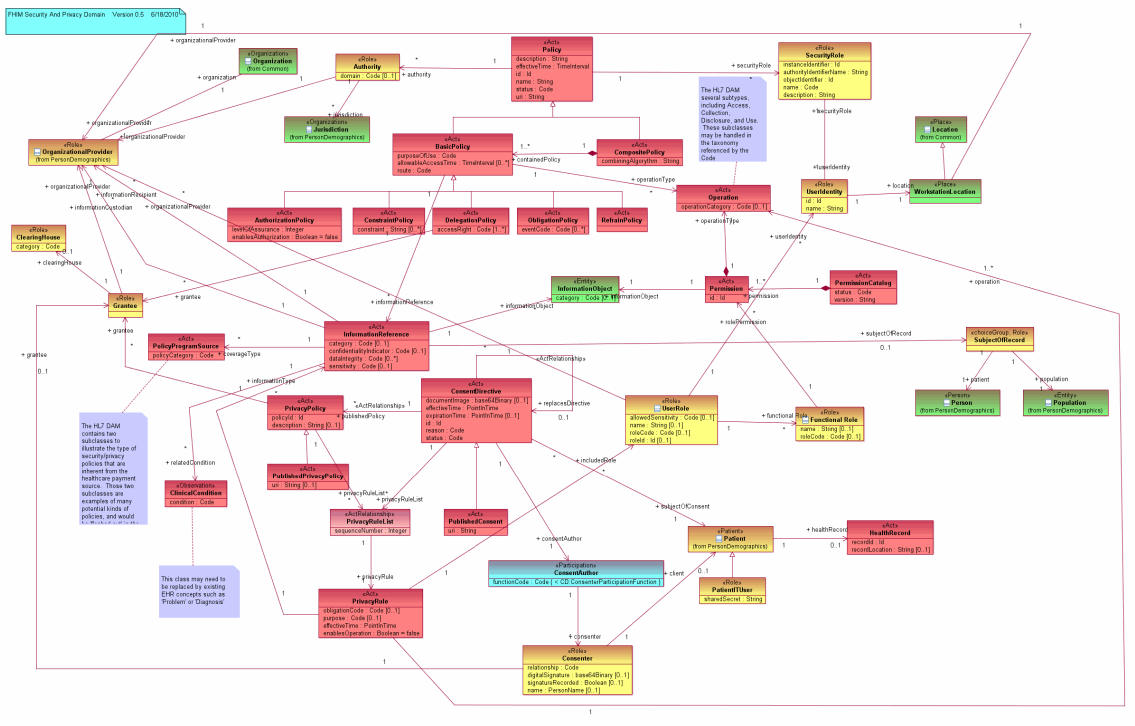

Figure _SecurityAndPrivacy

«Role» Class: Authority

This abstract class is used to designate the authority that issues the policy. Authority is an organization (either Jurisdictional or Provider) that is responsible for the Privacy Policy. This is the authority that grants authorization described in the privacy policy. This class is consistent with the 'Security Authority' specified by the ISO/IEC 15816 standard as 'The entity accountable for the administration of a security policy within a security domain.

Attribute 'Authority.domain' of type ' Code' with cardinality of [0..1]

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

Attribute 'Authority.jurisdiction' of type ' Jurisdiction' with cardinality of [*]

Represents a territorial authority organization that may be issuing privacy policies for a territory.

Attribute 'Authority.organizationalProvider' of type ' OrganizationalProvider' with cardinality of [*]

Specifies a healthcare organization that which will promulgate privacy policies for use within its organization.

«Act» Class: AuthorizationPolicy

This class is used to describe an authorization policy that may be exchanged across domains. An AuthorizationPolicy instance specifies 'permitted actions' according to ISO 22600-2. A positive/negative authorization policy defines the actions ('OperationType ') that a subject is permitted/forbidden to perform on a target. Actions encoded using the 'OperationType ' class represent the operations defined in the interface of a target object contrary to obligations/refrain policies, which are interpreted by the subject while the object might be open in this perspective.” The following are the attributes of an AuthorizationPolicy:

Attribute 'AuthorizationPolicy.enablesAuthorization' of type ' Boolean' with cardinality of [1]

This attribute is used to specify if the policy enables or declines an authorization. If this attribute is set to 'true' the policy authorizes the actions and conditions pertaining to the resources referenced by the policy. Otherwise the authorization is declined.

Attribute 'AuthorizationPolicy.levelOfAssurance' of type ' Integer' with cardinality of [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', and '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.

«Act» Class: 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. ISO-22600 specifies a security policy as 'plan or course of action adopted for providing computer security'. BasicPolicy a specialization of the abstract Policy class and thus inherits all its attributes. It also defines additional attributes and associations:

Attribute 'BasicPolicy.allowableAccessTime' of type ' TimeInterval' with cardinality of [*]

An access may be allowed only during specific time periods of the day (e.g., 9 am to 5 pm).

Association 'BasicPolicy.informationReference' of type ' InformationReference' with cardinality of [*]

This association references the attributes of the information referenced in the policy.

Association 'BasicPolicy.operationType' of type ' Operation' with cardinality of [*]

This association refers to the operation associated with the policy.

Attribute 'BasicPolicy.purposeOfUse' of type ' Code' with cardinality of [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.

Attribute 'BasicPolicy.route' of type ' Code' with cardinality of [1]

This attribute specifies whether access to protected information may only be granted for a specified route of access. For example, access may be restricted to remote users using a Virtual Private Network (VPN). The route is a context qualifier as specified by ISO/IEC 10164-9.

«Role» Class: ClearingHouse

An organization that consolidates medical claims from various providers for electronic submission to and payment from various payers.

Attribute 'ClearingHouse.category' of type ' Code' with cardinality of [1]

Identifies the type of clearinghouse

«Observation» Class: ClinicalCondition

The health condition(s) associated with the policy. Conditions when specified, are coded concepts expressed in a standard vocabulary (e.g., LOINC, SNOMED CT, etc.). These may include indications of 'substance abuse' or 'HIV-related' illnesses, etc. An obligationCode may be implemented as a 'condition'.

Attribute 'ClinicalCondition.condition' of type ' Code' with cardinality of [1]

Categorizes the health condition associated with the policy. Conditions when specified, are coded concepts expressed in a standard vocabulary (e.g., LOINC, SNOMED CT, etc.). These may include indications of 'substance abuse' or 'HIV-related' illnesses, etc.

«Act» Class: CompositePolicy

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. An instance of a CompositePolicy may include several Authorization, Delegation, Refrain, or Obligation policies. A CompositePolicy is specialization of Policy and inherits all its attributes and associations. In addition to the attributes it inherits

from its base class ('Policy') this type of class contains the following association and attribute:

Attribute 'CompositePolicy.combiningAlgorythm' of type ' String' with cardinality of [1]

This attribute is used to specify the policy combining algorithm that is used to process the contained policies.

Association 'CompositePolicy.containedPolicy' of type ' BasicPolicy' with cardinality of [1..*]

This association specifies the policies contained in a CompositionPolicy.

«Participation» Class: ConsentAuthor

A participation by which a person in the role of 'Consenter' creates or 'authors' a Consent Directive.

Association 'ConsentAuthor.consenter' of type ' Consenter' with cardinality of [1]

Identifies the person who created or 'authored' the consent directive

Attribute 'ConsentAuthor.functionCode' of type ' Code' with cardinality of [1]

Vocabulary Binding:

Concept Domain: ConsenterParticipationFunction

Further defines the kind of participation by which a person in the role of 'Consenter' creates or 'authors' a Consent Directive.

«Act» Class: ConsentDirective

This class is the focal class representing a set of consent directives issued by a consenter on behalf of self or someone else. This class is the root class or the entry class into the Consent Directive structure.

Association 'ConsentDirective.consentAuthor' of type ' ConsentAuthor' with cardinality of [1]

Identifies the person who created or 'authored' the consent directive

Attribute 'ConsentDirective.documentImage' of type ' base64Binary' with cardinality of [0..1]

This optional attribute references a signed paper document containing the client's consent directive.

Attribute 'ConsentDirective.effectiveTime' of type ' PointInTime' with cardinality of [1]

This attribute specifies the date when the policy/consent is in effect.

Attribute 'ConsentDirective.expirationTime' of type ' PointInTime' with cardinality of [0..1]

This attribute specifies when the consent directive automatically expires. A consent directive may be revoked prior to its expiration date.

Attribute 'ConsentDirective.id' of type ' Id' with cardinality of [1]

Unique identifier that refers to a specific Consent Directive instance. This id or the published URI may be used to lookup the client's consent directives in order to apply them to the collection, access, use, or disclosure of health records.

Association 'ConsentDirective.privacyRuleList' of type ' PrivacyRuleList' with cardinality of [*]

A list of zero or more consent rules applicable to this consent directive. A consent rule specifies the permission allowed to a user type by the consenter for a specific type of information. The person consenting may be either the subject of the record or a designated Substitute Decision Maker. One or more consent rules comprise a consent directive or privacy policy.

Association 'ConsentDirective.publishedPolicy' of type ' PrivacyPolicy' with cardinality of [*]

A set of rules that are intended to be enforced by security systems and are used as the basis for client consent directives.

Attribute 'ConsentDirective.reason' of type ' Code' with cardinality of [1]

This attribute is used to specify the reason for revoking a Consent Directive, e.g., requested vs. correction/error. An error would be a discrepancy between the intent of Consent Directive (as communicated by the Consenter) and that which was entered into the Consent Directive Management System (CDMS).

Association 'ConsentDirective.replacesDirective' of type ' ConsentDirective' with cardinality of [0..1]

Points to a previous Consent Directive superseded by the current instance.

Attribute 'ConsentDirective.status' of type ' Code' with cardinality of [1]

This attribute indicates whether the consent directive is active or not.

Attribute 'ConsentDirective.subjectOfConsent' of type ' Patient' with cardinality of [1]

Identifies the person to whom the consent directive applies. This person may or may not be the same person as the consent author, as in the case where the patient is a minor child or an incapacitated person.

«Role» Class: Consenter

This class is intended to capture the properties of a Consenter/Substitute Decision Maker - see 'Actors'.

Attribute 'Consenter.client' of type ' Patient' with cardinality of [0..1]

Identifies the person to whom the consent directive applies. This person may or may not be the same person as the consent author, as in the case where the patient is a minor child or an incapacitated person.

Attribute 'Consenter.digitalSignature' of type ' base64Binary' with cardinality of [0..1]

This attribute is used to store the consenter's signature.

Association 'Consenter.grantee' of type ' Grantee' with cardinality of [0..1]

Designates who/what has been delegated a specific right.

Attribute 'Consenter.name' of type ' PersonName' with cardinality of [0..1]

Contains the name of the person who granted consent.

Attribute 'Consenter.relationship' of type ' Code' with cardinality of [1]

This coded attribute is intended to specify the relationship between the consenter and the client. This may be a Substitute Decisions Maker, a legal guardian, etc.

Attribute 'Consenter.signatureRecorded' of type ' Boolean' with cardinality of [0..1]

If a digital signature is not allowed by policy, this attribute indicates whether a signature was captured.

«Act» Class: ConstraintPolicy

A constraint policy is intended to constrain an existing policy. For example a 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). A policy (BasicPolicy or CompositePolicy) can be constrained in the sense of profiles for tailoring a policy instance. Complex constraints (e.g., an OCL expression) may be applied and managed separately. For this definition and management purpose it is possible to separate externally-defined constraints and specify a 'ConstraintPolicy' with clearly defined associations to the constrained policy according to component model principles. Effectively, the result of applying constraints is just another CompositePolicy.

Attribute 'ConstraintPolicy.constraint' of type ' String' with cardinality of [*]

Constraint expression.

DataIntegrity

Data integrity is an implied privacy concept but it is explicit in security policy specifications.

«Act» Class: DelegationPolicy

A delegation policy is intended to delegate access rights to a specific individual or organization (a grantee). ISO 22600-2 defines delegation as 'conveyance of privilege from one entity that holds such privilege, to another entity' and a DelegationPolicy as 'defines what authorizations can be delegated to whom'.

Association 'DelegationPolicy.grantee' of type ' Grantee' with cardinality of [*]

Designates who/what has been delegated a specific right.

«Role» Class: Functional Role

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 protected information (including IIHI) from Organization B (when Organization A & B have entered into a trusted relationship) if that provider is associated with the Functional Group whose permissions grant access per that FunctionalRole. In summary, the functional role defines the access control decision. A functional role is bound to a policy.

Attribute 'Functional Role.name' of type ' String' with cardinality of [0..1]

This attribute is used to represent the user role name, if specified.

Attribute 'Functional Role.roleCode' of type ' Code' with cardinality of [0..1]

The functional role may specify that the user is part of the healthcare team that is directly involved in the client's care. This attribute refers to a functional role assigned by an organization to computer users.

Association 'Functional Role.rolePermission' of type ' Permission' with cardinality of [*]

This association identifies the permissions that are associated with a functional role.

«Role» Class: Grantee

This class is used to designate who/what has been delegated a specific right. For example, in the case of substance abuse related information, under certain conditions the authority to grant, withhold, or withdraw consent to the disclosure of the information, is granted to the client. In another example, a Clearinghouse may act an agent/proxy for a provider organization as an intermediary and therefore can be a grantee as well.

Association 'Grantee.clearingHouse' of type ' ClearingHouse' with cardinality of [0..1]

Additional information about the grantee when the grantee is a clearinghouse.

Attribute 'Grantee.organizationalProvider' of type ' OrganizationalProvider' with cardinality of [1]

Additional information about the grantee when the grantee is an organizational provider.

«Act» Class: HealthRecord

This class is used to store a reference to the health record that is the subject of the consent rules in the Consent Directive.

Attribute 'HealthRecord.recordId' of type ' Id' with cardinality of [1]

The id of the record that is the target of a consent directive.

Attribute 'HealthRecord.recordLocation' of type ' String' with cardinality of [0..1]

The location of the record that is the target of a consent directive.

«Entity» Class: InformationObject

This class represents a reference to specific type of information object that may be referenced by a policy or consent directive (e.g., document, order, etc.). This information object refers to the types of objects that may be used in a permission.

Attribute 'InformationObject.category' of type ' Code' with cardinality of [0..1]

Coded attribute that identifies the type of object referenced in the policy.

«Act» Class: InformationReference

This class and it associations specify the attributes of the protected information referenced by a policy (e.g., IIHI).

Attribute 'InformationReference.category' of type ' Code' with cardinality of [0..1]

Information category (e.g. medication, allergies, laboratory).

Attribute 'InformationReference.confidentialityIndicator' of type ' Code' with cardinality of [0..1]

The confidentiality indicator is a coded attribute that assigns access controls on client health records based on the information or type of access.

Attribute 'InformationReference.dataIntegrity' of type ' Code' with cardinality of [*]

This attribute was renamed from the DAM, wherein it was named 'integrityCode'. That attribute had no definition.

Attribute 'InformationReference.informationCustodian' of type ' OrganizationalProvider' with cardinality of [*]

Identifies the organizational provider that is the custodian of the record in question.

Association 'InformationReference.informationObject' of type ' InformationObject' with cardinality of [*]

A reference to specific type of information object that may be referenced by a policy or consent directive (e.g., document, order, etc.).

Attribute 'InformationReference.informationRecipient' of type ' OrganizationalProvider' with cardinality of [*]

Identifies the organizational provider that is the intended recipient of the record in question.

Association 'InformationReference.relatedCondition' of type ' ClinicalCondition' with cardinality of [*]

The health condition(s) associated with the policy. Conditions when specified, are coded concepts expressed in a standard vocabulary (e.g., LOINC, SNOMED CT, etc.). These may include indications of 'substance abuse' or 'HIV-related' illnesses, etc. An obligationCode may be implemented as a 'condition'.

Attribute 'InformationReference.sensitivity' of type ' Code' with cardinality of [0..1]

Coded attribute that describes the sensitivity of a user or information artifact. Sensitivity is a characteristic of a resource which implies its value or importance, and may include its vulnerability [ISO 7498-2:1989]. Sensitivity may be associated with a user or information artifact.

Association 'InformationReference.subjectOfRecord' of type ' SubjectOfRecord' with cardinality of [0..1]

This class represents the patient or population that is the subject of the record in question.

«Act» Class: 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 fully describe a patient's access control preferences. In some cases an obligation policy may be used to indicate that the receiver of an information object may not be allowed to re-disclose it or persist that information object indefinitely. According to ISO 22600-2, ObligationPolicy instances 'are event-triggered and define actions to be performed by manager agent'.

Attribute 'ObligationPolicy.eventCode' of type ' Code' with cardinality of [*]

This attribute identifies the action required before completing the step in the workflow. We assume it is coded concept but in today's implementations it's primarily an ad-hoc rule reference (e.g., the name of a data base stored procedure). 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 an audit record be created.

«Act» Class: Operation

This abstract class specifies the permission that is assigned by the consenter to specific users of client health record information. The permission may control collection, access, use, or disclosure of a specific type of protected information (including IIHI). Note that this class was named 'OperationType' in the original DAM.

Attribute 'Operation.operationCategory' of type ' Code' with cardinality of [0..1]

This attribute identifies the operation that is either allowed or prohibited by the permission. Note that this property was named 'OperationCode' in the original DAM.

«Role» Class: PatientITUser

This class represents additional properties of the Patient when communicating with them electronically. This class was called simply 'Patient' in the HL7 Security and Privacy DAM, the definition of which is: 'This class is intended to capture the properties of a Consenter/Client or 'Patient'. See 'Actors' specified in the Use Case Analysis for additional detail. A consenter may be the person whose preferences it represents or their designated Substitute Decision Maker (SDM).'

Attribute 'PatientITUser.sharedSecret' of type ' String' with cardinality of [1]

This keyword/shared secret may be used by a patient to provide temporary access to their electronic health records. This attribute is required to support use case P.12 originated in Canada.

«Act» Class: Permission

This class corresponds to a Role-Based Access Control (RBAC) permission. It specifies an information object and action/operation allowed on that object. A permission contains one operation and precisely one information reference.

Attribute 'Permission.id' of type ' Id' with cardinality of [1]

This attribute is used to specify the unique identifier of the permission.

Association 'Permission.informationObject' of type ' InformationObject' with cardinality of [1]

This association identifies the information resources specified by a permission.

Association 'Permission.operationType' of type ' Operation' with cardinality of [1]

This association identifies the action or operation that is specified by a permission.

«Act» Class: PermissionCatalog

The permission catalog specifies a set of standard permissions. The permission catalog is the subject of separate HL7 standards. This reference is intended to show it relates to the rest of the information classes required to support the use cases.

Association 'PermissionCatalog.permission' of type ' Permission' with cardinality of [1..*]

A Role-Based Access Control (RBAC) permission. It specifies an information object and action/operation allowed on that object. A permission contains one operation and precisely one information reference.

Attribute 'PermissionCatalog.status' of type ' Code' with cardinality of [1]

Identifies the current state of the Permission. The state should correspond to the HL7 Act State

machine.

«Act» Class: Policy

This is the abstract class from which all concrete policy classes in this model are derived and instantiated. Because this class is abstract, it cannot be instantiated as a security policy for healthcare, however, it specifies the properties reused by all policies. ISO 22600-2 specifies a policy as 'set of legal, political, organizational, functional and technical obligations for communication and cooperation'.

Association 'Policy.authority' of type ' Authority' with cardinality of [*]

This is an association to the Authority that issued the policy.

Attribute 'Policy.description' of type ' String' with cardinality of [1]

This attribute specifies the narrative description of the policy.

Attribute 'Policy.effectiveTime' of type ' TimeInterval' with cardinality of [1]

This attribute specifies the period of time (e.g., start date, end date) during which the privacy policy described by ePolicy is in effect.

Attribute 'Policy.id' of type ' Id' with cardinality of [1]

Uniquely identifies the policy

Attribute 'Policy.name' of type ' String' with cardinality of [1]

A human discernible name for the policy

Association 'Policy.securityRole' of type ' SecurityRole' with cardinality of [*]

ISO-22600 specifies a role as 'set of competences and/or performances which is associated with a task'. A role is a specialization of CompositePolicy that define a group of policies (authorization, obligation, delegation and refrain policies).

Attribute 'Policy.status' of type ' Code' with cardinality of [1]

This attribute indicates whether the policy is active or not

Attribute 'Policy.uri' of type ' String' with cardinality of [1]

The location of published policy.

«Act» Class: PolicyProgramSource

Specifies the source of payment for the healthcare services documented by electronic health records. In order to meet specific privacy policy needs, it is necessary to specify if the information protected by the rule was produced through public healthcare or other type of insurance.

Attribute 'PolicyProgramSource.policyCategory' of type ' Code' with cardinality of [1]

The HL7 DAM contains two subclasses to illustrate the type of security/privacy policies that are inherent from the healthcare payment source. Those two subclasses are examples of many potential kinds of policies, and would be 'fleshed out' in the terminology referenced by this code.

«Act» Class: PrivacyPolicy

This is the main/focal class for electronic privacy policies. It contains a set of rules that are intended to be enforced by security systems and are used as the basis for client consent directives.

Association 'PrivacyPolicy.authority' of type ' Authority' with cardinality of [*]

This is an association to the Authority that issued the policy.

Attribute 'PrivacyPolicy.description' of type ' String' with cardinality of [0..1]

This attribute is a narrative description of the privacy policy.

Association 'PrivacyPolicy.grantee' of type ' Grantee' with cardinality of [*]

Designates who/what has been delegated a specific right.

Attribute 'PrivacyPolicy.policyId' of type ' Id' with cardinality of [1]

This attribute specifies the unique identifier of for a privacy policy.

Association 'PrivacyPolicy.privacyRuleList' of type ' PrivacyRuleList' with cardinality of [*]

A list of zero or more privacy rules applicable to this consent directive. A privacy rule specifies the permission allowed to a user type by the consenter for a specific type of information. The person consenting may be either the subject of the record or a designated Substitute Decision Maker. One or more consent rules comprise a consent directive or privacy policy.

«Act» Class: PrivacyRule

A privacy or consent rule specifies the permission allowed to a user type by the consenter for a specific type of information. The person consenting may be either the subject of the record or a designated Substitute Decision Maker. One or more consent rules comprise a consent directive or privacy policy.

Attribute 'PrivacyRule.effectiveTime' of type ' PointInTime' with cardinality of [1]

This attribute specifies the date/time when the Privacy Policy comes into effect.

Attribute 'PrivacyRule.enablesOperation' of type ' Boolean' with cardinality of [1]

Enables the operation (e.g., disclosure) or disables it depending on its value.

Association 'PrivacyRule.includedRole' of type ' UserRole' with cardinality of [*]

Identifies a particular the role of a user of a computer system that is referenced by the Privacy Rule.

Association 'PrivacyRule.informationType' of type ' InformationReference' with cardinality of [*]

Identifies the type of protected information referenced by the Privacy Rule.

Attribute 'PrivacyRule.obligationCode' of type ' Code' with cardinality of [0..1]

This coded attribute specifies a pre-defined obligation associated with a policy or consent. The Obligation Code is an Act.Code

Association 'PrivacyRule.operation' of type ' Operation' with cardinality of [1..*]

Identifies the type of operation (i.e., collection, access, use, or disclosure) of a specific type of protected information referenced by the Privacy Rule.

Attribute 'PrivacyRule.purpose' of type ' Code' with cardinality of [0..1]

This attribute is used to specify the purpose to permit a specific type of action/operation according to the policy. Example: TREATMENT The PurposeCode is an Act.ReasonCode

«ActRelationship» Class: PrivacyRuleList

An Act Relationship which describes the sequence in which Privacy Rules are to be processed as part of a Privacy Policy or a Consent Directive.

Association 'PrivacyRuleList.privacyRule' of type ' PrivacyRule' with cardinality of [1]

A privacy or consent rule specifies the permission allowed to a user type by the consenter for a specific type of information. The person consenting may be either the subject of the record or a designated Substitute Decision Maker. One or more consent rules comprise a consent directive or privacy policy.

Attribute 'PrivacyRuleList.sequenceNumber' of type ' Integer' with cardinality of [1]

This attribute specifies the sequence of a specific consent directive in the Consent Directive set.

«Act» Class: PublishedConsent

This specialization of the ConsentDirective class is used to describe a consent directive published to a registry. If a client’s consent directive is published, a URL/URI is made available for reference. The client may use this URI to allow providers access to the consent directive created by the consenter.

Attribute 'PublishedConsent.uri' of type ' String' with cardinality of [1]

If a specific consent directive (for a client) is published, this attribute provides the means to locate and download the consent directive from a registry.

«Act» Class: PublishedPrivacyPolicy

This class encapsulates the location of a human-readable version of the Electronic Privacy Policy. The human-readable version is accessible to any authorized system and user via the supplied URI.

Attribute 'PublishedPrivacyPolicy.uri' of type ' String' with cardinality of [0..1]

The location of published policy.

«Act» Class: 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 “BasicPolicy” class. It does not have any additional attributes but implies a different behavior. ISO 22600-2 species that a RefrainPolicy 'defines actions the subjects must refrain from performing'.

«Role» Class: SecurityRole

ISO-22600 specifies a role as 'set of competences and/or performances which is associated with a task'. A role is a specialization of CompositePolicy that define a group of policies (authorization, obligation, delegation and refrain policies).

Attribute 'SecurityRole.authorityIdentifierName' of type ' String' with cardinality of [1]

This attribute is defined by ISO 22600-2 as 'String'.

Attribute 'SecurityRole.description' of type ' String' with cardinality of [1]

This attribute is defined by ISO 22600-2 as 'CodedSimpleValue'.

Attribute 'SecurityRole.instanceIdentifier' of type ' Id' with cardinality of [1]

This is the role_identifier property in the security DAM. The definition of that property is 'This attribute is defined by ISO 22600-2 as 'Set of InstanceIndentifier'.' WE RENAMED THIS. WAS THIS OK TO DO????

Attribute 'SecurityRole.name' of type ' Code' with cardinality of [1]

This attribute is defined by ISO 22600-2 as 'CodedSimpleValue'.

Attribute 'SecurityRole.objectIdentifier' of type ' Id' with cardinality of [1]

This is the role_identifier_ID property in the Security DAM. The definition of that property is 'This attribute is defined by ISO 22600-2 as 'ISO ObjectIdentifier'.' WE RENAMED THIS. WAS THIS OK TO DO????

Association 'SecurityRole.userIdentity' of type ' UserIdentity' with cardinality of [1]

Specifies the user identification attributes.

«choiceGroup, Role» Class: SubjectOfRecord

This class represents the type of subject of record: patient or population.

Attribute 'SubjectOfRecord.patient' of type ' Person' with cardinality of [1]

Captures the properties of a Consenter/Client or 'Patient'. See 'Actors' specified in the Use Case Analysis for additional detail. A consenter may be the person whose preferences it represents or their designated Substitute Decision Maker (SDM).

Attribute 'SubjectOfRecord.population' of type ' Population' with cardinality of [1]

Specifies that the target of a policy may be an entire population. This class may be used to specify a privacy policy that applies to a specific group or population.

«Role» Class: UserIdentity

This class is used to specify the user identification attributes. Note that the user here is typically a provider.

Attribute 'UserIdentity.id' of type ' Id' with cardinality of [1]

This attribute is used to represent the user's identifier. Note that the user here is typically a provider.

Association 'UserIdentity.location' of type ' WorkstationLocation' with cardinality of [1]

This association is used to specify the provider's location when using or requesting IIHI.

Attribute 'UserIdentity.name' of type ' String' with cardinality of [1]

This attribute specifies the user's name. Note that the user here is typically a provider.

Association 'UserIdentity.securityRole' of type ' SecurityRole' with cardinality of [1]

ISO-22600 specifies a role as 'set of competences and/or performances which is associated with a task'. A role is a specialization of CompositePolicy that define a group of policies (authorization, obligation, delegation and refrain policies).

«Role» Class: UserRole

This class is used to specify the role of a user of a computer system. The role is typically associated with the Information Requester and specifies what capabilities are available to a specific type of computer user (i.e., in the Windows operating system, a user may have the role of Administrator which enables the

capability to add new users).

Attribute 'UserRole.allowedSensitivity' of type ' Code' with cardinality of [0..1]

Coded attribute that describes the level sensitivity of the protected information (including IIHI) that the user may access or use. Sensitivity is a characteristic of a resource which implies its value or importance.

Association 'UserRole.functional Role' of type ' Functional Role' with cardinality of [*]

This attribute refers to a coded structural role specified by an external coding system.

Attribute 'UserRole.name' of type ' String' with cardinality of [0..1]

This attribute is used to specify the role name, if available.

Attribute 'UserRole.organizationalProvider' of type ' OrganizationalProvider' with cardinality of [*]

The organizational provider with which the user is associated.

Attribute 'UserRole.roleCode' of type ' Code' with cardinality of [0..1]

This coded descriptor is used to specify a user role. It is an identifier of a 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. This attribute refers to a coded structural role specified by an external coding system.

Attribute 'UserRole.roleId' of type ' Id' with cardinality of [0..1]

This attribute is used to represent a unique role identifier.

Association 'UserRole.userIdentity' of type ' UserIdentity' with cardinality of [*]

A unique identifier for the role.

«Place» Class: WorkstationLocation

Access may be granted only to initiators on specific end-systems, workstations or terminals, or only to initiators in a specific physical location. This class is required to support user authorization as specified by the business requirements (use case S.1).

Attribute 'WorkstationLocation.organizationalProvider' of type ' OrganizationalProvider' with cardinality of [1]

The organizational provider with which the workstation is associated.