Michigan Health Information Network Shared Services

Respond to Social Security Administration (SSA) Requests for CCD Implementation Guide

Version 5.0

26 February 2015

Document History

Date	Version	Section(s) Revised	Description	Modifier
10/21/14	1.0	All	Initial Draft	Ward
11/11/14	2.0	All	Internal MiHIN review	Ward
12/19/14	3.0	All	Edit terms based on MiHIN's documentation rules	Vo
02/04/15	4.0	All	Edit terms based on MiHIN's documentation rules	Ward
02/26/15	5.0	Introduction, Specifications	References to SSA documentation updated	Ward

Acronyms and Abbreviations Guide

Object	Description
AA	Assigning Authority
AD	Advance Directive
C32	HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component - http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=32
C62	The HITSP Unstructured Document Component is provided for the capture and storage of patient identifiable, unstructured document content, such as text, PDF, and images rendered in PDF. It is based on the Cross-Enterprise Sharing of Scanned Documents (XDS-SD) profile from IHE - http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=62
C83	The HITSP CDA Content Modules Component. The CDA Content Modules Component defines the content modules for document based HITSP constructs utilizing clinical information- http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=83
CCD	Continuity of Care Document

Object	Description
CGS	Common Gateway Service
CHDR	Clinical Data Repository / Health Data Repository
CMS	Centers for Medicare or Medicaid Services - http://www.cms.gov/
CONNECT	An open source software solution that supports health information exchange – both locally and at the national level. CONNECT uses Nationwide Health Information Network standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country (http://www.connectopensource.org/). This software solution was initially developed by federal agencies to support their health-related missions, but it is now available to all organizations and can be used to help set up health information exchanges and share data using nationally-recognized interoperability standards.
CQO	Consumer Qualified Data Sharing Organization
DS Message	A message specific to the Document Submission (DS) Specification that conforms in content and format to the Integrating the Healthcare Enterprise's (IHE) Cross-enterprise Document Reliable Interchange specification.
DSO	Data Sharing Organization or Qualified Organization (QO)
EdgeSim	Simulators that are utilized in a testing environment to simulate testing with a Data Sharing Organization
EHR	Electronic Health Record
esMD	CMS Electronic Submission of Medical Documentation - http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/index.html?redirect=/ESMD
FedSim	Simulators that are utilized in a testing environment to simulate testing with a federal partner e.g. SSA or VA
HIE-QO	Health Information Exchange Qualified Data Sharing Organization
HITSP	Health Information Technology Standards Panel - http://hitsp.org/
IHE	IHE (Integrating the Healthcare Enterprise) is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information (http://www.ihe.net/). IHE promotes the coordinated use of

Object	Description
	established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. The NwHIN specifications utilize underlying IHE specifications for various services for health data exchange
MDCH	Michigan Department of Community Health - http://www.michigan.gov/mdch
MiHIN	Michigan Health Information Network Shared Services - http://mihin.org/
Nationwide Health Information Network	The Nationwide Health Information Network (NwHIN) is intended to provide a secure, nationwide, interoperable health information infrastructure that connects providers, consumers, and others involved in supporting health and healthcare.
NHIO	Health Information Organizations which act as nodes on the Nationwide Health Information Network are termed as NHIOs. The NHIOs use the NwHIN web services to facilitate exchange of information with other nodes in the network.
NwHIN	Nationwide Health Information Network specified web service interfaces
NwHIN Authorization Framework Specification	The purpose of this specification is to define the required exchange of information describing the initiator of a request between HIOs participating in the NwHIN network. This enables a responding NHIO to evaluate the request based on the initiating NHIOs assertions and its own local policies and permissions.
NwHIN Document Submission (DS) Web Service Interface Specification	The purpose of this specification is to provide the ability to "submit" data for a given patient from an exchange partner to a HIE using configuration on the submission side.
NwHIN Gateway	An implementation of the Nationwide Health Information Network specified web service interfaces. These web service interfaces communicate over HTTPS secured using Public Key Infrastructure supported by the Nationwide Health Information Network Operational Infrastructure.
NwHIN interface	The gateway accepts messages from the Nationwide Health Information Network into the gateway using web services as defined by the NwHIN specifications. These messages are then processed by various components in the gateway. These components may also be configured to work in pass-through mode, in which case the message is accepted from the Nationwide Health Information Network and

Object	Description
	passed directly to the adapter without additional processing like policy checks, patient correlation checks etc.
NwHIN Messaging Platform Specification	The purpose of this specification is to define a base set of messaging standards and web service protocols which must be implemented by each node in the NwHIN network and applies to all NwHIN transactions.
NwHIN Patient Discovery (PD) Web Service Interface Specification	The purpose of this specification is to define the mechanism by which one NwHIN node can query another to reciprocally establish patient identity and to determine if a node may be a source of information for a specific patient.
NwHIN Query for Documents (QD) Web Service Interface Specification	The purpose of this specification is to define the mechanism by which an initiating NwHIN node can request a patient-specific list of available documents from a responding node using the patient ID obtained by a prior Patient Discovery (PD) transaction.
NwHIN Retrieve Documents (RD) Web Service Interface Specification	The purpose of this specification is to define the mechanism by which an Initiating NwHIN node can retrieve specific documents from a responding node using the Document Reference IDs obtained using a prior Query for Documents (QD) transaction.
OID	Object Identifier, as issued by HL7 (http://www.hl7.org/oid/index.cfm)
ONC	Office of the National Coordinator
PO	Participating Organization - DSO onboarding to the Common Gateway Service
PD Message	A message specific to the Patient Discovery (PD) Web Services Interface Specification that references the Integrating the Healthcare Enterprise's (IHE) Cross-Community Patient Discovery (XCPD) specification.
PHR	Personal Health Record
PoM	Peace of Mind - Advance Directive Registry

Object	Description
QD Message	A message specific to the Query for Documents (QD) Web Services Interface Specification that references the Integrating the Healthcare Enterprise's (IHE) Cross-Community Access (XCA) specification.
QO	Qualified Data Sharing Organization
RD Message	A message specific to the Retrieve Documents (RD) Web Services Interface Specification that references the Integrating the Healthcare Enterprise's (IHE) Cross-Community Access (XCA) specification.
REST	REST stands for **Re**presentational **S**tate **T**ransfer. (It is sometimes spelled "ReST".) It relies on a stateless, client-server, cacheable communications protocol -- and in virtually all cases, the HTTP protocol is used.
SOAP	SOAP originally defined as Simple Object Access Protocol is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics. For the Nationwide Health Information Network to be a truly scalable, secure and interoperable network, a common transport layer is essential. The Messaging Platform is based on SOAP 1.2 messages over HTTP.
Specification	Specifications provide a standard set of service interfaces that enable the exchange of interoperable health information among the Health Information Exchanges (HIEs).
SSA	Social Security Administration - http://www.ssa.gov/
SSO	Sponsored Data Sharing Organization
SSSO	State Sponsored Data Sharing Organization
Target HIE	The HIE or Nationwide Health Information Network Node that the message or feedback is being addressed.
UCA	Use Case Agreement
UCS	Use Case Summary
VA	Department of Veterans Affairs - http://www.va.gov/
VPN	Virtual Private Network

Object	Description
VQO	Virtual Qualified Data Sharing Organization
XCA	Cross Community Access
XDR	Cross-Enterprise Document Reliable Interchange
XDS	Cross-Enterprise Document Sharing

Table of Contents

Introduction

Purpose of Use Case

The Social Security Administration (SSA) utilizes the ONC Nationwide Health Information Network (NwHIN) specifications to assist in clinical document exchange between a healthcare participant and the Social Security Administration. SSA requests medical documentation from a healthcare provider with the patient's authorization for the purpose of disability determination. This use case allows Participating Organizations within the Michigan Health Information Network (MiHIN) to supply patient documentation through MiHIN to SSA, while also retrieving patient authorization documents from SSA.

The purpose of this guide is to give an overview of the ONC Nationwide Health Information Network (NwHIN) interoperability messaging that occurs between the Social Security Administration (SSA) and the Participating Organization (PO) via MiHIN.

Introduction to MiHIN

Currently there are numerous Data Sharing Organizations in Michigan (i.e. HIEs, Payers, Pharmacies, State Agencies), which have completed the necessary legal documents to become a Qualified Organization (QO) for data sharing in Michigan. These DSOs are already linked to MiHIN using various forms of transport: secure https POST or LLP over VPN, and Direct Secure Messaging. Some of the DSOs are regionally focused while others have members throughout the state. The DSOs work with the healthcare providers in their regions to implement systems for electronically exchanging healthcare information.

MiHIN is working with DSOs from other states along with the Federal agencies VA, SSA, and CMS esMD, to promote the secure exchange of healthcare information across state lines using the eHealth Exchange (formerly Nationwide Health Information Network) and using Direct Secure Messaging, for claims and cases where someone who moves or is traveling needs health care in a different state.

This Use Case relies on MiHIN infrastructure called the Common Gateway Service. The Common Gateway Service offers the capability to both submit, request and exchange healthcare data throughout Michigan or with other states.

Common Gateway Service and Use Cases

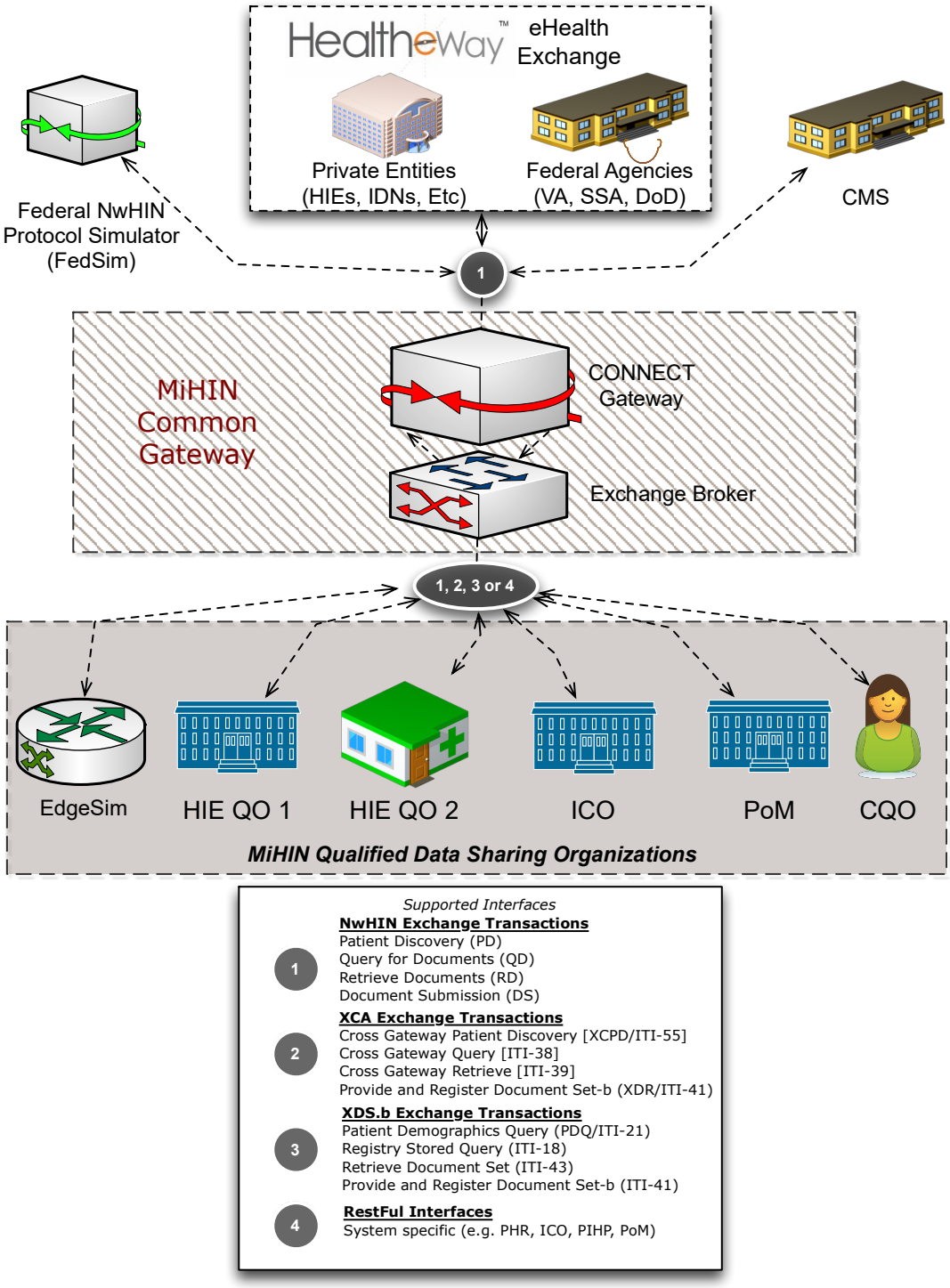
The Common Gateway Service consists of a CONNECT Gateway together with an Exchange Broker.

The CONNECT Gateway utilizes ONC Nationwide Health Information Network (NwHIN) SOAP based messaging to submit healthcare information using the Document Submission (DS) message, or healthcare information request using the Patient Discovery (PD), Document Query (DQ), and Document Retrieve (DR) messages to other eHealth Exchange participants, such as the federal agencies (SSA, VA, CMS esMD).

The Exchange Broker manages message transformation and routing not only to and from the eHealth Exchange but also to and from Michigan's Data Sharing Organizations (DSOs). The transformation services allow DSOs to send and receive in a number of protocols whether it is NwHIN SOAP, or the more widely used IHE standards for XCA or XDS.b. While the routing services send messages to applicable DSOs and eHealth Exchange participants based on the use cases a DSO has agreed to.

The Common Gateway Service is depicted below:

Common Gateway Service Context Diagram



When DSOs agree to exchange data through MiHIN there are a number of Use Cases where the Common Gateway Service can be used as the transport method:

1. **Exchange Advance Directives** – exchanging Advance Directive documents (e.g. between MyHealthPortal (myHB)/ MyHealthButton (myHP) and Peace of Mind (PoM); and/or Hospital Systems (through HIE), and PoM and/or PHRs
2. **Exchange Integrated Care Bridge Record (ICBR)** – exchanging Integrated Care Bridge Records either internal to an Integrated Care Organization (ICO) within their associated Integrated Care Teams (ICT), or between ICOs and/or Pre-paid Inpatient Health Plans (PIHPs)
3. **Exchange Patient Continuity of Care Documents Statewide** - exchanging patient healthcare information within Michigan
4. **Exchange Continuity of Care Documents with VA** - exchanging veterans' healthcare information between DSO providers and the Department of Veterans Affairs (VA)
5. **Respond to SSA Disability Determination Requests for CCD** - Responding to Social Security Administration (SSA) eligibility claims for patients within a DSO(s) network of providers
6. **Respond to CMS Electronic Submission of Medical Documentation (eSMD) Request for CCD** - Submitting documents to the Centers for Medicare and Medicaid Services Electronic Submission of Medical Documentation System (CMS esMD) in support of eligibility determinations for patients within a DSO(s) network of providers
7. **Exchange Continuity of Care Documents Outside Michigan (non-VA/SSA)** - exchanging patient healthcare information between DSO providers and other non-federal organizations outside of Michigan

As indicated in the diagram above MiHIN has developed two simulators to aid DSOs onboarding into the Common Gateway Service by simulating either the Federal Agency Use Cases (FedSim) or other DSOs (EdgeSim). This allows MiHIN and a DSO to extensively test and verify that their systems work together and are ready enter production.

Data Flow and Actors

In this Use Case, MiHIN brokers the messaging between the Social Security Administration and the Participating Organization (PO).

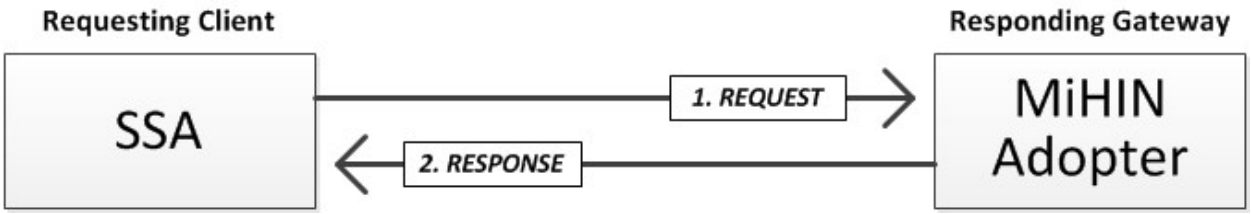
Web Services between MiHIN and SSA

Three of the primary component web services of the document exchange process between SSA and MiHIN are:

- **Patient Discovery (PD)**
- **Query for Documents (QD)**
- **Retrieve Documents (RD)**

Patient Discovery (PD)

The Patient Discovery, or PD, web service interface is used by the requesting entity to determine if the patient exists in the responding entity's system and has supporting documents. When making a determination, the Social Security Administration first sends a PD request to the PO. The SSA gateway acts as the requesting gateway with the PO's gateway acting as the responding gateway:



Query for Documents (QD)

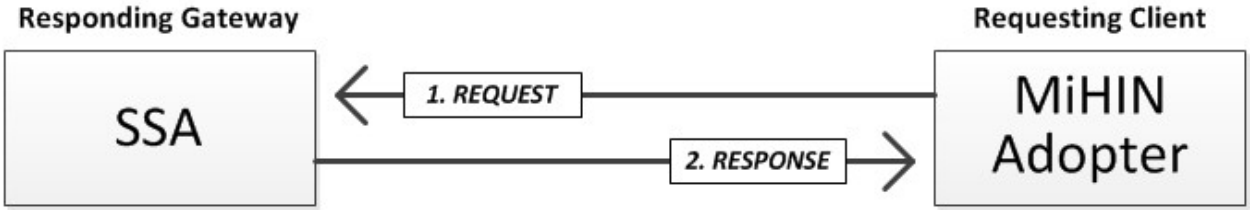
The Query for Documents, or QD, web service interface is used to identify the medical documents available from the PO for the patient specified by the Patient ID in the Patient Discovery transaction. For these web services, the SSA gateway acts as the requesting client with the PO's gateway acting as the responding gateway.

The PO's gateway also acts as the requesting gateway for the Query for Documents and Retrieve Document web services interfaces that are hosted by the SSA NwHIN gateway. The SSA hosted services are used by the adopter to retrieve the access consent policy documents.

Retrieve Documents (RD)

The Retrieve Documents, or RD, web service interface is used to obtain medical documents from the PO for the patient using the document metadata in the Query for Documents response. For these web services, the SSA gateway acts as the requesting client with the PO's gateway acting as the responding gateway.

On the occasions when the roles are reversed with the PO initiating the request to SSA (as when it is seeking the proper Access Control Policies from SSA for a particular PD exchange), the PO gateway acts as the requesting client with SSA acting as the responding gateway for both Query for Documents and Retrieve Documents services:



Web Services between PO and MiHIN

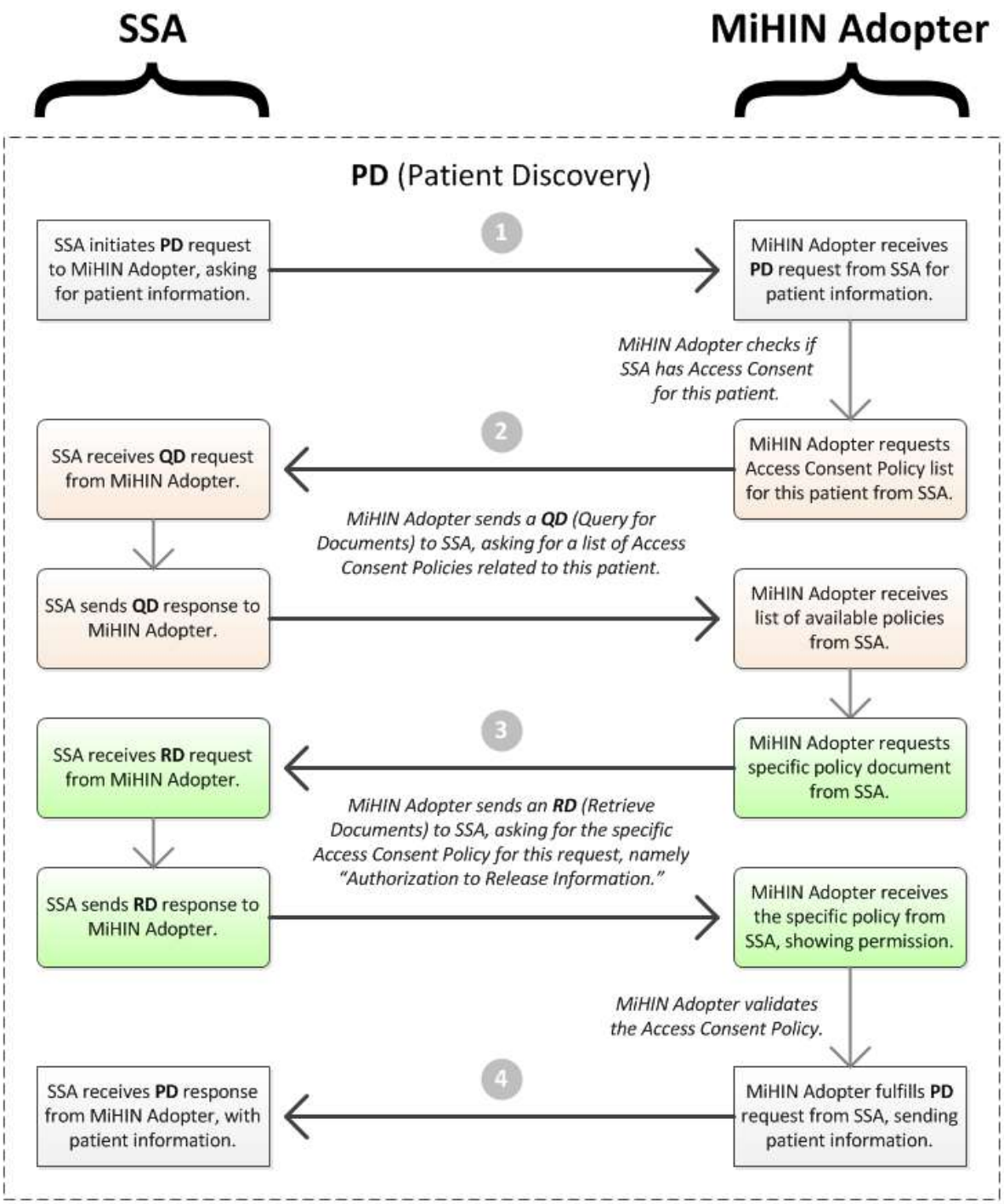
MiHIN considers itself "transport agnostic" and offers multiple options for DSOs to exchange data via MiHIN.

While transactions between Common Gateway Service and SSA strictly follow NwHIN standards, eHealth Exchange policy and specifications; MiHIN offers support for other IHE transactions to support organizations within the Michigan qualified data sharing network that do not have capabilities to generate NwHIN transactions. MiHIN bridges the gap between the underlying IHE specifications like XCPD and the requirements or constraints additionally stipulated by NwHIN by providing additional configurations at the broker to facilitate exchange.

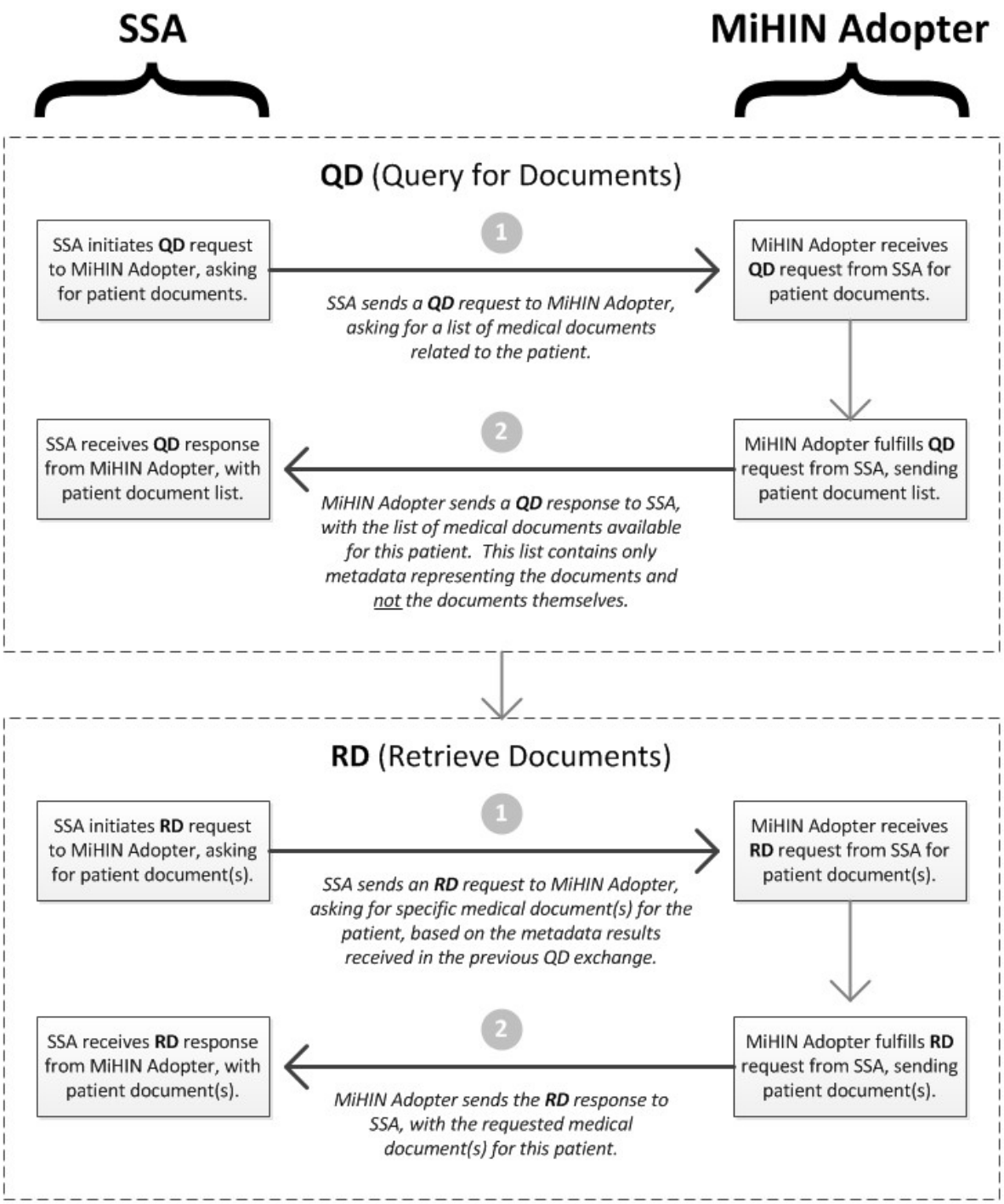
For more information on transactions supported by the Common Gateway Service and their specifications and the specifications for Patient Discovery, Query for Documents and Retrieve Documents, see Common Gateway Service Transactions and Specifications.

General Sequence of Messages

Communication between SSA and the PO begins with the PD exchange, as diagrammed here:



After a successful PD exchange between the Social Security Administration and the PO, SSA can subsequently initiate QD and RD messages to the PO to obtain medical documents related to the patient in question.



For details on each step of the messaging sequence and fields required for each transaction, refer to the SSA_eHEX_Interoperability_Guide_V_3_0.pdf documentation.

Standard Overview

Message

The **Message Content and Notices** submitted to and received from the Common Gateway Service meets the following standards:

- the ONC NwHIN Specifications set forth on the Healtheway website - Exchange Specifications, or
- the IHE Cross-Community Access (XCA) specifications, supplemented with the message content required for a NwHIN SAML assertion.
- the IHE Cross-Enterprise Document Sharing (XDS.b) specifications, supplemented with the message content required for a NwHIN SAML assertion.

Content

The **Message Payload** submitted to to and received from the Common Gateway Service meets the following standards for HITSP C32 or C62 formats or the HL7 C-CDA format, both with the underlying CCD specification as per HL7:

- Continuity of Care Document (CCD) - HL7/ASTM Implementation Guide for CDA® R2 Continuity of Care Document (CCD®) Release 1

Meaningful Use Stage 1:

- HITSP C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) Component
- HITSP C62 - Unstructured Document Component

Meaningful Use Stage 2:

- Consolidated Clinical Document Architecture (C-CDA) - HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, Release 1.1 - US Realm
- Consolidated Clinical Document Architecture (C-CDA R2) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes

Onboarding Process and Testing

Initial Onboarding

For organizations to share data with MiHIN under this use case, the organization undergoes two onboarding processes simultaneously. The two onboarding processes are legal onboarding and technical connectivity onboarding. These may occur in parallel – i.e. the organization can review and complete legal agreements with MiHIN while simultaneously establishing and testing technical connectivity. To initiate these two parallel onboarding processes, notify MiHIN via email at **help@mihin.org**.

Initial Legal Process

The first time an organization undergoes the legal onboarding process with MiHIN, the organization negotiates and enters into a master Participating Organization agreement which then allows the Participating Organization to enter into one or more use cases via Use Case Agreements. There are numerous different kinds of master Participating Organization agreements, available at http://mihin.org/about-mihin/resources/mihin-legal-document-templates.

Once an organization has entered into a master Participating Organization agreement, the organization can enter into an unlimited number of use cases with MiHIN. All of MiHIN's use cases are available at http://mihin.org/about-mihin/resources/mihin-legal-document-templates.

Initial Technical Connectivity Process

First steps for connecting to the staging Common Gateway Service are as follows:

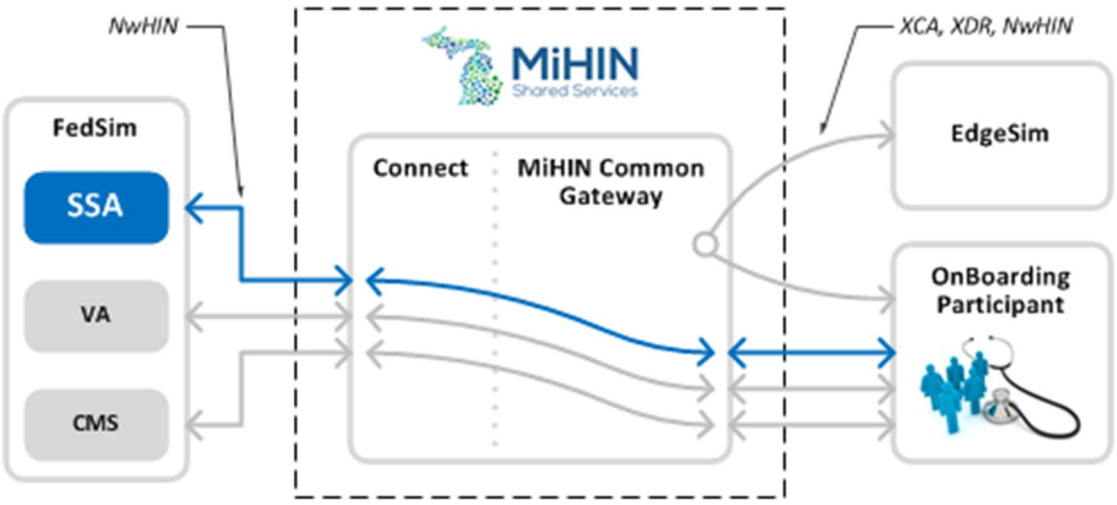
1. Request and subsequently submit the MiHIN site-to-site VPN request form. Form includes technical contacts, reason for VPN request, IP and port values for connecting server.
2. New participating organization is added onto the MiHIN VPN. (Confirmation performed using telnet from both sides).
3. Participating organization supplies the following information to MiHIN:
    1. Self-signed Certificate from organization server (to be added to Common Gateway trust store)
    2. Organization Home Community ID (unique OID)
    3. Organization Assigning Authority (unique OID)
    4. Organization Repository ID (unique OID)
    5. DS, PD, QD, RD service endpoints

6. Organization assertion information

4. Participating organization is supplied by MiHIN with:
    1. Self-signed Certificate from Common Gateway server (to be added to participating organization's server trust store)
    2. Common Gateway DS, PD, QD, RD service endpoints
    3. Staging simulators' HCID, assigning authority, and repository ID for onboard testing
5. Organizations should select one or more connectivity methods for message transport (e.g. PD, XCPD, or PDQ) based on their technical capabilities, and should communicate the selection(s)

Technical onboarding and testing

Context diagram of the Common Gateway testing environment



Technical onboarding and testing is a three step process, first starting with connectivity testing utilizing MiHIN simulators of the federal environment, followed by more focused use case testing with the simulators and finally an end to end testing between the trading partners.

Connectivity and smoke test with Federal Simulator (FedSim) (non-use case specific)

If the on-boarding participant has not had any prior testing for any exchange use cases, smoke tests for connectivity is required. The smoke tests includes basic tests into the broker with the goal of hitting the Federal Simulator's PD, QD, and RD (and DS if applicable). The participants service is smoke tested as well with the Federal Simulator sending out PD, QD, RD and possibly DS requests via the staging Common Gateway. The results of the tests and various log files in the MiHIN servers will be confirmed for connectivity.

Testing utilizing Federal Simulator (inbound and outbound) - SSA transaction flow

The Federal Simulator can mock the various SSA workflows specifically in regards to ACP lookups. The on-boarding participant are provided test data to test the SSA work flows through the simulator. The goal of this testing phase is to ensure the participant can respond to an inbound patient discovery, can perform the needed ACP lookup and processing, and can subsequently have documents for that patient queried and retrieved.

Testing with SSA Disability Determination Use Case

On completion of testing with FedSim, the PO commences testing with the SSA via MiHIN.

These test cases below provide an overview of the tests that SSA tests with every partner on the Exchange. For a detailed list of test case documents and test data refer to the SSA NHIN Test case documentation.

SSA Disability Determination Test cases (for participants with a single Assigning Authority)

Basic flow for Access Control decision cycle

Each test case scenario for participants with a single Assigning Authority begins with the following Access Control decision cycle, either as one synchronous flow or as a series of manually-triggered events:

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters ***Includes references from SSA NHIN Interoperability Guide***
1	SSA initiates a PD request to the NwHIN participant's gateway	• First Name • Middle Name • Last Name • Alias • Gender • DOB • SSN • Address	QD request for Access Consent Policy document from the NwHIN participant's gateway	$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:ebxmlregrep: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 is SSA Interoperability guide) that is included in the SAML assertion authorization decision statement of the Patient Discovery request from SSA.

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters *Includes references from SSA NHIN Interoperability Guide*
2	NwHIN participant sends QD request to SSA (for Access Consent Policy Document)	• patientId = value of the patient Identifier from SAML assertion • availabilityStatus=urn:oasis:names:tc:ebxml-regrep:StatusType:Approved • classCode = LOINC (57016-8) or Class code from participant • **(O)** eventCodeList = InstanceAccessPolicy value included in the SAML assertion sent by SSA.	N/A	N/A
3	SSA initiates a QD response to NwHIN participant (for Access Consent Policy Document)	N/A	RD request for Access Consent Policy Document from the NwHIN participant's gateway	The request message uses 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 is 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 is no longer be allowed.
4	NwHIN participant sends a RD request to SSA to retrieve Access Consent Policy documents	• homeCommunityOID must be that of SSA i.e. 2.16.840.1.113883.3.184.6.1 • repositoryUniqueId • documentUniqueId	N/A	The request message uses 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 is 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 the access consent policy is no longer allowed.

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters *Includes references from SSA NHIN Interoperability Guide*
5	SSA sends a RD Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA

Patient not found scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a Retrieve Document Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response consisting of an empty result set	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA
6	NwHIN participant sends a PD response to SSA.	PD response with an empty result set	N/A	N/A

Patient is an ambiguous match and PD Response is 'AnswerNotAvailable' scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a RD Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD Response with error code 'AnswerNotAvailable', as described in section 4 of the NwHIN PD specification	N/A
6	NwHIN participant sends a PD response to SSA.	PD Response with error code 'AnswerNotAvailable', as described in section 4 of the NwHIN PD specification	N/A	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA

Patient is an unambiguous match and no clinical documents returned scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a RD Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response with a patient identifier	N/A
6	NwHIN participant sends a PD response to SSA.	PD response with a patient identifier	N/A	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
7	SSA sends a QD Request for Patient Documents (for Clinical Documents)	N/A	NwHIN participant's gateway sends QD response with zero document references	N/A
8	NwHIN participant's gateway sends a QD response to SSA (for Clinical Documents)	QD response with zero document references	N/A	N/A

Patient is an unambiguous match and one or more clinical documents are returned scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a RD Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response with a patient identifier	N/A

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
6	NwHIN participant sends a PD response to SSA.	PD response with a patient identifier	N/A	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA
7	SSA sends a QD Request for Patient Documents (for Clinical Documents)	• patientID= patient ID sent in PD-response • serviceStopTimeFrom • availabilityStatus=urn:oasis:names:tc:ebxml-regrep:StatusType:Approved. May contain additional values for static or dynamic creation i.e. urn:ihe:iti:2010:StatusCode:Active, or urn:ihe:iti:2010:StatusCode:DeferredCreation respectively formatCode=urn:ihe:pcc:xphr:2007 (for CCDs)	NwHIN participant's gateway sends QD response with one or more document references	N/A

8	NwHIN participant's gateway sends a QD response to SSA (for Clinical Documents)	QD response with one or more document references with the following XDS metadata: • Where defined in the XDS profile, all classification UUIDs must match those of the XDS profile • All XDS slot names must follow the exact format, spelling and letter casing as specified in the standard • Home OID must match the NwHIN participant's OID • availabilityStatus must match the value(s) specified in the QD request • Size is a non-zero integer. Must be '-1' for dynamically generated documents • Hash contains hash value. Must be '-1' for dynamically generated documents • confidentialityCode=N • creationTime precision level must be at or higher than YYYYMMDD • healthcareFacilityType = SNOMED-CT code • practiceSetting = SNOMED-CT code • sourcePatientID must match the ID sent in the PD Response • repositoryUniqueId must match the home OID for the registry object • uniqueId must contain a valid document reference • classCode = LOINC (34133-9) for CCD or other LOINC code depending on document type. Must correspond to the formatCode if specified in the QD request. Coding scheme must be 2.16.840.1.113883.6.1 • **(O)** typeCode: If specified in the QD response it must correspond to the formatCode value sent in the QD request. May contain the same value as classCode • **(O)** formatCode: If specified in the QD request it must match the value sent in the QD request. If not specified in the QD request, the value can be any valid XDS document format code. Coding scheme must be 1.3.6.1.4.1.19376.1.2.3 • **(O)** mimeType matches the value for the requested document type (e.g. mimeType="text/xml" for CCD) • patientId must match the ID sent in the PD Response	N/A	N/A

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
		• **(O)** If specified, sourcePatientInfo elements must conform to the HL7 Patient Identification (PID) segment semantics • **(O)** If specified, the author attribute represents the machine and/or humans that authored the document. Sub-attributes of author are authorPerson, authorInstitution, authorRole, and authorSpecialty. There must be one instance of the authorPerson sub-attribute, and the rest of the sub-attributes can have zero or more instances.		
9	SSA sends a separate RD request for each document reference returned in the QD response	Document data returned in QD response	NwHIN participant's gateway sends an RD response containing a document, for each corresponding RD request	N/A
10	NwHIN participant's gateway sends a RD response to SSA (for Clinical Documents) for each corresponding RD request	Each document returned must have metadata matching the following criteria: • homeCommunityId matches the OID of the NwHIN Participant • repositoryUniqueId matches the value sent in the RD-Request • documentUniqueId matches the value sent in the RD-Request • mimeType matches the value for the requested document type (e.g. mimeType="text/xml" for CCD)	N/A	N/A

SSA Disability Determination Test cases (for participants with multiple Assigning Authorities)

Basic flow for Access Control decision cycle

Each test case scenario for participants with multiple Assigning Authorities begins with the following Access Control decision cycle, either as one synchronous flow or as a series of manually-triggered events:

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
1	SSA initiates a PD request to the NwHIN participant's gateway	• First Name • Middle Name • Last Name • Alias • Gender • DOB • SSN • Address	QD request for Access Consent Policy document from the NwHIN participant's gateway	$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:ebxmlregrep: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.
2	NwHIN participant sends QD request to SSA (for Access Consent Policy Document)	• patientId = value of the patient Identifier from SAML assertion • availabilityStatus=urn:oasis:names:tc:ebxml-regrep:StatusType:Approved • classCode = LOINC (57016-8) or Class code from participant • **(O)** eventCodeList = InstanceAccessPolicy value included in the SAML assertion sent by SSA.	N/A	N/A

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
3	SSA initiates a QD response to NwHIN participant (for Access Consent Policy Document)	N/A	RD request for Access Consent Policy Document from the NwHIN participant's gateway	The request message uses 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 is 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 is no longer allowed.
4	NwHIN participant sends a RD request to SSA to retrieve Access Consent Policy documents	• homeCommunityOID must be that of SSA i.e. 2.16.840.1.113883.3.184.6.1 • repositoryUniqueId • documentUniqueId	N/A	The request message uses 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 is 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 is no longer allowed.

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SA sends a Retrieve Document Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA

Patient not found scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a Retrieve Document Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response consisting of an empty result set	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
6	NwHIN participant sends a PD response to SSA.	PD response with an empty result set	N/A	N/A

Patient is an ambiguous match and PD Response is 'AnswerNotAvailable' scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a Retrieve Document Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD Response with error code 'AnswerNotAvailable', as described in section 4 of the NwHIN PD specification	N/A
6	NwHIN participant sends a PD response to SSA.	PD Response with error code 'AnswerNotAvailable', as described in section 4 of the NwHIN PD specification	N/A	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA

Patient is an unambiguous match and no clinical documents returned scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a Retrieve Document Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response with a single patient identifier for each assigning authority for which the match happened	N/A
6	NwHIN participant sends a PD response to SSA.	PD response with a single patient identifier for each assigning authority for which the match happened	N/A	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA
7	SSA sends a QD request for each of the patient identifiers returned in the PD response	N/A	NwHIN participant's gateway sends QD response with zero document references, for each corresponding QD request	N/A
8	NwHIN participant's gateway sends one or more QD responses to SSA (for Clinical Documents)	QD response with zero document references for each corresponding QD request	N/A	N/A

Patient is an unambiguous match and one or more clinical documents are returned scenario

(Continues from Step 5 from the Basic flow for Access Control decision cycle)

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
5	SSA sends a RD Response (Access Consent Policy Document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their access control policies.	N/A	PD response with a single patient identifier for each assigning authority for which the match happened	N/A
6	NwHIN participant sends a PD response to SSA	PD response with a single patient identifier for each assigning authority for which the match happened	N/A	NwHIN participant shall use the Access Consent Policy identifier as a reference mechanism when establishing the permissions for SSA
7	SSA sends a QD request for each of the patient identifiers returned in the PD response	• patientID= patient ID sent in PD-response • serviceStopTimeFrom • availabilityStatus=urn:oasis:names:tc:ebxml-regrep:StatusType:Approved. May contain additional values for static or dynamic creation i.e. urn:ihe:iti:2010:StatusCode:Active, or urn:ihe:iti:2010:StatusCode:DeferredCreation respectively formatCode=urn:ihe:pcc:xphr:2007 (for CCDs)	NwHIN participant's gateway sends QD response with one or more document references, for each corresponding QD request	N/A

8	NwHIN participant's gateway sends one or more QD responses to SSA (for Clinical Documents)	QD response with one or more document references with the following XDS metadata (for each QD request): • Where defined in the XDS profile, all classification UUIDs must match those of the XDS profile • All XDS slot names must follow the exact format, spelling and letter casing as specified in the standard • Home OID must match the NwHIN participant's OID • availabilityStatus must match the value(s) specified in the QD request • Size is a non-zero integer. Must be '-1' for dynamically generated documents • Hash contains hash value. Must be '-1' for dynamically generated documents • confidentialityCode=N • creationTime precision level must be at or higher than YYYYMMDD • healthcareFacilityType = SNOMED-CT code • practiceSetting = SNOMED-CT code • sourcePatientID must match the ID sent in the PD Response • repositoryUniqueId must match the home OID for the registry object • uniqueId must contain a valid document reference • classCode = LOINC (34133-9) for CCD or other LOINC code depending on document type. Must correspond to the formatCode if specified in the QD request. Coding scheme must be 2.16.840.1.113883.6.1 • **(O)** typeCode: If specified in the QD response it must correspond to the formatCode value sent in the QD request. May contain the same value as classCode • **(O)** formatCode: If specified in the QD request it must match the value sent in the QD request. If not specified in the QD request, the value can be any valid XDS document format code. Coding scheme must be 1.3.6.1.4.1.19376.1.2.3 • **(O)** mimeType matches the value for the requested document type (e.g. mimeType="text/xml" for CCD) • patientId must match the ID sent in the PD Response	N/A	N/A

Step	Scenario	Request parameters	Expected response	Access Consent Policy parameters
		• **(O)** If specified, sourcePatientInfo elements must conform to the HL7 Patient Identification (PID) segment semantics • **(O)** If specified, the author attribute represents the machine and/or humans that authored the document. Sub-attributes of author are authorPerson, authorInstitution, authorRole, and authorSpecialty. There must be one instance of the authorPerson sub-attribute, and the rest of the sub-attributes can have zero or more instances.		
9	SSA sends a separate RD request for each document reference returned in the QD response	Document data returned in QD response(s)	NwHIN participant's gateway sends an RD response containing a document, for each corresponding RD request	N/A
10	NwHIN participant's gateway sends a RD response to SSA (for Clinical Documents) for each corresponding RD request	Each document returned must have metadata matching the following criteria: • homeCommunityId matches the OID of the NwHIN Participant • repositoryUniqueId matches the value sent in the RD-Request • documentUniqueId matches the value sent in the RD-Request • mimeType matches the value for the requested document type (e.g. mimeType="text/xml" for CCD)	N/A	N/A

Specifications

Message Format

For all messaging requirement details refer to SSA_eHEX_Interoperability_Guide_V_3_0.pdf. Some key notes:

1. PD request from SSA includes - Name (first, middle, last), Gender, Date of birth, Social Security Number, and Address
2. QD request from DSO to SSA for Access Consent policy requires-
    1. $XDSDocumentEntryPatientId - Patient Identifier value that was included in the SAML assertion of the PD request from SSA,
    2. $XDSDocumentEntryStatus – 'urn:oasis:names:tc:ebxml-regrep:StatusType:Approved'
    3. $XDSDocumentEntryClassCode - 57016-8 (optional)
    4. $XDSDocumentEntryEventCodeList - InstanceAccessPolicy value that is included in the SAML assertion authorization decision statement of the PD request from SSA.
3. QD response from SSA metadata values for Access Consent policy
    1. availabilityStatus - urn:oasis:names:tc:ebxml-regrep:StatusType:Approved
    2. classCode - 57016-8 (LOINC)
    3. classCode DisplayName - Privacy Policy Acknowledgement
    4. confidentialityCode - N (Normal)
    5. formatCode - urn:ihe:iti:bppc-sd:2007
    6. formatCode codeSystem - 1.3.6.1.4.1.19376.1.2.3
    7. healthcareFacilityTypeCode - 385432009 (SNOMED CT code for Not Applicable)
    8. mimeType - text/xml
    9. practiceSettingCode - 385432009 (SNOMED CT code for Not Applicable)
    10. serviceStartTime - Effective start date of privacy policy (authorization)
    11. serviceStopTime - Effective end date of privacy policy (authorization)
    12. Title - AUTHORIZATION TO DISCLOSE INFORMATION TO THE SOCIAL SECURITY ADMINISTRATION
4. QD request from SSA to DSO for Clinical document includes-
    1. Query parameters- $XDSDocumentEntryPatientId, $XDSDocumentEntryServiceStartTimeFrom, $XDSDocumentEntryServiceStartTimeTo, $XDSDocumentEntryServiceStopTimeFrom, $XDSDocumentEntryServiceStopTimeTo, $XDSDocumentEntryStatus
5. SAML assertions initiated from SSA include the following
    1. Subject ID - MEGAHIT
    2. Subject Organization - Social Security Administration

3. Subject Organization ID - 2.16.840.1.113883.3.184
4. Home Community ID - urn:oid: 2.16.840.1.113883.3.184.xxx.yyy
5. Subject Role - *Value set from HITSP C80*
6. Purpose of Use - COVERAGE
7. ResourceID/Patient Identifier - Only used to retrieve ACP document

For more information on Common Gateway Service supported transactions and specifications- Common Gateway Service Transactions and Specifications.

Message Example

Sample Common Gateway Service transaction messages can be found here - Common Gateway Service Sample Messages.

Content Format and Examples

For details on the CCD content specifications and examples required for each transaction, refer to the SSA_Electronic_Health_Document_Implemenation_Guide_v4.pdf documentation.

Troubleshooting

A list of common questions regarding SSA Disability Determination can be found at:

http://mihin.org/about-mihin/faqs/

If experiencing difficulties or have questions, please contact the MiHIN Help Desk:
Email: help@mihin.org
Phone: (517) 336-1430
Monday – Friday 8:00 AM – 5:00 PM (Eastern)

Legal Advisory Language

This reminder applies to all Use Cases covering the exchange of electronic health information:
The Data Sharing Agreement ("DSA") establishes the legal framework under which Participating Organizations can exchange messages through the HIN Platform, and sets forth the following approved reasons for which messages may be exchanged:

(a) By health care providers for Treatment, Payment and/or Health Care Operations consistent with the requirements set forth in HIPAA;
(b) Public health activities and reporting as permitted by HIPAA and other Applicable Laws and Standards;
(c) To facilitate the implementation of "Meaningful Use" criteria as specified in the American Recovery and Reinvestment Act of 2009 and as permitted by HIPAA;
(d) Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative in accordance with HIPAA;
(e) By Data Sharing Organizations for any and all purposes, including but not limited to pilot programs and testing, provided that such purposes are consistent with Applicable Laws and Standards; and
(f) **For any additional purposes as specified in any Use Case, provided that such purposes are consistent with Applicable Laws and Standards**.

Under the DSA, "***Applicable Laws and Standards***" means all applicable federal, state, and local laws, statutes, acts, ordinances, rules, codes, standards, regulations and judicial or administrative decisions promulgated by any governmental or self-regulatory agency, including the State of Michigan, the Michigan Health Information Technology Commission, or the Michigan Health and Hospital Association, as any of the foregoing may be amended, modified, codified, reenacted, promulgated or published, in whole or in part, and in effect from time to time. "Applicable Laws and Standards" includes but is not limited to HIPAA; the federal Confidentiality of Alcohol and Drug Abuse Patient Records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2; the Michigan Mental Health Code, at MCLA §§ 333.1748 and 333.1748a; and the Michigan Public Health Code, at MCL § 333.5131, 5114a.

It is each DSO's obligation and responsibility to ensure that it is aware of Applicable Laws and Standards as they pertain to the content of each message sent, and that its delivery of each message complies with the Applicable Laws and Standards. This means, for example, that if a Use Case is directed to the exchange

of physical health information that may be exchanged without patient authorization under HIPAA, the DSO must not deliver any message containing health information for which an express patient authorization or consent is required (e.g., mental or behavioral health information).

Disclaimer: The information contained in this implementation guide was current as of the date of the latest revision in the Document History in this guide. However, Medicare and Medicaid policies are subject to change and do so frequently. HL7 versions and formatting are also subject to updates. Therefore, links to any source documents have been provided within this guide for reference. MiHIN applies its best efforts to keep all information in this guide up-to-date. It is ultimately the responsibility of the Participating Organization and Sending Facilities to be knowledgeable of changes outside of MiHIN's control.