Nationwide Health Information Network (NHIN)

Authorization Framework

Specification

V 2.0

1/29/2010

Contributors

Name	NHIO Represented	Organization
Richard Franck	NCHICA	IBM
Tony Mallia	Fed NHIO	VA
Victoria Vickers	Fed NHIO	FHA
Deborah Lafky		ONC
David Riley	FHA	FHA
Tom Davidson	SSA	SSA
Rich Kernan	ONC/NHIN	Deloitte
Jackie Key	ONC/NHIN	Deloitte
John Moehrke	HITSP	GE Healthcare

Document Change History

Version	Date	Changed By	Items Changed Since Previous Version
1.4	4/16/08	Tony Mallia, Richard Franck	
1.4.1	4/29/08	Deborah Lafky	Format, preparation for HITSP review
1.5	5/22/08	Tony Mallia, Richard Franck	Change User Role codes to SNOMED CT
1.6	7/22/2008	David L. Riley	Added Appendix A: SAML Rules and Appendix B: Sample Messages
1.7	10/07/08	Dave Riley Victoria Vickers	Integrated in decisions regarding ws-Security elements, <Issuer> and <Subject> elements, Role and PurposeForUse <AttributeValue> elements
1.8	11/18/2008	Richard Franck	Changes related to SSA Authorized Release of Information use case; editing and clean up
1.9	11/24/2008	Victoria Vickers	Addition of descriptions to support Digital Signatures
1.9.1	01/30/2009	David L. Riley	Minor edits to prepare for publication
1.9.2 [1]	8/11/2009	Richard Franck	Modified to be consistent with XSPA profile of SAML
1.9.21	9/3/2009	Richard Franck	Added attribute for Home Community ID
1.9.22	9/24/2009	Tom Davidson	Added XSPA attribute resource-id Change Subject Discovery to Patient Discovery Removed references to Audit Log Query Specification. Changes to Authorization Decision Statement attributes to support HITSP TP30. Removed references to SSA Use Case. SSA Use Case Implementation guide should refer to this specification.
1.9.23	11/3/2009	Tom Davidson, Richard Franck	fixed errors; noted deprecated attributes from Trial Implementation.
2.0	1/29/2010	Tom Davidson, Richard Franck, Rich Kernan Jackie Key	Added NPI attribute. Changed namespace for Authorization Decision Statement action. Applied consistent formatting/language and enhanced clarity.

Document Approval

Version	Date	Approved By	Role
1.6	10/6/2008	NHIN Cooperative Technical and Security Working Group	

[1] These unpublished draft versions have been re-numbered to conform to subsequently defined versioning conventions.

2.0	1/25/2010	NHIN Technical Committee	

Table of Contents

1 Preface

1.1 Introduction

The Nationwide Health Information Network (NHIN) Foundation specifications define the primary set of services and protocols needed to establish a messaging, security, and privacy foundation for the NHIN. It is upon this foundation that the functional set of NHIN web service interfaces operates.

This specification does not describe a web service interface. Instead, it defines the required exchange of information describing the initiator of a request between Health Information Organizations (HIOs) participating as nodes on the NHIN. The purpose of this information exchange is to enable a responding NHIO to evaluate the request based on the information contained in the initiating NHIOs assertions and its own local policies and permissions. This Authorization Framework specification is foundational to the NHIN and applies to every message.

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. HIOs which act as nodes on the NHIN are termed NHIOs. This specification document is intended to provide an understanding of the context in which the web 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

In order to evaluate a request sent by an initiating NHIN node, a responding NHIO must be supplied with a standard set of information which characterizes the initiator of the request. The NHIN Authorization Framework specification defines this information as well as the mechanism for its exchange.

Further, the Authorization Framework is required to support two of the NHIN's central design principles:

Local Autonomy – acknowledges that the decision to release information from one NHIN node to another is a local decision is governed by Federal and State regulations and local policies and permissions specific to the responding node. Given this principle, NHIN transactions must include information about the requestor (or sender, depending on whether it is a push or pull transaction) in order to enable the responding node to make a decision about whether to participate in the requested information exchange.

Local Accountability - each NHIN node is accountable for the accuracy of the information it provides to assist the decision making process embodied in the local autonomy principle. This includes end-user authentication assertions.

Together with the NHIN Messaging Platform, this specification is part of the NHIN's messaging, security, and privacy foundation. All other service interface specifications assume this foundation.

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:** OASIS

Reference # / Spec Name: Assertions and Protocols for Security Assertion Markup Language (SAML)

Version #: v2.0

Underlying Specs:

NHIN Deviations or Constraints:

Link: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

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

Reference # / Spec Name: Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare

Version #: v1.0

Underlying Specs:

NHIN Deviations or Constraints:

Link: http://www.oasis-open.org/committees/download.php/33396/saml-xspa-1%200-cd04.doc

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

Reference # / Spec Name: Authentication Context for Security Assertion Markup Language (SAML)

Version #: v2.0

Underlying Specs:

NHIN Deviations or Constraints:

Link: http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

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

Reference # / Spec Name: Web Services Security: SOAP Message Security

Version #: v1.1 (WS-Security 2004)

Underlying Specs:

NHIN Deviations or Constraints:

Link: http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

5) **Org/SDO name:** WS-I

Reference # / Spec Name: Security Profile

Version #: v1.1

Underlying Specs:

- Transport Layer Security v1.0

- XML Signature v1.0
- Web Services Description Language (WSDL) v1.1
- Symmetric Encryption Algorithm and Key Length AES 128-bit
- X.509 Token Profile v1.0
- Attachment Security v1.0

Link: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

1.5 Relationship to Other NHIN Specifications

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

- **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 with the Messaging Platform, the Authorization Framework defines the foundational messaging, security and privacy mechanisms for the NHIN.

The Authorization Framework is not specifically related as part of a transaction to the NHIN Discovery and Information Exchange Services. Rather, it describes the information which must accompany the requests enabled by each of these NHIN web services.

2 Framework Description

2.1 Definition

The Authorization Framework defines the exchange of metadata used to characterize the initiator of an NHIN request so that it may be evaluated by responding NHIOs in local authorization decisions.

Along with the Messaging Platform, this specification forms the NHIN's messaging, security, and privacy foundation. It employs SAML 2.0 assertions

The purpose of this 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.

Note that the term "subject" in SAML and XACML refers to the individual making the request. In this specification, the term "User" is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.

2.1.1 Request Definition

NHIN requests are defined by the applicable service interface, the interface operation, and the identity of the record target (unambiguous person identity in the responding NHIO, when known).

2.1.2 Identity of the Record Target

In most NHIN requests, Patient Discovery a notable exception, the record target is the unambiguous person identity in the responding NHIO. The assertion contained in the Authorization Framework declares that the initiating user is authorized by the initiating NHIO to access information about this person. It is also required for HIPAA Privacy Disclosure Accounting.

2.2 Design Principles and Assumptions

The following assumptions or design principles underlie this specification:

- All inter-node requests on the NHIN must utilize the Authorization Framework.
- There is not assumed to be Cross Provisioning of users between NHIOs
- The initiating NHIO is required to and is responsible for the authentication and authorization of its users. Refer to Local Accountability, as described in section 1.3 of this specification.
- The responding NHIO uses the information conveyed via the Authorization Framework to inform its local authorization decision. Refer to Local Autonomy, as described in section 1.3 of this specification.
- NHIO architectures are decoupled and externally opaque. While each NHIO must conform to the NHIN messaging, security, and privacy foundations for inter-NHIO transactions, internal security mechanisms and standards are to be defined by each NHIO.
- The initiating NHIO must include all REQUIRED attributes in each request. It is at the discretion of the receiving NHIO to decide which attributes to consider in it's local authorization decision
- The assertion attribute definitions specified in this document are not intended to be an exhaustive and restrictive list of attributes that may be specified in the SAML assertions. Additionally, this document recognizes that some integration profiles may have a need for custom assertion statements, and does not preclude their use.

2.3 Triggers

NHIN Authorization Framework is central to the messaging, security, and privacy foundation. All NHIN requests must conform to this specification.

2.4 Transaction Standard

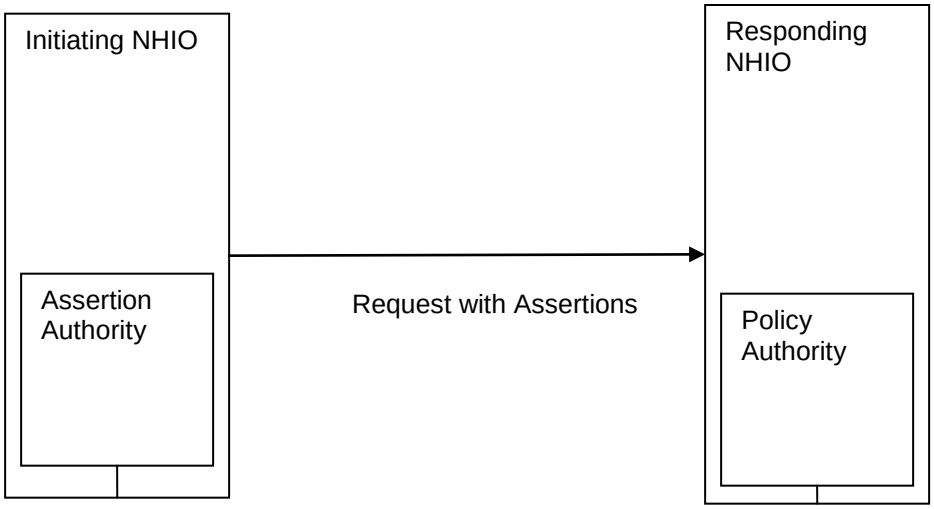
The NHIN Authorization Framework is based on the Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, the Authentication Context for SAML V2.0, the Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML for Healthcare Version 1.0 and the OASIS Web Services Security: SAML Token Profile 1.1 specifications .

3 Framework Definition

3.1 Interaction Behavior

According to the NHIN's local accountability principle, the initiating NHIO must determine if a local user is authorized to perform a given function; in this context, to make a specific request. If the request is authorized, the initiating NHIO attaches the user-centric assertions to the request.

The responding NHIO receives the request with the understanding that the initiating NHIO has locally authorized the user to make the request. However, according to the local autonomy principle, the decision to grant the request is that of the responding NHIO. The information needed to inform that decision is conveyed via SAML assertions.



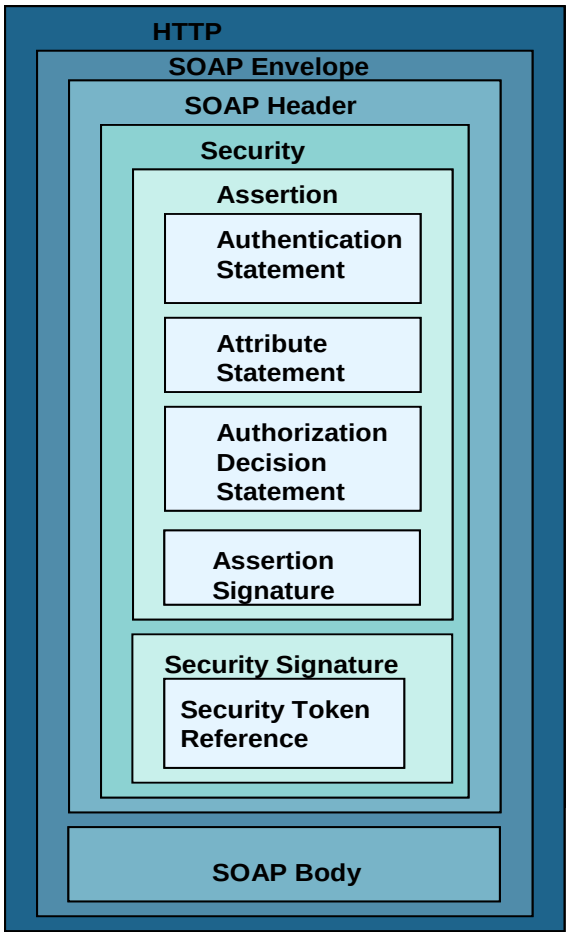
The responding NHIO receives the request with assertions and consults a local Policy Authority or Policy Enforcement Point (which could be a SAML authority) to establish whether it should perform the function. Assertions can convey information about methods used to authenticate the user, user attributes, and authorization decisions about whether users are allowed to access certain resources. A single assertion may contain several different internal statements about authentication, authorization, and attributes.[2]

[2] SAML v2.0

3.2 Specific NHIN Assertions

The following set of SAML assertions are designated as required or optional for all communications between NHIOs.[3]

Figure 1 depicts how the SAML header adopted here is carried within the <Security> element within the header of the SOAP envelope as defined by WS-Security.



Authorization Statement	
Element/Attribute	**Required/ Optional**
SAML:Assertion	R
Version	R
ID	R
IssueInstant	R
Issuer	R
Subject	R
AuthnStatement	R
AuthnContext	R
SubjectLocality	O
AuthnInstant	R
SessionIndex	O
AttributeStatement	R
subject-id	R
organization	R
organization-id	R
homeCommunityId	R
subject:role	R
purposeofuse	R
resource-id	O
NPI	O
Authorization Decision Statement	O
Action	R
Decision	R
Resource	R
Evidence	R
Assertion Signature	R
SignedInfo	R
SignatureValue	R
KeyInfo	R

Figure 1: Position of the SAML Assertion within the SOAP Header

3.2.1 Namespaces

Prefix	Namespace
ds	http://www.w3.org/2000/09/xmldsig#
S11	http://schemas.xmlsoap.org/soap/envelope/
S12	http://www.w3.org/2003/05/soap-envelope
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsse11	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
xenc	http://www.w3.org/2001/04/xmlenc#

Table 1: Common Namespaces used in SOAP Message Security

[3] Reference OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)

3.2.2 Timestamp

Each NHIN Request shall have a <wsse:Security> element which contains the entire SAML token. This is per the Web Services Security: SAML Token Profile 1.1 specification. Also as per the spec the <wsse:SecurityTokenReference> tags should also be present after the saml:Assertion.
The <wsse:Security> element will contain a <wsu:Timestamp> element to provide the ability to express the creation and expiration times of the message. The ID attribute provides the ability to reference this timestamp in an XML Signature. The <wsu:Timestamp> element will contain both a <wsu:Created> and an <wsu:Expires> element to express the temporal security semantics. All times must be in UTC format as specified by the XML Schema type (dateTime). The ordering of the elements must have <wsu:Created> followed by <wsu:Expires>. The following illustrates the syntax of this element:

```
<wsu:Timestamp wsu:Id="_1">
  <wsu:Created>2008-10-07T13:00:34Z</wsu:Created>
  <wsu:Expires>2008-10-07T13:05:34Z</wsu:Expires>
</wsu:Timestamp>
```

In order to prevent the manipulation of the stated range of valid times for the given message by a third party in a replay attack, the security timestamp is digitally signed. The <wsse:Security> element will contain a <ds:Signature> element which specifies the algorithms and transformations applied during the signing process. This element must conform to the XML Signature specification, which is described in section 3.3.4. However, in this case, enclosed within the <ds:KeyInfo> element of the <ds:Signature> is the <wsse:SecurityTokenReference> element. This element provides the ability to reference the SAML Assertion.

The wsse11:TokenType attribute is used to declare the type of the referenced token for SAML v2.0. This is defined to be: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0. The <wsse:KeyIdentifier> has a ValueType attribute which defines the type of value contained in this element. For SAML v2.0 this is defined to be: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID. The value contained will reference the SAML Assertion's identifier. The following illustrates the syntax of this element:

```
<ds:KeyInfo>
  <wsse:SecurityTokenReference  wsu:Id="uuid_2ca69267-90bd-4785-a28e-ad9cee6d962e"
    wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0">
    <wsse:KeyIdentifier
 ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID"
    >ed62b6fb-4d73-4011-9f7c-43e0575b6317</wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

In addition to the Security element timestamp signature described in this section, the SAML Assertion must also be digitally signed as described in Section 3.3.4 of this specification.

3.3 SAML Assertions

Each NHIN Request shall have a saml:Assertion element containing child elements saml:Issuer, saml:Subject, saml:AuthnStatement, and saml:AttributeStatement. (No saml:Assertion element is required on a response to a NHIN Request.) The use of saml:AuthorizationDecisionStatement is optional.

SAML Assertions must include:

1. Version attribute which defines SAML v2.0 as the version

2. ID attribute which is an xs:ID as defined by http://www.w3.org/TR/xml-Id/

3. IssueInstant attribute which is an xs:dateTame as defined by http://www.w3.org/TR/xmlschema-2/

   The following illustrates the syntax of this element:

```
<saml2:Assertion ID="ed62b6fb-4d73-4011-9f7c-43e0575b6317"
        IssueInstant="2008-10-07T13:00:34.484Z" Version="2.0">
```

4. The <Issuer> element shall identify the individual responsible for issuing the Assertions carried in the message. This element includes a NameID Format attribute which declares the format used to express the value contained in this element. This is normally the system security officer for the sending NHIO. SAML 2.0 NameID Formats are provided in Table 2 of this specification.

5. The <Subject> element shall identify the Subject[4] of the assertion. This element also includes a NameID Format attribute which declares the format used to express the value contained in this element – the person making the request at the initiating NHIO. SAML 2.0 NameID Formats are provided in Table 2 of this specification, however only formats “X509SubjectName” and “emailAddress” are allowed in this element. For further explanation of the other elements and attributes contained in the <Subject> element, refer to the SAML 2.0 standard as referenced in section 1.4 of this specification.

The following is an example of the <Subject> element:

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    CN=Alex G. Bell,O=1.22.333.4444,UID=abell
  </NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
    <SubjectConfirmationData>
      <ds:KeyInfo>
        <ds:KeyValue>
          <ds:RSAKeyValue>
            <ds:Modulus>vYxVZKIzVdGMSBkW4bYnV80MV/RgQKV1bf/DX8laMO45P6uYp+snzz2XM0S6o3JGQtXQ=
            </ds:Modulus>
            <ds:Exponent>AQAB</ds:Exponent>
          </ds:RSAKeyValue>
        </ds:KeyValue>
      </ds:KeyInfo>
    </SubjectConfirmationData>
  </SubjectConfirmation>
</Subject>
```

[4] Note that the term “subject” in SAML and XACML refers to the individual making the request. In this specification, the term “User” is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.

Format	URI
Unspecified	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Email Address	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
X.509	urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
Windows	urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
Kerberos	urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
Entity	urn:oasis:names:tc:SAML:2.0:nameid-format:entity
Persistent	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
Transient	urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Table 2: NameID Format URIs

6. SAML Statement Elements - The SAML statement elements used are separated into Authentication, Attribute, and Authorization Decision statements. Each statement will be further defined in the following paragraphs.

3.3.1 Authentication Statement

The authentication assertions are associated with authentication of the Subject (User). The <AuthnStatement> element is required to contain an <AuthnContext> element and a AuthnInstant attribute. The saml:AuthnStatement shall contain one saml:AuthnContextClassRef element identifying the method by which the subject was authenticated. Other optional elements of saml:AuthnStatement may also be included, such as a <SubjectLocality> element and a SessionIndex attribute. Each of these is described in more detail in the sections that follow.

The saml:Authentication is comprised of the following 4 Attributes or Elements:

1. AuthnContext
2. Subject Locality (Optional)
3. AuthnInstant
4. Session Index (Optional)

3.3.1.1 Authentication method

The <AuthnContext> element (required) indicates how that authentication was done. Note that the authentication statement does not provide the means to perform that authentication, such as a password, key, or certificate. This element will contain an authentication context class reference.[5]
Available authentication methods and their corresponding URNs are provided in the following table:

Authentication Method	URN
Internet Protocol	urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
Internet Protocol Password	urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
Password	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
Password Protected Transport	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Kerberos	urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
Previous Session	urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
Secure Remote Password	urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
SSL/TLS Certificate	urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
X.509 Public Key	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
PGP Public Key	urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
SPKI Public Key	urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
XML Digital Signature	urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
Unspecified	urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

[5] OASIS: http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

Table 3: Authentication Methods

3.3.1.2 Subject Locality from Where the User was Authenticated

The <SubjectLocality> element (optional) specifies the DNS domain name and IP address for the system entity that was authenticated.

3.3.1.3 Authentication Instant

The AuthnInstant attribute (required) specifies the time at which the authentication took place.

3.3.1.4 Session Index

The SessionIndex attribute (optional) identifies the session between the Subject and the Authentication Authority.

3.3.1.5 Authentication Example

```
<saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="67775277772">
  <saml:SubjectLocality Address="112.16.133.144" DNSName="ME001122.cs.mynetwork.net"/>
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
```

3.3.2 Attribute Statement

The <AttributeStatement> element describes a statement by the SAML authority asserting that the requesting user is associated with the specified attributes. The <AttributeStatement> is required to contain <Attribute> elements as defined by the OASIS XSPA profile of SAML and described in the sections that follow.

The saml:AttributeStatement is comprised of the following 8 Attributes:

1. Subject ID
2. Subject Organization
3. Subject Role
4. Purpose of Use
5. Home Community ID
6. Organization ID
7. Resource ID (Optional)
8. National Provider Identifier (Optional)

The value on the Subject ID and Subject Organization attributes shall be a plain text description of the user's name (not user ID) and organization, respectively. These are primarily intended to support auditing.

3.3.2.1 Subject ID Attribute

This <Attribute> element shall have the Name attribute set to "urn:oasis:names:tc:xspa:1.0:subject:subject-id". The name of the user as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element. (Keep in mind that the term "subject" in SAML and XACML refers to the individual making the request; in this specification, the term "User" is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.)

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
  <saml:AttributeValue>Walter H.Brattain IV</saml:AttributeValue>
</saml:Attribute>
```

The NHIN Trial Implementation “UserName” attribute has been replaced by the Subject ID attribute defined in this section.

3.3.2.2 Subject Organization Attribute

This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:organization”. In plain text, the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element.

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
  <saml:AttributeValue>Family Medical Clinic</saml:AttributeValue>
</saml:Attribute>
```

The NHIN Trial Implementation “UserOrganization” attribute has been replaced by the Subject Organization attribute defined in this section.

3.3.2.3 Subject Organization ID Attribute

This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:organization-id” A unique identifier for the organization that the user is representing in performing this transaction shall be placed in the value of the <AttributeValue> element. This organization ID shall be consistent with the plain-text name of the organization provided in the User Organization Attribute. 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.

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
  <saml:AttributeValue>http://familymedicalclinic.org</saml:AttributeValue>
</saml:Attribute>
```

3.3.2.4 Home Community ID Attribute

This <Attribute> element shall have the Name attribute set to “urn:nhin:names:saml:homeCommunityId”. The value shall be the Home Community ID (an Object Identifier) assigned to the NHIO that is initiating the request, using the urn format (that is, “urn:oid:” appended with the OID). For information regarding OIDs, refer to http://www.oid-info.com/faq.htm

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:nhin:names:saml:homeCommunityId">
  <saml:AttributeValue>urn:oid:2.16.840.1.113883.3.190</saml:AttributeValue>
</saml:Attribute>
```

3.3.2.5 Role Attribute

This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xacml:1.0:subject:role”. The value of the <AttributeValue> element is a child element, “Role”, in the namespace “urn:hl7-org:v3”, whose content is defined by the “CE” (coded element) data type from the HL7 version 3 specification.

The codeSystem is defined to be “2.16.840.1.113883.6.96" and the codeSystemName is defined to be "SNOMED_CT". The Role Element shall contain the SNOMED CT value representing the role that the

user is playing when making the request. The value set to be used is “User Role” and the OID 2.16.840.1.113883.3.18.6.1.15[6] as defined in HITSP C80.

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
  <saml:AttributeValue>
    <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001"
       codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT"
       displayName="Pharmacist"/>
  </saml:AttributeValue>
</saml:Attribute>
```

The NHIN Trial Implementation “UserRole” attribute has been replaced by the Subject Role attribute defined in this section.

3.3.2.6 Purpose of Use Attribute

This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:purposeofuse”[7]. The value of the <AttributeValue> element is a child element, “PurposeOfUse”, in the namespace “urn:hl7-org:v3”, whose content is defined by the “CE” (coded element) data type from the HL7 version 3 specification.

The PurposeOfUse element shall contain the coded representation of the Purpose for Use that is in effect for the request.

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
  <saml:AttributeValue>
    <PurposeForUse xmlns="urn:hl7-org:v3" xsi:type="CE" code="OPERATIONS"
        codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"
        displayName="Healthcare Operations"/>
  </saml:AttributeValue>
</saml:Attribute>
```

Codes are assigned as below. The codeSystem is defined to be “2.16.840.1.113883.3.18.7.1”. The codeSystemName is defined to be “nhin-purpose”. The value of the Purpose of Use attribute shall be a urn:hl7-org:v3:CE element, specifying the coded value representing the user's purpose in issuing the request, choosing from the value set listed in this specification. The codeSystem attribute of this element must be present, and must specify the OID of the "Purpose of Use" code system created by the NHIN Cooperative, 2.16.840.1.113883.3.18.7.1 .

The value set for Purpose of Use is defined in Table 4, below.

The NHIN Trial Implementation “PurposeForUse” attribute has been replaced by the PurposeOfUse attribute defined in this section.

[6] At this time, it is not anticipated that this value set OID is required for any particular purpose, but it is defined as a vocabulary best practice.

[7] Readers of the XSPA Profile of SAML referenced in section 3.3.2 of this specification may note that the Conformance Table shows xspa:1,0 rather than xspa:1.0. NHIN believes this to be a typo and has specified the use of a decimal rather than a comma.

Purpose of Use vocabulary	Code
Treatment	TREATMENT
Payment	PAYMENT
Healthcare Operations	OPERATIONS
System Administration	SYSADMIN
Fraud detection	FRAUD
Use or disclosure of Psychotherapy Notes	PSYCHOTHERAPY
Use or disclosure by the covered entity for its own training programs	TRAINING
Use or disclosure by the covered entity to defend itself in a legal action	LEGAL
Marketing	MARKETING
Use and disclosure for facility directories	DIRECTORY
Disclose to a family member, other relative, or a close personal friend of the individual,	FAMILY
Uses and disclosures with the individual present.	PRESENT
Permission cannot practicably be provided because of the individual's incapacity or an emergency	EMERGENCY
Use and disclosures for disaster relief purposes.	DISASTER
Uses and disclosures for public health activities.	PUBLICHEALTH
Disclosures about victims of abuse, neglect or domestic violence.	ABUSE
Uses and disclosures for health oversight activities.	OVERSIGHT
Disclosures for judicial and administrative proceedings.	JUDICIAL
Disclosures for law enforcement purposes.	LAW
Uses and disclosures about decedents.	DECEASED
Uses and disclosures for cadaveric organ, eye or tissue donation purposes	DONATION
Uses and disclosures for research purposes.	RESEARCH
Uses and disclosures to avert a serious threat to health or safety.	THREAT
Uses and disclosures for specialized government functions.	GOVERNMENT
Disclosures for workers' compensation.	WORKERSCOMP
Disclosures for insurance or disability coverage determination	COVERAGE
Request of the Individual	REQUEST

Table 4: NHIN PurposeOfUse Code Description

3.3.2.7 Patient Identifier Attribute

This attribute is OPTIONAL, as it may not be needed for cases in which the data being exchanged does not pertain to a specific patient (e.g. population health data). The value of the Patient Identifier attribute MUST be specified when the InstanceAccessConsentPolicy attribute is specified in an Authorization Decision Statement.

This <Attribute> element shall have the Name attribute set to "urn:oasis:names:tc:xacml:2.0:resource:resource-id". The patient identifier of the requesting organization shall be placed in the value of the <AttributeValue> element.

The patient identifier MUST consist of two parts; the OID for the assigning authority and the identifier of the patient within that assigning authority. The value MUST be formatted using the following syntax:

IDNumber^^^&OIDofAA&ISO

where IDNumber is the identifier of the patient within the assigning authority, and OIDofAA is the OID for the assigning authority. As an example, a patient identifier of 543797436 for an assigning authority with an OID of 1.2.840.113619.6.197, has been encoded into the follow SAML assertion snippet. Please note that the '&' character has been properly encoded in the XML content.

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
  <saml:AttributeValue>543797436^^^&amp;1.2.840.113619.6.197&amp;ISO</saml:AttributeValue>
</saml:Attribute>
```

3.3.2.8 National Provider Identifier (NPI) Attribute

A National Provider Identifier (NPI) is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services (CMS). This attribute provides the ability to specify an NPI value as part of the SAML assertion that accompanies a message that is transmitted across the NHIN.

The NPI attribute is OPTIONAL, and is therefore, NOT required for ALL NHIN messages. When this attribute is included in the SAML assertion, the <Attribute> element SHALL have the Name attribute set to "urn:oasis:names:tc:xspa:2.0:subject:npi". An example of the syntax of this element follows:

```
<saml:Attribute Name=" urn:oasis:names:tc:xspa:2.0:subject:npi">
  <saml:AttributeValue>1234567890</saml:AttributeValue>
</saml:Attribute>
```

3.3.2.9 Attribute Statement Example

```
<saml:AttributeStatement>
  <saml:Attribute Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
    <saml:AttributeValue>Dr Joe Smith</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
    <saml:AttributeValue>Best Clinic</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
    <saml:AttributeValue>urn:oid: 2.16.840.1.113883.3.18.101</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:nhin:names:saml:homeCommunityId">
    <saml:AttributeValue>urn:oid:2.16.840.1.113883.3.190</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
    <saml:AttributeValue>
      <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="112247003"
          codeSystem="2.16.840.1.113883.6.96"
          codeSystemName="SNOMED CT" displayName="Medical doctor"/>
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
    <saml:AttributeValue>
      <PurposeForUse xmlns="urn:hl7-org:v3" xsi:type="CE" code="TREATMENT"
          codeSystem="2.16.840.1.113883.3.18.7.1"
          codeSystemName="nhin-purpose" displayName="Treatment"/>
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
    <saml:AttributeValue>543797436^^^&amp;1.2.840.113619.6.197&amp;ISO</saml:AttributeValue>
  </saml:Attribute>

</saml:AttributeStatement>
```

3.3.3 Authorization Decision Statement

The <AuthzDecisionStatement> element describes a statement by the SAML authority asserting that a request for access by the statement's subject to the specified resource has resulted in the specified authorization decision on the basis of some optionally specified evidence. This OPTIONAL element provides the requesting NHIO an opportunity to assert that it holds an Access Consent Policy which the responding NHIN may wish to evaluate in order to determine if access to the requested resource(s) should be allowed.
The information conveyed within the Authorization Decision Statement may be used by the responding NHIO to retrieve the asserted Access Consent Policy. The format of the Access Consent Policy is defined in the NHIN Access Consent Policy specification.

The Authorization Decision Statement WILL be used when the consumer (patient) has granted the requesting NHIO permission to access to their medical records, and the requester needs to make that authorization known to another (responding) NHIO.

The underlying assumption for this use case is that the responding NHIO has medical records for the consumer, but has access restrictions in place that would ordinarily prevent disclosure of the patient's records to the requesting NHIO. A variation of this use case is that the responding NHIO's policies or access restrictions would prevent disclosure of the patient's identity to the requesting NHIO through the NHIN Patient Discovery mechanism, effectively preventing the requesting NHIO from making a query and subsequent request for medical records.

3.3.3.1 Authorization Decision Statement Content

The Authorization Decision Statement has the following content:

1. Action. This action must be specified using a Namespace of 'urn:oasis:names:tc:SAML:1.0:action:rwedc' and a value of Execute.[8]
2. Decision. The Decision attribute of the Authorization Decision Statement must be "Permit".
3. Resource. The Resource attribute of the Authorization Decision Statement must be the URI of the endpoint to which the request is addressed or an empty URI reference ("").
4. The Authorization Decision Statement must contain an <Evidence> element, containing a single <Assertion> child element.
5. This <Assertion> element must contain an ID attribute, an IssueInstant attribute, a Version attribute, an Issuer element, and an Attribute Statement element.
6. There must be at least one of the following Attributes in the Attribute Statement.
    1. An <Attribute> element with the name "AccessConsentPolicy" and NameFormat "http://www.hhs.gov/healthit/nhin". The value(s) for this attribute will be the OIDs of the access policies that the asserting entity has previously agreed to with other entities. The OIDs MUST be expressed using the urn format (e.g. - urn:oid:1.2.3.4).
    2. An <Attribute> element with the name "InstanceAccessConsentPolicy" and NameFormat "http://www.hhs.gov/healthit/nhin". The value(s) of this attribute will be the OIDs of the patient specific access policy instances. The OIDs MUST be expressed using the urn format (e.g. - urn:oid:1.2.3.4.123456789). If a requestor specifies this Attribute, the

[8] This document was updated to specify this namespace prior to publication, but after the previous namespace had been incorporated in Connect 2.3. There will be a short period of time where the namespace used in the Connect Gateway does not conform to this spec.

requestor MUST support the ability for the specified policy document(s) to be retrieved via the transactions defined in HITSP TP30.

3. The “ContentReference”, “ContentType”, and “Content” attributes from the Trial Implementation specifications have been removed and should no longer be used.

3.3.3.2 Authorization Decision Statement Example

```
<saml2:AuthzDecisionStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
 Decision="Permit"
 Resource="">
      <saml2:Action
       Namespace="urn:oasis:names:tc:SAML:1.0:action:rwedc">Execute</saml2:Action>
      <saml2:Evidence>
          <saml2:Assertion ID="da20c267-0f95-4cf4-8bc1-6daa5d84201e"
              IssueInstant="2008-10-20T19:59:10.843Z" Version="2.0">
            <saml2:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
            >CN=SAML User,OU=SU,O=SAML User,L=Los Angeles,ST=CA,C=US</saml2:Issuer>
            <saml2:Conditions NotBefore=”2008-10-20T19:59:10.843Z
                              NotOnOrAfter="2008-12-25T00:00:00.000Z"/>
           <saml2:AttributeStatement>
                <saml2:Attribute Name="AccessConsentPolicy"
                    NameFormat="http://www.hhs.gov/healthit/nhin">
                   <saml2:AttributeValue>urn:oid:1.2.3.4</saml2:AttributeValue>
                </saml2:Attribute>
               <saml2:Attribute Name="InstanceAccessConsentPolicy"
                         NameFormat="http://www.hhs.gov/healthit/nhin">
                   <saml2:AttributeValue
                      xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance"
                      xmlns:ns7="http://www.w3.org/2001/XMLSchema"
                      ns6:type="ns7:string">urn:oid:1.2.3.4.123456789
                   </saml2:AttributeValue>
               </saml2:Attribute>
            </saml2:AttributeStatement>
          </saml2:Assertion>
      </saml2:Evidence>
</saml2:AuthzDecisionStatement>
```

3.3.4 Assertion Signature

An assertion signed by the asserting party supports assertion integrity, authentication of the asserting party to the receiving party, and, if the signature is based on the SAML authority’s public/private key pair, non-repudiation of origin. For NHIN purposes the <ds:Signature> element is required to contain a <ds:SignedInfo> element , a <ds:SignatureValue> element, and a <ds:KeyInfo> element.

3.3.4.1 SignedInfo Element

The <ds:SignedInfo> element is a container which specifies the <ds:CanonicalizationMethod>, the <ds:SignatureMethod>, and a <ds:Reference>.

It is recommended that Exclusive Canonicalization be used, http://www.w3.org/2001/10/xml-exc-c14n#. Use of Exclusive Canonicalization ensures that signatures created over SAML messages embedded in an XML context can be verified independent of that context.

The <ds:SignatureMethod> identifies the cryptographic functions involved in the signature operation. It is recommended that SAML processors support the use of RSA signing and verification, http://www.w3.org/2000/09/xmldsig#rsa-sha1.

XML Digital Signatures are applied to data objects through an indirection or URI reference; when signing the SAML assertion the URI reference must match the Assertion ID attribute value. The <ds:Reference> element also specifies the transformation algorithms the digest method and the calculated digest value.

The transformation algorithms must be listed in the order that they are to be applied and may only consist of a subset of enveloped signature transform, exclusive canonicalization transform, and exclusive canonicalization with comments.

http://www.w3.org/2000/09/xmldsig#enveloped-signature http://www.w3.org/2001/10/xml-exc-c14n# http://www.w3.org/2001/10/xml-exc-c14n#WithComments

The <ds:DigestMethod> defines the digest algorithm that is applied. For the NHIN the Basic128 Algorithm Suite has been designated; such that the digest algorithm is defined to be SHA1; http://www.w3.org/2000/09/xmldsig#sha1.

3.3.4.2 SignatureValue Element

The SignatureValue element contains the actual value of the digital signature; it is always encoded using base64. The procedure to generate the digital signature is as stated below:

1) Identify the Assertion object to be signed
2) Apply the transformations provided in the <ds:Transformations> element to the Assertion object in the order as specified.
3) Apply the digest method which will result in generating the digest value
4) Create the <ds:Reference> element using the URI reference to the Assertion object and by enclosing the transformations, the digest method, and the calculated value.
5) Create the <ds:SignedInfo> element by enclosing the Canonicalization method, the Signature method, and the Reference as created above.
6) Apply the Canonicalization method to the created <ds:SignedInfo> element.
7) Apply the Signature method to generate the Signature value.

3.3.4.3 KeyInfo Element

The <ds:KeyInfo> element provides the means by which the signature is validated. This element must contain a <ds:KeyValue> element which contains a single public key that will be used to validate the signature. The enclosed <ds:RSAKeyValue> element identifies the structured format of the NHIN provided keys to be RSA. This element declares the modulus, which applies to both the public and the private key, and the public key exponent. Each private key exponent is determined by a congruence relationship with the public key exponent and is known only to the party generating the signature. These arbitrary-length integers are represented in XML as octet strings as defined by the ds:CryptoBinary type which is a base64Binary

3.3.4.4 Signature Example

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#51cb7689-0957-46a2-938e-1add75577ab7">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>a3XVN23H2N/ga+08AGqGHD1euKc=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>L8Liyz+6pLwNP9YBfIRbrDVUJtM2YcLuN3+HPjspQEHmZ2uTXWYuy7XTM9dqmN93w0ypVM7egjRe
=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:KeyValue>
      <ds:RSAKeyValue>
        <ds:Modulus>vYxVZKIzVdGMSBkW4bYnV80MV/RgQKV1bf/DoMTX8laMO45P6=</ds:Modulus>
        <ds:Exponent>AQAB</ds:Exponent>
      </ds:RSAKeyValue>
    </ds:KeyValue>
  </ds:KeyInfo>
</ds:Signature>
```

4 Error Handling

No additional faults are specified beyond the basic SOAP faults as identified in the NHIN Messaging Platform Service Interface Specification.

5 Auditing

See each NHIN service specification for specification-specific audit events.

Appendix A: SAML Assertion Rules

1. Each NHIN Request shall have a <wsse:Security> element which contains the entire SAML token. This is per the Web Services Security: SAML Token Profile 1.1 specification. Also as per the spec the <wsse:SecurityTokenReference> tags should also be present after the saml:Assertion.
2. Each NHIN Request shall have a saml:Assertion element containing child elements saml:Issuer, saml:Subject, saml:AuthnStatement, and saml:AttributeStatement. (No saml:Assertion element is required on a response to a NHIN Request.)
3. The saml:Issuer element shall identify the individual responsible for issuing the Assertions carried in the message. This is normally the system security officer for the sending NHIO.
4. The saml:Issuer element may use any of the Name Identifier Formats defined in Section 8.3 of the SAML 2.0 Specification
5. The saml:Subject element shall identify the individual issuing the request -- the "end user". The saml:Subject element may use only the Name Identifier Formats for “X509SubjectName” and “emailAddress”.
6. The saml:AuthnStatement shall contain one saml:AuthnContextClassRef element identifying the method by which the subject was authenticated. Other optional elements of saml:AuthnStatement may also be included.
7. The saml:AttributeStatement shall contain six Attributes: Subject ID, Subject Organization, Subject Role, Purpose of Use, Home Community ID, and Organization ID.
8. The value on the Subject ID and Subject Organization attributes shall be a plain text description of the user's name (not user ID) and organization, respectively. These are primarily intended to support auditing.
9. The value of the Role attribute shall be a urn:hl7-org:v3:CE element, specifying the coded value representing the issuing user's role, choosing from the value set listed in the specification. The codeSystem attribute of this element must be present, and must specify the OID of the SNOMED CT code system, 2.16.840.1.113883.6.96
10. The value of the Purpose of Use attribute shall be a urn:hl7-org:v3:CE element, specifying the coded value representing the user's purpose in issuing the request, choosing from the value set listed in this specification. The codeSystem attribute of this element must be present, and must specify the OID of the "Purpose of Use" code system created by the NHIN Cooperative, 2.16.840.1.113883.3.18.7.1 .
11. The value of the Patient Identifier attribute MUST be specified when the InstanceAccessConsentPolicy attribute is specified in an Authorization Decision Statement.