HIE API Connectivity for Syndromic Surveillance Submissions to the Washington Department of Health

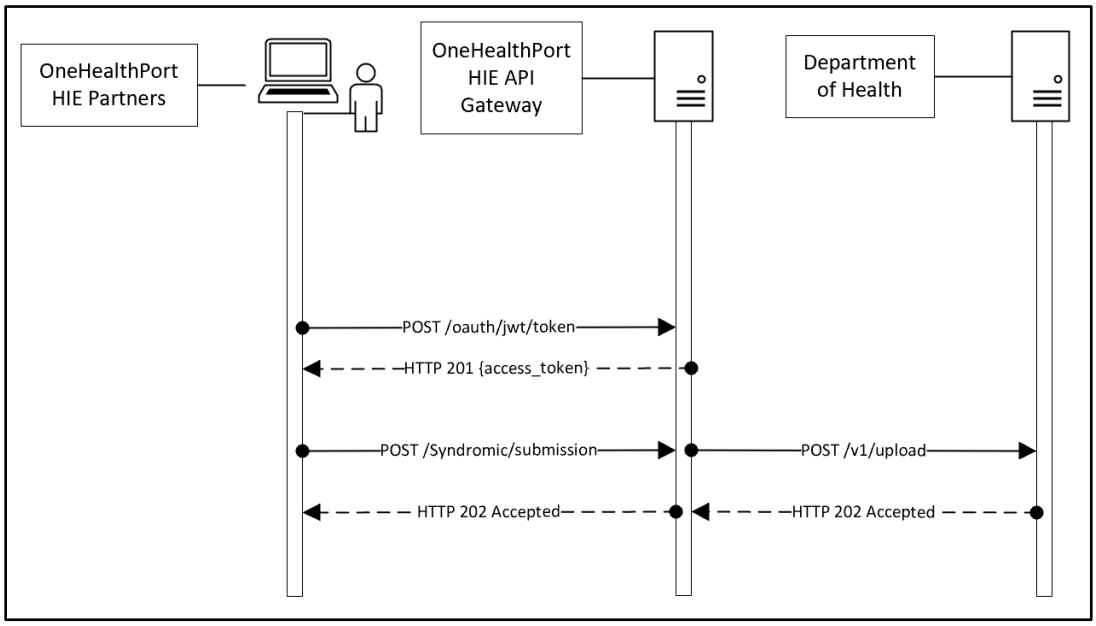
Purpose

This document presents the OneHealthPort HIE's API connectivity that supports the Syndromic Surveillance 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.

HIE Connectivity - APIs over HTTPS

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

OneHealthPort HIE Syndromic Surveillance Data Submissions



Syndromic Surveillance 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 a Syndromic Surveillance 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 Syndromic Surveillance 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 Syndromic Surveillance data

OneHealthPort HIE API Endpoints

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

Endpoint Description	Endpoint
Authorization API User Acceptance Testing (UAT) – used with OAuth 2.0 JWT token to receive access token.	https://uat-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token
Syndromic Surveillance API UAT – used with unique access token to post Syndromic Surveillance message for data submission to DOH.	https://uat-v2-onehealthport-api.axwaycloud.com/doh/phchub/PHC-Hub/ss
Authorization API Production – used with OAuth 2.0 JWT token to receive access token.	https://prd-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token
Syndromic Surveillance API Production – used with unique access token to post Syndromic Surveillance message for data submission to DOH.	https://prd-v2-onehealthport-api.axwaycloud.com/doh/phchub/PHC-Hub/ss

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

HTTPS Header for Syndromic Surveillance	Definition
x-doc-type	OneHealthPort HIE document type: • Syndromic
x-org-facility-id	OneHealthPort HIE organization identifier provide 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.

Important note: Use of the HTTPs header does not change the structure of the MSH or the content of the HL7 2.5.1 Syndromic Surveillance 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 Syndromic Surveillance Messages

Retrieve access token from OneHealthPort API gateway to use in the Syndromic Surveillance 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=eyJhbGciOiJFUzUxMiIsImtpZCI6ImU3NGYzNmMzNjU2ZTRhMGFhM2RmYmQ3OTYzZDE4MGEzIiwidHlwIjoiSldUIn0.eyJzdWJfb3JnX25hbWUiOiJPSFAgUmVncmVzc2lvbiAmIFRlc3QgQ2xpbmljIDEiLCJzdWIiOiI3dXljc280MSIsImp0aSI6ImYyNWRlMzI2YWFkODRmMjNiZjllMWZmNmU5MTIxMTA1IiwiZXhwIjoxNjY4NjAzNzIwLCJpc3MiOiJodHRwczovL3VhdC1hcGkub25laGVhbHRocG9ydC5jb20vc2VydmljZW9wZXJhdGlvbnMvandrcyIsImlhdCI6MTY1MjczMTQzMywibmJmIjoxNjUyNzA2MTIwfQ.AeLSsgN4xt823yAmUwlkH6SUPisuAcIFN3coHmWANhGxS-oR29taEbg3WY0TyjLzbWFXlR3lXlkKwcMbCE5hg6EhAJl-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: 0tECFYgAAAAD2O3mXTAjVQrifN9mTvwAzQVRMMzMxMDAwMTEwMDM3ADIxYTBhMzIxLTc5ZmEtNDQ3OS1iYTExLWY1ZGFiZTVjMjx0x0
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 Syndromic

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

HTTP status code for 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 Syndromic Surveillance 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 Syndromic Surveillance message

POST /doh/phchub/PHC-Hub/ss HTTP/1.1
Authorization: **Bearer** 30b23804090844ec90b6ae7bb2ceacd6a3c4b082e61f4b1d8d4a75b43b52xoxo
x-ref-id: 23uilh2iul3klj23h1lkxoxo
x-doc-type: Syndromic
x-org-facility-id: 7uycso22
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.0
Accept: */*
Cache-Control: no-cache
Postman-Token: 230f1c1c-2889-4ff2-b962-3d53795f295e
Host: uat-v2-onehealthport-api.axwaycloud.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 5581

The HTTP headers highlighted in blue in the example are required for the Syndromic Surveillance message POST.

Note, in Content-Type indicate application/json only

{
"body":"MSH|^~\\&#|SyS|SyndromicSurveillance^2.16.840.1.113883.3.4272.14.1^ISO|WADOHPHEEDS^2.16.840.1.113883.3.237.4.6^ISO|dn1fro00|20220924083537||ADT^A08^ADT_A01|3299342|T|2.5.1|||||||PH_SS-NoAck^SS Sender^2.16.840.1.114222.4.10.3^ISO\rEVN||20220924083537|||||facility name^2.16.840.1.113883.3.4272.14.1^ISO\rPID|1||E1901468691^^^^MR||First^Last^^^^^L||19580212|F||2028-9^Asian^CDCREC|^^VANCOUVER^53^98682^USA^^^53011||||||||||2186-5^Not Hispanic of Latino^CDCREC|||||||||\rPV1|1|O|||||||||||||||||540239400^^^^VN|||||||||||||||||||||||||20220924081347|||||||||\rPV2|||^fever^|||||||||||||||||||||||||||||||||||||||||||||\rOBX|1|CWE|8661-1^CHIEF COMPLAINT:FIND:PT:PATIENT:NOM:REPORTED^LN|1|^^^^^^^^REFERRAL||||||F|||||||||||||\rOBX|2|NM|21612-7^AGE TIME PATIENT REPORTED^LN|2|57|a^YEAR^UCUM|||||F|||||||||||||\rOBX|3|CWE|SS003^FACILITY/VISIT TYPE^PHINQUESTION|3|261QP2300X^PRIMARY CARE^NUCC|||||F|||||||||||||\rOBX|4|TX|44833-2^DIAGNOSIS.PRELIMINARY:IMP:PT:PATIENT:NOM^LN|4|Dark mole on R leg calf ||||||F|||||||||||||\rOBX|5|XAD|SS002^TREATING FACILITY LOCATION^PHINQUESTION|5|12345 NE Washington AVE^^VANCOUVER^53^98686-1448^|||||F|||||||||||||\rDG1|1||70909^OTHER DYSCHROMIA^I9CDX|||F\rDG1|2||2169^BENIGN NEOPLASM OF SKIN SITE UNSPECIFIED^I9CDX|||F\rDG1|3||V0481^NEED PROPHYLACTIC VACCINATION\\T\\INOCULATION FLU^I9CDX|||F"
}

HTTP status code for access token expiration: If you do not use the retrieved access token in the Syndromic Surveillance 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 Syndromic Surveillance 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 Syndromic Surveillance 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 Syndromic Surveillance 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 Syndromic Surveillance file was accepted

HTTP/1.1 202 Accepted
Max-Forwards: 20
Via: 1.0 axwc-api-21-v2 ()
Connection: close
X-CorrelationID: Id-3584846251548294983 2x0x0 0
Date: Wed, 18 May 2022 05:29:26 GMT
Request-Context: appId=
x-doc-type: Syndromic
x-org-facility-id: 7uycso22
x-ref-id: 23uilh2iul3klj23h1lkxoxo
X-TRACKEDOBJECT-IDENTITY: 1
X-TRACKEDOBJECT-NAME: API_Sentinel
X-TRACKING_CYCLED: Id-3584846251548294983 2x0x0
Content-Type: text/plain; charset=utf-8

Submitted item has been received. x-ref-id:23uilh2iul3klj23h1lkxoxo

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	Bad Request **Action:** Review response for additional detail for conformance errors. Make corrections and resubmit. 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.
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 Syndromic Surveillance 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, *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.
415	Unsupported media type **Action for vendor or partner when receiving a 415 response:** The 415 error could occur for the following reasons: • The payload format is not in a supported format. • The content-type is incorrect. • The content encoding is incorrect.
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 or DOH systems are taken offline for maintenance. **Action: The submitter needs to hold submissions until notified systems are online and operational.**
504	Timeout generated by the DOH system if processing is delayed. **Action:** Resubmit messages that received this response.

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 Syndromic Surveillance 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 Syndromic Surveillance 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 Accepted.
- Maintenance schedules are posted on the OneHealthPort HIE web page under Maintenance Schedule.