CareQuality Integration

Netsmart

Contents

Information to Exchange

This document contains the information that 3rd Parties will need in order to perform testing. In addition, Netsmart will need the following information:

- 3rd Party SSL Certificate
  - If the cert was created by CareQuality, we can trust the CA
- 3rd Party Endpoints (Test and Production)
- 3rd Party OIDs

Netsmart Endpoints

These endpoints are necessary for finding a patient, finding documents for that patient, and retrieving those documents.

Netsmart Endpoints

- XCPD: https://labsdev.netsmartcloud.com/Inbound/XCPDRespondingGateway
- XCA Query: https://labsdev.netsmartcloud.com/Inbound/XCAGatewayQuery
- XCA Retrieve: https://labsdev.netsmartcloud.com/Inbound/XCAGatewayRetrieve

Client Certificate

Download Netsmart certificate (Used as both Client and Server certificate) - named "public.netsmartcloud.com "

- Navigate to https://demopaas.netsmartcloud.com
  - Click lock icon by URL
    - Click “Details” in Chrome, “More Information” in Firefox, Omit for IE
    - Click “View Certificate”
  - Navigate to Details tab
    - Click “Copy to File”
    - Click “Next”
    - Select Base-64 encoded X.509
    - Click “Next”
  - Browse to where you want to store the certificate
    - Name the certificate “public.netsmartcloud.com”
    - Click "Save"
    - Click “Next”
    - Click “Finish”

OIDs

Preferred testing involves 2 different OIDs to make sure connection is working properly.

Netsmart Test OIDs

- 2.16.840.1.113883.3.3569
- 2.16.840.1.113883.3.3569.1

Patient Information

Two test Patients must be used for each OID. In this case, 4 test patients must be generated. Either party may generate these test patients.

Encryption

Data is encrypted using TLS/SSL: + SAML Signature.

Implementation Guide

The latest implementation guide can be found at the bottom of this page, under Implementation Guides: http://sequoiaproject.org/carequality/resources/ Select 'Query-Based Document Exchange Implementation Guide.' We only respond to treatment based queries. We support consent both directions in the XCA query and follow the standards that are outlined in the CareQuality implementation guide.

XCA Version 2.1

Cross-Community Access Profiles support the means to query and retrieve patient data held by other communities. A community consists of facilities and enterprises working together under a common set of policies in order to share clinical information. Facilities and enterprises may be a member of multiple communities, which may be XDS Affinity Domains or other document sharing structures. Systems that are a member of an XDS Affinity Domain will be grouped with an individual domain inside of the Affinity Domain. This will allow the system to retrieve documents from each domain within the XDS Affinity Domain, as well as from other communities.

The following actions can be taken in order to mitigate risks.

- All parties will be grouped within an ATNA Secure Node and a CT Time Client.
- Document metadata shall include SHA1 hash of the document content and the ability to verify the SHA1 hash if corruption detection is requested.
- Overloading through excessive volume of response data shall be handled by discontinuing the read on the socket and closing it. The Gateways should respond by discontinuing the processing of responses.

- Queries should always supply a patient identifier or unique document entry identifier. Queries with unknown, improperly formatted, or no patient identifier shall return 0 documents with no further information or XDSUnknownPatientID. By not returning an error code, the ability of applications to fish for data is reduced.

Digitally sign all documents using the IHE DSG Profile in order to mitigate the risk of a document being maliciously changed. This mitigation is optional, and there are 3 ways to do it.

- An Enveloping Signature contains a signature block and the content that is signed. Remove the Enveloping – Digital Signature to access the contained content.
- A Detached Signature contains a manifest that points at independently managed content and leaves the document in its original form. This is the recommended method in Document Sharing infrastructures.
- A SubmissionSet Signature is a Detached Signature that contains a manifest of all documents in the set and a reference to the SubmissionSet.

The following mitigations are the responsibility of the vendors, XDS Affinity Domains, and enterprises.

- Backup systems for documents, metadata, and gateway configurations.
- Network protection services to guard against service attacks and data corruption on all interfaces.
- A process that reviews audit records and acts on inappropriate actions.

XCPD Version 2.1

The Cross Community Patient Discovery Profile supports the means to locate communities that hold patient relevant health data and the translation of patient identifiers across communities holding the same patient's data. A community is a group of facilities/enterprises that agree to work together under a common set of policies in order to share health information using any type of EHR. Each facility/enterprise may be a member of multiple communities, including XDS Affinity Domains using the XDS Profile, or any other internal sharing structure.

The following actions will be taken in order to mitigate risks.

- All parties will be grouped within an ATNA Secure Node and CT Time Client. As a result, all incoming and outgoing messages will be sent over a secure communication channel, including the asynchronous response messages.
- Implement network protection services to guard against service attacks and data corruption on all interfaces.
- Implement a process that reviews audit records and acts on inappropriate actions.

Date	Modification	Modified By
1/9/2017	Initial Draft	Kayla Rowton

For questions, e-mail CConnect@ntst.com