

HIE API Connectivity for Electronic Laboratory Reporting Submissions to the Washington Department of Health

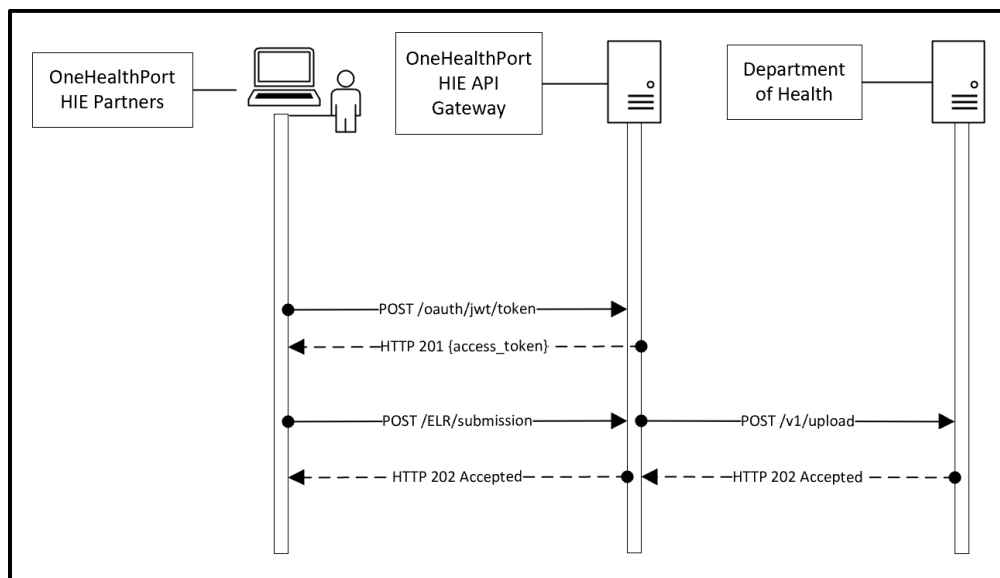
Purpose

This document presents the OneHealthPort HIE's API connectivity that supports the Electronic Laboratory Reporting (ELR) data submissions to the Washington Department of Health (DOH). It is intended for use by provider organization technical teams or their vendors responsible for setting up connectivity for these data submissions.

Connectivity - APIs over HTTPS

The diagram below provides an overview of the API connectivity and data submission flow for ELR data submissions.

OneHealthPort HIE ELR Data Submissions



ELR Data Submission 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 an ELR data submission through its lifecycle. Please see HTTPS header requirements below.
6. OneHealthPort HIE API Gateway verifies access token and forwards the message to DOH.
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 ELR 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 ELR data

OneHealthPort HIE API Endpoints

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

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
ELR API UAT – used with unique access token to post ELR message for data submission to DOH.	https://uat-v2-onehealthport-api.axwaycloud.com/doh/phchub/PHC-Hub/elr
Authorization API Production – used with OAuth 2.0 JWT to receive access token.	https://prd-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token
ELR API Production – used with unique access token to post ELR message for data submission to DOH.	https://prd-v2-onehealthport-api.axwaycloud.com/doh/phchub/PHC-Hub/elr

- 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 ELR data submissions to the API gateway. Listed below are the header requirements.

HTTPS Header for ELR	Definition
x-doc-type	OneHealthPort HIE document type: <ul style="list-style-type: none"> • ELR
x-org-facility-id	OneHealthPort HIE organization identifier provided by the HIE 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. The file name or identifier used is limited to 61 characters.

Important note: Use of the HTTPS header does not change the structure of the MSH or the content of the HL7 2.5.1 ELR messages per specifications set forth by the Washington Department of Health. API submissions also do not require any special encoding such as Base64.

HTTPS Header Example for ELR Messages

Retrieve access token from OneHealthPort API gateway to use in the ELR 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=eyJhbGciOiJIUzU1IiwiaXNjaW50IjoiPSFAgUmVncmVzc2lubiAmIFRlc3QgQ2xpbmljIDEiL
4MGEzliwidHlwjoiSldUIn0.eyJzdWJfb3JnX25hbWU0IjoiPSFAgUmVncmVzc2lubiAmIFRlc3QgQ2xpbmljIDEiL
CjZdWliOiI3dXlhc280MSlmp0aSI6ImYyNWRLMzI2YWFKODRmMjNiZjllMwZmNmU5MTIxMTA1liwiZXhwij
oxNjY4NjAzNzlwLCJpc3MiOiJodHRwczovL3VhdC1hcGkub25laGVhbHRocG9ydC5jb20vc2VydmljZW9wZXI
hdGlbnMvMvandrvcylslmhdCI6MTY1MjczMTQzMywibmJmljoxNjUyNzA2MTIwIj0.eyJhbGciOiJIUzU1IiwiaXNjaW50IjoiPSFAgUmVncmVzc2lubiAmIFRlc3QgQ2xpbmljIDEiL
H6SUPisuAcIFN3coHmWANhGxS-or29taEbg3WY0TyjLzbWFXIR3IXIkKwCMbCE5hg6EhAJI-
urPoIP_fNyv9qMUMHZ3_hHtcs47el4ewTyzNCgsna0O1xvAq2CHuFr3ujw2pXBicumjyoY4ehHjx0x0

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: appId=cid-v1:2fb10c65-a180-4921-8c35-c497fb775c0c
X-Azure-Ref:
0tECFYgAAAAD2O3mXTAjVQrifN9mTvwAzQVRMMzMxMDAwMTEwMDM3ADIXYTBhMzIxLTc5ZmEtNDQ
3OS1iYTEXLWY1ZGFIZTVjMjx0x0
X-Cache: CONFIG_NOCACHE
X-Powered-By: ASP.NET
Content-Type: application/json

This is an example of an
access token that will be used
in the Authorization HTTP
header of the ELR message

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

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 ELR 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 an ELR message

POST /doh/phchub/PHC-Hub/elr HTTP/1.1

Authorization: Bearer b84d5e02c1604a98ba173030153918bb2d807a43e9434a5f9ef50d8df2cbxoxo

x-ref-id: ac53cc6b-7ddd-47cc-a341-6ef7ec80xoxo

x-doc-type: ELR

x-org-facility-id: 7uycso22

Content-Type: application/json

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 ELR message POST.

Note, in Content-Type indicate application/json only

```
{ "body": "MSH|^~\&#|NIST^2.16.840.1.113883.3.72.5.20^ISO|NIST^2.16.840.1.113883.3.72.5.21^ISO|WADOHPHRED^2.16.840.1.113883.3.237.4.2^ISO|dn1fro00^1.3.6.1.4.1.38630.2.1.1.19^ISO|20120821140551-0500||ORU^R01^ORU_R01|OHP_TEST_11111|T|2.5.1|||NE|NE|||PHLabReport-NoAck^HL7^2.16.840.1.113883.9.11^ISO|vSFT|NIST Lab, Inc.^L^NIST&2.16.840.1.113883.3.987.1&ISO^XX^123544|3.6.23|A-1 Lab System|6742873-12||20100617^PID|1||PATID99999^2.16.840.1.113883.3.72.5.24^ISO^MR^Any Cnty Hlth C&2.16.840.1.113883.3.0&ISO||LastName^FirstName^X^L||99999999|M||9999-9^Pink^CDCREC|101 Any Road^AnyCity^XX^99999^USA^H|^APRN^PH^A1^407^2351234|||N^Not Hispanic or Latino^HL79999^NL^not latino^L^2.5.1^rORC|RE|ORD999999-9^2.16.840.1.113883.3.72.5.24^ISO|R-783274-4^LIS^2.16.840.1.113883.3.72.5.25^ISO|||57422^LastName^Any Doctor^A^Dr.^A^NPI&2.16.840.1.999999.4.6&ISO^L^A^NPI|^APRN^PH^A407^2341212|||Any County Health Clinic|999 Any Ave^AnyCity^XX^33333^AB|^WPN^PH^A813^8847284|999 Any Ave^AnyCity^XX^33333^AB^rOBR|1|ORD999999-9^2.16.840.1.113883.3.72.5.24^ISO|R-783274-4^LIS^2.16.840.1.113883.3.72.5.25^ISO|625-4^Bacteria identified in Stool by Culture^LN^3456543^CULTURE STOOL^99USI^2.40||20110528|||57422^LastName^Any Doctor^A^Dr.^A^NPI&2.16.840.1.999999.4.6&ISO^L^A^NPI|^APRN^PH^A407^2341212|||201106010900-0500|||F^rOBX|1|CWE|625-4^Bacteria identified in Stool by Culture^LN^Bacteria identified^99USI^2.40||3092008^Staphylococcus aureus (organism)^SCT^SAUR^Staphylococcus aureus^LAS aureus|||F||20110528|||20110531130655-0500|||Any County Health Department Laboratory^A^2.16.840.1.113883.3.72.5.30.1&ISO^XX^987|6756 Any Avenue^AnyCity^XX^33333^AB|10092^LastName^AnyName^A^2.16.840.1.113883.3.72.5.30.1&ISO^L^A^NPI^rSPM|1|^ORD999999-9&&2.16.840.1.113883.3.72.5.24^ISO||119339001^Stool specimen^SCT^A^07/31/2012|||20110528|20110529"} }
```

HTTP status code for access token expiration: If you do not use the retrieved access token in the ELR 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 ELR 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 ELR submission.

HTTP Statuses:

- 201 Created (access token retrieved successfully)
- 202 Accepted (submission has been accepted by DOH)
- 400 Bad Request (submission rejected for conformance reasons)
- 403 Forbidden (user has not been permitted by OneHealthPort HIE to submit a ELR message)
 - Action item for vendor or partner when receiving a 403 response:
 - 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 you have received a 403 forbidden error and provide the content of the error message.
- 500 Internal Server (resubmit the failed message)
- 503 Service Unavailable (resubmit the failed message when DOH systems available)
- 504 Timeout (resubmit the failed message)

Synchronous 202 accepted response from DOH system that ELR file was accepted

HTTP/1.1 202 Accepted
Max-Forwards: 20
Via: 1.0 axwc-api-11-v2 ()
Connection: close
X-CorrelationID: Id-3e3d8562bb7cec010ea56496 0
Date: Wed, 18 May 2022 18:38:54 GMT
Request-Context: appld=
x-doc-type: ELR
x-org-facility-id: 7uycso22
x-ref-id: ac53cc6b-7ddd-47cc-a341-6ef7ec80xoxo
X-TRACKEDOBJECT-IDENTITY: 1
X-TRACKEDOBJECT-NAME: API_Sentinel
X-TRACKING-CYCLEID: Id-3e3d8562bb7cec010ea56496
Content-Type: text/plain; charset=utf-8

Submitted item has been received. **x-ref-id:** ac53cc6b-7ddd-47cc-a341-6ef7ec80xoxo

HTTP Responses

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

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

202	Accepted - DOH successful message submission response passed back by the API gateway.
400	<p>Bad Request</p> <p>Action: Review response for additional detail for conformance errors. Make corrections and resubmit.</p> <p>Typical conformance errors occur because special characters are not properly escaped and fail JSON body formatting conformance requirements. Please verify payload special characters are properly escaped before submission.</p>
401	<p>Unauthorized</p> <p>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.</p> <p>If the 401 is related to the access token in the ELR submission, the access token may be expired or compromised. Please retrieve a new access token and resubmit.</p>
403	<p>Forbidden</p> <p>The OAuth 2.0 JWT token is not configured for the document type included in the submission.</p> <p>Action for vendor or partner when receiving a 403 response:</p> <p>Submit a OneHealthPort HIE Support Request form.</p> <p>In the section of the form called, <i>Issue or Question area</i>, select the option called HIE connectivity set-up.</p> <p>In the section of the form called, <i>Detail description of issue or question being reported</i>, please indicate you have received a 403</p>

	forbidden error and provide the content of the error message.
415	<p>Unsupported media type</p> <p>Action for vendor or partner when receiving a 415 response:</p> <p>The 415 error could occur for the following reasons:</p> <ul style="list-style-type: none"> • The payload format is not in a supported format. • The content-type is incorrect. • The content encoding is incorrect.
500	<p>Internal Server Error</p> <p>Action: Resubmit messages that receive this response.</p>
503	<p>Service Unavailable. This response is sent from the OneHealthPort HIE gateway when the OneHealthPort or DOH systems are taken offline for maintenance.</p> <p>Action: The submitter needs to hold submissions until notified systems are online and operational.</p>
504	<p>Timeout generated by the DOH system if processing is delayed.</p> <p>Action: Resubmit messages that received this response.</p>

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 ELR 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 ELR data submissions unless DOH takes down their systems 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 202.
- Maintenance schedules are posted on the OneHealthPort HIE [web page](#) under Maintenance Schedule.