Version 1.1



1.0 OVERVIEW 1

1.1 Purpose 1

1.2 Intended Audience 1

1.3 Specifications 1

1.4 Document Conventions 2

2.0 Web Service Interfaces 3

2.1 Patient Discovery 3

2.2 Query For Documents and Retrieve Documents 3

3.0 Messaging Requirements 4

3.1 Base Messaging Requirements 4

3.2 WS-Addressing and Asynchronous Support 4

4.0 Message Sequencing 5

4.1 Patient Discovery Request 6

4.2 Initial Access Control Decision 6

4.3 Query for Documents Request (for Access Consent Policy) 7

4.4 Query for Documents response (for Access Consent Policy) 8

4.5 Retrieve Document Request (for Access Consent Policy) 9

4.6 Retrieve Document Response (for Access Consent Policy) 9

4.7 Final Access Control Decision 10

4.8 Patient Discovery response 10

4.9 Query for Documents Request (for Clinical Document) 11

4.10 Query for Documents Response (for Clinical Document) 12

4.11 Retrieve Documents Request (for Clinical Document) 13

4.12 Retrieve Documents Response (for Clinical Document) 13

5.0 SSA Security Assertion 14

5.1 Subject ID 14

5.2 Subject Organization 14

5.3 Subject Organization ID 14

5.4 Home Community ID 15

5.5 Subject Role 15

5.6 Purpose Of Use 16

5.7 Patient Identifier 16

5.8 Authorization Decision Statement 17

6.0 Access Consent 19

# OVERVIEW

## Purpose

The purpose of this guide is to provide an overview of the Nationwide Health Information Network (NHIN) Interoperability messaging that will occur between the Social Security Administration (SSA) and a Health IT Partner / National Health Information Exchange (NHIE) that integrates via the NHIN. This document is intended to provide an understanding of the flow of web services transactions that are to be used and the information contained within those transactions.

## Intended Audience

The primary audiences for this guide are the individuals responsible for implementing the software solution that will integrate with the Social Security Administration via the NHIN.

## Specifications

In February 2010, the Office of the National Coordinator for Health Information Technology (ONCHIT) released the Final Production Specifications for the NHIN. The specifications can be found at the <http://healthit.hhs.gov> web site under the ONC Initiatives / Nationwide Health Information Network (NHIN) / Resources section. The information contained within this document is based on those specifications.

### Referenced NHIN Specifications

* Access Consent Policies Production Specification v1.0, dated 01/29/2010
* Authorization Framework Production Specification v2.0, dated 01/29/2010
* Query for Documents Production Specification v2.0, dated 01/29/2010
* Retrieve Documents Production Specification v2.0, dated 01/29/2010
* Messaging Platform Production Specification v2.0, dated 01/29/2010
* Patient Discovery Production Specification v1.0, dated 01/29/2010

## Document Conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY"1, and "NEED NOT" in this document are to be interpreted as described in the HL7 Version 3 Publishing Facilitator's Guide (<http://www.hl7.org/v3ballot/html/help/pfg/pfg.htm>).

# Web Service Interfaces

The integration with SSA via the NHIN is comprised of the following three web service interfaces:

* Patient Discovery,
* Query for Documents, and
* Retrieve Documents

## Patient Discovery

The Patient Discovery Web Service Interface adopted by the NHIN is based on the Integrating the Healthcare Enterprise (IHE) Cross Community Patient Discovery (XCPD) profile, and, as the name implies, is used to discover if a patient is known within an NHIE. Health IT Partners integrating with SSA via the NHIN **SHALL** implement this interface. The SSA NHIN gateway will act as the requesting client with the Health IT Partner’s gateway acting as the responding service. Details of the requirements related to this Web service can be found in the NHIN Patient Discovery Production Specification.

## Query For Documents and Retrieve Documents

The Query for Documents and Retrieve Document Web Services Interfaces adopted by the NHIN are based on the IHE Cross Community Access (XCA) and the Cross Enterprise Document Sharing (XDS.b) profiles. These interfaces are used to enumerate and retrieve patient-related documents. Health IT Partners integrating with SSA via the NHIN **SHALL** implement these interfaces. For these web services, the SSA NHIN gateway will act as the requesting client with the Health IT Partner’s gateway acting as the responding gateway. These services will be used to retrieve the patient’s medical information after a patient is discovered to be known at the NHIE.

The Health IT Partner’s gateway will also act as a client of the Query for Documents and Retrieve Document web service interfaces that are hosted by the SSA NHIN gateway. The SSA hosted services will be used by the Health IT Partner to retrieve the access consent policy that has been signed by the patient, or the patient’s legal representative, which authorizes SSA to retrieve the patient’s medical records. In the scenario, the Health IT Partner gateway serves as the requesting gateway, with the SSA NHIN gateway acting as the responder.

More information about these Web services may be found in the NHIN Query for Documents and Retrieve Documents Production Specifications. For more information regarding the access consent policy document, please refer to the Access Consent section (6.0) in this document.

# Messaging Requirements

## Base Messaging Requirements

All messages sent between SSA and a Health IT Partner will be Simple Object Access Protocol (SOAP) 1.2 specification compliant and transmitted over HTTP/S using 2-way SSL authentication.

The Office of the National Coordinator will be establishing a certificate authority and as part of the on-boarding process will provide the appropriate security certificates to the NHIN participants. Please refer to the NHIN Messaging Platform Production Specification for additional information regarding the base messaging requirements of the NHIN.

## WS-Addressing and Asynchronous Support

All three web service interfaces, Patient Discovery, Query for Documents, and Retrieve Documents, require that service implementers (responding gateways) support both synchronous and asynchronous invocations of these Web services, where the responding gateways behavior is determined by the SOAP Header <ReplyTo> element from the requesting gateways SOAP message. Implementers need to be aware that the IHE Technical Framework Technical Committee is prepared to incorporate Change Proposal 420 into the Technical Framework and Supplemental profile specifications, which will align the IHE Asynchronous Web Service support with the Organization for the Advancement of Structured Information Standards (OASIS) Web Services Addressing (WS-Addressing) specification. For additional information please see the text of the change proposal, which may be found at the following link.

<http://wiki.ihe.net/index.php?title=ITI_Change_Proposals_2010>

This change affects the asynchronous support for all three NHIN Web Service interfaces described in this document.

# Message Sequencing

This section describes the sequencing of the Patient Discovery, Query for Documents, and Retrieve Document messages that comprise the integration with SSA. The following diagram depicts the message sequence.



Figure : NHIN Messaging between SSA and Health IT Partner

A detail description of each step in Figure 1 is provided below.

## Patient Discovery Request

Figure 2 depicts Step1 in the messaging sequence where SSA sends the **Patient Discovery Request** message to the Health IT Partner (NHIE).



Figure : Patient Discovery Request

The Patient Discovery request will include the following patient’s data:

* Name (first, middle, last),
* Gender,
* Date of birth,
* Social Security Number, and
* Address.

SSA will be using the Demographic Query only mode of the Patient Discovery transaction (only the demographics of the patient are included in the request) and will not be including a patient identifier in the body of the request. While the Security Assertion Markup Language (SAML) assertion included in the Patient Discovery request from SSA will include a Patient Identifier (see Section 5.7), this identifier is only intended for supporting the privacy policy retrieval and **SHALL** not be used for creating a patient correlation.

The MinimumDegreeMatch element in the request will be set to 100, the highest value defined, to indicate that the responder should have the highest confidence in their patient match response.

Additional information about the SAML assertion can be found in the SSA Security Assertion section 5.0 of this document.

## Initial Access Control Decision

Figure 3 depicts the Step 2 in the sequence where the Health IT Partner performs the **initial security evaluation**.



Figure : Initial Access Control Decision

The Health IT Partner evaluates the SAML assertion information, source organization, purpose of use, role, and asserted privacy policies and takes a decision whether to act upon the SSA Patient Discovery request.

If the Health IT Partner does not accept the SAML assertion statements, the Health IT Partner **SHOULD** return an HTTP Error 403 Forbidden error code and include a reason for the refusal.

## Query for Documents Request (for Access Consent Policy)

Figure 4 depicts Step 3 in the messaging sequence where the Health IT Partner sends a **Query for Documents Request** messageto SSA.



Figure : Query for Documents Request

When issuing the Query for Documents request message to SSA, the Health IT Partner **SHALL** set the value of the patient identifier in the Query for Documents request message to the Patient Identifier value (see Section 5.7) that was included in the SAML assertion of the Patient Discovery request (Section 4.1) from SSA.

$XDSDocumentEntryPatientId **SHALL** be populated with the Patient Identifier value that was included in the SAML assertion of the Patient Discovery request from SSA

$XDSDocumentEntryStatus **SHALL** be populated with ‘urn:oasis:names:tc:ebxml-regrep:StatusType:Approved’

$XDSDocumentEntryClassCode **MAY** be populated with the LOINC code of 57016-8

$XDSDocumentEntryEventCodeList **SHALL** be populated with the InstanceAccessPolicy value (see Section 5.8) that is included in the SAML assertion authorization decision statement of the Patient Discovery request from SSA.

## Query for Documents response (for Access Consent Policy)

Figure 5 depicts Step 4 in the messaging sequence where SSA sends a **Query for Documents Response** message to the Health IT Partner



Figure : Query for Documents Response

The Query for Documents Response will contain the list of access consent policies that can be retrieved for the patient. Since SSA is not a supplier of health data, this list will only include access consent policy documents that can be retrieved by the Health IT Partner. Please note that an access consent policy may be available in multiple formats and the Health IT Partner should ensure that they retrieve the document format that is most compatible with their system.

The following table contains a sample of the XDS metadata values that the Health IT Partner can expect to receive from SSA.

|  |  |
| --- | --- |
| **XDS Metadata** | **Value** |
| availabilityStatus | urn:oasis:names:tc:ebxml-regrep:StatusType:Approved |
| classCode  | 57016-8 (LOINC) |
| classCode DisplayName | Privacy Policy Acknowledgement |
| confidentialityCode | N (Normal) |
| formatCode | urn:ihe:iti:bppc-sd:2007 |
| formatCode codeSystem | 1.3.6.1.4.1.19376.1.2.3 |
| healthcareFacilityTypeCode | 385432009 (SNOMED CT code for Not Applicable) |
| mimeType | text/xml |
| practiceSettingCode | 385432009 (SNOMED CT code for Not Applicable) |
| serviceStartTime | Effective start date of privacy policy (authorization) |
| serviceStopTime | Effective end date of privacy policy (authorization) |
| Title | AUTHORIZATION TO DISCLOSE INFORMATION TO THE SOCIAL SECURITY ADMINISTRATION |

Table 1: Access Consent Policy XDS Metadata

## Retrieve Document Request (for Access Consent Policy)

Figure 6 depicts Step 5 in the messaging sequence where the Health IT Partner sends a **Retrieve Document Request** message to SSA to retrieve access consent policy documents.



Figure : Retrieve Document Request

The request message will use the information that was returned in the previous step, Query for Documents Response for Access Consent Policy (Section 4.4). The ability to retrieve the access consent policy document will be valid throughout the complete transaction sequence between SSA and Health IT Partner. Once SSA has received the last Retrieve Document response message, the ability to retrieve to the access consent policy will no longer be allowed.

## Retrieve Document Response (for Access Consent Policy)

Figure 6 depicts Step 5 in the messaging sequence where SSA sends **Retrieve Document Response** message to the Health IT Partner.



Figure : Retrieve Document Response

SSA will respond with the access consent policy document (Authorization to Release Information) identified in the Retrieve Document request message. Please refer to the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Basic Patient Privacy Consents (BPPC) Integration Profile Trial Implementation for additional information regarding the document structure[[1]](#footnote-1).

## Final Access Control Decision

Figure 8 depicts Step 7 in the messaging sequence where the Health IT Partner makes the final **access control decision**.



Figure : Final Access Control Decision

During this step, the Health IT Partner reviews the access consent policy (authorization to release information) obtained in the previous step, Retrieve Document Request for Access Consent Policy (Section 4.6), and based on the Health IT partner’s state and local policies, takes a decision regarding whether they will accept the policy and allow for the release of medical information. If the Health IT partner accepts the policy, the Health IT partner should establish the necessary security permissions to enable SSA to retrieve the patient medical information. The Health IT Partner **SHOULD** use the access consent policy identifier as a reference mechanism when establishing the permissions for SSA. This will prevent the Health IT partner from having to retrieve the access consent policy document on each request message from SSA.

## Patient Discovery response

Figure 9 depicts Step 8 in the messaging sequence where the Health IT Partner sends a **Patient Discovery Response** message to SSA.



Figure : Patient Discovery Response

If the patient discovery query results in no matches, the Health IT Partner should return an empty result set per the specification.

If the patient discovery request results in an ambiguous match, the Health IT Partner should return an empty result set, as the ambiguous match most likely does not meet the MinimumDegreeMatch requirements of the request[[2]](#footnote-2). When ambiguous matches are close, the Health IT partner may use a response code of ‘AnswerNotAvailable’.

If the patient query results in an unambiguous match for the Health IT partner, in addition to returning the Health IT partner identifier for the patient, the Health IT Partner **SHOULD** return the patient demographics from their system that the Health IT Partner matched on. Providing the patient demographics in the response enables the requester (SSA) to apply their own patient matching algorithms to ensure the quality of the results, and reduce the possibility of a false-positive match.

## Query for Documents Request (for Clinical Document)

Figure 10 depicts Step 9 in the messaging sequence where SSA sends a **Query for Documents request** message to the HIT Partner.



Figure : Query for Documents Request

SSA will initiate a Query for Documents request message for each of the patient identifiers that were returned in the Patient Discovery response message (Section 4.8).

The Health IT Partner **SHALL** support queries based on the following parameters (slots):

$XDSDocumentEntryFormatCode

$XDSDocumentEntryPatientId

$XDSDocumentEntryServiceStartTimeFrom

$XDSDocumentEntryServiceStartTimeTo

$XDSDocumentEntryServiceStopTimeFrom

$XDSDocumentEntryServiceStopTimeTo

$XDSDocumentEntryStatus

For Health IT Partners that support dynamic creation of documents, the partner **SHALL** explicitly look for queries where the $XDSDocumentEntryStatus is set to a value of ‘urn:ihe:iti:2010:StatusCode:DeferredCreation’. In this situation, the document data **SHALL** honor the service start and stop time values, if they are specified in the request.

For Health IT Partners that support a repository of static documents, the partner **SHALL** explicitly look for queries where the $XDSDocumentEntryStatus is set to a value of ‘urn:ihe:iti:2010:StatusCode:Active’. In this situation, the list of available documents **SHALL** honor the service start and stop time values, if they are specified in the request.

NOTE: Empty strings in a query **SHALL** be treated as being equal to NULL or empty value, which is not the same as an unspecified value.

## Query for Documents Response (for Clinical Document)

Figure 11 depicts Step 10 in the messaging sequence where the Health IT Partner sends the **Query for Documents response** message to SSA.



Figure : Query for Documents Response

The response message contains the list of electronic medical record documents that SSA can retrieve.

## Retrieve Documents Request (for Clinical Document)

Figure 12 depicts Step 11 in the messaging sequence where SSA sends **Retrieve Document request** message to Health IT Partner



Figure : Retrieve Document Request

SSA will send a Retrieve Document request message for each of the document references that were returned to SSA in the Query for Documents response message.

## Retrieve Documents Response (for Clinical Document)

Figure 13 depicts Step 12 in the messaging sequence where the Health IT Partner sends **Retrieve Document response** message to SSA.



Figure : Retrieve Document Response

The response message contains the requested document.

# SSA Security Assertion

In accordance with the NHIN Authorization Framework specification, all requests initiated by the Social Security Administration, will include the following security assertion information.

## Subject ID

The subject ID of the assertion will be the Medical Evidence Gathering and Analysis through Health IT (MEGAHIT) application, which is responsible for examining the list of medical sources associated with a disability case and automatically triggering the request for medical records via the NHIN.

The following is a SAML assertion code snippet for this attribute.

<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">

 <saml:AttributeValue>MEGAHIT</saml:AttributeValue>

</saml:Attribute>

## Subject Organization

The subject organization assertion attribute will contain the following value:

Social Security Administration

The following is a SAML assertion code snippet for this attribute.

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

 <saml:AttributeValue>Social Security Administration</saml:AttributeValue>

</saml:Attribute>

## Subject Organization ID

The subject organization ID assertion attribute will contain the following value:

2.16.840.1.113883.3.184

When defining or evaluating security access policies, Health IT Partners **SHOULD** use this Object Identifier (OID) value, and NOT the OID contained in the Home Community ID assertion attribute

The following is a SAML assertion code snippet for this attribute.

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

 <saml:AttributeValue>2.16.840.1.113883.3.184</saml:AttributeValue>

</saml:Attribute>

## Home Community ID

The value contained within the home community ID assertion attribute will be dependent upon the software development lifecycle (SDLC) environment that the request originates. The value will be a sub-arc of the primary Social Security Administration OID, however, the production home community OID will be different from the home community OID that is assigned to a testing environment. Additionally, SSA maintains multiple testing environments, each with its own set of web services endpoints. The value contained within this element can be used to identify the endpoints in the NHIN Universal Description Discovery and Integration (UDDI) registry. This value **SHOULD NOT** be used in defining or evaluating security access policies.

The following is a SAML assertion code snippet for this attribute. The Home Community OID in the example is non-normative, and the actual values for ‘xxx’ and ‘yyy’ will be dependent upon the requesting SSA SDLC environment.

<saml:Attribute Name="urn:nhin:names:saml:homeCommunityId">

 <saml:AttributeValue>urn:oid: 2.16.840.1.113883.3.184.xxx.yyy</saml:AttributeValue>

</saml:Attribute>

## Subject Role

The SSA requests will use a SNOMED CT concept code. Please refer to the HITSP C80 - Clinical Document and Message Terminology Component[[3]](#footnote-3) specification for a current list of values.

The following is a SAML assertion code snippet for this attribute, which is using the Social Worker concept for the subject’s role.

<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">

 <saml:AttributeValue>

 <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="106328005"

 codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED\_CT"

 displayName="Social worker"/>

 </saml:AttributeValue>

</saml:Attribute>

## Purpose Of Use

The SSA requests will use the COVERAGE concept code from the Purpose of Use table in the NHIN Authorization Framework Specification

The following is a SAML assertion code snippet for this 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="COVERAGE"

 codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"

 displayName="Disclosures for insurance or disability coverage determination" />

 </saml:AttributeValue>

</saml:Attribute>

## Patient Identifier

The value provided as the patient identifier will be encoded per the NHIN Authorization Framework specification, and will be unique to the Health IT Partner. This value will only be valid for the duration of the transaction sequence between SSA and Health IT Partner as defined in this document.

The Patient Identifier includes in the SAML Assertion **SHOULD NOT** be used as a correlation identifier. This identifier may only be used to support the Health IT Partner’s ability to retrieve the Access Consent Policy Document.

The following is a SAML assertion code snippet for this attribute.

<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">

 <saml:AttributeValue>54379^^^&amp;2.16.840.1.113883.3.184&amp;ISO</saml:AttributeValue>

</saml:Attribute>

## Authorization Decision Statement

In addition to the security assertion attributes listed above (in sections 5.1 - 5.7), the SAML Assertion that accompanies the SSA requests will also include an **Authorization Decision Statement**.

Per the SAML 2.0 Core specification[[4]](#footnote-4), the Authorization Decision Statement element is a mechanism that 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.

In this instance, the NHIN is using the Authorization Decision Statement to enable an entity to assert the requester should be permitted to execute the transaction based on a specific security policy.

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 enables SSA to convey to a Health IT Partner (responding NHIE) that an access consent privacy policy exists that SSA believes should be considered. The access consent privacy policy will be referenced by value in the InstanceAccessConsentPolicy attribute.

The following is a SAML Authorization Decision statement code snippet.

<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">

 O=Social Security Administration,L=Baltimore,ST=Maryland,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="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:2.16.840.1.113883.3.184.500.123456789

 </saml2:AttributeValue>

 </saml2:Attribute>

 </saml2:AttributeStatement>

 </saml2:Assertion>

 </saml2:Evidence>

</saml2:AuthzDecisionStatement>

For more information regarding these attributes, please refer to the NHIN Authorization Framework specification.

# Access Consent

Under the Health Insurance Portability and Accountability Act (HIPAA), SSA is not considered to be a covered entity, in that, releasing information to SSA is not considered to be related to treatment, payment, or operations. Under HIPAA, SSA must collect a signed authorization from the patient or the patients’ representative in order to gather the patient’s medical information. Within SSA, the authorization document is known as Form SSA-827: Authorization to Disclose Information to Social Security Administration. A PDF version of the form may be downloaded from the following web site: <http://www.ssa.gov/online/ssa-827.pdf>. When this document is retrieved from SSA, it will be in embedded within an HL7 Clinical Document Architecture (CDA) document. The format of the document will be based on the Integrating the Healthcare Enterprise (IHE) Basic Patient Privacy Consents (BPPC) Profile. The XDS metadata for the document will indicate that it is a Privacy Policy Acknowledgement with a LOINC value of 57016-8., and format code of ‘urn:ihe:iti:bppc-sd:2007’.

For more information regarding Access Consent, please refer to the NHIN Access Consent Policies specification. Additional information regarding the IHE BPPC profile may be found in the IHE ITI Technical Framework specifications[[5]](#footnote-5).

1. <http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_6-0_Vol3_FT_2009-08-10-2.pdf> [↑](#footnote-ref-1)
2. Refer to section 4.1 [↑](#footnote-ref-2)
3. <http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=80> [↑](#footnote-ref-3)
4. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf> [↑](#footnote-ref-4)
5. <http://www.ihe.net/Technical_Framework/>

 <http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_6-0_Vol3_FT_2009-08-10-2.pdf> [↑](#footnote-ref-5)