



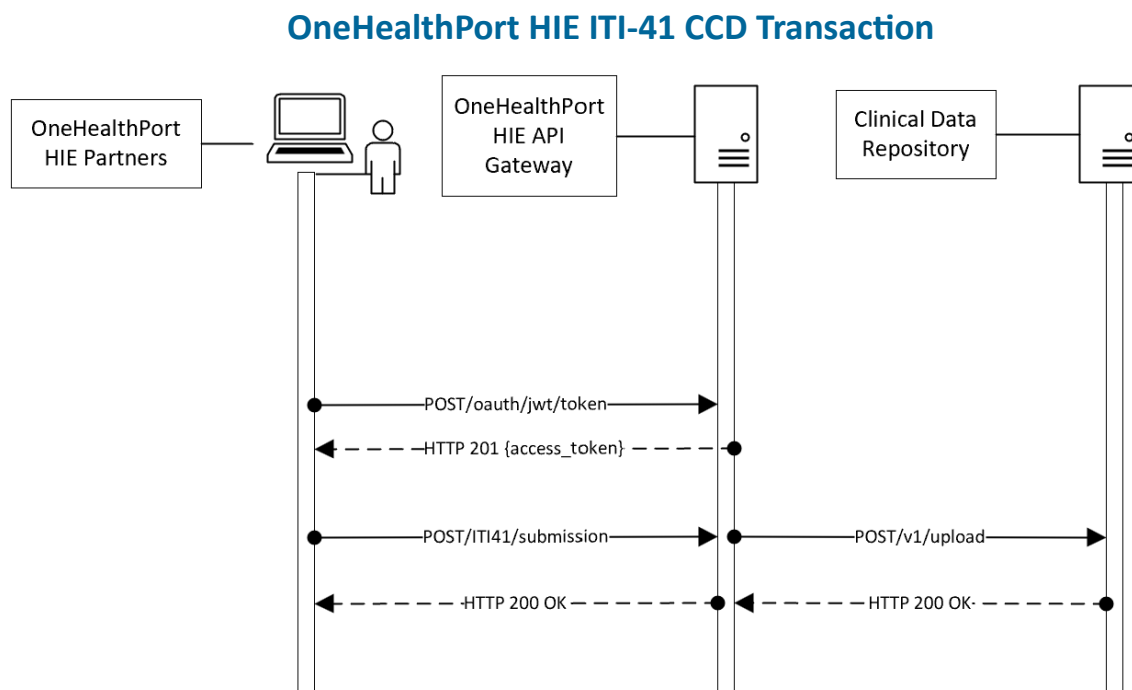
HIE API Connectivity for ITI-41 Continuity of Care Documents with the Washington Health Care Authority Clinical Data Repository

Purpose

This document presents the OneHealthPort HIE's API connectivity supporting the Washington Health Care Authority Clinical Data Repository (CDR) submission of Continuity of Care Documents (CCDs) from provider organizations in an ITI-41 format. It is intended for use by provider organization technical teams or their vendors responsible for setting up connectivity for this data transaction.

Connectivity - APIs over HTTPS

The diagram below provides an overview of the API connectivity and data submission flow for ITI-41 CCDs.



ITI-41 CCD Data Transaction Description:

1. OneHealthPort HIE onboarding team provides an OAuth 2.0 JWT token to submitting organization. OAuth 2.0 JWT tokens are valid for 6 months.
2. Submitting organization uses the OAuth 2.0 JWT token (to be included in the request header) to call the authorization endpoint and receives an access token upon successful authentication.
3. When the authorization endpoint is called, OneHealthPort HIE API Gateway performs verification of the OAuth 2.0 JWT token at the API Gateway. Upon verification, a unique access token is generated by the API Gateway and is valid for 3600 seconds (1 hour).
4. The partner calls the data submission API with the access token included in the request header.
5. The OneHealthPort HIE partner or their vendor will be required to include a file name or identifier for tracking the clinical documents data transaction through its lifecycle. Please see HTTPS header requirements below.
6. OneHealthPort HIE API Gateway verifies access token and forwards the message to CDR.
7. The OneHealthPort HIE returns a synchronous HTTP response to the submitting system.

Getting Connected to the OneHealthPort HIE API Gateway

Step 1 – Request OAuth 2.0 JWT token

OneHealthPort HIE provides OAuth 2.0 JWT token to the partner or their vendor via secure mail.

Different OAuth 2.0 JWT tokens will be provided for each OneHealthPort technical environment – UAT and Production.

To request a OAuth 2.0 JWT token, submit a OneHealthPort HIE Support Request [form](#).

- In the section of the form called, *Issue or Question area*, select the option called **HIE connectivity set-up**.
- In the section of the form called, *Detail description of issue or question being reported*, please request an OAuth 2.0 JWT token for ITI-41 API connectivity set up.

When the support request is received, the OneHealthPort HIE team will set up the vendor or partner at the API gateway for authentication and send the OAuth 2.0 JWT token to the vendor or partner via secure mail.

Step 2 – Set up APIs to retrieve access token and submit clinical documents

OneHealthPort HIE API Endpoints

OneHealthPort HIE vendor or partner will use the endpoints in the table below to retrieve access tokens and submit clinical documents.

Endpoint Description	Endpoint
Authorization API User Acceptance Testing (UAT) – used with OAuth 2.0 JWT to receive access token.	https://uat-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token
ITI-41 Format CCD API UAT – used with unique access token to post ITI-41 CCD submission to the CDR.	https://uat-v2-onehealthport-api.axwaycloud.com/web/service/ITI41NS
Authorization API Production – used with OAuth 2.0 JWT to receive access token.	https://prd-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token
ITI-41 Format CCD API Production – used with unique access token to post ITI-41 CCD submission to the CDR.	https://prd-v2-onehealthport-api.axwaycloud.com/web/service/ITI41NS

- OneHealthPort HIE onboarding team sets up partner or their vendor for authentication at the API gateway.
- Partner or their vendor calls the authorization endpoint with the OAuth 2.0 JWT token and upon authorization, retrieves a unique access token.
- Partner or their vendor will use the following HTTPS header along with the unique access token to call the API and post ITI-41 CCD submissions to the API gateway. Listed below are the header requirements.

Clinical Documents	
HTTPS Header	Definition
x-doc-type	OneHealthPort HIE document type: • ITI41
x-org-facility-id	OneHealthPort HIE organization identifier provided by the CDR onboarding team.
x-ref-id	Note – The reference identifier can be a file name or identifier that can be used by partner or vendor to manage message through its life cycle.

HTTPS Header Example for ITI-41 CCD Messages

Retrieve access token from OneHealthPort API gateway to use in the ITI-41 CCD message submission

POST /ohp/oauth/jwt/token HTTP/1.1
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 632
Host: uat-v2-onehealthport-api.axwaycloud.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.5.6 (Java/1.8.0_222)

grant_type=urn:ietf:params:oauth:grant-type:jwt-bearer&assertion=eyJhbGciOiJIUzUxMiIsImtpZCI6ImU3NGYzNmMzNjU2ZTRhMGFhM2RmYmQ3OTYzZDE4MGEzliwidHlwIjoiaSldUIn0.eyJzdWJfb3JnX25hbWUiOiJPSFAGUmvc2VydmJjZW9wZXJhdGlvbnMvandrcylsImhhdCI6MTY1MjczMjQzMjwibmJmljoxNjUyNzA2MTIwfwQ

OneHealthPort API Gateway response to retrieval of access token

HTTP/1.1 201 Created
Max-Forwards: 20
Via: 1.0 axwc-api-11-v2 ()
Connection: close
X-CorrelationID: Id-b3408562ee7d3edc9a71760d 0
Date: Wed, 18 May 2022 18:53:40 GMT
Request-Context: appld=cid-v1:2fb10c65-a180-4921-8c35-c497fb775c0c
X-Azure-Ref:
0tECFYgAAAAD2O3mXTAjVQrifN9mTvwAzQVRMMzMxMDAwMTEwMDM3ADIXYTBhMzIxLTc5ZmEtNDQ3OS1iYTEwLWY1ZGFIZTVjMjx0x0
X-Cache: CONFIG_NOCACHE
X-Powered-By: ASP.NET
Content-Type: application/json

```
{
  "access_token":
  "d2932b2e1eb740c19885e35ff42e80c692251194b35b4e7895f0a36630c71cc6",
  "token_type": "Bearer",
  "expires_in": "3600"
}
```

This is an example of an access token that will be used in the Authorization HTTP header of the ITI-41 CCD message POST.

HTTP status code for access token retrieval: If you do not use a valid OAuth 2.0 JWT token to retrieve the access token you will receive a **401 Unauthorized** response. Please follow the instructions below to receive a valid OAuth 2.0 JWT token from the OneHealthPort HIE.

- Submit a OneHealthPort HIE Support Request [form](#).
- In the section of the form called, *Issue or Question area*, select the option called **HIE connectivity set-up**.
- In the section of the form called, *Detail description of issue or question being reported*, please request a new OAuth 2.0 JWT token for ITI-41 connectivity set up.

When the support request is received, the OneHealthPort HIE team will send the new OAuth 2.0 JWT token to the vendor or partner via secure mail.

POST submission of a clinical document message

POST /webservice/ClinicalDocuments HTTP/1.1

Authorization: **Bearer** b84d5e02c1604a98ba1730307a43e9434a5f9ef50d8df2cbxoxo

x-ref-id: ac53cc6b-a341-6ef7ec80xoxo

x-doc-type: ITI41

x-org-facility-id: 7uyco22

Content-Type: **application/xml**

Content-Length: 2043

Host: uat-v2-onehealthport-api.axwaycloud.com

Connection: Keep-Alive

User-Agent: Apache-HttpClient/4.5.6 (Java/1.8.0_222)

Accept-Encoding: gzip,deflate

The HTTP headers highlighted in blue in the example are required for the ITI-41 CCD message POST.

Note, in Content-Type indicate application/xml.

<ClinicalDocument xmlns="urn:hl7-org:v3"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<realmCode code="US"/>

<typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040"/>

<templateId root="2.16.840.1.113883.10.20.22.1.1"/>

<templateId root="2.16.840.1.113883.10.20.22.1.2"/>

<id root="9a01933e-ff94-4088-a124-c4240d35eaa5"/>

<code code="34133-9" displayName="API2: PDQ-no-match"

codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC"/>

<title>API2: PDQ-no-match</title>

<effectiveTime value="202306261110-0700"/>

```

        <confidentialityCode code="N" displayName="Normal"
codeSystem="2.16.840.1.113883.5.25" codeSystemName="Confidentiality Code"/>
        <languageCode code="en-US"/>
        <recordTarget>
            <patientRole>
                <!-- OHP Organization Test OID -->
                <id root="1.3.6.1.4.1.38630.2.1.1.117" extension="XXX"/>
            </patientRole>
        </recordTarget>
        <author></author>
        <custodian></custodian>
        <documentationOf></documentationOf>
        <component></component>
    </ClinicalDocument>

```

HTTP status code for access token expiration: If you do not use the retrieved access token in the clinical document submission before it expires (access tokens expire in 3600 seconds), you will receive a **401 Unauthorized** response. You will then need to repeat the process to retrieve a new access token and resubmit the NBS message.

Step 3 – Receiving synchronous responses

Responses are returned ***synchronously***, *meaning they are returned in the same connectivity thread opened during the submission.*

HTTP Status Codes: Responses are returned for each ITI-41 submission.

HTTP Responses

HTTP response codes shown below are sent back by the OneHealthPort HIE API gateway.

HTTP Response Code	Definition
200	OK
201	Created - OneHealthPort HIE API Gateway successful response for retrieval of access token.
401	Unauthorized

	Action: Verify that the correct OAuth 2.0 JWT token is being used correctly to obtain access token. If not, submit a OneHealthPort HIE Support Request form to request a new OAuth 2.0 JWT token. If the 401 is related to the access token in the ITI-41 CCD submission, the access token may be expired or compromised. Please retrieve a new access token and resubmit.
403	Forbidden - The OAuth 2.0 JWT token is not configured for the document type included in the submission. Action for vendor or partner when receiving a 403 response: Submit a OneHealthPort HIE Support Request form. In the section of the form called, <i>Issue or Question area</i>, select the option called HIE connectivity set-up. In the section of the form called, <i>Detail description of issue or question being reported</i>, please indicate you have received a 403 forbidden error and provide the content of the error message.
500	Internal Server Error Action: Resubmit messages that receive this response.
503	Service Unavailable. This response is sent from the OneHealthPort HIE gateway when the OneHealthPort CDR is offline for maintenance. Action: The submitter needs to hold submissions until notified systems are online and operational.
504	Timeout generated by the CDR if processing is delayed. Action: Resubmit messages that receive this response.
514	Unknown Patient Id specified in request. Action: Confirm patient meets criteria for CDR submission and resubmit the message if necessary.
515	Unknown Source Id provided in the request. Action: Confirm organization identifiers are correct and resubmit the message.

Synchronous 200 accepted response from CDR that ITI-41 CCD message was accepted

HTTP/1.1 200 OK
Max-Forwards: 20
Via: 1.0 axwc-api-11-v2 ()
Connection: close
X-CorrelationID: Id-0ad5996464e09dda4e9e98bb 0
Date: Mon, 26 Jun 2023 18:12:53 GMT
Request-Context: appld=cid-v1:b3be8b11-080a-45c0-ac14-22974d73c03f
x-doc-type: ITI41
x-org-facility-id: 7uycso22
x-ref-id: b0890c54-ed59-4b0a-8442-32fa8a002752
X-TRACKEDOBJECT-IDENTITY: 1
X-TRACKEDOBJECT-NAME: API_Sentinel
X-TRACKING-CYCLEID: Id-0ad5996464e09dda4e9e98bb
Content-Type: application/xml

```
<RegistryResponse>  
  <RegistryResult>  
    <Message>Success</Message>  
  </RegistryResult>  
</RegistryResponse>
```

Revocation of OAuth 2.0 JWT Token

If a OneHealthPort HIE partner's OAuth 2.0 JWT token becomes compromised, **immediately notify** the OneHealthPort HIE so the token can be revoked (rendered invalid) and a new one can be issued. Follow the process below for notification and to obtain a new OAuth 2.0 JWT token.

Notification Process for Compromised and Request for New OAuth 2.0 JWT Token

- Submit a OneHealthPort HIE Support Request [form](#).
- In the section of the form called, *Issue or Question area*, select the option called **HIE connectivity set-up**.
- In the section of the form called, *Detail description of issue or question being reported*, please indicate your OAuth 2.0 JWT token has been compromised and you would like the OneHealthPort team to provide a new OAuth 2.0 JWT token for ITI-41 CCD data submission.

Operations

The API connectivity at the OneHealthPort HIE API gateway will involve the following for operational consideration and management.

- OneHealthPort HIE systems are online and operational for ITI-41 CCD submissions unless the CDR is down for scheduled maintenance or systems are down for emergency maintenance.
- Partners will be responsible for reprocessing any messages that do not receive an acknowledgement or successful HTTP response code 200.
- Maintenance schedules are posted on the OneHealthPort HIE [home page](#) under Maintenance Schedule.