ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

QHIN 1.1 Conformance Testing Process: Overview

Version History

Version	Description of Change	Version Date
1.1	Initial Publication (derived from 1.0 documentation)	March 18, 2024

1. QHIN Conformance Testing Process Overview

The scope of the Recognized Coordinating Entity's (RCE) Qualified Health Information Network (QHIN) Conformance Testing Process is limited to the QHIN Technical Framework (QTF) Version 1.1, the information outlined in the Common Agreement, and related QHIN Testing Process document(s).

Changes to the QHIN Conformance Testing Process documents may be made in accordance with updates to the QTF, which may be updated in accordance with changes to industry standards and specifications.

The QHIN Conformance Testing Process document(s) support the following:

- Candidate QHINs in the Conformance Testing Process;
- Designated QHINs who wish to test new technology or retest as a condition of continued participation in the Common Agreement; and
- Vendors who wish to have their product(s) validated as QHIN compliant. The QHIN Conformance Testing Process verifies that a System both complies with the QTF and has the ability to interoperate with other QHINs.

2. QHIN Testing Process Components

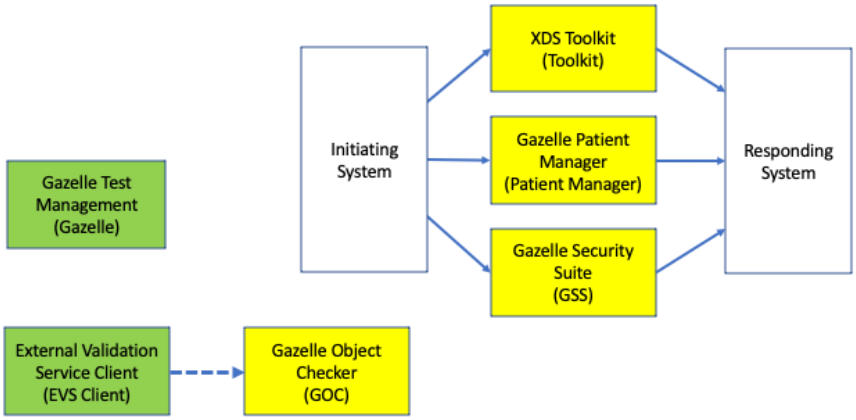
Candidate QHIN implementations will be tested using a set of tools, test data and procedures managed by the Sequoia Project. This document describes the test system components and includes the configuration items that are needed for testing. This document does not describe how to use the tools or run test cases. That information is found in the *QHIN 1.1 Conformance Testing Process 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 contained in the QTF. The software tools and testing procedures represent a "best effort" at reflecting those requirements 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 indicated in parenthesis. You will see both names in the documentation. 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 requirement(s). Examples of items that can be tested with this tool include C-CDA R2.1 documents and ATNA syslog messages.

3. Gazelle Object Checker (GOC): This is the most common Gazelle backend tool for validating different types of files or objects.
4. XDS Toolkit (Toolkit): This tool tests conformance to the XDS family of profiles, including 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 XCPD 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 TLS requirements.

2.2. General Testing Workflow

The Test Manager will configure the tooling to enable connectivity with your platform and provision your users.

Your organization will be required to provide first/last names, emails and phone contact information for each staff member/user who will need to be provisioned to access the tooling. Your users will see your organizational test lists and results, but they cannot see the results of other organizations.

Your staff members will work through the tests that are listed in this documented and described in more detail in *QHIN 1.1 Conformance Testing Process: Transport Test Cases* and QHIN 1.1 Conformance Testing Process: Security Test Cases. Some of the tests are designed to run in a specific order, but many tests can be run in any sequence. Consult with the Test Manager for guidance.

Candidate QHIN conformance 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

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

Conformance tests are grouped into four broad categories:

- Required Transport Tests: These are the set of tests your system will need to successfully execute to demonstrate conformance to the transport requirements in the QTF. There are required test patient data load requirements to complete these test cases.
- Required Security Tests: These required test cases validate conformance to the SOAP security, XML security, and SAML assertion element requirements. No specific preloading of data and/or associated document files are required.
- Conditional Tests: Individual tests are defined for discrete C-CDA R2.1 document types. QHINs will execute the appropriate test(s) depending on the types of C-CDA R2.1 documents they support in the Message Delivery Scenario and the Document Query Scenario.
- Optional Tests: The Conformance Testing Process includes optional tests that are intended to help diagnose issues and/or improve the robustness of QHIN functions. Examples are tests for behavior that is mentioned or allowed in the QTF or underlying standards but are not required by those same documents.

Test logs for the various types (Required Transport, Required Security, Conditional, and Optional) are segregated. This will allow you to run tests in one category (for example, Optional) without writing over the logs in another category (for example, Required).

3. Document Specific QTF Requirements and 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 document specific QTF requirements are mapped to test procedures. The QTF states these requirements concerning document content:

QTF-048	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-049	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-050	Responding QHINs SHOULD transmit any specific document format requests (provided by the Initiating QHIN via the IHE XDSDocumentEntryFormatCode XCA parameter) to Responding Sources.
QTF-051	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://carequality.org/wp-content/uploads/2022/04/Improve-C-CDA-Joint-Content-WG-v2.0-20220316-DISTRO.pdf
QTF-052	All C-CDA 2.1 format documents adhering to the Continuity of Care Document template MUST include all appropriate data classes and elements from the United States Core Data for Interoperability (USCDI) V1 when data are available. The RCE will update the QTF to enable the use of future versions of USCDI that are consistent with ONC rules for health IT certification compliance. The United States Core Data for Interoperability (USCDI) – available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

QTF-098	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://carequality.org/wp-content/uploads/2022/04/Improve-C-CDA-Joint-Content-WG-v2.0-20220316-DISTRO.pdf"
QTF-099	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-100	All C-CDA 2.1 format documents adhering to the Continuity of Care Document template MUST include all appropriate data classes and elements from USCDI V1 when data are available. The RCE will update the QTF to enable the use of future versions of USCDI that are consistent with ONC rules for health IT certification compliance. The United States Core Data for Interoperability (USCDI) – available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi
QTF-117	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-128	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-122.
QTF-123	A “Document Query Nominal Flow” of the test data per QTF-113 MUST return the C-CDA R2.1 document(s) associated with a test patient.

Based on prior experience with other testing programs supported by the Sequoia Project, 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

A QHIN that serves outpatient clinics and/or inpatient hospitals is required to test both Discharge Summary and Progress Note documents, per QTF-118. 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-118 (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.

- Transport tests for Document Query and Retrieve and Message Delivery 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 Progress 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 *QHIN 1.1 Conformance Testing Process 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 Gateway. You will be asked to send Patient Discovery Requests 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 Query and Retrieve Requests to one or more Responding Gateways. The Document Query Requests use the patient identity provided by the Responding Gateway. 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 use Message Delivery Requests to send documents to the Responding Gateway. 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 with a digital certificate issued by the RCE designed for the testing process. The Initiating 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 Patient Discovery tests using TLS connections that you initiate with the **Gazelle Patient Manger** and the **XDS Toolkit**.

3. You will complete the Document Query, Retrieve Documents, and Message Delivery 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 EVS Client**.

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.

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.
- 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:

- URLs for web user interfaces for all test tools.
- Web endpoints for all test services (both HTTPS and standard HTTP).
- List of test patients and medical histories to be used in testing. The test patients and medical histories are available with the test documentation.
- Value sets or related references for coded entries in XDS metadata, patient records and other records.

4.1. 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:

- *QHIN 1.1 Conformance Testing Process: Query Transport Test Cases*: Contains a section for each test case with instructions and expected results.
- *QHIN 1.1 Conformance Testing Process: 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 the two functions listed below. The testing process takes into consideration that an Initiating Gateway might submit one Patient Discovery request and cache the result for use in multiple Document Query and/or Document Retrieve requests.

1. Patient Discovery, 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***, 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. 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.
5. Your system produces the appropriate audit records. Individual test cases will have detailed instructions for submitting the audit records.

You will:

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

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 Document Query and Retrieve 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 Document 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 are not be repeated here.

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.

You will:

- Inform the Test Manager when you are ready for test assessment via email to qhintesting@sequoiaproject.org for the following:
    - Initiate one or more Document Query Requests with the XDS Toolkit.
        - Record the permanent link for all queries to share with the Test Manager via email to qhintesting@sequoiaproject.org.

- Initiate one or more Retrieve Document Requests with the XDS Toolkit.
  - Record the permanent link for all queries to share with the Test Manager via email to qhintesting@sequoiaproject.org.
- Email appropriate audit logs to qhintesting@sequoiaproject.org.

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. Message Delivery, including:
   a. Secure Channel
   b. Mutual Authentication
   c. User Authentication
   d. Authorization & Exchange Purpose
   e. Auditing

The Message Delivery Scenario does not use Patient Discovery and relies on the responding system to perform patient matching when any documents are received. 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 patient demographics for a defined patient. 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

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 but passing content testing is not required at this time.

Assessment for Message Delivery takes place in phases—some with automated conformance testing and the remainder with manual review by the Test Manager. You will submit your document or documents to the **XDS Toolkit** using XDS metadata as described in Section 8 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 qhintesting@sequoiaproject.org for the Test Manager for review.

4.2. 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. To pass the transport test cases, you will need to use the TLS endpoints 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, Document Query and Retrieve, and Message Delivery. Tests defined in *QHIN 1.1 Conformance Testing Process: 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 like the model used to test TLS connections. The same tools are used: **Gazelle Security Suite**, **Gazelle Patient Manager**, and **XDS Toolkit**.

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. To pass the transport test cases, the Test Manager will 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.

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 as defined in QTF 1.1 .

XCPD: The Responding Gateway responds to Patient Discovery Requests to identify a patient as known in your network. An Initiating Gateway tool 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** and **XDS Toolkit**. You will initiate transactions using the **Gazelle Patient Manager** and **XDS Toolkit** in a self-service manner to direct queries to your system under test. The tooling will indicate a pass or fail within the tooling. The Test Manager will use the **Gazelle Patient Manager** and **XDS Toolkit** 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 tool 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 tool. You will initiate Document Query and Retrieve Requests through the web user interface of the **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.

XCDR: The Responding Gateway is required to accept Message Delivery Requests 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 conformance 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 conformance to requirements when all testing is completed.

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 Patient Discovery tests using TLS connections that are initiated by the **Gazelle Patient Manger** and **XDS Toolkit**.
3. You will complete the Document Query, Retrieve Documents, and Message Delivery 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 EVS Client**.

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. You will be able to direct the **Patient Manager** and **XDS 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”. 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.
- List of IP addresses that will initiate and respond.
- Table of endpoints that indicates the URLs 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 Conformance Testing Process) 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 white list those systems if necessary.
- List of test patients and medical histories to be used in testing. The test patients and medical histories are available with the test documentation.
- 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:

- *QHIN 1.1 Conformance Testing Process: Query Transport Test Cases*: Contains a section for each test case with instructions and expected results.
- *QHIN 1.1 Conformance Testing Process: 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, 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***, you will be given demographic information for one patient you will load into your system. Using a self-service access, you will use the **Gazelle Patient Manager** or **XDS Toolkit** to send one or more Patient Discovery Requests to your Responding Gateway. Your Responding Gateway will accept and respond to SOAP transactions from the Gazelle Patient Manager based on requirements in QTF 1.1. In general,

1. Your Responding Gateway must support the TLS protocol using a version specified by the QTF.
2. Your Responding Gateway will perform mutual authentication with the **Gazelle Patient Manager** and **XDS Toolkit**.
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 via email to qhintesting@sequoiaproject.org.
- Use the **XDS Toolkit** to initiate Patient Discovery transactions with your Responding Gateway. The **XDS Toolkit** will record the results, and those will be available in your Toolkit testing session; there is no link to send to the Test Manager for the Toolkit tests.
- Email appropriate audit logs to the Test Manager via email to qhintesting@sequoiaproject.org.
- 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 Test Manager 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 outcome of the testing will be a comprehensive report detailing the individual assessments.

To test ***Document Query and Retrieve***, you will use the same test 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 Document 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 via email to qhintesting@sequoiaproject.org.
- Use the XDS Toolkit to initiate Retrieve Document 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 conformance review.

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. Message Delivery, including:
    a. Secure Channel
    b. Mutual Authentication
    c. User Authentication
    d. Authorization & Exchange Purpose
    e. Auditing

The Message Delivery Scenario does not use Patient Discovery and relies on the Responding Gateway to perform patient matching when it receives a document. 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***, the Test Tool will submit a document using defined demographics for one test patient. You will be required to demonstrate that your Responding Gateway can accept all the following document types from 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

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 exception (negative) cases. These exception cases are used to send transactions with flawed SAML assertions that should cause your system to reject the transaction.

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. 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 *QHIN Conformance Testing Process: 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 like 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. 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.

6. Comprehensive List of Tests

6.1. Initiating Gateway (IG) Tests

Identifier	Name	Type	Location
Patient Discovery Query			
Load Data as Initiating System	Load Patients Known by the Initiating Gateway	Required	Initialization
IG 1.1 Discover Patient 001	Initiating Gateway discovers patient QTFTEST-001	Required	Transport
IG 1.1 Discover Patient 002	Initiating Gateway discovers patient QTFTEST-002	Required	Transport
IG 1.1 Patient Discovery User Authentication	Initiating Gateway performs Patient Discovery with user authentication	Optional	Transport
IG 1.1 Patient Discovery Secured	Initiating Gateway performs Patient Discovery with all security provisions	Required	Transport
Document Query and Retrieve			
IG 1.1 Query Secured	Initiating Gateway queries with all security provisions	Required	Transport
IG 1.1 Query Stable Documents	Initiating Gateway DocumentEntry.objectType filter: Stable	Optional	Transport
IG 1.1 Query On-Demand Documents	Initiating Gateway DocumentEntry.objectType filter: On-Demand	Optional	Transport
IG 1.1 Query Availability Status Multiple	Initiating Gateway DocumentEntry.availabilityStatus filter: Multiple combinations	Optional	Transport
IG 1.1 Query Return Type	Initiating Gateway DocumentEntry.returnType filter: ObjectRef and LeafClass	Optional	Transport
IG 1.1 Retrieve Secured	Initiating Gateway retrieves document with all security provisions	Required	Transport
Message Delivery			
IG 1.1 Deliver Document T-TRTMNT	Initiating Gateway delivers one document with Exchange Purpose: Treatment	Required	Transport
IG 1.1 Deliver Document T-IAS	Initiating Gateway delivers one document with Exchange Purpose: Individual Access Services	Required	Transport

Notes:

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

6.2. Responding Gateway (RG) Tests

Identifier	Title	Type	Location
Patient Discovery Query			
1.1 Load Data as Responding System	Load Patients Known by the Responding Gateway	Required	Initialization
RG 1.1 Discover Patient 004 Secured	Gateway responds to Patient Discovery query for patient 004	Required	Transport

Identifier	Title	Type	Location
RG 1.1 Patient Discovery Exceptions	Responding Gateway supports Patient Discovery negative/exception tests	Required	Transport
RG 1.1 Patient Discovery Advanced	Gateway responds to advanced Patient Discovery queries	Optional	Transport
Document Query and Retrieve			
RG 1.1 Query Secured	Responding Gateway supports document query with all security provisions	Required	Transport
RG 1.1 Query Exceptions	Responding Gateway supports document query negative/exception tests	Required	Transport
RG 1.1 Query C-CDA 2.1 CCD	Responding Gateway supports Document Query for C-CDA R2.1 CCD	Conditional	Transport
RG 1.1 Query C-CDA 2.1 Discharge Summary	Responding Gateway supports Document Query for C-CDA R2.1 Discharge Summary	Conditional	Transport
RG 1.1 Query C-CDA 2.1 Progress Note	Responding Gateway supports Document Query for C-CDA R2.1 Progress Note	Conditional	Transport
RG 1.1 Query C-CDA 2.1 Unstructured Document	Responding Gateway supports Document Query for C-CDA R2.1 Unstructured Document	Conditional	Transport
RG 1.1 Optional Transactions	Gateway responds to optional transactions	Optional	Transport
RG 1.1 Retrieve Secured	Responding Gateway supports document retrieve with all security provisions	Required	Transport
RG 1.1 Retrieve C-CDA 2.1 CCD	Responding Gateway responds to retrieve request for C-CDA 2.1 CCD	Conditional	Transport
RG 1.1 Retrieve C-CDA 2.1 Discharge Summary	Responding Gateway responds to retrieve request for C-CDA 2.1 Discharge Summary	Conditional	Transport
RG 1.1 Retrieve C-CDA 2.1 Progress Note	Responding Gateway responds to retrieve request for C-CDA 2.1 Progress Note	Conditional	Transport
RG 1.1 Retrieve C-CDA 2.1 Unstructured Document	Responding Gateway responds to retrieve request for C-CDA 2.1 Unstructured Document	Conditional	Transport
Message Delivery			
RG 1.1 Accept Document Secured	Responding Gateway supports Message Delivery with all security provisions	Required	Transport
RG 1.1 Accept C-CDA 2.1 CCD	Accept C-CDA 2.1 CCD	Required	Transport
RG 1.1 Accept C-CDA 2.1 Discharge Summary	Accept C-CDA 2.1 Discharge Summary	Required	Transport
RG 1.1 Accept C-CDA 2.1 Progress Note	Accept C-CDA 2.1 Progress Note	Required	Transport
RG 1.1 Accept C-CDA 2.1 Unstructured Document	Accept C-CDA 2.1 Unstructured Document	Required	Transport
RG 1.1 Reject Metadata	Gateway rejects documents due to Metadata errors	Required	Transport
Security Test Cases			

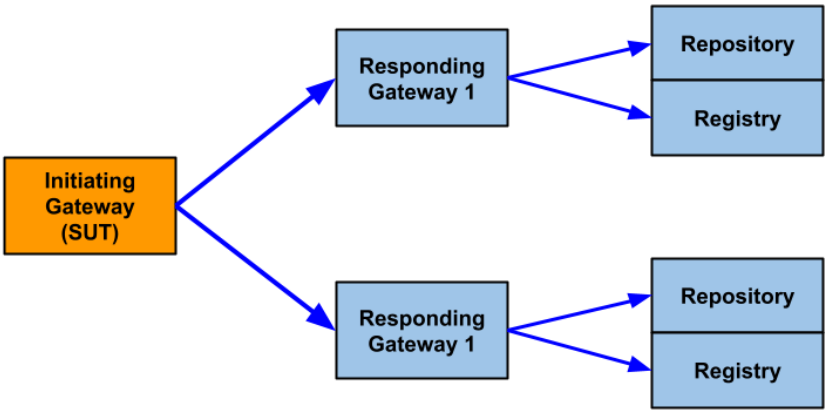
Identifier	Title	Type	Location
TC-MAPD-R-0003.000	Handle missing wsse:Security element	Required	Security
TC-MAPD-R-0003.201	Handle missing MessageID element	Required	Security
TC-MAPD-R-0003.301	Handle missing Assertion signature element	Required	Security
TC-MAPD-R-0003.302	Handle invalid Assertion signature	Required	Security
TC-MAPD-R-0003.326	Handle Missing KeyInfo in Assertion signature	Required	Security
TC-MAPD-R-0003.401	Handle missing Assertion element	Required	Security
TC:MAPD-R-0003.402	Handle an invalid Version in the Assertion	Required	Security
TC:MAPD-R-0003.403	Handle missing Version in Assertion element	Required	Security
TC:MAPD-R-0003.407	Handle invalid IssueInstant in Assertion element	Required	Security
TC:MAPD-R-0003.408	Handle IssueInstant much later than Message Timestamp	Required	Security
TC:MAPD-R-0003.409	Handle missing Issuer in Assertion element	Required	Security
TC-MAPD-R-0003.410	Handle Missing Issuer Format in Assertion	Required	Security
TC-MAPD-R-0003.411	Handle Invalid Issuer Email Name ID in Assertion	Required	Security
TC-MAPD-R-0003.412	Handle Invalid Issuer X.509 Name ID in Assertion	Required	Security
TC-MAPD-R-0003.413	Handle Invalid Issuer Windows Name ID in Assertion	Required	Security
TC-MAPD-R-0003.420	Handle Missing Subject element in Assertion	Required	Security
TC-MAPD-R-0003.421	Handle Missing Subject Name ID in Assertion	Required	Security
TC-MAPD-R-0003.422	Handle Invalid Subject Name ID in Assertion	Required	Security
TC-MAPD-R-0003.423	Handle Missing Subject Confirmation in Assertion	Required	Security
TC-MAPD-R-0003.424	Handle Missing Subject Confirmation Method in Assertion	Required	Security

7. 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.

8. 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 Manager / 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	Defined values for CCD, Discharge Summary and Progress Note.
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	Taken from the C-CDA LOINC code.
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.

9. Document Types and Metadata Requirements for Initiating QHINs

Initiating Gateways 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

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 values listed in the XDS Toolkit.

9.1. Initiating Gateway: C-CDA CCD

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	classCode	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	

9.2. Initiating Gateway: C-CDA Discharge Summary

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	classCode	18842-5, 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	

9.3. Initiating Gateway: C-CDA Progress Note

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	classCode	11506-3, 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	

9.4. Initiating Gateway: C-CDA Unstructured Document

Level	Field	Value
SubmissionSet	patientId	
SubmissionSet	sourceId	1.3.6.1.4.1.21367.4
DocumentEntry	classCode	
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	