Nationwide Health Information Network (NHIN)

Access Consent Policies

Specification

V 1.0

1/29/2010

Contributors

Name	NHIO Represented	Organization
Richard Franck	NCHICA	IBM
Rich Kernan	ONC/NHIN	Deloitte
Jackie Key	ONC/NHIN	Deloitte
Tom Davidson	SSA	Lockheed Martin
John Moehrke	HITSP	GE Healthcare

Document Change History

Version	Date	Changed By	Items Changed Since Previous Version
0.1	8/9/2009	Richard Franck	Initial Draft
0.2	9/3/2009	Richard Franck	Included Home Community ID as an allowed attribute
0.3	9/23/2009	Richard Franck	Updates for HITSP TP30 conformance
0.4	10/15/20009	Richard Franck	Updates for consistency with emerging HITSP Document metadata standards
0.5	11/3/2009	Richard Franck	Corrected errors and omissions from XACML specifications
1.0	1/29/2010	Rich Kernan, Jackie Key	Applied consistent formatting/language.

Document Approval

Version	Date	Approved By	Role
1.0	1/25/2010	NHIN Technical Committee	

Table of Contents

1 Preface

1.1 Introduction

The Nationwide Health Information Network (NHIN) content specifications define types of content that may be exchanged by nodes across the NHIN to address particular use cases or business needs. Health Information Organizations (HIOs) which act as nodes on the NHIN are termed NHIOs. These content specifications make use of the NHIN's discovery and information exchange capabilities and rest upon a foundational set of messaging, security, and privacy services.

This document presents the NHIN specification for Access Consent Policy (ACP). An ACP is an element of an optional SAML statement described in the NHIN Authorization Framework specification. The purpose of this specification is to:

1. Describe the content and format of Access Consent policies covering the electronic exchange of health information between NHIOs, and
2. Describe how Access Consent policies may be exchanged among NHIOs

1.2 Intended Audience

The primary audiences for NHIN Specifications are the individuals responsible for implementing software solutions that realize these interfaces at Health Information Organizations (HIOs) who are, or seek to be, nodes on the NHIN network. This specification document is intended to provide an understanding of the context in which the service interface is meant to be used, the behavior of the interface, the Web Services Description Language (WSDLs) used to define the service, and any Extensible Markup Language (XML) schemas used to define the content.

1.3 Business Needs Supported by this Specification

A core requirement of the NHIN is for consumers "to limit the type of data that may be available to any or selected providers."[1] This specification provides the first necessary step to facilitate this requirement: a standard language for expressing restrictions on access to health information.

Although the requirement to restrict access to and disclosure of health information is often described in the context of "consumers" (a term that is more broadly applicable than the term "patient", and is thus used in this specification), other types of users may also have the need to restrict access to health information. For example:

1. An NHIO that operates within a state may need to implement restrictions on access to health information as required by that state's laws.
2. A physician may wish to restrict access to newly created health information by patients until he/she has the opportunity to review the information for accuracy or for any health concerns that he/she wishes to discuss with the patient.

This specification may be used to describe these kinds of restrictions, in addition to those created and adopted by consumers.

1.3.1 Sample Scenario for Use

There are likely to be a number of scenarios that will be able to take advantage of this specification. The one described here should be considered as an example.

[1] Gartner Report, "Summary of the NHIN Prototype Architecture Contracts", Annex 4

A consumer moves to a new city and establishes themselves as a patient with a healthcare provider who participates in an NHIO. As part of establishing their identity within the NHIO, certain Access Consent policies are established as applying to this consumer. Those policies would permit the consumer's new healthcare provider to retrieve clinical information held by their previous healthcare providers.

When the new healthcare provider attempts to retrieve existing clinical information through the NHIN using the "Query for Documents" transaction, the NHIO may indicate (using a mechanism defined in the NHIN Authorization Framework specification) the Policy ID of an Access Consent policy that the requesting NHIO believes would be germane to the responding NHIO. Using the transactions and Access Consent policy formats defined in this specification, the responding NHIO initiates a Query for Documents and subsequent Retrieve Document transaction to retrieve the Access Consent policy and apply that policy in deciding whether to permit the original "Query for Documents" request.

1.4 Referenced Documents and Standards

The following documents and standards were referenced during the development of this specification. Deviations from or constraints upon these standards are identified below.

1) **Org/SDO name:** HITSP

   Reference # / Spec Name: TP-20 / Access Control Transaction Package

   Version #: v1.4

   Underlying Specs:

   NHIN Deviations or Constraints:

   Link: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=2&PrefixNumeric=20

2) **Org/SDO name:** HITSP

   Reference # / Spec Name: TP-30/ Manage Consent Directives Transaction Package

   Version #: v1.3

   NHIN Deviations or Constraints: This specification extends this capability to allow the transactions defined in TP30 to be used to exchange Access Consent Policies formatted as XACML, using metadata defined in this specification. Please see section 2.2 "Transaction Standard" for more details.

   Underlying Specs:

   - IHE ITI TF Supplement XCA TI (2009-8-10)
   - IHE ITI TF Vol. 1 & 2a, 2b, 2x, 3 Revision 6.0 (2009-8-10)
   - IHE Basic Patient Privacy Consents (BPPC) profile

   Link: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=2&PrefixNumeric=30

3) **Org/SDO name:** HITSP

   Reference # / Spec Name: C80/ Clinical Document and Message Terminology Component

   Version #: v1.2

NHIN Deviations or Constraints:

Underlying Specs:

Link: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=80

4) **Org/SDO name:** OASIS

Reference # / Spec Name: eXtended Access Control Markup Language (XACML) core

Version #: v 2.0

NHIN Deviations or Constraints: The XACML standard upon which this specification is based is designed to be extended, through identified extension points. The extensions described in this specification are consistent with the intended use of those extension points.

Constraints on XACML identified in this document are:

- Only the attribute types, data types, and match functions identified in this document may be used to specify an NHIN Access Consent Policy.
- For Access Consent policies that are intended to apply to a particular consumer (rather than generically apply to one or more consumers that may choose to adopt a policy) those policies must have a Target element (an attribute of the Policy, not its rules) that identifies one and only one consumer to whom the policy applies.

Underlying Specs:

Link:

http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

5) **Org/SDO name:** OASIS

Reference # / Spec Name: Cross-Enterprise Security and Privacy Authorization Profile of XACML

Version #: Committee Draft 04 (July 15, 2009)

NHIN Deviations or Constraints:

Underlying Specs:

Link:

http://www.oasis-open.org/committees/download.php/33395/xacml-xspa-1%200-cd04.doc

6) **Org/SDO name:** OASIS

Reference # / Spec Name: Core and Hierarchical Role Based Access Control (RBAC) Profile of XACML

Version #: v 2.0

NHIN Deviations or Constraints:

Underlying Specs:

Link:

http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf

1.5 Relationship to Other NHIN Specifications

This specification is related to other NHIN specifications as described below:

- **Authorization Framework** – defines the exchange of metadata used to characterize each NHIN request. The purpose of that exchange is to provide the responder with the information needed to make an authorization decision for the requested function. Each initiating message must convey information regarding end user attributes and authentication using SAML 2.0 assertions. The NHIN Authorization Framework specification defines a SAML assertion that can indicate a Policy ID that one NHIO may wish to retrieve from another NHIO.
- **Messaging Platform –** specifies a base set of messaging standards and web service protocols which must be implemented by each NHIN node and applies to all transactions. All NHIN inter-nodal messages are SOAP messages over HTTP using web services, must be encrypted and digitally signed.

Together, the Messaging Platform and the Authorization Framework define the foundational messaging, security and privacy mechanisms for the NHIN.

The following Query for Documents and Retrieve Documents services describe transactions that must be used when one NHIO wishes to retrieve an Access Consent Policy from another NHIO.

- **Query for Documents** – allows an initiating NHIN node to request a patient-specific list of available documents from a responding node using the Patient ID obtained via a prior Patient Discovery transaction. It represents the second of three steps in the typical NHIN Query/Retrieve information exchange pattern.
- **Retrieve Documents** – allows an initiating NHIN node to retrieve specific documents from a responding node using the Document Reference IDs obtained via a prior Query for Documents transaction. It represents the final of the three steps in the typical NHIN Query/Retrieve information exchange pattern.

2 Interface Definition

This specification provides a standard language for expressing restrictions on access to health information. These restrictions are also known as Access Consent Policies.

Access Consent Policies may be “off-the-shelf” policies that are adopted by or apply to a consumer, or they may be policies that are customized by a consumer to grant or deny access to specific types of information by specific types of users. Access Consent policies may also be created by users other than consumers; for example, physicians may create policies that restrict access to health information they create.

2.1 Definitions

Definitions are provided below for key terminology used throughout this specification:

- **Subject:** In the domain of access control, the term “subject” refers to the person about whom access restrictions apply – that is, the person requesting access to healthcare information. In this specification, the term “**user**” is used instead. Certain attributes defined in this specification contain the word “subject” as part of the attribute name, since these attributes are defined by XACML and carry the meaning (that is, the meaning of “user”) as defined by XACML.
- **Document:** The term “**document**” has the same meaning as in the NHIO Query for Documents and NHIO Retrieve Documents specifications: it refers to healthcare-related data about a consumer in the format that it is made available by an NHIO. It is important to note that a

document is the unit of exchange in the NHIN, and restrictions on access to clinical data are at the level of documents. Differential access restrictions cannot be applied to content within a document.

- **Access Consent Policy:** A set of rules (or Access Consent Directives) that control access to information or an operation. (This corresponds to a "Policy" in XACML.)
- **Access Consent Directive:** A single rule that restricts or grants access to a healthcare information. (This corresponds to a "Rule" in XACML.)
- **Consumer Preferences:** This term is preferred for referring to consumer empowerment tools that may cover a broad variety of use cases, including access consent, inter-NHIO exchange preferences, and third party authorizations. This term includes the notion of "**access consent**" as defined in the HITSP TP30 (Manage Consent Directives) transaction package, but also includes other kinds of consumer preferences, such as an advanced directive or dietary restriction.

2.2 Design Principles and Assumptions

The following assumptions or design principles underlie this specification:

- How an NHIO determines which other NHIOs to direct queries is not specified. This is a local NHIO decision. This specification does not include the business rules which define how an NHIO applies the consumer preferences during network exchange activities. This may be separately addressed by NHIO-specific business rules and/or NHIN Cooperative Operating Procedures.
- This specification does **not** describe:
  - The means by which an Access Consent policy is authored, or by which policies are managed over time.
  - The means by which consumers express their desire to "adopt" a particular policy to govern the exchange of their own health information.
  - The means by which an NHIO records which Access Consent policies apply to which patients or which pieces of health information.
  - The means by which a consumer may delegate to others the right to author and/or adopt an Access Consent policy on the consumer's behalf.
  - The circumstances under which an NHIO may choose to make an Access Consent policy that has been adopted by a consumer available to another NHIO.
  - The Access Consent policies that may or should be applied to the exchange of policies among NHIOs.
  - How an NHIO should reconcile potentially conflicting Access Consent policies that it retrieves from another NHIO with others that it may hold.

  Some of the items above are or will be specified in other HITSP or NHIN specifications. Other items on this list are implementation choices specific to an NHIO or other organization. Still others are matters that may be determined by the procedures or regulations that govern an NHIO or the NHIN

2.3 Transaction Standard

The format used by this specification for specifying restrictions on access to healthcare information is eXtended Access Control Markup Language (XACML), an OASIS standard. The specification adopts attributes defined by the "Cross-Enterprise Security and Privacy Authorization Profile of XACML", a draft OASIS standard. This specification adopts the mechanisms described in HITSP TP30, "Manage Consent Directives Transaction Package", for the exchange of Access Consent Policies among NHIOs.

This specification covers only a portion of the complete Access Control infrastructure described by HITSP/TP20, "Access Control Transaction Package." In the terms used in TP20, the capability of the NHIO that may send and receive Consumer Preferences Profiles using the transactions defined in this document is the "Service Provider Access Control Service."

TP20 implies the need for a complete vocabulary to describe Access Consent policies using XACML; that vocabulary is provided in this specification. This specification also incorporates some of the vocabulary for Role-based Access Control from the XACML-RBAC specification. In terms used by XACML, this specification defines the precise format and content of Policies that would be used by a "Policy Decision Point" to make a "permit or deny" decision about a particular request. This specification does not imply that an NHIO must implement the architecture implied by XACML (using Policy Enforcement Point and Policy Decision Point).

This specification adopts the mechanism for the exchange of Access Consent policies described by HITSP TP30, "Manage Consent Directives Transaction Package." TP30 describes, in Section 2.1.3.2, the use of XDS "Query Registry" and "Retrieve Document Set" by a Consent Directive Requester actor to retrieve Access Consent Policies. Other portions of TP30 imply that TP30 also allows the use of the corresponding transactions as defined by the IHE Cross-Community Access (XCA) profile, which are used between two HIOs. It is this use, using the "Cross Gateway Query" and "Cross Gateway Retrieve" transactions, as scoped in the NHIN Query for Documents Service Interface Specification and NHIN Retrieve Documents Service Interface Specification, that are adopted here.

HITSP TP30, in adopting the IHE Basic Patient Privacy Consents (BPPC) profile, is limited to Access Consent policies in the form of a CDA document, which does not currently have an access consent language. This specification extends this capability to allow the transactions defined in TP30 to be used to exchange Access Consent Policies formatted as XACML, using metadata defined in this specification. Documents formatted as described in BPPC (that is, as CDA documents) may be exchanged over the NHIN as well using the transactions adopted by this specification.

Further, this specification does not preclude the exchange of other Access Consent Policy document formats that may be defined in the future. However, at this time, the only computable format defined for Access Consent policies for the NHIN is the XACML format defined in Section 2.4 of this document.

HITSP C80 describes vocabulary to be used in various clinical documents, and includes a section describing the document metadata that is to be used in exchanging these documents through XDS document sharing protocols. This specification adopts the use of those document sharing protocols (as described in HITSP TP30), and consequently, adopts the vocabularies that are used for the document metadata (as described in C80). Please see Section 3.2, "Document Metadata for the exchange of NHIN Access Consent Policies", for more information regarding these values as adopted from HITSP C80.

3 NHIN Exchange of Access Consent Policies

This specification adopts the NHIN "Query for Documents" and "Retrieve Documents" specifications for the exchange of Access Consent Policies. This mechanism is the same as described in HITSP TP30, except that HITSP TP30 describes the exchange among entities within an HIO, while implying that the same scenario can occur using the cross-community (that is, HIO to HIO) transactions defined by IHE XCA (and adopted by the NHIN specifications). This scenario is depicted in Figure 2.1.3.2-1, "Request Consent Directive," of HITSP TP30 (version 1.2).

Figure 1 depicts the same exchange in the context of the NHIN.

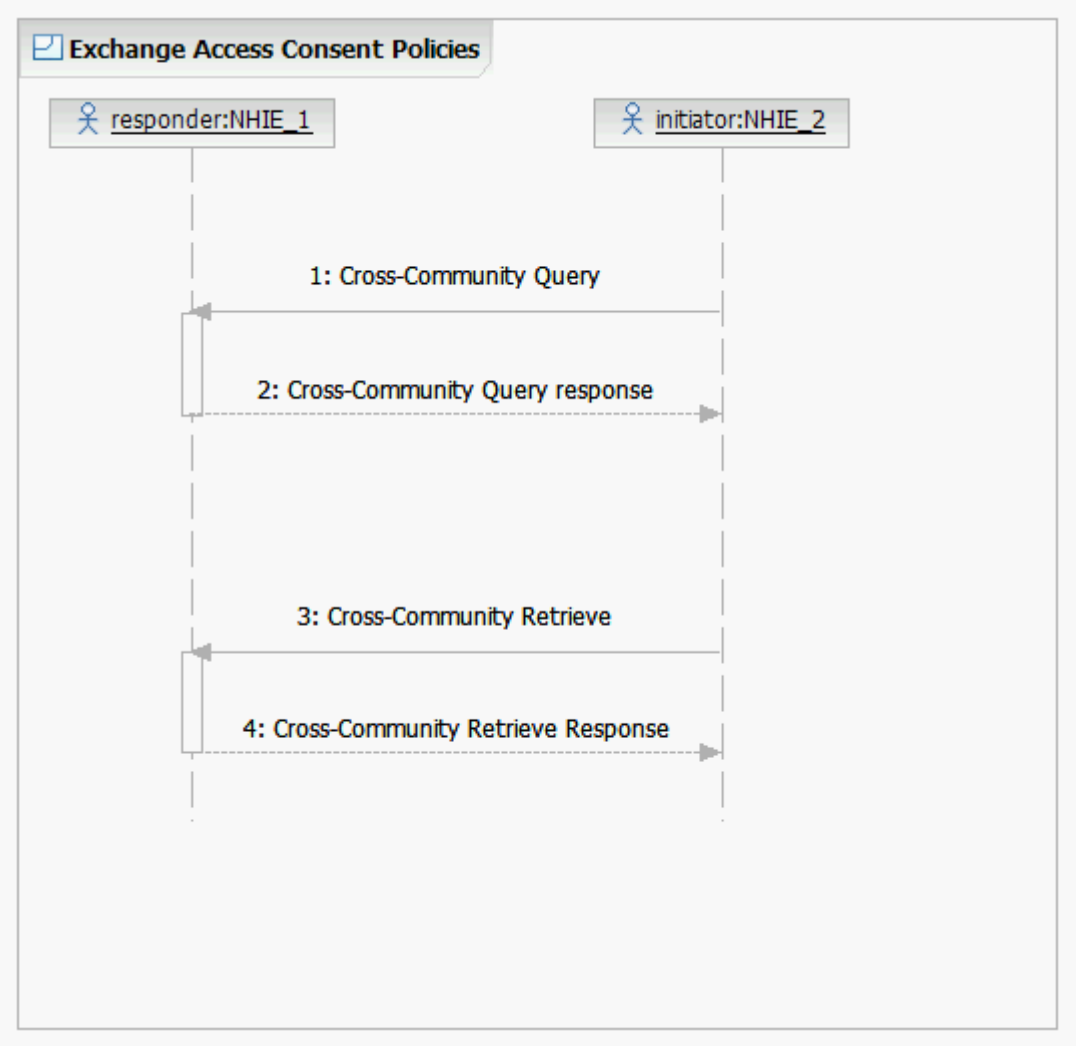

Figure 1 : Exchange Access Consent Policies sequence diagram

The NHIN Authorization Framework specification describes one scenario in which an NHIO may choose to query and/or retrieve Access Consent Policies from another NHIO, when a request carries an assertion that the requesting NHIO has an Access Consent Policy that may apply to the transaction. There may be other scenarios in which NHIOs may want to exchange Access Consent Policies, and this specification is not limited to any particular scenarios.

There may be cases where the Cross-Community Query is required, but not the retrieve. This would be the case when the query returns an Access Consent Policy identifier that is already known by the initiator. In that case, the initiator can apply the policy in the context of the patient who was the subject of the query without having to retrieve the policy.

3.1 Content Semantics

The Access Consent policy document is an XML document following the XACML standard. It's top level element is <Policy>, in the XACML namespace, "urn:oasis:names:tc:xacml:2.0:policy:schema:os".

This specification allows Access Consent policies to apply Access Consent Directives against the following attributes:

- The consumer (patient) ID.

- The Web Services operation, or "Action", that is making the request for healthcare information, that is, one or more transactions defined by the NHIN Interface Specifications.
- The role of the user requesting access.
- The organization of the user requesting access
- The Document Class of the document being requested
- The Unique Document ID of the document being requested
- The confidentiality code applied to the document being requested
- The start date/end date of the access consent directive
- The unique user ID of the user requesting access. (Currently, NHIOs will not have the capability to implement a restriction against a specific user, since there is no model for exchanging user identities in the NHIN Cooperative specifications. However, this specification includes the capability because it is an anticipated future capability, and imposes almost no additional complexity on the specification.)
- The Purpose for Use of the operation, specified using the coded vocabulary defined in the NHIN Authorization Framework.

None of these attributes is required. When any attribute is omitted, it is interpreted as applying to any value of that attribute. A meaningful policy will have at least one attribute, but no one attribute is required for every meaningful combination.

The following table lists these attributes, the Attribute Type that represents the attribute in XACML, and the identifier for the data type of the attribute.

Attribute	Attribute Type identifier	Data Type Identifier
Consumer (patient) ID	http://www.hhs.gov/healthit/nhin#subject-id	urn:hl7-org:v3#II
Action	urn:oasis:names:tc:xacml:1.0:action:action-id	http://www.w3.org/2001/XMLSchema#anyURI
User role	urn:oasis:names:tc:xacml:2.0:subject:role	http://www.w3.org/2001/XMLSchema#string
Organization ID	urn:oasis:names:tc:xspa:1.0:subject:organization-id	http://www.w3.org/2001/XMLSchema#anyURI
Home Community ID	http://www.hhs.gov/healthit/nhin#HomeCommunityId	http://www.w3.org/2001/XMLSchema#anyURI
Document Class	urn:oasis:names:tc:xspa:1.0:resource:hl7:type	http://www.w3.org/2001/XMLSchema#string
Unique Document ID	urn:oasis:names:tc:xacml:1.0:resource:resource-id	http://www.w3.org/2001/XMLSchema#string
Confidentiality Code	urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code	http://www.w3.org/2001/XMLSchema#string
Rule start date	http://www.hhs.gov/healthit/nhin#rule-start-date	http://www.w3.org/2001/XMLSchema#date
Rule end date	http://www.hhs.gov/healthit/nhin#rule-end-date	http://www.w3.org/2001/XMLSchema#date
User ID	urn:oasis:names:tc:xacml:1.0:subject:subject-id	urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name or urn:oasis:names:tc:xacml:1.0:data-type:x500Name
Purpose for Use	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	http://www.w3.org/2001/XMLSchema#string

The following table describes whether the attribute is a "Subject", "Action", "Resource", or "Environment" attribute as those terms are defined by XACML. This categorization determines how the attribute is represented in the XACML Policy document (in a <Subject>, <Action>, <Resource>, or <Environment> element within the policy target or policy rule). The table also describes the specific content requirements for each attribute.

Attribute	Attribute Type	Content Requirements
Consumer (patient) ID	Resource	The Attribute Value must be a child element “PatientId” in the urn:hl7-org:v3 namespace, with “root” and “extension” attributes. When specified, only one patient ID may be given in a single policy document, and it must appear as a descendent of <Target> element that is a direct child of the root <Policy> element. It may not appear as a descendent of a Rule.
Action	Action	The Web Services action to which this policy applies.
User role	Subject	A Role Code defined in the NHIN Authorization Framework specification. These are SNOMED CT codes
Organization ID	Subject	A unique identifier of the organization who the subject (user) is representing. The organization ID may be an Object Identifier (OID), using the urn format (that is, “urn:oid:” appended with the OID); or it may be a URL assigned to that organization.
Home Community ID	Subject	The unique Home Community ID of the NHIO that the subject (user) is initiating a request from. The Home Community ID must be an Object Identifier (OID), using the urn format (that is, “urn:oid:” appended with the OID).
Document Class	Resource	Must be a Document Class code defined in the NHIN document metadata specifications. These are LOINC codes.
Unique Document ID	Resource	As defined in IHE XDS.b profile.
Confidentiality Code	Resource	A Confidentiality code defined by the HL7 V3 “Confidentiality” code system.
Rule start date	Environment	In XML date format.
Rule end date	Environment	In XML date format.
User ID	Subject	Must be specified as either an e-mail address (rfc822Name) or an X500 name (x500Name).
Purpose for Use	Subject	A Purpose for Use code defined in the NHIN Authorization Framework.

Consistent with this list of attributes, the following “match functions” are required to evaluate the rules. The last item on this list is newly defined by this specification. No other match functions should be included in Consumer Preferences Profiles exchanged among NHIOs.

- urn:oasis:names:tc:xacml:1.0:function:string-equal
- urn:oasis:names:tc:xacml:1.0:function:date-greater-than-or-equal
- urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal
- urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match
- urn:oasis:names:tc:xacml:1.0:function:x500Name-match
- urn:oasis:names:tc:xacml:1.0:function:anyURI-equal
- http://www.hhs.gov/healthit/nhin/function#instance-identifier-equal . This function is defined to return true if both the “root” and “extension” attribute of the specified attribute value match the value provided in the request context, using a case-sensitive compare in the case of the “extension”.

The following rule-combining algorithms may be used in an Access Consent Policy under this specification:

- Deny-overrides
- Permit-overrides
- First-applicable

A set of example XACML Policy documents is found in Appendix A.

3.2 Document Metadata for the Exchange of NHIN Access Consent Policies

Table 1 lists the document metadata elements that must be used on Cross-Community Query transactions related to Access Consent Policies. Elements that are not listed should supply a value as

described in the IHE Technical Framework. These values are consistent with the emerging standards for document metadata found in HITSP C80[2].

Metadata Element	Value
authorPerson or authorInstitution	One of these elements should be used to provide information about the author of the Access Consent Policy.
authorRole	A value may be provided using one of the values from the NHIN Authorization Framework user role value set.
classCode	Must use the LOINC code `57017-6` to represent Access Consent Policy. The description for this code is "Privacy Policy".
eventCodeList	Populate with the value of the Policy Identifier as described in IHE BPPC. This value is an OID, which must be prefixed with "urn:oid:". Since OIDs do not have a coding scheme, use the value "N/A" in the coding scheme slot.
formatCode	For a XACML formatted document, use the value - `urn:nhin:names:acp:XACML` Other formats defined by TP30/BPPC may be used for documents that follow those formats: - `urn:ihe:iti:bppc:2007` - `urn:ihe:iti:bppc-sd:2007`
healthcareFacilityTypeCode	Use the SNOMED CT value 385432009, "Not Applicable", since policy documents do not document a clinical encounter.
mimeType	Use the value `text/xml` for a XACML coded document; or other mime type as appropriate.
practiceSettingCode	Use the SNOMED CT value 385432009, "Not Applicable", since policy documents do not document a clinical encounter.
serviceStartTime / serviceStopTime	If the policy applies for only a limited time, these elements may be used to provide the time range. Lack of serviceStartTime/serviceStopTime must be interpreted as meaning that the policy is not time limited.
typeCode	Must use the LOINC code `57017-6` to represent Access Consent Policy. The description for this code is "Privacy Policy". Other LOINC document codes may be used if LOINC defines more specific Access Consent Policy document types in the future.

Table 1 : Document metadata elements for Access Consent Policies

[Note: LOINC code 57017-6 has been defined by LOINC during 2009. It will be published in the 2009 version of LOINC. IHE intends to update the BPPC profile to use this code.]

[2] As of October, 2009, a draft of HITSP C80 has been produced with significant changes to the section on document metadata, and it is this draft that is being adopted by this specification. It is expected that HITSP will formally adopt and publish these changes sometime in early 2010.

Appendix A: Sample Policy Document

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    PolicyId="12345678-1234-1234-1234-123456781234"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
    <Description>Sample XACML policy for NHIN</Description>

<!-- The Target element at the Policy level identifies the subject to whom the Policy applies -->
    <Target>
        <Resources>
            <Resource>
                <ResourceMatch
         MatchId="http://www.hhs.gov/healthit/nhin/function#instance-identifier-equal">
                    <AttributeValue DataType="urn:hl7-org:v3#II" xmlns:hl7="urn:hl7-org:v3">
                        <hl7:PatientId root="2.16.840.1.113883.3.18.103" extension="00375"/>
                    </AttributeValue>
                    <ResourceAttributeDesignator
                         AttributeId="http://www.hhs.gov/healthit/nhin#subject-id"
                        DataType="urn:hl7-org:v3#II"/>
                </ResourceMatch>
            </Resource>
        </Resourcess>
        <Actions>
            <!-- This policy applies to all document query and document retrieve transactions -->
            <Action>
                <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        urn:ihe:iti:2007:CrossGatewayRetrieve
                    </AttributeValue>
                    <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:action"
                        DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </ActionMatch>
            </Action>
            <Action>
                <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        urn:ihe:iti:2007:CrossGatewayQuery
                    </AttributeValue>
                    <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:2.0:action"
                        DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </ActionMatch>
            </Action>
        </Actions>
    </Target>

    <Rule RuleId="133" Effect="Permit">
        <Description>Permit access to all documents to all physicians and nurses</Description>
        <Target>
            <Subjects>
                <Subject>
                    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <!-- coded value for physicians -->
                        <AttributeValue
           DataType="http://www.w3.org/2001/XMLSchema#string">112247003</AttributeValue>
                        <SubjectAttributeDesignator
                          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                          DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </SubjectMatch>
                </Subject>
                <Subject>
                    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <!-- coded value for nurses -->
                        <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">106292003</AttributeValue>
                        <SubjectAttributeDesignator
                          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                          DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

```
                </SubjectMatch>
            </Subject>
        </Subjects>
        <!-- since there is no Resource element, this rule applies to all resources -->
    </Target>
</Rule>

<Rule RuleId="134" Effect="Permit">
    <Description>Allow access Dentists and Dental Hygienists Access from the
       Happy Tooth dental practice to documents with "Normal"
       confidentiality for a defined time period.</Description>
    <Target>
        <Subjects>
            <Subject>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <!-- coded value for dentists -->
                    <AttributeValue
   DataType="http://www.w3.org/2001/XMLSchema#anyURI">106289002</AttributeValue>
                    <SubjectAttributeDesignator
                      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                      DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </SubjectMatch>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI"
                      >http://www.happytoothdental.com</AttributeValue>
                    <SubjectAttributeDesignator
                      AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
                      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </SubjectMatch>
            </Subject>
            <Subject>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <!-- coded value for dental hygienists -->
                    <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">26042002</AttributeValue>
                    <SubjectAttributeDesignator
                     AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                     DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </SubjectMatch>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <AttributeValue
                      DataType="http://www.w3.org/2001/XMLSchema#anyURI"
                      >http://www.happytoothdental.com</AttributeValue>
                    <SubjectAttributeDesignator
                      AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
                      DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </SubjectMatch>
            </Subject>
        </Subjects>
        <Resources>
            <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue
 DataType="http://www.w3.org/2001/XMLSchema#string">N</AttributeValue>
                    <ResourceAttributeDesignator
  AttributeId="urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code"
                       DataType="http://www.w3.org/2001/XMLSchema#string"/>
                </ResourceMatch>
            </Resource>
        </Resources>
        <Environments>
            <Environment>
<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:date-greather-than-or-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">2009-07-01</AttributeValue>
    <EnvironmentAttributeDesignator
      AttributeId="http://www.hhs.gov/healthit/nhin#rule-start-date"
      DataType="http://www.w3.org/2001/XMLSchema#date"/>
</EnvironmentMatch>
            </Environment>
            <Environment>
```

```
   <EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal">
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">2009-12-31</AttributeValue>
        <EnvironmentAttributeDesignator
           AttributeId="http://www.hhs.gov/healthit/nhin#rule-end-date"
           DataType="http://www.w3.org/2001/XMLSchema#date"/>
   </EnvironmentMatch>
               </Environment>
            </Environments>
        </Target>
    </Rule>

    <Rule RuleId="135" Effect="Deny">
        <Description>deny all access to documents.  Since this rule is last, it will
                     be selected if no other rule applies,
                      under the rule combining algorithm of first applicable.</Description>
        <Target/>
    </Rule>
</Policy>
```