Social Security Determination

Implementation Guide

Version 8
April 24, 2019

Document History

Date	Version	Sections Revised	Description	Modifier
04/24/19	8	All	Revised into new template	S. Southard

Table of Contents

Acronyms and Abbreviations Guide

AA	Assigning Authority
AD	Advance Directive
ACP	Access Consent Policy
API	Application Programming Interface
CCD	Continuity of Care Document
CDA	Clinical Document Architecture
CGS	Common Gateway Service
CMS	Centers for Medicare & Medicaid Services
DS	Document Submission
DSM	Direct Secure Messaging
DSO	Data Sharing Organization
EHR	Electronic Health Record
esMD	CMS Electronic Submission of Medical Documentation
FHIR	Fast Healthcare Interoperability Resources
HCID	Home Community ID
HIE	Health Information Exchange
HL7	Health Level Seven
ICBR	Integrated Care Bridge Record
ICN	Identification Control Number
ICO	Integrated Care Organization
ICT	Integrated Care Teams
IHE	Integrating the Healthcare Enterprise
LLP	Limited Liability Partnership

MiHIN	Michigan Health Information Network Shared Services
MPI	Message Passing Interface
MU	Meaningful Use
MUCA	Master Use Case Agreement
myHB	MyHealthButton
myHP	MyHealthPortal
NHIE	Nationwide Health Information Exchange
NHIO	Nationwide Health Information Organizations
NIST	
NwHIN	Nationwide Health Information Network
OID	Object Identifier
ONC	Office of the National Coordinator
PD	Patient Discovery
PHR	Personal Health Record
PID	HL7 Patient Identification
PIHP	Prepaid Inpatient Health Plans
PO	Participating Organization
PoM	Peace of Mind
PQRS	Physician Quality Reporting System
QD	Query for Documents
RAS	Registration and Attestation System
RD	Retrieve Documents
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol

SSA	Social Security Administration
SSO	Sponsored Data Sharing Organization
SSSO	State Sponsored Data Sharing Organization
UCA	Use Case Agreement
UCS	Use Case Summary
URL	Uniform Resources Locators
VA	Department of Veterans Affairs
VLER	Virtual Lifetime Electronic Record
VPN	Virtual Private Network
VQO	Virtual Qualified Data Sharing Organization
XCA	Cross Community Access
XCPD	Cross-Community Patient Discovery
XDR	Cross-Enterprise Document Reliable Interchange
XDS	Cross-Enterprise Document Sharing
XML	Extended Mark-Up Language

Definitions

Advance Directive. A document in which consumers specify what type of medical care they want in the future, or who should make medical decisions if they become unable to make decisions for themselves.

Applicable Laws and Standards. In addition to the definition set forth in the Data Sharing Agreement, 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.

C32. HITSP Summary Documents Using HL7 Continuity of Care Document 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

Common Gateway. The method by which data is sent and received by MiHIN using various national standard protocols (e.g. NwHIN SOAP, IHE XCA, IHE XDS.b).

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.

Data Sharing Agreement. Any data sharing organization agreement signed by both MiHIN and a participating organization. Data sharing organization agreements include but are not limited to: Qualified Data Sharing Organization Agreement, Virtual Qualified Data Sharing Organization Agreement, Consumer Qualified Data Sharing Agreement, Sponsored Shared Organization Agreement, State Sponsored Sharing Organization Agreement, Direct Data Sharing Organization Agreement, Simple Data Sharing Organization Agreement, or other data sharing organization agreements developed by MiHIN.

DS Message. A message specific to the document submission (DS) specification that conforms in content and format to the Integrating the Healthcare Enterprise's Cross-enterprise Document Reliable Interchange specification.

EdgeSim. Simulators that are utilized in a testing environment to simulate testing with a data sharing organization.

Electronic Address. A string that identifies the transport protocol and end point address for communicating electronically with a recipient. A recipient may be a person, organization or other entity that has designated the electronic address as the point at which it will receive electronic messages. Examples of an electronic address include a secure email address (Direct via secure SMTP) or secure URL (SOAP / XDR / REST / FHIR). Communication with an electronic address may require a digital certificate or participation in a trust bundle.

Electronic Medical Record or Electronic Health Record (EMR/EHR). A digital version of a patient's paper medical chart.

Electronic Service Information (ESI). All information reasonably necessary to define an electronic destination's ability to receive and use a specific type of information (e.g, discharge summary, patient summary, laboratory report, query for patient/provider/healthcare data). ESI may include the type of information (e.g. patient summary or query), the destination's electronic address, the messaging framework supported (e.g., SMTP, HTTP/SOAP, XDR, REST, FHIR), security information supported or required (e.g., digital certificate) and specific payload definitions (e.g., CCD C32 V2.5). In addition, ESI may include labels that help identify the type of recipient (e.g., medical records department).

Exhibit. Collectively, a use case exhibit or a pilot activity exhibit.

FedSim. Simulators that are utilized in a testing environment to simulate testing with a federal partner e.g. SSA or VA

Health Level 7 (HL7). An interface standard and specifications for clinical and administrative healthcare data developed by the Health Level Seven organization and approved by the American National Standards Institute (ANSI). HL7 provides a method for disparate systems to communicate clinical and administrative information in a normalized format with acknowledgement of receipt

Health Information. Any information, including genetic information, whether oral or recorded in any form or medium, that (a) is created or received by a health provider, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Information Network (HIN). An organization or group of organizations responsible for coordinating the exchange of protected health information (PHI) in a region, state, or nationally.

Health Plan. An individual or group plan that provides, or pays the cost of medical care (as "group health plan" and "medical care" are defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)). Health plan further includes those entities defined as a health plan under HIPAA, 45 C.F.R 160.103.

Health Professional means (a) any individual licensed, registered, or certified under applicable Federal or State laws or regulations to provide healthcare services; (b) any person holding a nonclinical position within or associated with an organization that provides or coordinates healthcare or healthcare related services; and (c) people who contribute to the gathering, recording, processing, analysis or communication of health information. Examples include, but are not limited to, physicians, physician assistants, nurse practitioners, nurses, medical assistants, home health professionals, administrative assistants, care managers, care coordinators, receptionists and clerks.

Health Provider means facilities/hospitals, health professionals, health plans, caregivers, pharmacists/other qualified professionals, or any other person or organization involved in providing healthcare.

Information Source. Any organization that provides information that is added to a MiHIN infrastructure service.

Integrating the Healthcare Enterprise. 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 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

Master Use Case Agreement (MUCA). Legal document covering expected rules of engagement across all use cases. Trusted data sharing organizations sign master use case agreement one time, then sign use case exhibits for participation in specific use cases.

Meaningful Use. Using certified EHR technology to improve quality, safety and efficiency of healthcare, and to reduce health disparities as further contemplated by title XIII of the the American Recovery and Reinvestment Act of 2009.

Message. A mechanism for exchanging message content between the participating organization to MiHIN services, including query and retrieve.

Message Content. Information, as further defined in an Exhibit, which is sent, received, found or used by a participating organization to or from MiHIN services. Message content includes the message content header.

Message Header ("MSH") or Message Content Header. The MSH segment present in every HL7 message type that defines the Message's source, purpose, destination, and certain syntax specifics such as delimiters (separator characters) and character sets. It

is always the first segment in the HL7 message, with the only exception being HL7 batch messages.

Michigan Health Information Network Shared Services. The MiHIN for the State of Michigan.

MiHIN Infrastructure Service. Certain services that are shared by numerous use cases. MiHIN infrastructure services include, but are not limited to, Active Care Relationship Service (ACRS), Health Directory, Statewide Consumer Directory (SCD), and the Medical Information DIrect GATEway (MIDIGATE®).

MiHIN Services. The MiHIN infrastructure services and additional services and functionality provided by MiHIN allowing the participating organizations to send, receive, find, or use information to or from MiHIN as further set forth in an exhibit.

Nationwide Health Information Network (NwHIN). See the definition for Sequoia Project.

Nationwide Health Information Organizations (NHIO). Nodes on the eHealth Exchange that use the NwHIN web services to facilitate exchange of information with other nodes in the network.

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 eHealth Exchange 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 "send" data for a given patient from an exchange partner to an HIE using configuration on the sender side.

NwHIN Gateway. An implementation of the Nationwide Health Information Network specified web service interfaces. These web service interfaces communicate over secured HTTPS using Public Key Infrastructure supported by the NwHIN Operational Infrastructure.

NwHIN Interface. An implementation of the NwHIN specified web service interfaces. These web service interfaces communicate over secured HTTPS using Public Key Infrastructure supported by the NwHIN Operational Infrastructure.

NwHIN Messaging Platform Specifications 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 eHealth Exchange network and applies to all eHealth Exchange transactions.

NwHIN Patient Discovery Web Service Interface Specification. The purpose of this specification is to define the mechanism by which one eHealth Exchange 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 Web Service Interface Specification. The purpose of this specification is to define the mechanism by which an initiating eHealth Exchange node can request a patient-specific list of available documents from a responding node using the patient ID obtained by a prior Patient Discovery transaction.

NwHIN Retrieve Documents Web Service Interface Specification. The purpose of this specification is to define the mechanism by which an Initiating eHealth Exchange node can retrieve specific documents from a responding node using the Document Reference IDs obtained using a prior Query for Documents transaction.

Patient Data. Any data about a patient or a consumer that is electronically filed in a participating organization or participating organization participant's systems or repositories. The data may contain protected health information (PHI), personal credit information (PCI), and/or personally identifiable information (PII).

Person Record. Any record in a MiHIN infrastructure service that primarily relates to a person.

Provider Community. A healthcare provider with an active care relationship with the applicable patient.

Query for Documents Message. A message specific to the Query for Documents Web Services Interface Specification that references the Integrating the Healthcare Enterprise's Cross-Community Access specification.

REST. REST stands for Representational State Transfer, which is an architectural style, and an approach to communications that is often used in the development of web services.

Retrieve Documents Message. Retrieve documents web services interface specification that references the Integrating the Healthcare Enterprise's Cross-Community Access specification.

Send / Receive / Find / Use (SRFU). Means sending, receiving, finding, or using message content. Sending involves the transport of message content. Receiving involves accepting and possibly consuming or storing message content. Finding means querying to locate message content. Using means any use of the message content other than sending, receiving and finding. Examples of use include consuming into workflow, reporting, storing, or analysis. Send/Receive/Find/Use (SRFU) activities must comply with Applicable Laws & Standards or State Administrative Code as that term is defined in this agreement and the data sharing agreement.

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 eHealth Exchange 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.

Source System. A computer system, such as an electronic health record system, at the participating organization, that sends, receives, finds or uses message content or notices.

Specifications. Specifications provide a standard set of service interfaces that enable the exchange of interoperable health information among the health information exchanges.

Target HIE. The HIE or eHealth Exchange Node that the message or feedback is being addressed.

Transactional Basis. The transmission of message content or a notice within a period of time of receiving message content or notice from a sending or receiving party as may be further set forth in a specific exhibit.

Transitions of Care. The movement of a patient from one setting of care (e.g. hospital, ambulatory primary care practice, ambulatory specialty care practice, long-term care, rehabilitation facility) to another setting of care and can include transfers within a healthcare organization.

Trusted Data Sharing Organization (TDSO). An organization that has signed any form of agreement with MiHIN for data sharing.

Use Case. (a) A use case agreement previously executed by a participating organization; or (b) the use case summary, use case exhibit and a use case implementation guide that participating organization or TDSO must follow to share specific message content with the MiHIN.

Use Case Exhibit. The legal agreement attached as an exhibit to the master use case agreement that governs participation in any specific use case.

Use Case Implementation Guide (UCIG). The document providing technical specifications related to message content and transport of message content between participating organization, MiHIN, and other TDSOs. use case implementation guides are made available via URLs in exhibits.

Use Case Summary. The document providing the executive summary, business justification and value proposition of a use case. Use case summaries are provided by MiHIN upon request and via the MiHIN website at www.mihin.org.

View Download Transmit (VDT). A requirement for Meaningful Use with the objective to provide patients with the ability to view online, download and transmit their health information within a certain period of the information being available to an eligible professional.

XCA. The IHE (Integrating the Healthcare Enterprise®) standard for Cross-Community Access which provides specifications to query and retrieve patient relevant health information held by other communities.

XDS.b. The IHE (Integrating the Healthcare Enterprise®) standard for Cross-Enterprise Document Sharing revision b, which provides specifications to query and retrieve patient relevant healthcare data held within a community.

1. Introduction

1.1 Purpose of Use Case

Enables a participating organization to retrieve patient authorization documents from the SSA and to then respond electronically to the SSA request by submitting clinical Continuity of Care Documents (CCDs) through the statewide health information network and through the Sequoia Project (formerly eHealth Exchange) to the SSA.

The Social Security Administration (SSA) receives and must respond to millions of claims for disability benefits each year. In the past, this process was entirely manual, labor-intensive, paper-intensive, and very costly. The SSA has now developed the ability to augment determination process for eligibility that saves both time and money.

Annual disability claims submitted to the Social Security Administration (SSA) are growing at a rate of 11%. In fiscal year 2011, the SSA received 3.3 million initial disability requests, 800,000 requests for reconsideration of the initial decision, and 650,000 requests for administrative law judge reviews. In that same year, the SSA requested medical evidence data 15 million times (typically 3-4 requests per disability application) from more than 500,000 doctors, hospitals and other care providers.

To provide perspective on the scope of these requests, mid-size hospitals submit an estimated 400 medical records per month to the SSA with each submission averaging 50 pages per mailing/fax. At 15 million medical record submissions in 2011, that means the SSA may be receiving and processing 750 million pages of mailed/faxed medical evidence per year.

Yet, due to the sheer volume of information being requested, received, processed and reviewed, the disability determination period under the current process can still take 18 to 24 months, impacting final determinations and payment to hospitals.

In response to the volume of work required to process disability claims, the SSA funded several vendors to:

- Develop electronic claims processing to help reduce paper work
- Eliminate manual record processing
- Expedite responses to SSA requests
- Ensure more complete medical record information
- Standardize medical record data formats
- Eliminate medical record information security breaches
- Enable faster payment (a few days, vs. months before)
- Reduce significant overhead through streamlining the process

This process is a burden and resource drain on all participants, from healthcare providers to the SSA itself, and, more importantly, to patients waiting on approvals. Healthcare providers devote significant personnel resources to processing and submitting this medical evidence, and the SSA is overwhelmed handling the volume of applications it receives and paperwork it requests from providers.

As part of these efforts, the SSA connected to the Sequoia Project (previously the Nationwide Health Information Network [NwHIN] and eHealth Exchange) to enable the exchange of health information from other organizations around the U.S. that are connected to the Sequoia Project. As a participant in the Sequoia Project, MiHIN has established the necessary connectivity enabling organizations to respond to SSA requests electronically.

The SSA benefits from streamlining the current process as do other stakeholders, including hospitals, health systems, and patients. Facilitating electronic submission of information to the SSA using an electronic claims processing service helps hospitals and healthcare providers realize:

- Service, efficiency, and quality advantages
- Enhanced security and breach avoidance
- Cost reduction maximization
- Improved ROI of hospital HIE investment
- Revenue optimization (uncompensated care recovery)

More importantly, patients receive benefits responses much sooner (within days as opposed to more than a year) and hospitals are reimbursed much sooner in addition to the reduced costs.

A four-hospital integrated health system realized an incremental year one revenue recovery of $1.9M associated with more timely claims processing and a three-year recovery of $6.1M between 2009 and 2012.[1]

Faster, easier SSA request processing offers hospitals and health systems the opportunity to:

- Reduce Full-Time-Equivalent (FTE) personnel handling medical record requests or redirect current FTEs to revenue-producing activities;
- Decrease medical record vendor copy fees; minimize office supplies; avoid increasing postage fees (which are no longer paid by SSA);
- Expedite replies to SSA requests leading to timely accurate processing of disability cases (resulting in faster payments, greater provider reimbursement, and better patient care)
- Enhance integrity of patient information by minimizing potential in-house patient record security breaches; eliminate the need to outsource SSA record submissions

[1] S. Feldman, T. Horan, and D. Drew, *Claremont University Case Study – MedVirgina HIE and Bon Secour Hospitals, Health Systems,1–13*

This use case scenario enables responses to electronic eligibility determination requests via a sending of CCDs through MiHIN's infrastructure service called Common Gateway Service (CGS). CGS offers the capability to send, find, receive, and use healthcare data throughout Michigan or with other states. CGS consists of a CONNECT Gateway together with an exchange broker, and utilizes NwHIN's SOAP-based messaging for:

- Document submission (DS)
- Patient discovery (PD)
- Query for document (QD)
- Document retrieve (DR)

The exchange broker manages message transformation and routing to and from the Sequoia Project (these messages work with Sequoia Project participants, such as federal agencies including SSA, Department of Veterans Affairs, and Centers for Medicare and Medicaid Service) and also to and from trusted data-sharing organizations (TDSOs). The message transformation services allow TDSOs to send and receive messages in a number of protocols whether NwHIN SOAP, or the more widely used IHE standards for XCA and XDS.b.

1.2 Message Content

For this use case, message content means HL7 Consolidated Clinical Document Architecture (C-CDA) document conforming to the CCD template.

1.3 Common Gateway Service and Use Cases

CGS consists of a CONNECT Gateway together with an exchange broker.

The CONNECT Gateway utilizes Office of the National Coordinator's (ONC) Nationwide Health Information Network (NwHIN) SOAP-based messaging to send healthcare information using the Document Submission (DS) message, or healthcare information request using the Patient Discovery (PD), Query for Document (QD), and Document Retrieve (DR) messages to other eHealth Exchange participants, such as Federal agencies.

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

The Common Gateway Service is depicted below:

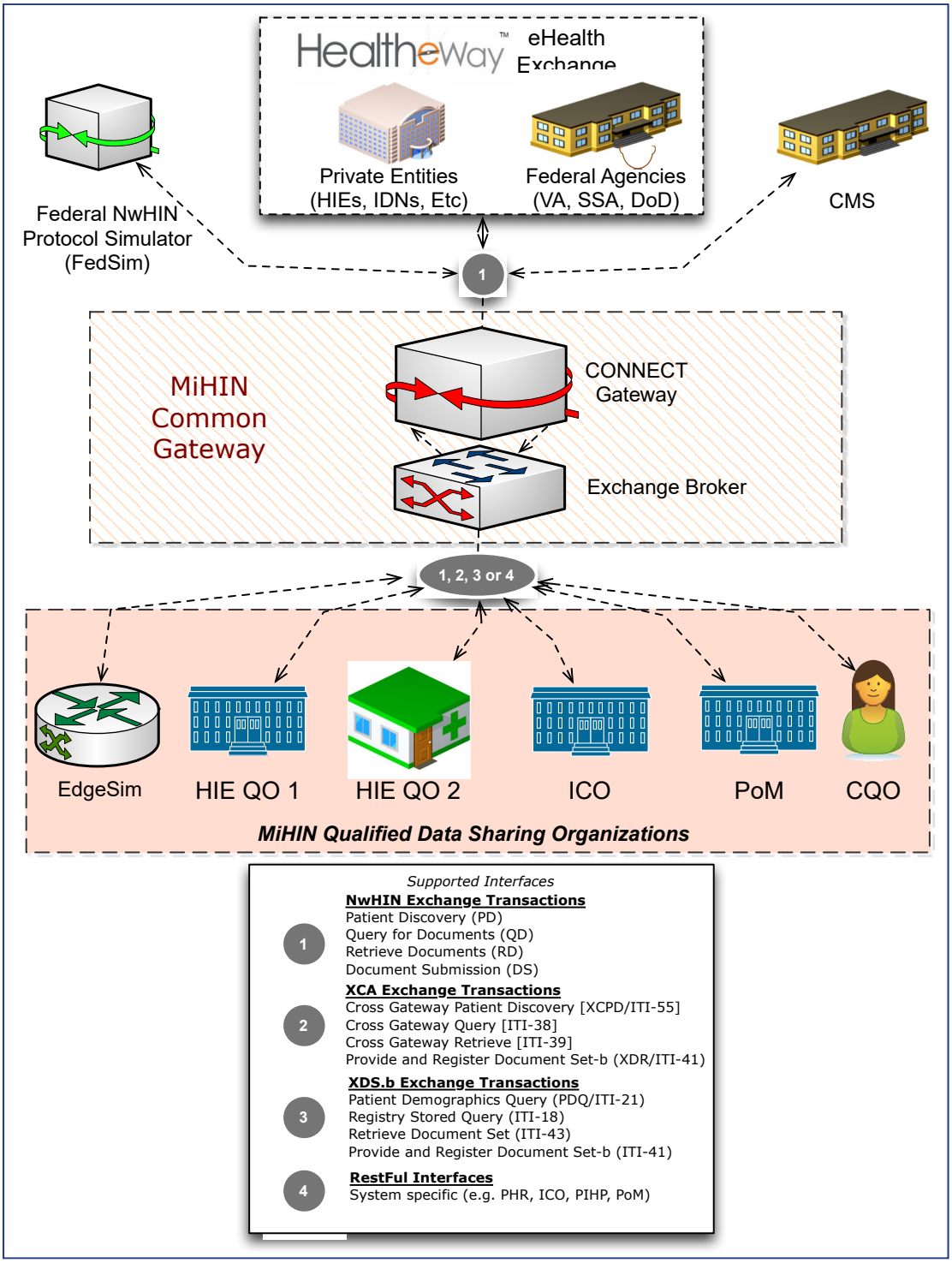

Figure 1. Common Gateway Service Context Diagram

When TDSOs agree to exchange data through MiHIN there are a number of use cases where the CGS can be used as the transport method:

1. *Exchange Advance Directives:* Exchanging advance directive documents, e.g. between MyHealthPortal (myHP)/ MyHealthButton (myHB) and Peace of Mind (PoM); and/or

Hospital Systems (through HIE [Health Information Exchange]), and PoM and/or PHRs (Personal Health Records)

2. *Exchange Integrated Care Bridge Record:* Exchanging integrated care bridge records (ICBRs) either internal to an Integrated Care Organization (ICO) within their associated integrated care teams (ICT), or between ICOs and/or prepaid inpatient health plans (PIHPs)
3. *Exchange Patient CCDs Statewide:* Exchanging patient healthcare information within Michigan
4. *Exchange CCDs with VA:* Exchanging veteran healthcare information between TDSO providers and the VA
5. *Respond to SSA Disability Determination Requests for CCD:* Responding to the SSA eligibility claims for patients within a DSO(s) network of providers
6. *Respond to CMS Electronic Submission of Medical Documentation Request for CCD:* Sending documents to the CMS Electronic Submission of Medical Documentation System (esMD) in support of eligibility determinations for patients within aT DSO(s) network of providers
7. *Exchange CCDs Outside Michigan (non-VA/SSA):* Exchanging patient healthcare information between DSO providers and other non-federal organizations outside of Michigan

As indicated in Figure 1 (above), MiHIN has developed two simulators to aid TDSOs onboarding into the CGS 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.

1.4 Data Flow and Actors

In this use case scenario, MiHIN brokers the messaging between the SSA and the participating organization.

Figure 2. Data Flow for This Use Case Scenario

1.4.1 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
- Query for Documents
- Retrieve Documents

1.4.1.1 Patient Discovery

The 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 SSAs first sends a PD request to the participating organization. The SSA gateway acts as the requesting gateway with the participating organizations gateway acting as the responding gateway:

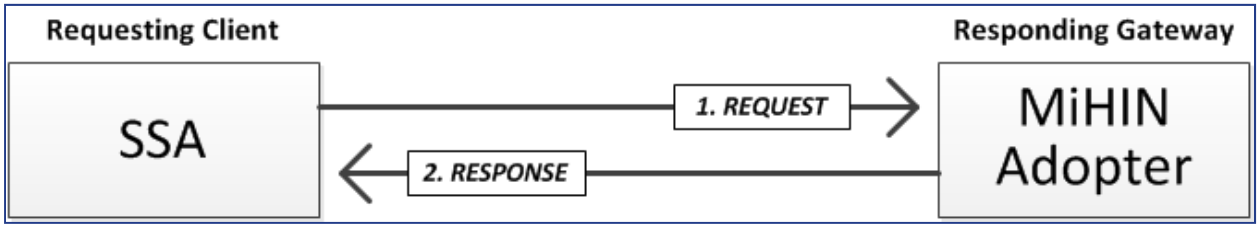

Figure 3. Patient Discovery

1.4.1.2 Query for Documents

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

The participating organization's gateway also acts as the requesting gateway for the QD and RD web services interfaces that are hosted by the SSA NwHIN gateway. The SSA hosted services are used by the adopter to receive the access consent policy (ACP) documents.

1.4.1.3 Retrieve Documents

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

On the occasions when the roles are reversed with the participating organization initiating the request to SSA (as when it is seeking the proper access control policies from SSA for a particular PD exchange), the organization's gateway acts as the requesting client with SSA acting as the responding gateway for both QD and RD services:

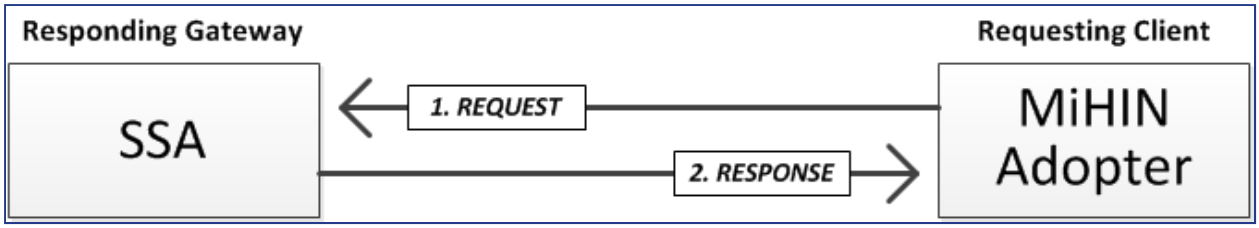

Figure 4. Retrieve Documents

1.4.2 Web Services Between Participating Organizations and MiHIN

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

While transactions between CGS 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 (Cross-Community Patient Discovery) 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 CGS and their specifications and the specifications for PD, QD, and RD, see Common Gateway Service Transactions and Specifications.

1.4.2.1 General Sequence of Messages

Communication between SSA and the participating organizations begins with the PD exchange, as diagrammed below.

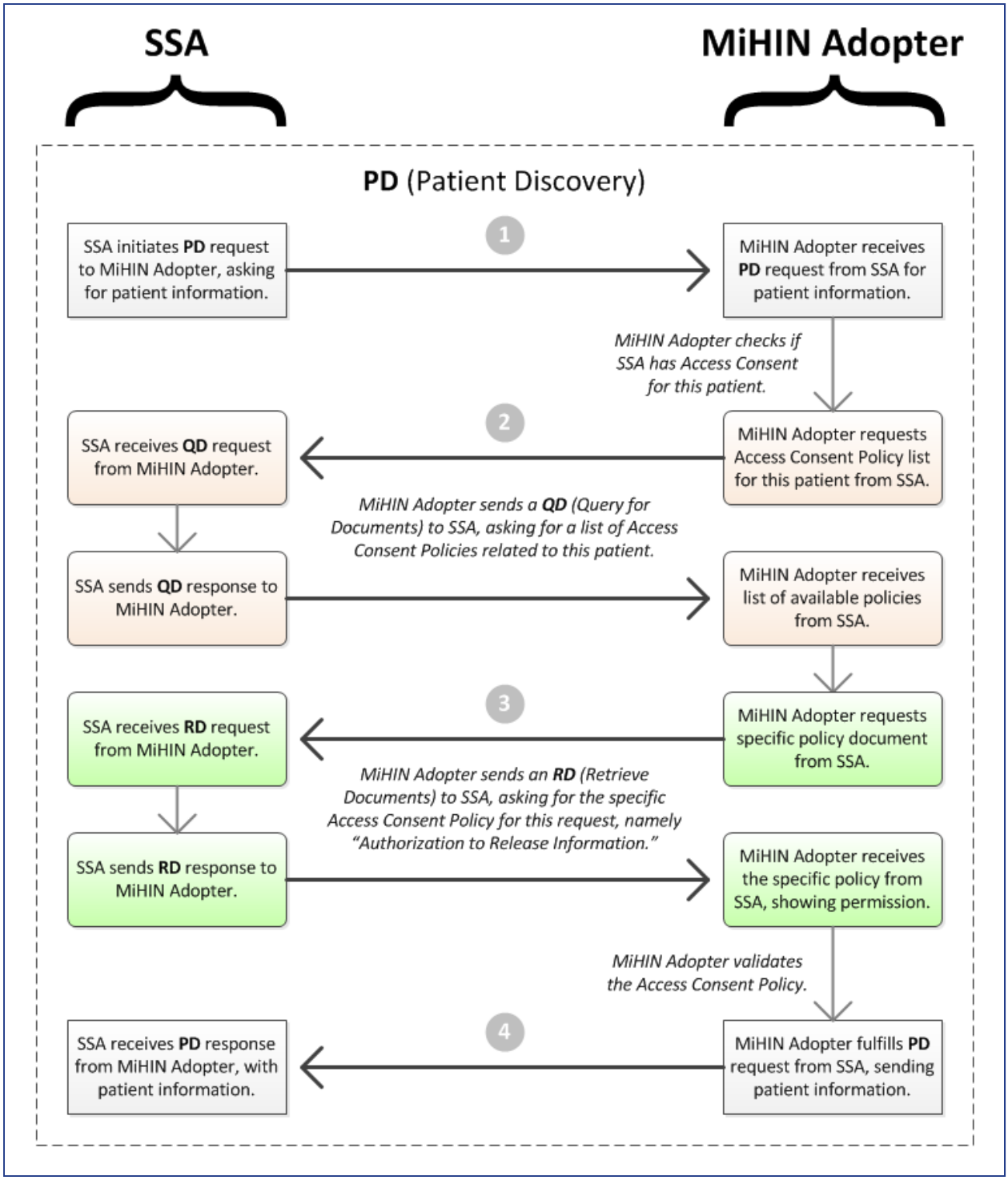

Figure 5. PD Exchange

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

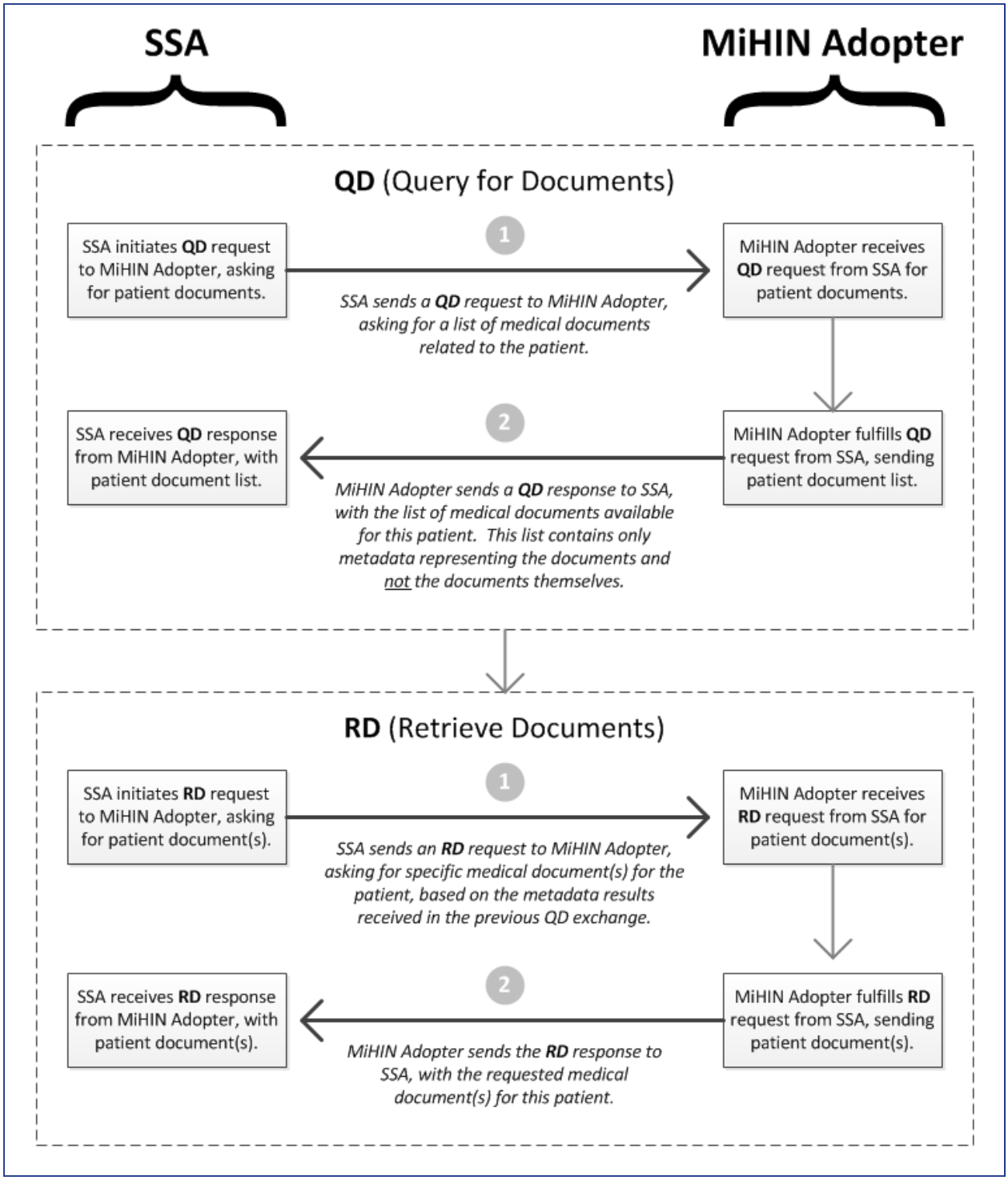

Figure 6. QD and RD Exchange

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.

2 Standard Overview

2.1 Message

The message content and notices sent to and received from the CGS meets the following standards:

- the ONC NwHIN specifications set forth on the Healtheway website - Exchange Specifications
- 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.

2.1.1 Message Payload

The Message Payload sent to and received from the CGS 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:* 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:* HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, Release 1.1 - US Realm
- Consolidated Clinical Document Architecture: HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes

3 Onboarding Process and Testing

3.1 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 http://mihin.org/requesthelp/.

3.1.1 Initial Legal Process

The first time an organization undergoes the legal onboarding process with MiHIN, the organization negotiates and enters into a master organization agreement and master use case agreement which then allows the organization to enter into one or more use cases via use case exhibits.

Once an organization has entered into a master 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/

3.1.2 Initial Technical Connectivity Process

First steps for connecting to the staging CGS are as follows:

1. Request and subsequently send 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:
   a. Self-signed certificate from organization server (to be added to Common Gateway trust store)
   b. Organization Home Community ID (unique OID)
   c. Organization assigning authority (unique OID)
   d. Organization repository ID (unique OID)
   e. DS, PD, QD, RD service endpoints
   f. Organization assertion information
4. Participating organization is supplied by MiHIN with:
   a. Self-signed certificate from common gateway server (to be added to participating organization's server trust store)
   b. Common Gateway DS, PD, QD, RD service endpoints
   c. Staging simulators' Home Community ID (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)

3.2 Technical Onboarding and Testing

Technical onboarding and testing is a three-step process:

1. Connectivity testing utilizing MiHIN simulators of the federal environment
2. More focused use case testing with the simulators
3. End-to-end testing between the trading partners

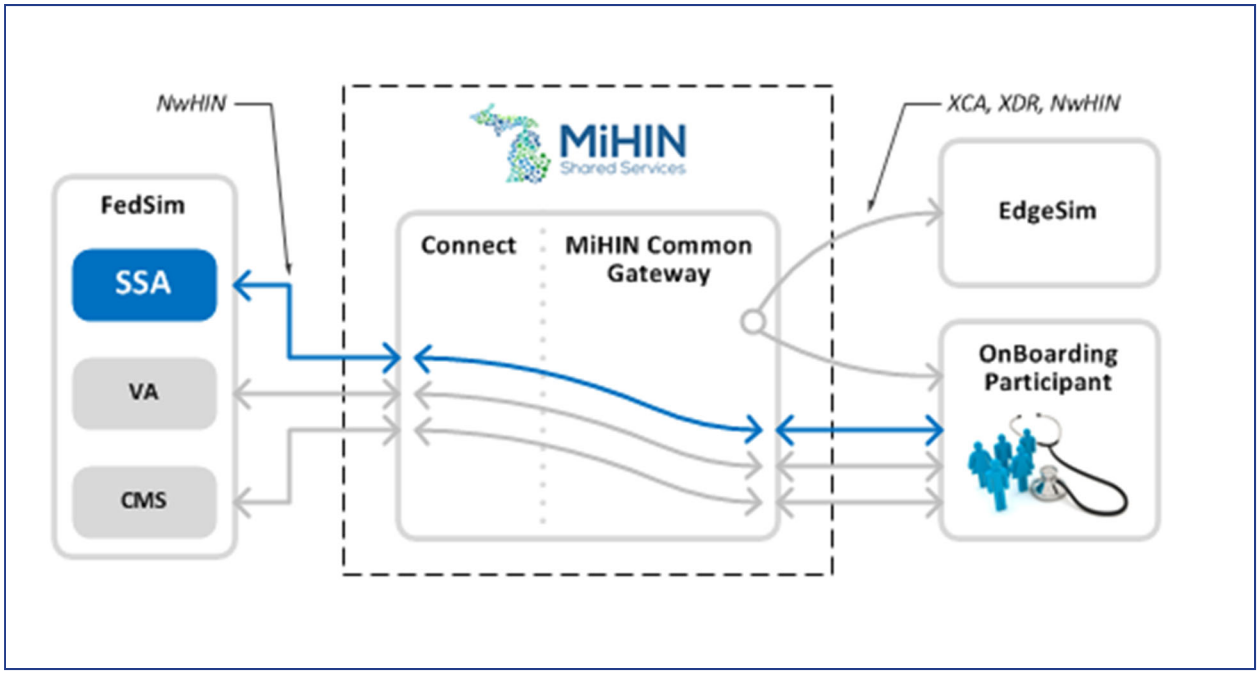

Figure 7. Context Diagram of the Common Gateway Testing Environment

3.3 Connectivity and Smoke Test With Federal Simulator (Non-Use Case Specific)

If the onboarding 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.

3.4 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.

3.5 Testing With SSA Disability Determination Use Case

On completion of testing with FedSim, the participating organization 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.

3.5.1 SSA Disability Determination Test Cases (for Participants With a Single Assigning Authority)

3.5.1.1 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	ACP Parameters[2]
1	SSA initiates a PD request to the NwHIN participant's gateway	■ First name ■ Middle name ■ Last name ■ Alias ■ Gender ■ Date of birth (DOB) ■ Social Security Number (SSN) ■ Address	QD request for ACP 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.
2	NwHIN participant sends QD request to SSA (for ACP 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

[2] This column i**ncludes references from SSA NHIN Interoperability Guide.**

Step	Scenario	Request Parameters	Expected Response	ACP Parameters[2]
3	SSA initiates a QD response to NwHIN participant (for ACP document)	N/A	RD request for ACP document from the NwHIN participant's gateway	The request message uses the information that was returned in the previous step, QD Response for ACP (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 RD response message, the ability to retrieve to the ACP is no longer be allowed.
4	NwHIN participant sends a RD request to SSA to retrieve ACP 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, QD response for ACP (Section 4.4). The ability to retrieve the ACP document is valid throughout the complete transaction sequence between SSA and Health IT partner. Once SSA has received the last RD response message, the ability to receive the ACP is no longer allowed.
5	SSA sends a RD Response (ACP 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 ACP identifier as a reference mechanism when establishing the permissions for SSA

3.5.1.2 Patient Not Found Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP 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

3.5.1.3 Patient Is an Ambiguous Match and PD Response Is "AnswerNotAvailable" Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP identifier as a reference mechanism when establishing the permissions for SSA

3.5.1.4 Patient Is an Unambiguous Match and No Clinical Documents Returned Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP identifier as a reference mechanism when establishing the permissions for SSA
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

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
8	NwHIN participant's gateway sends a QD response to SSA (for clinical documents)	QD response with zero document references	N/A	N/A

3.5.1.5 Patient Is an Unambiguous Match and One or More Clinical Documents Are Returned Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP 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:	N/A	N/A

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
		■ Where defined in the XDS profile, all classification UUIDs must match those of the XDS profile ■ ll 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		

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
		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 ■ (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	N/A	N/A

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
		■ mimeType matches the value for the requested document type (e.g. mimeType="text/xml" for CCD)		

3.5.2 SSA Disability Determination Test Cases (for Participants With Multiple Assigning Authorities)

3.5.2.1 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	ACP 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 ACP 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 PD 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 PD request from SSA.
2	NwHIN participant sends QD request to SSA (for ACP 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	N/A	N/A

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
		■ **(O)** eventCodeList = InstanceAccessPolicy value included in the SAML assertion sent by SSA.		
3	SSA initiates a QD response to NwHIN participant (for ACP document)	N/A	RD request for ACP document from the NwHIN participant's gateway	The request message uses the information that was returned in the previous step, QD response for ACP (Section 4.4). The ability to receive the access consent policy document is valid throughout the complete transaction sequence between SSA and Health IT partner. Once SSA has received the last RD response message, the ability to receive to the ACP is no longer allowed.
4	NwHIN participant sends a RD request to SSA to receive ACP 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, QD response for ACP (Section 4.4). The ability to receive the ACP document is valid throughout the complete transaction sequence between SSA and Health IT Partner. Once SSA has received the last RD response message, the ability to receive to the ACP is no longer allowed.
5	SA sends a RD response (ACP 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 ACP identifier as a reference mechanism when establishing the permissions for SSA

3.5.2.2 Patient Not Found Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP 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

3.6.2.3 Patient Is an Ambiguous Match and PD Response Is "AnswerNotAvailable" Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP identifier as a reference mechanism when establishing the permissions for SSA

3.6.2.4 Patient Is an Unambiguous Match and No Clinical Documents Returned Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD response (ACP 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 ACP 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

3.6.2.5 Patient Is an Unambiguous Match and One or More Clinical Documents Are Returned Scenario

This continues from step 5 from the basic flow for access control decision cycle.

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
5	SSA sends a RD Response (ACP document) message to the NwHIN participant's gateway. NwHIN participant evaluates the response according to their	N/A	PD response with a single patient identifier for each assigning authority for which the match happened	N/A

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
	access control policies.			
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 ACP 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	N/A	N/A

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
		■ 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 ■ (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		

Step	Scenario	Request Parameters	Expected Response	ACP Parameters
		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

4 Specifications

4.1 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 ACP requires:
   a. $XDSDocumentEntryPatientId – PID value that was included in the SAML assertion of the PD request from SSA
   b. $XDSDocumentEntryStatus – urn:oasis:names:tc:ebxml-regrep:StatusType:Approved
   c. $XDSDocumentEntryClassCode – 57016-8 (optional)
   d. $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 ACP:
   a. availabilityStatus – urn:oasis:names:tc:ebxml-regrep:StatusType:Approved
   b. classCode – 57016-8 (LOINC)
   c. classCode DisplayName – Privacy policy acknowledgement
   d. confidentialityCode – N (Normal)
   e. formatCode – urn:ihe:iti:bppc-sd:2007
   f. formatCode codeSystem – 1.3.6.1.4.1.19376.1.2.3
   g. healthcareFacilityTypeCode – 385432009 (SNOMED CT code for Not Applicable)
   h. mimeType – text/xml
   i. practiceSettingCode – 385432009 (SNOMED CT code for Not Applicable)
   j. serviceStartTime – Effective start date of privacy policy (authorization)
   k. serviceStopTime – Effective end date of privacy policy (authorization)
   l. Title – AUTHORIZATION TO DISCLOSE INFORMATION TO THE SOCIAL SECURITY ADMINISTRATION
4. QD request from SSA to DSO for Clinical document includes:
   a. Query parameters – $XDSDocumentEntryPatientId, $XDSDocumentEntryServiceStartTimeFrom, $XDSDocumentEntryServiceStartTimeTo, $XDSDocumentEntryServiceStopTimeFrom, $XDSDocumentEntryServiceStopTimeTo, $XDSDocumentEntryStatus
5. SAML assertions initiated from SSA include the following
   a. Subject ID – MEGAHIT
   b. Subject Organization – Social Security Administration
   c. Subject Organization ID – 2.16.840.1.113883.3.184
   d. Home Community ID – urn:oid: 2.16.840.1.113883.3.184.xxx.yyy
   e. Subject Role – *Value set from HITSP C80*
   f. Purpose of Use – COVERAGE
   g. ResourceID/PID – Only used to receive ACP document

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

4.2 Message Example

Sample Common Gateway Service transaction messages can be found at Common Gateway Service Sample Messages.

4.3 Content Format and Examples

For details on the CCD content specifications and examples required for each transaction, refer to the SSA Electronic Health Document Implementation Guide v4.pdf documentation.

5 Troubleshooting

5.1 Production Support

	Severity Levels			
	1	***2***	***3***	***4***
Description	***Critical Impact/ System Down:*** Business critical software is down or critical interface has failed. The issue is impacting all production systems, causing all participating organizations' or other organizations' ability to function to be unusable.	***Significant Business Impact:*** Software component severely restricted. Entire organization is unable to continue business functions, causing all communications and transfer of messages to be halted.	**Partial Failure or Downtime:** Program is useable and less significant features unavailable. The service is online, though may not working as intended or may not currently working as intended or may not currently be accessible, though other systems are currently available.	**Minimal Business:** A non-critical software component is malfunctioning, causing minimal impact, or a test system is down.
Example	All messages to and from MiHIN are unable to be sent and received, let alone tracked	MiHIN cannot communication (send or receive) messages between single or multiple participating organizations, but can still successfully communicate with other organizations.	Messages are lost in transit; messages can be received but not sent.	Additional feature requested.
Primary Initiation Method	***Phone:*** (517) 336-1430	***Phone:*** (517) 336-1430	Web form at http://mihin.org/ requesthelp	Web form at http://mihin.org/ requesthelp
Secondary Initiation Method	Web form at http://mihin.org/ requesthelp	Web form at http://mihin.org/ requesthelp	Email to help@mihin.org	Email to help@mihin.org
Tertiary Initiation Method	Email to help@mihin.org	Email to help@mihin.org	N/A	N/A
Initial Response	Within 2 hours	Within 2 hours	1 business day	1 business day
Resolution Goal	24 hours	24 hours	3 business days	7 business days

A list of common questions regarding the Social Security Determination Use Case can be found at:

https://mihin.org/social-security-determination-use-case-2/

If you have questions, please contact the MiHIN Help Desk:

- www.mihin.org/requesthelp
- Phone: (517) 336-1430
- Monday – Friday 8:00 AM – 5:00 PM (Eastern)

6 Legal Advisory Language

This reminder applies to all UCEs or PAEs covering the exchange of electronic health information:

The data sharing agreement establishes the legal framework under which PO 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 UCE or PAE, provided that such purposes are consistent with Applicable Laws and Standards**.

Under these agreements, "***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 agency, including the State of Michigan, or the Michigan Health Information Technology Commission 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 which is enforceable against a Party. Without limiting the generality of the foregoing, "Applicable Laws and Standards" includes 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 PO'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 UCE is directed to the exchange of physical health information that may be exchanged without patient authorization under HIPAA, the PO 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 will apply 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.