Testing Program Overview

For Prospective QHIN Exchange Testing

TABLE OF CONTENTS

1. Sequoia RCE QHIN Testing Program Overview

The scope of the Recognized Coordinating Entity (RCE)/Qualified Health Information Network (QHIN) Testing program is limited to the QHIN Technical Framework (QTF) Version 1 Specification; the information outlined in the Common Agreement and related test materials adopted by the RCE, collectively called "Standard Operating Procedures".

Changes to the base standards, Specifications, and Test Materials may be made in accordance with the applicable version of the QTF as described in the Trusted Exchange Framework and Common Agreement (TEFCA).

The Sequoia Project QHIN Testing Program verifies that a System both complies with the QTF specifications and has the ability to interoperate with other QHIN Networks. The Sequoia Project QHIN Testing program supports the following:

- Applicants who wish to onboard as a QHIN;
- Existing QHINs who wish to test new technology or retest as a condition of continued participation in the TEFCA; and
- Vendors who wish to have their product(s) validated as QHIN compliant.

2. Sequoia RCE QHIN Test Components

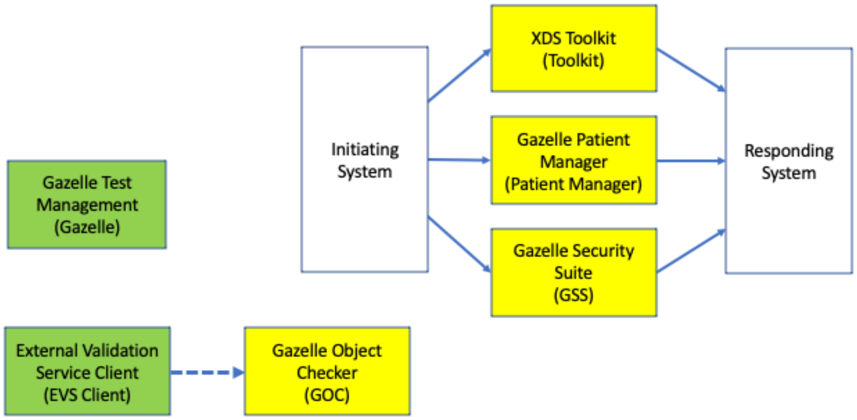
QHIN implementations will be tested using a set of software tools, test data and procedures managed by the Sequoia Project. This document describes the test system components and includes the configuration items that are needed for testing. This document does not describe how to use the tools or run test cases. That information is found in the *QHIN Testing User Guide*. This document provides the terminology used in the User Guide and other documents including workflows for various testing scenarios. Of note, the authoritative requirements for QHINs are only contained in the relevant specifications. The software tools and testing procedures represent a "best effort" at reflecting those specifications, but should not be construed to be authoritative in their results.

2.1. Tool Index

The figure below represents the testing environment including initiating and responding systems being tested. The color scheme is as follows:

- White rectangle: represents a System Under Test (SUT).

- Green rectangle: represents a testing tool where the primary interaction with the user is through a web-based user interface. The green rectangles normally do not communicate directly with the SUT. The green tools may communicate with the yellow boxes; those arrows are mostly not shown to minimize clutter.
- Yellow rectangle: represents a conformance testing tool that might play the role of an initiating system or a responding system. Individual conformance testing tools will process transactions and perform validation on messages from the SUT. These tools often have a web-based user interface that will be used to drive specific tests. The conformance test tools might communicate with each other and/or share results with the web-based UI components (green boxes).



Each tool in the diagram has a formal name and a shorter name. You will see both names in the documentation. Documentation for the various tools can be found below. This is a summary of the scope and function of the individual tools.

1. Gazelle Test Management (Gazelle): This is the overall tool for test management. It presents a list of tests to run that are based on your role or roles (Initiating System, Responding System). Gazelle collects evidence for individual tests and allows the test managers to review those results and validate individual test results. Test managers also use Gazelle to provide overall test status through a dashboard that is easy to search and filter for specific results. Gazelle Test Management includes a single sign on feature that is used by other tools in the environment.
2. External Validation Service Client (EVS Client): You will upload documents and messages through the web UI of this tool. The EVS Client will submit your payload to one of

several backend systems that will validate the content for conformance to the relevant specification. You might be testing an ATNA syslog message or a specific CDA document.

3. Gazelle Object Checker (GOC): This is the most common Gazelle backend tool for validating different types of files or objects. Depending on the type of object to be validated, the Gazelle Object Checker will use a tool based on handwritten tools or tools automatically generated from a specification.
4. XDS Toolkit (Toolkit): This tool tests conformance to the XDS family of profiles. That includes XDS.b, XDR, XDM, XCA and XCDR. Your system will communicate directly with the XDS Toolkit in the appropriate role. You or a test manager will use the web UI of the Toolkit to initiate and validate tests.
5. Gazelle Patient Manager (Patient Manager): The Patient Manager tool tests IHE patient discovery transactions. It has a web user interface that allows you to initiate tests and evaluate results.
6. Gazelle Security Suite (GSS): The Gazelle Security Suite is designed to test requirements defined by the ATNA profile. It supports testing of TLS transactions and validates IHE syslog messages.

2.2. General Testing Workflow

The application form that you complete contains the systems and roles that you intend to test. A Test Manager will transcribe that information into Gazelle Test Management. The Gazelle Test Management system will produce a list of required and optional tests that are tailored to your registration.

Each of your staff members who will participate in testing will create an account in the Gazelle system, and each account will be linked to your organization. Your members will see your test lists and results, but they cannot see the results of other organizations.

Staff members will work through the list of tests on the Gazelle dashboard. Your staff and management can monitor progress as tests are completed and then reviewed by a Test Manager. The dashboard provides both a high-level view (*XCA/Initiating Gateway is complete*) and details on the individual tests. Some of the tests are designed to run in a specific order, but many tests can be run in any sequence. You can divide the tests among your team members. You will have a great deal of flexibility as you choose which tests to address first.

QHIN requirements are based on several layers of specifications written by both IHE and HL7. The broad categories are:

- Transport Protocols
  - IHE Cross-Community Patient Discovery (XCPD)
  - IHE Cross-Community Access (XCA)

    - IHE Cross-Community Document Reliable Interchange (XCDR)
- Security Considerations
    - IHE Audit Trail and Node Authentication (ATNA)
- User Authentication and Authorization
    - IHE Cross Enterprise User Assertion (XUA)
- Document Content
    - HL7 C-CDA R2.1
    - HL7 CDA Release 2
    - PDF

The tests are designed in a way that will allow you to work through the transport protocols either with or without the ATNA and XUA requirements. While you must implement all requirements, you might find it easier to test the transport protocols first without the ATNA and/or the XUA components.

2.3. Test Categories and Test Logs

The Conformity Assessment tests are grouped into three broad categories:

- Smoke Tests: These are the set of tests your system will need to successfully execute to demonstrate conformance to the requirements in the QTF.
- Provisional Tests: These are tests that are run in support of provisional or optional behavior of the Initiating or Responding Gateway.
- Diagnostic Tests: These are derived from the Smoke or Provisional Tests. They are intended to assist you in working through issues by omitting either the XUA or TLS requirements or providing additional test steps with better logging information.

Test logs for the various types (Smoke, Provisional, Diagnostic) are segregated. This will allow you to run tests in one category (for example, Diagnostic) without writing over the logs in another category (for example, Smoke).

3. Document Specific Tests

While some of the tests are agnostic to the types of documents produced or consumed by QHIN participants, other tests do rely on specific document types. This section provides a guide to helping you understand how the QHIN requirements are mapped to test procedures. The QTF states these requirements concerning document content:

QTF-043	When a Responding Source is unable to generate C-CDA R2.1 format documents, QHINs MAY offer document conversion services, except where the use of another format is consistent with QTF-045 and QTF-048.
QTF-044	A QHIN converting a document to C-CDA R2.1 format MUST convert to one of the templates as defined in HL7 CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes - US Realm. C-CDA (HL7 CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes - US Realm) available at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=492
QTF-045	Responding QHINs SHOULD transmit any specific document format requests (provided by the Initiating QHIN via the IHE XDSDocumentEntryFormatCode XCA parameter) to Responding Sources.
QTF-046	Responding QHINs SHOULD provide C-CDA R2.1 documents that follow recommendations as presented in Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes. Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes -- available at https://ceq-project.s3.amazonaws.com/wp-content/uploads/2019/04/11013830/20190201_Improve_C-CDA_Joint_Content_WG_IHE_v1.1_Final.pdf
QTF-047	All C-CDA R2.1 format documents adhering to the Continuity of Care Document template SHOULD include all appropriate data classes and elements from the United States Core Data for Interoperability (USCDI) V1 prior to January 1, 2023 and MUST include all appropriate data classes and elements from USCDI V1 after January 1, 2023. The RCE will determine ongoing requirements of using newer versions of the USCDI as they are released. The United States Core Data for Interoperability (USCDI) – available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

QTF-090	A Responding Actor SHOULD provide C-CDA R2.1 documents that follow recommendations as presented in Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes, when the information held by that Responding Actor is organized around a clinical encounter construct. Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes -- available at https://ceq-project.s3.amazonaws.com/wp-content/uploads/2019/04/11013830/20190201_Improve_C-CDA_Joint_Content_WG_IHE_v1.1_Final.pdf
QTF-091	A Responding Actor MUST use nationally standardized code systems for all data exchange, where such code systems exist (e.g., LOINC, RxNORM, SNOMED-CT, etc.).
QTF-092	All C-CDA R2.1 format documents adhering to the Continuity of Care Document template SHOULD include all appropriate data classes and elements from the United States Core Data for Interoperability (USCDI) V1 prior to January 1, 2023 and MUST include all appropriate data classes and elements from USCDI V1 after January 1, 2023. The RCE will determine ongoing requirements of using newer versions of the USCDI as they are released. The United States Core Data for Interoperability (USCDI) – available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi
QTF-109	The test patient data MUST include at least one C-CDA R2.1 document with fictional clinical data that can be queried and retrieved.
QTF-110	All QHINs SHOULD create at least one C-CDA Discharge Summary and Progress Note template document for the test patient. QHINs serving outpatient clinics and inpatient hospitals MUST create such documents. Any encounters, etc. MUST be linked to the clinician created for QTF-114.
QTF-115	A "Document Query Nominal Flow" of the test data per QTF-105 MUST return the C-CDA R2.1 document(s) associated with a test patient.

Based on prior experience with the eHealth Exchange, the RCE will prioritize these C-CDA R2.1 document types during the initial testing rollout:

- Continuity of Care Document (CCD)
- Discharge Summary
- Progress Note
- Unstructured Document

Testing will also support PDF files that are not wrapped in a C-CDA R2.1 Unstructured Document.

Please reference QTF-110. A QHIN that serves outpatient clinics and/or inpatient hospitals is required to test both Discharge Summary and Progress Note documents. A QHIN is required to test any of the other document types listed above that it produces in either the initiating or responding roles. That is, a QHIN that will produce four types of documents must test all four types of documents and not just rely on testing the Discharge Summary and Progress Note.

A QHIN that does not meet the requirement specified in QTF-110 (outpatient clinic and/or inpatient hospital) is required to test at least one of the document types listed above. That QHIN is also required to test any of the other document types listed above that it produces in either the initiating or responding roles.

There is a further consideration for testing document content. A network of participants that will supply documents through a gateway might have different software implementations at the participant sites. There is no requirement that the gateway normalize the documents and/or correct defects, but the gateway must deliver documents that conform to the C-CDA R2.1 requirements.

- QHINs will be required to submit and test all variants of the specific document types that will be delivered to other QHINs. For example, a QHIN that serves a network with three different implementations of Discharge Summary documents will need to provide samples and test all three variants. Instructions on document testing are found in *Document Content Test Cases*.
- Transport tests for Document Query and Retrieve and Message Delivery also depend on document types supported within the QHIN. Some test cases rely on specific document types, and you will be required to run the tests that are relevant to your environment. For example, if your network does not produce/share a C-CDA R2.1 Procedure Note, you will not run any of the transport tests based on that document type.

4. Testing Your Initiating Gateway

This section describes high level requirements for the Initiating Gateway, test tools involved in the process, and the general steps you will follow. While the discussion of the tests will often refer to work that a Test Manager might perform after you submit your data, you can often use the tools to review the test data and results yourself. Those procedures will be discussed in the User Guide.

XCPD: The Initiating Gateway needs to send patient discovery requests to one or more Responding Gateways to identify that patient as known to the Responding QHIN. You will be asked to send patient discovery queries to the **Gazelle Patient Manager**. The Gazelle Patient Manager will both log and respond to your requests. Requests will be evaluated by a Test Manager on an asynchronous basis.

XCA: The Initiating Gateway is required to send document discovery and document retrieve requests to one or more Responding Gateways. The document discovery requests use the patient identity provided by the Responding QHIN. You will be asked to send XCA requests to the **XDS Toolkit**. The XDS Toolkit will both log and respond to your requests. Requests will be evaluated by a Test Manager on an asynchronous basis.

XCDR: The Initiating Gateway is required to send documents to the Responding QHIN using the XCDR Integration Profile. You will be asked to submit documents to the **XDS Toolkit**. The XDS Toolkit will provide some immediate validation (metadata well formed, coded values are taken from a defined value set) as you submit each document. There is an asynchronous process where both you and a Test Manager can automatically run tests at another level of detail. Those detailed steps will test if the document metadata is properly aligned with the type of document that was submitted (mime type, format code, etc.).

ATNA: The Initiating Gateway is required to initiate connections using specified versions of the TLS protocol and supporting mutual authentication. The Prospective QHIN's Initiating and Responding Gateway is also required to produce audit records for each of the transactions it initiates.

You will test the TLS requirements using different tools:

1. You will initiate TLS connections with the **Gazelle Security Suite** as a basic test of TLS and proper protocol version.
2. You will complete the XCPD tests using TLS connections that you initiate with the **Gazelle Patient Manger**.

3. You will complete the XCA and XCDR tests using TLS connections that you initiate with the **XDS Toolkit**.
4. You will export/capture your audit records and submit these to the Test Manager. The Test Manager will evaluate each record using the **Gazelle Security Suite**.

XUA: The Initiating Gateway is required to include SAML 2.0 assertions in the header of the SOAP envelope for all transactions. A Test Manager will view and evaluate the assertions after you have submitted the transactions.

Your system will need to sign the assertions with a digital certificate issued by the RCE. This certificate need not be the same one used for the establishment of the TLS connection, but it often is. Regardless, all certificates used for connections and digital signatures must be those issued by the RCE.

4.1. Configuration Required for Testing an Initiating Gateway

You will need to provide the following for testing:

- List of all team members so Test Managers can create system accounts and communicate with them.
- Attestation that the certificate enrollment process has been completed with DirectTrust.
- Attestation that the proper network configuration has been completed to allow mTLS with the RCE ITP including list of IP addresses from which you will initiate connections to the test tools. Access to testing results is controlled by IP address.

Test managers will provide you with the following configuration information:

- URL’s for web user interfaces for all test tools.
- Web endpoints for all test services (both TLS and standard HTTP).
- List of test patients and medical histories to be used in testing.
- Value sets or related references for coded entries in XDS metadata, patient records and other records.

4.2. Workflows for Testing Initiating Gateway Transport

This section provides context, steps you are expected to perform, and assessment procedures when performing transport tests as an Initiating Gateway. The following documents provide detailed information:

- *Transport Test Cases*: Contains a section for each test case with instructions and expected results
- *User Guide*: Includes instructions on how to execute test steps using the Test Tools.

Document Query Scenario

To support this scenario, the Initiating Gateway performs these functions:

1. Patient Discovery Query, including
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing
2. Document Query and Retrieve, including
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing

To test ***Patient Discovery Query***, you will be given demographic information for one patient that exists in the Test Tools. You will be required to demonstrate that your Initiating Gateway can send an appropriate XCPD request to discover the patient in the **Gazelle Patient Manager** and then use the proper patient identifier for later document query transactions. While you might perform initial testing without the required security protocols in place, you will be required to use those security protocols to complete testing. In detail, your Initiating Gateway will initiate SOAP transactions with the Gazelle Patient Manager based on requirements in the QTF. In general,

1. The TCP channel you initiate must use the TLS protocol using a version specified by the QTF.
2. Your Initiating Gateway will perform mutual authentication with the Gazelle Patient Manager.
3. Your SOAP transactions will include required SAML assertions that identify the user requesting the information.
4. Your SOAP transactions will include required SAML assertions that provide authorization and accept values for exchange purpose.

Your system produces the appropriate audit records.

You will:

- Initiate a Patient Discovery Query with the Gazelle Patient Manager.

  - Record the permanent link with for all queries to share with the Test Manager.
- Email appropriate audit logs to the Test Manager.
- Inform the Test Manager when you are ready for test assessment.

The Test Manager will review both the audit logs and log data to assess results.

To test ***Document Query and Retrieve***, you use the patient identifier for the patient discovered above. You will be required to demonstrate that your Initiating Gateway can send appropriate XCA requests to find documents in the **XDS Toolkit** and then retrieve those documents. The XDS Toolkit will be configured with two Responding Gateway simulators representing two different communities. Some documents will be available in both simulated communities; other patient documents will only be found in a single community. You will be required to demonstrate that you can send appropriate XCA query and retrieve requests to find the documents in both simulated communities and retrieve the documents. The same security protocols described for Patient Discovery are in place for Document Query and Retrieve and will not be repeated in this document.

Test cases for an Initiating Gateway require some discussion. Your Initiating Gateway receives inputs or stimuli from your network participants using protocols defined by your network agreements. The testing system cannot specify the form or content of those inputs. For example, participants in your network might simply request a search for all documents for a patient, and your Initiating Gateway would only support such a query. In a different network, the participants might limit the searches by supplying specific metadata values. The Initiating QHIN in that network might pass those parameters to Responding Gateways, or the Initiating QHIN might query for all documents and filter the results that are then returned to the requesting participant. We believe the test cases will allow for these differences and not force your Initiating Gateway to implement a query that does not occur in your network. Should you find a test case that assumes or requires such a query, please inform the Test Manager.

Section 6 of this document describes the XDS Toolkit configuration and documents that are available to be retrieved.

You will:

- Initiate one or more Document Query requests with the XDS Toolkit.
  - Record the permanent link for all queries to share with the Test Manager.
- Initiate one or more Document Retrieve requests with the XDS Toolkit.
  - Record the permanent link for all queries to share with the Test Manager.
- Email appropriate audit logs to the Test Manager.
- Inform the Test Manager when you are ready for test assessment.

The Test Manager will review both the audit logs and log data to assess results.

Message Delivery Scenario

To support this scenario, the Initiating Gateway performs these functions:

1. Patient Discovery Query, including
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing
2. Message Delivery, including
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing

The Message Delivery Scenario does not define new requirements for the Patient Discovery Query and uses the same testing structure described above. The security protocols for Message Delivery are the same as those for Document Query and Retrieve and are not repeated in this section.

To test ***Message Delivery***, you use the patient identifier for the patient discovered above. You will be required to demonstrate that your Initiating Gateway can send at least one of the following document types to the XDS Toolkit:

- C-CDA R2.1 Continuity of Care Document (CCD)
- C-CDA R2.1 Discharge Summary
- C-CDA R2.1 Progress Note
- C-CDA R2.1 Unstructured Document
- PDF

Participants in your network might support more than one of these document types, and you will be encouraged to submit as many different types as your platform supports.

Assessment for Message Delivery takes place in phases—some with automated conformity assessment and the remainder with manual review by the Sequoia Project staff. You will submit your document or documents to the XDS Toolkit using XDS metadata as described in Section 7 of this document. The XDS Toolkit will reject your submission if it is improperly formatted or if any of the metadata values used are not from the values configured in the Toolkit. In this first phase, specific metadata values are not tested, nor is the document structure tested. You drive this phase of the testing by submitting as many transactions as you wish. The transaction response from the XDS toolkit will guide you on the mechanics of this first phase.

In the second phase, XDS Toolkit will examine the metadata associated with the document transaction. For example, submission of a Discharge Summary might require specific values in one or more metadata fields. Rather than just testing for a metadata value that is part of the accepted code table, the XDS Toolkit will search for transactions where the specific metadata values are present. If any one of your transactions satisfies all metadata requirements, the XDS Toolkit will indicate that the specific test has been successfully completed. If no transaction is found that meets all the requirements, that test will fail. See Section 8 of this document for the mapping of document types to required metadata values.

In the third phase, the Test Manager will review and assess the audit messages your system produces when it exports a document. As with the cases above, you will email those audit messages to testing@sequoiaproject.org for the Test Manager for review.

The structure of your document or documents is assessed in the fourth phase. You will email your document samples to the Test Manager who will assess them for conformance to the appropriate standards, most likely C-CDA. This version of testing does not review clinical content.

4.3. Workflows for Testing Initiating Gateway Security

Security tests for the Initiating Gateway cover these categories:

- TLS connections (mutual authentication and support for required TLS versions)
- Audit logs
- SAML assertions for user authentication, user authorization and exchange purpose

TLS Connections

TLS Connections are tested with the Gazelle Security Suite, the Gazelle Patient Manager, and the XDS Toolkit.

You will initiate TLS connections with the Gazelle Security Suite and test both positive and negative test cases. The positive test cases are designed to ensure that your system supports mutual authentication with the required TLS versions and that your system is using a proper digital certificate. For the negative test cases, your Initiating Gateway should determine that the

Gazelle Security Suite is trying to accept your connection using a certificate or TLS version that is out of specification. Your system is required to reject the connection and not conduct any transactions.

The Gazelle Patient Manager and XDS Toolkit are used to test transport cases as described above. These tools test a more complete workflow and support both HTTP and HTTPS connections. You are allowed to practice with plain HTTP connections as you work through the transport test cases. To pass the transport test cases, you will need to enable TLS connections on the Gazelle Patient Manager and XDS Toolkit. These tools will further test that your Initiating Gateway supports the positive test cases for digital certificates, mutual authentication, and TLS versions. These two tools do not implement negative test cases.

Audit Logs

Audit logs are tested as part of the overall workflow for Patient Discovery Query, Document Query and Retrieve, and Message Delivery. Tests defined in *Query Transport Test Cases* include a step where you are required to collect and send the appropriate audit message to the Test Manager for assessment.

SAML Assertions

SAML Assertions are tested using a model similar to the model used to test TLS connections. The same tools are used: Gazelle Security Suite, Gazelle Patient Manager, and XDS Toolkit.

The Gazelle Security Suite will initiate connections with your Initiating Gateway and test both positive and negative test cases. The positive test cases are designed to ensure that your system recognizes valid SAML assertions. The negative test cases utilize valid mTLS connections but contain various faults in the message structure. Your Initiating Gateway is required to respond appropriately with either a fault message or no response depending on your local policies.

The Gazelle Patient Manager and XDS Toolkit are used to test transport cases as described above. These tools test a more complete workflow and support SAML assertions. You are allowed to practice without SAML assertions as you work through the transport test cases. To pass the transport test cases, you will need to enable SAML assertions on the Gazelle Patient Manager and XDS Toolkit. These tools will further test that your Initiating Gateway supports the positive test cases. These two tools do not implement negative test cases as part of the testing workflow.

4.4. Workflows for Testing Initiating Gateway Document Content

Transport tests described above only test the message transport—not the document structure and content. The transport tests ensure that your system can search for and retrieve documents and also submit documents to another QHIN. In addition, the Prospective QHIN Testing Program requires prospective QHINs to complete testing for document structure and content.

Your Initiating Gateway needs to provide one or more specific document types in the Message Delivery Scenario. These are:

1. C-CDA R2.1 CCD
2. C-CDA R2.1 Discharge Summary
3. C-CDA R2.1 Progress Note
4. C-CDA R2.1 Unstructured Document
5. PDF

For each C-CDA document type that you support, you will be required to supply at least one sample document. These can either be emailed to a Test Manager for uploading and evaluation, or you can upload them to the EVS Client and validate them yourself. If you choose to validate them yourself, record the permanent link to the evaluation from EVS Client to supply to the Test Manager.

5. Testing Your Responding Gateway

This section describes high level requirements for the Responding Gateway, test tools involved in the process, and the general steps you will follow. The procedure to test your Responding Gateway differs from the procedure for testing an Initiating Gateway. You will be asked to create an environment that mimics the participants in your network. You will load patient records into that environment. Test tools will then initiate transactions defined in the QTF documentation.

XCPD: The Responding Gateway responds to patient discovery requests to identify a patient as known in your network. An Initiating Gateway initiates a query with demographic information. The Responding Gateway is responsible for finding patients that match the demographics and returning those patients to the Initiating Gateway. Your system will be tested using the **Gazelle Patient Manager**. The Responding Gateway will be able to access Patient Manager in a self-service manner to direct queries to the system under test. The tooling will indicate a pass or fail within the tooling. The Test Manager will use the Gazelle Patient Manager to review responses for conformity to requirements as well as content when all testing is completed.

XCA: The Responding Gateway accepts document query and retrieve requests from an Initiating Gateway and delegates those requests to participant systems in the network. The Responding Gateway gathers results from participant systems and returns those to the Initiating Gateway. A Test Manager will initiate query and retrieve requests through the web user interface of the **XDS Toolkit**. The Toolkit will initiate transactions with your Responding Gateway, record the responses and evaluate those responses for conformity to requirements.

XCDR: The Responding Gateway is required to accept XCDR transactions and route the documents to the proper network participant to support the Message Delivery scenario. The Responding Gateway will be able to access **XDS Toolkit** in a self-service manner. The Toolkit will initiate transactions with your Responding Gateway, record the responses and evaluate those responses for conformity to requirements. The tooling will indicate a pass or fail within the tooling. The Test Manager will use the XDS Toolkit to review responses for conformity to requirements as well as content when all testing is completed. The Test Manager will also ask you to provide evidence that you have routed the document to the intended recipient.

ATNA: The Responding Gateway is required to accept connections using specified versions of the TLS protocol supporting mutual authentication. The Responding Gateway is also required to produce audit records for all transactions.

You will test the TLS requirements using different tools:

1. A Test Manager will initiate TLS connections with your Responding Gateway using the **Gazelle Security Suite** as a basic test of TLS and proper protocol version.
2. You will complete the XCPD tests using TLS connections that are initiated by the **Gazelle Patient Manger**.
3. You will complete the XCA and XCDR tests using TLS connections that are initiated with the **XDS Toolkit**.
4. You will export/capture your audit records and submit these to the Test Manager. The Test Manager will evaluate each record using the **Gazelle Security Suite and other tools**.

XUA: The Responding Gateway is required to properly understand SAML 2.0 assertions included in the header of the SOAP envelope for all transactions. The Responding Gateway will use the assertions to manage authorization directly or will delegate that responsibility to participants in the network. A Test Manager will direct the Patient Manager and Toolkit to initiate transactions with your Responding Gateway. You will be expected to accept and process transactions with valid SAML assertions. Depending on the details of the error case, your Responding Gateway might reject a transaction or possibly respond with an indication that the user was not authorized or that no records were found. Test cases will provide details on the expected response.

Note: Language in the sections that follow may be of the form “Your Responding Gateway will perform function X” or “Your Responding QHIN will perform function Y”. Your responding system provides an interface that is being tested. The gateway system (software + hardware) might delegate some functions to participants in your network. The black box testing used by the RCE does not require you to expose where the functions are implemented. You are only required to test and demonstrate that the interface to your gateway system meets the requirements for a Responding QHIN.

5.1. Configuration Required for Testing a Responding Gateway

You will need to provide the following for testing:

- List of all team members so Test Managers can create system accounts and communicate with them.
- Attestation that the digital certificate(s) used for TLS negotiation is properly installed. The procedure to obtain the certificate is defined here.
- List of IP addresses that will initiate and respond.
- Table of endpoints that indicates the URL’s for each transaction that your Responding QHIIN will accept. The table will include an entry for both HTTP (provided as a convenience for testing troubleshooting but not evaluated in the testing program) and HTTPS endpoints.

Test Managers will provide you with the following configuration information:

- IP addresses of all tools that will initiate an HTTP or HTTPS transaction with your Responding Gateway. You can use this information to allow list those systems.
- List of test patients and medical histories to be used in testing.
- Value sets for coded entries in XDS metadata, patient records and other records.

5.2. Workflows for Testing Responding Gateway Transport

This section provides context, steps you are expected to perform, and assessment procedures when performing transport tests with a Responding Gateway. The following documents provide detailed information:

- *Transport Test Cases*: Contains a section for each test case with instructions and expected results
- *User Guide*: Includes instructions on how to execute test steps using the Test Tools.

Document Query Scenario

To support this scenario, the Responding Gateway performs these functions:

1. Patient Discovery Query, including
    a. Secure Channel
    b. Mutual Authentication
    c. User Authentication
    d. Authorization & Exchange Purpose
    e. Auditing
2. Document Query and Retrieve, including
    a. Secure Channel
    b. Mutual Authentication
    c. User Authentication
    d. Authorization & Exchange Purpose
    e. Auditing

To test ***Patient Discovery Query***, you will be given demographic information for one patient you will load into your system. The Test Manager will use the **Gazelle Patient Manager** to send one or more Patient Discovery queries to your Responding Gateway. While you might perform initial testing without the required security protocols in place, you will be required to use those security protocols to complete testing. In detail, your Responding Gateway will accept and respond to SOAP transactions from the Gazelle Patient Manager based on requirements in the QTF. In general,

1. The TCP channel you accept must use the TLS protocol using a version specified by the QTF.
2. Your Responding Gateway will perform mutual authentication with the Gazelle Patient Manager.
3. You will ensure that the SAML assertions included in the SOAP transactions are used to provide appropriate user authentication and authorization in your network.
4. Your system produces the appropriate audit records.
5. Your system responds appropriately to negative test cases concerning SAML assertions.

You will:

- Use the Gazelle Patient Manager to initiate Patient Discovery transactions with your Responding Gateway.
    - Record the permanent link for all queries to share with the Test Manager.
- Email appropriate audit logs to the Test Manager.
- Inform the Test Manager when you are ready for conformity assessment review once the testing process is complete and the tooling shows passing for the required test cases. The Sequoia Project is unable to assess partial submissions and can only provide assessment on complete submissions.

The Test Manager will review both the audit logs and log data to assess results. The final outcome of the testing will be a comprehensive report detailing the outcomes.

To test ***Document Query and Retrieve***, you use the patient that was previously loaded for Patient Discovery tests. You will associate one or more documents with that patient in your test network of participants and respond to query and retrieve requests that are launched by the XDS Toolkit. The same security protocols described for Patient Discovery are in place for Document Query and Retrieve and will not be repeated in this document.

Section 9 of this document lists the types of documents that can be used for testing Document Query and Retrieve and associated metadata values. You will be required to support at least one of the document types as appropriate for your network participants.

You will:

- Use the XDS Toolkit to initiate Document Query requests
  - Record the time stamp for all queries to share with the Test Manager.
- Use the XDS Toolkit to initiate Document Retrieve requests
  - Record the time stamp for all queries to share with the Test Manager.
- Email appropriate audit logs to the Test Manager.
- Inform the Test Manager when you are ready for conformity assessment.

The Test Manager will review both the audit logs and log data to assess results.

Message Delivery Scenario

To support this scenario, the Responding Gateway performs these functions:

1. Patient Discovery Query, including
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing
2. Message Delivery, including
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing

The Message Delivery Scenario does not define new requirements for the Patient Discovery Query and uses the same testing structure described above. The security protocols for Message Delivery are the same as those for Document Query and Retrieve and are not repeated here in this document.

To test ***Message Delivery***, you use the patient identifier for the patient discovered above. You will be required to demonstrate that your Initiating Gateway can accept at least one of the following document types to the XDS Toolkit:

- C-CDA R2.1 CCD
- C-CDA R2.1 Discharge Summary
- C-CDA R2.1 Progress Note
- C-CDA R2.1 Unstructured Document
- PDF

Participants in your network might support more than one of these document types, and you will be encouraged to accept as many different types as possible.

5.3. Workflows for Testing Responding Gateway Security

Security tests for the Responding Gateway cover these categories:

- TLS connections (mutual authentication and support for required TLS versions)
- Audit logs
- SAML assertions for user authentication, user authorization, and exchange purpose

TLS Connections

TLS Connections are tested with the Gazelle Security Suite, the Gazelle Patient Manager, and the XDS Toolkit.

The Gazelle Security Suite will initiate TLS connections with your Responding Gateway testing both positive and negative test cases. The positive test cases are designed to ensure that your system supports mutual authentication with the required TLS versions and that your system is using a proper digital certificate. Your system must accept connections for the positive cases. The negative cases initiate connections that your system should reject. For example, these would test connections where the Gazelle Security Suite uses an expired certificate, a certificate that is not recognized by the RCE, and/or TLS versions that do not meet the QHIN requirements.

The Gazelle Patient Manager and XDS Toolkit are used to test transport cases as described above. These tools test a more complete workflow and support both HTTP and HTTPS connections. You are allowed to practice with plain HTTP connections as you work through the transport test cases.

To pass the transport test cases, you will need to enable TLS connections on the Gazelle Patient Manager and XDS Toolkit. These tools will further test that your Responding Gateway supports the positive test cases for digital certificates, mutual authentication, and TLS versions. These two tools do not implement negative test cases.

Audit Logs

Audit logs are tested as part of the overall workflow for Patient Discovery Query, Document Query and Retrieve, and Message Delivery. Tests defined in *Query Transport Test Cases* include steps where you are required to collect and send the appropriate audit message to the Test Manager for assessment.

SAML Assertions

SAML Assertions are tested using a model similar to the model used to test TLS connections. The same tools are used: Gazelle Security Suite, Gazelle Patient Manager, EVS Client and XDS Toolkit.

The Gazelle Security Suite is self-service and will initiate connections with your Responding Gateway testing both positive and negative test cases. The positive test cases are designed to ensure that your system recognizes valid SAML assertions. The negative cases initiate connections that your system accepts at the TLS level but rejects at the application level. The SAML assertions used for the negative tests are missing required values and/or have invalid values. Your Responding Gateway is required to return either an error (such as a SOAP fault) or non-response (depending on your local policies) rather than a valid response.

The Gazelle Patient Manage and XDS Toolkit are used to test transport cases as described above. These tools test a more complete workflow and support SAML assertions. You are allowed to practice without SAML assertions as you work through the transport test cases. To pass the transport test cases, you will need to enable SAML assertions on the Gazelle Patient Manager and XDS Toolkit. These tools will further test that your Responding Gateway supports the positive test cases. The Gazelle Patient Manager does not implement negative test cases; the XDS Toolkit does cover some negative tests.

5.4. Workflows for Testing Responding Gateway Document Content

The transport tests described above do not test document structure and content. Rather, the above tests ensure that your system can respond to document queries, provide documents when they are requested, and accept documents when submitted to your system by another QHIN. However, there are also requirements related to document content.

Your Responding Gateway needs to return one or more specific document types in the Document Query Scenario. These are:

1. C-CDA R2.1 CCD
2. C-CDA R2.1 Discharge Summary
3. C-CDA R2.1 Progress Note
4. C-CDA R2.1 Unstructured Document
5. PDF

For each C-CDA document type that you support, you will be required to supply at least one sample document. These can either be emailed to a Test Manager for uploading and evaluation, or you can upload them to the EVS Client and validate them yourself. If you choose to validate them yourself, record the permanent link to the evaluation from EVS Client to supply to the Test Manager.

6. Common Tests for Both Initiating and Responding Gateways

6.1. Common Document Content Tests

Document Content tests are the same for a QHIN when acting in either the initiating or responding role. There is no distinction made between documents that are delivered in response to retrieve requests (XCA) and documents that are delivered using the Message Delivery Scenario (XCPD). You will produce samples for every supported document type and from every different source within your network. You will use the web user interface on the Gazelle External Validation Service (EVS) to upload each sample and validate the conformance of the sample. When you have uploaded conformant documents, you will alert the Test Manager who will review the results. Details are provided in *Document Test Cases*.

7. Comprehensive List of Tests

7.1. Initiating Gateway (IG) Tests

Identifier	Name	Type
Onboarding & Designation SOP	QHIN Candidate completes Onboarding & Designation SOP	Documentation
IG Remediation 1	Initiating Gateway documents remediation plans for QHIN to QHIN connections	Documentation
IG Remediation 2	Initiating Gateway documents remediation plans for connections with network participants	Documentation
IG Certificate Requirements	Initiating Gateway documents server certificate technical parameters	Documentation
IG Cryptographic Modules	Initiating Gateway documents adherence to requirements for cryptographic modules	Documentation
IG Participant TLS 1.2	Affirm mutual authentication with network participants using TLS 1.2 or higher	Documentation
IG TLS 1.3 Schedule	Initiating Gateway documents schedule for implementation of TLS 1.3	Documentation
IG User Authentication 1	Initiating Gateway documents mechanisms for network participants to supply authentication information	Documentation

Identifier	Name	Type
IG Authorization 1	Initiating Gateway documents mechanisms for network participants to supply authorization information	Documentation
IG Participant Interface	Initiating Gateway documents participant interface	Documentation
IG Routing	Initiating Gateway documents mechanism for gathering routing information	Documentation
IG Reporting Requirements	Initiating Gateway documents plans to support reporting requirements	Documentation
IG User Authentication 2	Initiating Gateway demonstrates user authentication with network participants	Smoke
IG Routing	Initiating Gateway documents mechanism for gathering routing information	Smoke
IG Reporting Requirements	Initiating Gateway documents plans to support reporting requirements	Smoke
IG Discover Patient 001	Initiating Gateway discovers patient QTFTEST-001	Smoke
IG Discover Patient 002	Initiating Gateway discovers patient QTFTEST-002	Smoke
IG In Network Patient Discovery	Initiating Gateway demonstrates patient discovery interface with network participants	Smoke
IG Basic Query	Initiating Gateway sends a basic Query Document request	Smoke
IG Retrieve Basic	Initiating Gateway sends a basic Retrieve Document request	Smoke
IG Deliver Document	Deliver one document	Smoke
IG Deliver CCD	Submit CCD	Smoke[1]
IG Deliver Discharge Summary	Submit Discharge Summary	Smoke[1]
IG Deliver Progress Note	Submit Progress Note	Smoke[1]
IG Deliver Unstructured Document	Submit Unstructured Document	Smoke[1]
IG Participant XCDR Interface	Initiating Gateways demonstrates interface with network participants for Message Delivery	Smoke

Identifier	Name	Type
IG TLS 1.2 Parameters	Initiating Gateway TLS 1.2 parameters are tested	Smoke
IG TLS 1.3 Parameters	Initiating Gateway TLS 1.3 parameters are tested	Smoke
IG Participant TLS 1.2	Initiating Gateway demonstrates TLS 1.2 connections with network participants	Smoke
IG Participant Server Authentication	Initiating Gateway demonstrates server authentication with network participants	Smoke
IG Internal Audit Messages	Initiating Gateway tests audit messages for internal network events	Smoke
IG Exchange Purpose Tests	IG demonstrates purpose of use	Smoke
IG Message Delivery User Authentication	Initiating Gateway tests SAML assertions during Message Delivery Scenario	Smoke
IG Error Handling External	Initiating Gateway demonstrates error handling with external systems	Smoke
IG Error Handling Internal	Initiating Gateway demonstrates error handling with network participants	Smoke
IG Demonstrate Participant Interface	Initiating Gateway demonstrates software interface for network participants	Smoke
IG Participant Patient Discovery Interface	Initiating Gateway demonstrates software interface for network participants performing patient discovery	Smoke

Notes:

1. Initiating Gateway must complete at least one of these tests.

7.2. Responding Gateway Tests

Identifier	Title	Type
Onboarding & Designation SOP	QHIN Candidate completes Onboarding & Designation SOP	Documentation
RG Remediation 1	Responding Gateway documents remediation plans for QHIN to QHIN connections	Documentation
RG Remediation 2	Responding Gateway documents remediation plans for connections with network participants	Documentation

Identifier	Title	Type
RG Certificate Requirements	Responding Gateway documents server certificate technical parameters	Documentation
RG Cryptographic Modules	Responding Gateway documents adherence to requirements for cryptographic modules	Documentation
RG Participant TLS 1.2	Affirm mutual authentication with network participants using TLS 1.2 or higher	Documentation
RG TLS 1.3 Schedule	Responding Gateway documents schedule for implementation of TLS 1.3	Documentation
RG User Authentication 1	Responding Gateway documents mechanisms for supplying user authentication information to network participants	Documentation
RG Authorization 1	Responding Gateway documents mechanisms for network participants to supply authorization information	Documentation
RG Participant Interface	Responding Gateway documents participant interface	Documentation
RG Patient Demographics Requirements	Responding Gateway documents conformance to patient demographic requirements	Documentation
RG Patient Identity Resolution SLA	Responding Gateway documents conformance to patient identity resolution SLA requirements	Documentation
RG Retrieve Document Types	Responding Gateway documents all document types available for retrieve	Documentation
RG Standardized Code Systems	Responding Gateway documents conformance to code system requirements	Documentation
RG Routing	Responding Gateway documents mechanism for gathering routing information	Documentation
RG Reporting Requirements	Responding Gateway documents plans to support reporting requirements	Documentation
RG User Authentication 2	Responding Gateway demonstrates user authentication with network participants	Smoke
RG Discover Patient Basic 003	Gateway responds to basic Patient Discovery query for patient 003	Smoke
RG Discover Patient Basic 004	Gateway responds to basic Patient Discovery query for patient 004	Smoke

Identifier	Title	Type
RG Discover Patient Advanced	Gateway responds to advanced Patient Discovery queries	Provisional
RG Discover Patient Errors	Responding Gateway responds to non-conformant Patient Discovery queries	Provisional
RG In Network Patient Discovery	Responding Gateway demonstrates patient discovery interface with network participants	Smoke
RG Basic Query	Gateway responds to basic document query	Smoke
RG Advanced Query	Gateway responds to advanced document query	Smoke
RG Basic Retrieve	Gateway responds to request to retrieve single document	Smoke
RG Retrieve C-CDA 2.1 CCD	Responding Gateway responds to retrieve request for C-CDA 2.1 CCD	Smoke
RG Retrieve C-CDA 2.1 Discharge Summary	Responding Gateway responds to retrieve request for C-CDA 2.1 Discharge Summary	Smoke
RG Accept CCD	Accept CCD	Smoke[1]
RG Accept Discharge Summary	Accept Discharge Summary	Smoke[1]
RG Accept Progress Note	Accept Progress Note	Smoke[1]
RG Accept Unstructured Document	Accept Unstructured Document	Smoke[1]
RG Accept PDF	Accept PDF	Smoke[1]
RG Participant XCDR Interface	Responding Gateways demonstrates interface with network participants for Message Delivery	Smoke
RG Route to Different Destinations	Responding Gateway routes document to different destinations	Smoke

Identifier	Title	Type
RG C-CDA Conversion	Responding Gateway demonstrates C-CDA conversion	Provisional
IG TLS 1.2 Parameters	Initiating Gateway TLS 1.2 parameters are tested	Smoke
IG TLS 1.3 Parameters	Initiating Gateway TLS 1.3 parameters are tested	Smoke
RG Participant TLS 1.2	Responding Gateway demonstrates TLS 1.2 connections with network participants	Smoke
RG Participant Server Authentication	Responding Gateway demonstrates server authentication with network participants	Smoke
RG Internal Audit Messages	Responding Gateway tests audit messages for internal network events	Smoke
RG Error Handling External	Responding Gateway demonstrates error handling with external systems	Smoke
RG Error Handling Internal	Responding Gateway demonstrates error handling with network participants	Smoke
RG Exchange Purpose Tests	Responding Gateway tested for Purpose of Exchange	Smoke
RG Patient Discovery User Authentication	Responding Gateway responds to Patient Discovery with user authentication	Smoke
RG Query Document User Authentication	Responding Gateway responds to Query Document with user authentication	Smoke
RG Message Delivery User Authentication	Responding Gateway accepts Message Delivery with user authentication	Smoke
TC-MAPD-R-0003.000	Handle missing wsse:Security element	Smoke

Identifier	Title	Type
TC-MAPD-R-0003.101	Handle missing Security/Timestamp element	Smoke
TC-MAPD-R-0003.201	Handle missing MessageID element	Smoke
TC-MAPD-R-0003.301	Handle missing Assertion signature element	Smoke
TC-MAPD-R-0003.302	Handle invalid Assertion signature	Smoke
TC-MAPD-R-0003.303	Handle missing timestamp signature element	Smoke
TC-MAPD-R-0003.306	Handle missing CanonicalizationMethod element in Timestamp signature	Smoke
TC-MAPD-R-0003.307	Handle missing CanonicalizationMethod algorithm in Timestamp signature	Smoke
TC-MAPD-R-0003.308	Handle missing SignatureMethod element in Timestamp signature	Smoke
TC-MAPD-R-0003.315	Handle missing DigestValue element in Timestamp signature reference	Smoke
TC-MAPD-R-0003.316	Handle Invalid DigestValue in Timestamp signature reference	Smoke
TC-MAPD-R-0003.317	Handle missing SignatureValue element in Timestamp signature	Smoke
TC-MAPD-R-0003.318	Handle missing KeyInfo element in timestamp signature	Smoke
TC-MAPD-R-0003.319	Handle missing KeyInfo/SecurityTokenReference element in timestamp signature	Smoke
TC-MAPD-R-0003.320	Handle missing /KeyInfo/SecurityTokenReference/@TokenType attribute in timestamp signature	Smoke
TC-MAPD-R-0003.321	Handle invalid TokenType version in timestamp signature	Smoke

Identifier	Title	Type
TC-MAPD-R-0003.323	Handle missing /SecurityTokenReference/KeyIdentifier/@ValueType attribute in timestamp signature	Smoke
TC-MAPD-R-0003.324	Handle Invalid ValueType version in timestamp signature	Smoke
TC-MAPD-R-0003.325	Handle Invalid KeyIdentifier (AssertionID) in timestamp signature	Smoke
TC-MAPD-R-0003.326	Handle Missing KeyInfo in Assertion signature	Smoke
TC-MAPD-R-0003.401	Handle missing Assertion element	Smoke
TC-MAPD-R-0003.410	Handle Missing Issuer Format in Assertion	Smoke
TC-MAPD-R-0003.411	Handle Invalid Issuer Email Name ID in Assertion	Smoke
TC-MAPD-R-0003.412	Handle Invalid Issuer X.509 Name ID in Assertion	Smoke
TC-MAPD-R-0003.413	Handle Invalid Issuer Windows Name ID in Assertion	Smoke
TC-MAPD-R-0003.420	Handle Missing Subject element in Assertion	Smoke
TC-MAPD-R-0003.421	Handle Missing Subject Name ID in Assertion	Smoke
TC-MAPD-R-0003.422	Handle Invalid Subject Name ID in Assertion	Smoke
TC-MAPD-R-0003.423	Handle Missing Subject Confirmation in Assertion	Smoke
TC-MAPD-R-0003.424	Handle Missing Subject Confirmation Method in Assertion	Smoke
TC-MAPD-R-0003.426	Handle Missing Subject Confirmation Data in Assertion	Smoke

Identifier	Title	Type
TC-MAPD-R-0003.427	Handle Missing Subject Confirmation Key Info in Assertion	Smoke
TC-MAPD-R-0003.429	Handle Invalid RSA Public Key Modulus in Assertion	Smoke
TC-MAPD-R-0003.430	Handle Missing RSA Public Key Exponent in Assertion	Smoke
TC-MAPD-R-0003.431	Handle Invalid RSA Public Key Exponent in Assertion	Smoke

Notes:

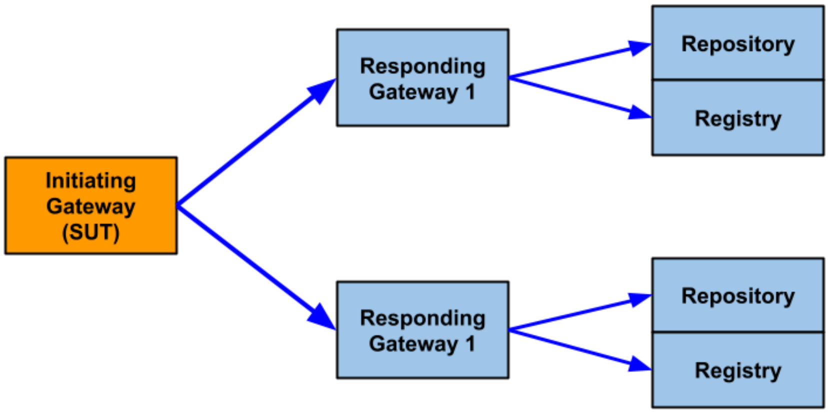
1. Responding Gateway must complete at least one of these tests.

8. NIST XDS Toolkit Configuration for Testing Initiating Gateways

The figure below shows the relationship between the Initiating Gateway System Under Test in orange and the NIST XDS Toolkit simulators in blue. The blue boxes represent simulators needed to support two communities. You will configure your Initiating Gateway to communicate with both Responding Gateway simulators. That information includes:

- Endpoints for transactions
- Home Community ID for each community
- Repository Unique ID for each Document Repository

Information for those values will be found in the XDS Toolkit as part of the testing environment and is not repeated here.



Configuration also includes the patients and documents that are known to the XDS Toolkit.

9. XDS Metadata Requirements For Message Delivery

Documents sent under the Message Delivery Scenario will include XDS metadata items as required by the IHE XCDR profile. Some values are specific to the document type while other values are dependent on the clinical scenario and/or source of the document. The table below contains a list of metadata items and describes how the Initiating Gateway will populate these for Message Delivery.

The table below says that some values shall be taken from the Testing Value Set. This value set is configured as part of the XDS Toolkit in an XML file. You will be able to have direct access to that file so you can configure your system. If you attempt to submit a document with a coded value that is not in that XML configuration file, your submission will be rejected by the XDS Toolkit software.

Level	Field	Comment
SubmissionSet	patientId	Defined by Test Manger / Test Plan
SubmissionSet	contentTypeCode	
SubmissionSet	sourceId	Defined by Test Manager. You shall configure your Initiating Gateway to use the value specified in the test plans.
DocumentEntry	classCode	Must be taken from Testing Value Set. A specific value is not required.
DocumentEntry	eventCodeList	Must be taken from Testing Value Set. A specific value is not required.
DocumentEntry	formatCode	Document dependent. Will have requirements defined by Test Plan.
DocumentEntry	homeCommunityID	Defined by Test Manger / Test Plan
DocumentEntry	mimeType	Document dependent. Will have requirements defined by Test Plan.
Document Entry	objectType	Fixed value defined by IHE
DocumentEntry	patientId	Defined by Test Manger / Test Plan
DocumentEntry	typeCode	Must be taken from Testing Value Set. A specific value may be required, depending on document type.
DocumentEntry	uniqueId	For a CDA document, this is to be taken from the ClinicalDocument.id. No requirements are defined for non-CDA documents. DICOM images that would trigger other requirements are out of scope.

10. Document Types and Metadata Requirements for Initiating QHINs

Initiating QHINs are required to support at least one of the following document types for the Message Delivery Scenario:

1. C-CDA R2.1 CCD
2. C-CDA R2.1 Discharge Summary
3. C-CDA R2.1 Progress Note
4. C-CDA R2.1 Unstructured Document
5. PDF

Each section below includes a table that lists required values for specific metadata fields. In those cases where a metadata field is not listed, you shall populate the field per the notes in Section 7 of this document.

10.1.Initiating QHIN: C-CDA CCD

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	typeCode	34133-9, LOINC
DocumentEntry	formatCode	urn:hl7-org:sdwg:ccda-structuredBody:2.1
DocumentEntry	homeCommunityID	
DocumentEntry	mimeType	text/xml
Document Entry	objectType	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1
DocumentEntry	patientId	

10.2.Initiating QHIN: C-CDA Discharge Summary

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	typeCode	ValueSet DischargeSummaryDocumentTypeCode urn:oid:2.16.840.1.113883.11.20.4.1
DocumentEntry	formatCode	urn:hl7-org:sdwg:ccda-structuredBody:2.1
DocumentEntry	homeCommunityID	
DocumentEntry	mimeType	text/xml
Document Entry	objectType	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1

Level	Field	Value
DocumentEntry	patientId	

10.3.Initiating QHIN: C-CDA Progress Note

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	typeCode	ValueSet ProgressNoteDocumentTypeCode urn:oid:2.16.840.1.113883.11.20.8.1
DocumentEntry	formatCode	urn:hl7-org:sdwg:ccda-structuredBody:2.1
DocumentEntry	homeCommunityID	
DocumentEntry	mimeType	text/xml
Document Entry	objectType	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1
DocumentEntry	patientId	

10.4.Initiating QHIN: C-CDA Unstructured Document

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	typeCode	
DocumentEntry	formatCode	urn:hl7-org:sdwg:ccda-nonXMLBody:2.1
DocumentEntry	homeCommunityID	
DocumentEntry	mimeType	text/xml
Document Entry	objectType	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1
DocumentEntry	patientId	

10.5.Initiating QHIN: PDF

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	typeCode	
DocumentEntry	formatCode	
DocumentEntry	homeCommunityID	
DocumentEntry	mimeType	application/pdf
Document Entry	objectType	urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1

Level	Field	Value
DocumentEntry	patientId	

11. Document Types and Metadata Requirements for Responding QHINs

Responding QHINs are required to support at least one of the following document types for the Document Query Scenario:

1. C-CDA R2.1 CCD
2. C-CDA R2.1 Discharge Summary
3. C-CDA R2.1 Progress Note
4. C-CDA R2.1 Unstructured Document
5. PDF

We define the metadata values that are expected by the test tools in the sections below. In some cases, a specific metadata value will be required for a particular document type. In other cases, the metadata value need only be part of the value set for the metadata field.