Nationwide Health Information Network (NHIN)

Trial Implementations

Service Interface Specifications

Authorization Framework

V 1.9.1

1/30/2009

Contributors

Name	Organization	NHIE represented
Richard Franck	IBM	NCHICA
Tony Mallia	VA	Fed NHIE
Victoria Vickers	FHA	Fed NHIE
Deborah Lafky	ONC	
David Riley	FHA	FHA

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

Document Approval

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

Table of Contents

1 Preface

1.1 Introduction

The NHIN Trial Implementations Service Interface Specifications constitute the core services of an operational Nationwide Health Information Network. They are intended to provide a standard set of service interfaces that enable Nationwide Health Information Exchange (NHIE) to NHIE exchange of interoperable health information. These services provide such functional capabilities as patient look-up, document query and retrieve, notification of consumer preferences, and access to logs for determining who has accessed what records and for what purpose for use. These functional services rest on a foundational set of messaging and security services. The current set of defined core services includes the following:

1. NHIN Trial Implementations Message Platform Service Interface Specification,
2. NHIN Trial Implementations Authorization Framework Service Interface Specification,
3. NHIN Trial Implementations Subject Discovery Service Interface Specification,
4. NHIN Trial Implementations Query for Documents Service Interface Specification,
5. NHIN Trial Implementations Document Retrieve Service Interface Specification,
6. NHIN Trial Implementations Audit Log Query Service Interface Specification,
7. NHIN Trial Implementations Consumer Preferences Service Interface Specification
8. NHIN Trial Implementations Health Information Event Messaging Service Interface Specification
9. NHIN Trial Implementations NHIE Service Registry Interface Specification
10. NHIN Trial Implementations Authorized Case Follow-Up Service Interface Specification

It is expected that these core services will be implemented together as a suite since the functional level services are dependent on the foundational services. Specifications #1 through #7 were the focus of the August 2008 testing event and September AHIC demonstrations. Specifications #1 through #9 were included in the November testing and demonstrations during the December 2008 NHIN Trial Implementations Forum.

1.2 Intended Audience

The primary audience for the NHIN Trial Implementations Service Interface Specifications is the individuals responsible for implementing software solutions that realize these interfaces for an NHIE. After reading this specification, one should have 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, any Extensible Markup Language (XML) schemas used to define the content and what “compliance” means from an implementation testing perspective.

1.3 Focus of this Specification

This document discusses the exchange of information about the user (initiator) of a request between NHIEs. The purpose of the information is for the responding NHIE to enable authorization of the function to be performed based on a combination of the assertions passed and its local information, permissions and policies. These assertions are carried with every request.

1.4 Definitions

1.5 Related Documents

1.6 Relationship to HITSP Constructs

1.7 Relationship to Other NHIN Cooperative Specifications

The NHIN Trial Implementations Authorization Framework Service Interface Specification provides the details for users to assert the basis for their requests for access to information on the NHIN. It is implemented along with the NHIN Trial Implementations Messaging Platform Service Interface Specification as a part of a comprehensive security and privacy framework for securing the information exchanged on the NHIN. All other service interface specifications assume these implementations.

2 Interface Description

2.1 NHIN Interface Descriptive Name:

Audit Log Query Service Interface Specification

2.2 NHIN Interface level:

NHIE to NHIE cross community type of interface

2.3 Definition

2.3.1 Interaction Behavior

The responding NHIE in receiving the request now knows that the user in the initiating NHIE is authorized there but will not know the access controls associated with the identity of the user. An Initiating NHIE determines whether the function is allowed and if so attaches the user focused assertions to the request to the other NHIE.

The responding NHIE 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 authentication acts that were previously performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources. A single assertion might contain several different internal statements about authentication, authorization, and attributes.[1]

[1] SAML v2.0

2.3.2 Request Definition

Requests are defined by the interface which is addressed, the operation on the interface, and the identity of the record target person (unambiguous person identity in the responding NHIE when known).

2.3.3 NHIN Interfaces and Operations

1. Subject Discovery
2. Query For Documents
3. Retrieve Documents
4. Audit Log Query
5. Subscribe/Unsubscribe/Notify

2.3.4 Identity of the record target

In most cases except for SubjectDiscovery: Announce Subject, the record target (i.e. the person who is the subject of the records) is the unambiguous person identity in the responding NHIE. The assertion here is that the user is authorized by the initiating NHIE to access information about this person. It is also required for HIPAA Privacy Disclosure Accounting.

2.4 Triggers

All requests issued in the NHIN utilize must implement the NHIN Trial Implementations Messaging Platform Service Interface Specification and the NHIN Trial Implementations Authorization Framework Service Interface Specification

2.5 Transaction Standard

The authorization framework is based on the implementation of the Oasis WS-I Security Profile SAML Token Profile as specified in the NHIN Trial Implementations Messaging Platform Service Interface Specification. SAML 2.0 is the base specification for expressing assertions in the NHIN.

2.6 NHIN Core Services

This service interface specification addresses the following NHIN Core Services identified in the Gartner Report from the NHIN Prototype Contracts:

- User and Subject Identity Management Services
  - User identity proofing
  - User authentication strength
- Data Services
  - The SAML assertion captures the detail about users and purposes for use that are required to support auditing and HIPAA accounting
- Consumer Services
  - The data about the user making requests contained in the SAML assertion and logged in the audit enables consumers to determine who has accessed their data for what purpose for use and when

2.7 Technical Pre-conditions

Assumptions

- Cross Provisioning of users between NHIEs is not feasible in the short term
- Architectures of the NHIEs are decoupled and are opaque from the outside (i.e. from another NHIE). The NHIEs need not use the same security mechanisms or standards internally.

- The initiating NHIE authorizes the issuing of the request and it is required that they do so.
- Consumer Sharing Permissions are applied within each NHIE and are **not** communicated between NHIEs at this stage. The mechanism for the NHIE to persist permissions is opaque (from the NHIE to NHIE viewpoint)

2.8 Technical Post-conditions

All cross community requests for personally identifiable information on the NHIN must use the Authorization Framework. All of the following NHIN Core Services will have SAML assertions:

1. Subject Discovery
2. Query For Documents
3. Retrieve Documents
4. Audit Log Query
5. Subscribe/Unsubscribe/Notify

3 Interface Definition

3.1 Specific NHIN Assertions

This set of assertions is proposed for the NHIE to NHIE communication and the assertion responses from the Assertion Authority will be SAML assertions carried within the <Security> element within the header of the SOAP envelope as defined by WS-Security.[2].

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

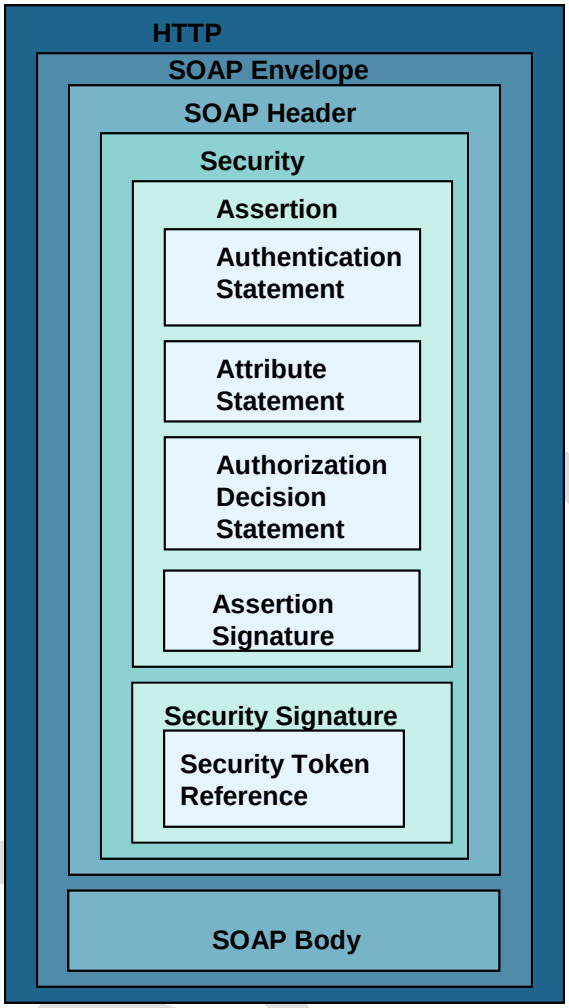

Figure 1: Position of the SAML Assertion within the SOAP Header

3.1.1 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

3.1.2 Timestamp

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 5.5. 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>
```

3.2 SAML Assertions

SAML Assertions must include the Version attribute which defines SAML v2.0 as the version, an ID attribute which is an xs:ID as defined by http://www.w3.org/TR/xml-id/ , and an IssueInstant attribute which is an xs:dateTame as defined by http://www.w3.org/TR/xmlschema-2/.3 The following illustrated the syntax of this element:

```
<saml2:Assertion ID="ed62b6fb-4d73-4011-9f7c-43e0575b6317"
        IssueInstant="2008-10-07T13:00:34.484Z" Version="20">
```

The <Issuer> element is a required element of the SAML assertion and has a Format attribute which declares the Name Identifier format used in expressing the contained value of this element.

The <Subject> element is also a required element when using the <AuthnStatement>. This element is used to define the Subject of the assertion and will contain the User's identification information. Like the <Issuer> element the <Subject> element has a Format attribute which declares the Name Identifier format used in expressing the contained value of this element. The user identification found in this element must correlate with the user identified in the XACML policy document during retrieval of the claimant's authorization document, and should therefore follow the email or X509 format. As part of the validation and processing of the assertion, the receiver must establish the relationship between the subject and claims of the SAML statements and the entity providing the evidence to satisfy the confirmation method defined for the statement. Statements attested for by the holder-of-key method must

[3] OASIS: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

be associated with one or more holder-of-key SubjectConfirmation elements. The SubjectConfirmation elements must include a <ds:KeyInfo> element that identifies a public key that can be used to confirm the identity of the subject. 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>
```

Both the <Issuer> and the <Subject> elements take a Name Identifier Format. The following table provides the available URIs:

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: Name Identification Format URIs

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

3.2.1 Authentication Statement

The authentication assertions are associated with authentication of the Subject (User). Assertions containing a <AuthnStatement> element must also contain a <Subject> element.
The <AuthnStatement> element is required to contain an <AuthnContext> element, and a AuthnInstant attribute. It may also optionally contain a <SubjectLocality> element and a SessionIndex attribute. Each of these is described in more detail in the following paragraphs.

3.2.1.1 Authentication method

The <AuthnContext> element 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.[4]
Available authentication methods and their corresponding URNs are provided in the following table:

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

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

Table 3: Authentication Methods

3.2.1.2 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.

3.2.1.3 Authentication Instant

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

3.2.1.4 Session Index

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

3.2.1.5 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>
```

3.2.2 Attribute Statement

The <AttributeStatement> element describes a statement by the SAML authority asserting that the requesting user is associated with the specified attributes. These attribute assertions are not controlled by SAML and are those recommended for the NHIN Authorization Framework.
The <AttributeStatement> is required to contain <Attribute> elements as defined in the following sections. These attributes are in a consistent place so that interception such as HIPAA Disclosure accounting is facilitated.

Each <Attribute> element is required to specify a Name attribute and a NameFormat attribute. The NameFormat attribute must be set to http://www.hhs.gov/healthit/nhin for NHIN. The <AttributeValue> element is formed specific to each usage within the <Attribute> element.

3.2.2.1 User_Name Attribute

This <Attribute> element shall have the Name attribute set to “UserName”. The name of the user 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="UserName" NameFormat="http://www.hhs.gov/healthit/nhin">
  <saml:AttributeValue>Walter H.Brattain IV</saml:AttributeValue>
</saml:Attribute>
```

3.2.2.2 User Organization Attribute

This <Attribute> element shall have the Name attribute set to “UserOrganization”. The organization that the user belongs to as required by HIPAA PrivacyDisclosure Accounting shall be placed in the value of the <AttributeValue> element. It is in plain language. An example of the syntax of this element is as follows:

```
<saml:Attribute Name="UserOrganization" NameFormat="http://www.hhs.gov/healthit/nhin">
  <saml:AttributeValue>Family Medical Clinic</saml:AttributeValue>
</saml:Attribute>
```

3.2.2.3 User Role Attribute

This <Attribute> element shall have the Name attribute set to “UserRole”. The value of the <AttributeValue> element is a nhin:CodedElement as defined in the following schema (which is taken from the Consumer Preferences specification).

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:nhin="http://www.hhs.gov/healthit/nhin" targetNamespace="http://www.hhs.gov/healthit/nhin">
  <xsd:complexType name="InstanceIdentifier">
    <xsd:attribute name="root" type="xsd:string"/>
    <xsd:attribute name="extension" type="xsd:string"/>
  </xsd:complexType>
  <xsd:element name="PatientId" type="nhin:InstanceIdentifier"/>
  <xsd:element name="UserAddress" type="xsd:string"/>
  <xsd:complexType name="CodedElement">
    <xsd:attribute name="code" type="xsd:string"/>
    <xsd:attribute name="codeSystem" type="xsd:string"/>
    <xsd:attribute name="codeSystemName" type="xsd:string" use="optional"/>
    <xsd:attribute name="displayName" type="xsd:string" use="optional"/>
  </xsd:complexType>
  <xsd:element name="Role" type="nhin:CodedElement"/>
  <xsd:element name="PurposeForUse" type="nhin:CodedElement"/>
</xsd:schema>
```

The nhin:CodedElement will contain assignments for each defined attribute which will come from SNOMED CT. It is the role that the user is playing when making the request. An example of the syntax of this element is as follows:

```
<saml:Attribute Name="UserRole" NameFormat="http://www.hhs.gov/healthit/nhin">
  <saml:AttributeValue><nhin:Role code="46255001" codeSystem="2.16.840.1.113883.6.96"
    codeSystemName="SNOMED_CT" displayName="Pharmacist"/></saml:AttributeValue>
</saml:Attribute>
```

The SNOMED CT code is mapped to ASTM E1986-98(2005) Standard Guide for Information Access Privileges to Health Information. The codeSystem is defined to be “2.16.840.1.113883.6.96" and the codeSystemName is defined to be "SNOMED_CT". The displayName shall correlate with the assigned code as given in the following table.

This guide covers the process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider, and organizational data in the

healthcare domain. It addresses a wide range of data and data elements not all traditionally defined as healthcare data, but all elemental in the provision of data management, data services, and administrative and clinical healthcare services. In addition, this guide addresses specific requirements for granting access privileges to patient-specific health information during health emergencies.
The codes are assigned from SNOMED CT. The value set defined below is defined to have the name "NHIN-ROLE" and the OID 2.16.840.1.113883.3.18.6.1.15. (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.)

Description (taken from SNOMED CT)	SNOMED CT Code
Audiologist	309418004
Dental Hygienist	26042002
Dentist	106289002
Dietitian	159033005
Complementary Healthcare worker	224609002
Professional nurse	106292003
Optometrist	28229004
Pharmacist	46255001
Chiropractor	3842006
Osteopath	76231001
Medical doctor	112247003
Medical pathologist	61207006
Podiatrist	159034004
Psychiatrist	80584001
Medical Assistant	22515006
Psychologist	59944000
Social worker	106328005
Speech therapist	159026005
Medical Technician	307988006
Orthotist	309428008
Physiotherapist AND/OR occupational therapist	106296000
Veterinarian	106290006
Paramedic/EMT	397897005
Minister of religion AND/OR related member of religious order	106311007
Philologist, translator AND/OR interpreter	106330007
clerical occupation	159483005
Administrative healthcare staff	224608005
Infection control nurse	224546007
insurance specialist (health insurance/payor)	307785004
Patient	116154003
Patient advocate	429577009
Profession allied to medicine (non-licensed care giver)	309398001
IT Professional	265950004
law occupation	271554005
Public health officer	307969004

Table 4: NHIN Role Codes

3.2.2.4 Purpose for Use Attribute

This <Attribute> element shall have the Name attribute set to “PurposeForUse”. The value of the <AttributeValue> element is a nhin:CodedElement as defined in the schema in the User Role section above.

The nhin:CodedElement will contain assignments for each defined attribute which will define the value of Purpose for Use that is in effect for the request and will come from HIPAA privacy as required by HIPAA Privacy Disclosure Accounting and may be extended. An example of the syntax of this element is as follows:

```
<saml:Attribute Name="PurposeForUse" NameFormat="http://www.hhs.gov/healthit/nhin">
  <saml:AttributeValue><nhin:PurposeForUse 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 set for Purpose for use includes the following items.

Purpose for Use vocabulary	Code
Treatment	TREATMENT
Payment	PAYMENT
Healthcare Operations	OPERATIONS
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

Table 5: NHIN PurposeForUse Code Description

3.2.2.5 Attribute Statement example

```
<saml:AttributeStatement>
  <saml:Attribute NameFormat=”http://www.hhs.gov/healthit/nhin” Name=“UserName”>
    <saml:AttributeValue>Dr Joe Smith</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute NameFormat=”http://www.hhs.gov/healthit/nhin” Name=“UserOrganization”>
    <saml:AttributeValue>Best Clinic</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute NameFormat=”http://www.hhs.gov/healthit/nhin” Name=“UserRole”>
    <saml:AttributeValue>
      <nhin:Role code=“112247003” codeSystem="2.16.840.1.113883.6.96"
          codeSystemName=”SNOMED CT” displayName=”Medical doctor”>
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute NameFormat=“http://www.hhs.gov/healthit/nhin” Name=“PurposeForUse”>
    <saml:AttributeValue>
      <nhin:PurposeForUse code=“TREATMENT” codeSystem= "2.16.840.1.113883.3.18.7.1"
         codeSystemName=”nhin-purpose” displayName=”Treatment”>
    </saml:AttributeValue>
  </saml:Attribute>
```

```
</saml:AttributeStatement>
```

3.2.3 Authorization Decision Statement

The <AuthzDecisionStatement> element describes a statement by the SAML authority asserting that a request for access by the statement's subject (the "user") to the specified resource has been authorized on the basis of some evidence, which is included within the Authorization Decision Statement.

Authorization Decision Statement will be used when the consumer (patient) has granted the requesting NHIE access to their medical records through a means outside the NHIN, and the requester needs to make that authorization known to another (responding) NHIE. The underlying assumption for this use case is that the responding NHIE 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 NHIE. A variation of this use case is that the responding NHIE's policies or access restrictions would prevent disclosure of the patient's identity to the requesting NHIE through the NHIN Subject Discovery mechanism, effectively preventing the requesting NHIE from making a query and subsequent request for medical records, and also preventing the requesting NHIE from using the Consumer Preference Profile specification to make new consent restrictions available to the responding NHIE.

The Authorization Decision Statement is expected to be used in restricted circumstances where the NHIN has adopted a policy allowing its use by particular parties in fulfillment of particular use cases. The first such use case is the "SSA Authorized Release of Information" use case.

3.2.3.1 Authorization Decision Statement Content

The Authorization Decision Statement has the following content:

1. Action. This action must be specified using a Namespace of

http://www.hhs.gov/healthit/nhin and a value of one of:

    1. subjectDiscovery (this is the only value allowed for the SSA Authorized Release of Information use case)
    2. retrieveDocuments
    3. queryDocuments
    4. queryAuditLog

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.
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 will be three Attributes defined in the Attribute Statement. Each Attribute is defined as follows:

    1. The first <Attribute> element must contain the name "ContentReference" and NameFormat "http://www.hhs.gov/healthit/nhin". The value of this attribute may be any String that can be used by the requester as a reference to the evidence. This is primarily for audit purposes.

2. The next <Attribute> element must contain the name “ContentType” and NameFormat “http://www.hhs.gov/healthit/nhin”. The value of this attribute is the MIME type of the evidence included on the “Content” attribute element.
3. The last <Attribute> element must contain the name “Content” and NameFormat “http://www.hhs.gov/healthit/nhin”. The value of this attribute is the supporting evidence, in base64 encoded data format.

3.2.3.2 Authorization Decision Statement Example

```
<saml2:AuthzDecisionStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
 Decision="Permit"
 Resource="https://nchica.ibmhsp.net:444/ICServices_Web/api/SubjectDiscoveryQuery">
      <saml2:Action
       Namespace="http://www.hhs.gov/healthit/nhin">subjectDiscovery</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="ContentReference"
                   NameFormat="http://www.hhs.gov/healthit/nhin">
                  <saml2:AttributeValue>(some value)</saml2:AttributeValue>
               </saml2:Attribute>
               <saml2:Attribute Name="ContentType"
                    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">application/pdf
                   </saml2:AttributeValue>
               </saml2:Attribute>
               <saml2:Attribute Name="Content"
                    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:base64Binary"> (base64 encoded data here)
                   </saml2:AttributeValue>
               </saml2:Attribute>
          </saml2:AttributeStatement>
         </saml2:Assertion>
    </saml2:Evidence>
</saml2:AuthzDecisionStatement>
```

3.2.4 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.

3.2.4.1 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.

3.2.4.2 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.

3.2.4.3 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

3.2.4.4 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 Trial Implementations Messaging Platform Service Interface Specification.

5 Auditing

See the NHIN Trial Implementations Audit Log Query Service Interface Specification for specific audit events and the individual service interface specifications for specification specific audit events.

6 Potential Future Considerations

No additional future considerations identified at this time.

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. The use of a saml:AuthzDecisionStatement is anticipated for the SSA Use Case and will be further specified by the Working Group at a later time. (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 NHIE.
4. The saml:Subject element shall identify the individual issuing the request -- the "end user".
5. The saml:Issuer and saml:Subject elements may use any of the Name Identifier Formats defined in Section 8.3 of the SAML 2.0 Specification
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 four Attributes: UserName, UserOrganization, UserRole, and PurposeForUse.
8. These four attribute statements shall have a NameFormat of http://www.hhs.gov/healthit/nhin
9. The value on the UserName and UserOrganization 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.
10. The value of the UserRole attribute shall be a nhin:Role 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
11. The value of the PurposeForUse attribute shall be a nhin:PurposeForUse element, specifying the coded value representing the user's purpose in issuing the request, 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 "Purpose for Use" code system created by the NHIN Cooperative, 2.16.840.1.113883.3.18.7.1 .