

## HIE API Connectivity for Prescription Monitoring Program (PMP) Submissions to the Washington Department of Health

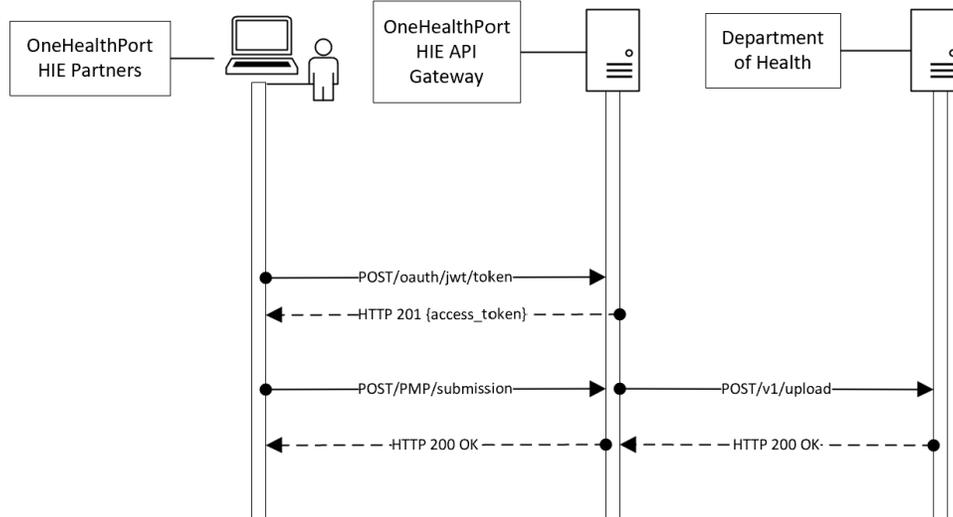
### Purpose

This document presents the OneHealthPort HIE's API connectivity that supports the Prescription Monitoring Program (PMP) 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 PMP data submissions.

### OneHealthPort HIE PMP Data Submissions



### **PMP 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 PMP 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 PMP 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 PMP data

### OneHealthPort HIE API Endpoints

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

Endpoint Description	Endpoint
<b>Authorization API User Acceptance Testing (UAT)</b> – used with OAuth 2.0 JWT to receive access token.	<a href="https://uat-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token">https://uat-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token</a>
<b>PMP API UAT</b> – used with unique access token to post PMP message for data submission to DOH.	<a href="https://uat-v2-onehealthport-api.axwaycloud.com/ncdpd_requests">https://uat-v2-onehealthport-api.axwaycloud.com/ncdpd_requests</a>
<b>Authorization API Production</b> – used with OAuth 2.0 JWT to receive access token.	<a href="https://prd-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token">https://prd-v2-onehealthport-api.axwaycloud.com/ohp/oauth/jwt/token</a>
<b>PMP API Production</b> – used with unique access token to post PMP message for data submission to DOH.	<a href="https://prd-v2-onehealthport-api.axwaycloud.com/ncdpd_requests">https://prd-v2-onehealthport-api.axwaycloud.com/ncdpd_requests</a>

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

HTTPS Header for PMP	Definition
x-doc-type	OneHealthPort HIE document type: <ul style="list-style-type: none"> <li>• PMP</li> </ul>
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.



**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 PMP 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 PMP message

POST /ncdpd\_requests HTTP/1.1

**Authorization:** Bearer

aba887347fcf44cda4c9f176b5833f4ef51f21361d00415987951ce00ae4089e

**x-ref-id:** id-23uilh2iul3klj23h1lkj12

**x-doc-type:** PMP

**x-org-facility-id:** 7uycso22

**Content-Type:** text/xml or application/xml

User-Agent: PostmanRuntime/7.51.0

Accept: \*/\*

Cache-Control: no-cache

Postman-Token: b048a3a1-aaab-45a8-9092-f0e38a773400

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

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

Content-Length: 1877

Cookie: AWSALB=Ws67Rb1u+7JdoOzN4zwy7HoPVwOF86L2nC8OHjjhmKM4L

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

```
<Message xmlns="http://www.ncdpd.org/schema/SCRIPT"
  release="006"
  version="010">
  <Header>
    <To Qualifier="ZZZ">WA-OHP</To>
    <From Qualifier="D">OHP HIE OrgID</From>
    <MessageID>16163115</MessageID>
    <SentTime>2024-10-08T18:09:51.0Z</SentTime>
    <Security>
```

```

    <UsernameToken>
      <Username></Username>
    </UsernameToken>
    <Sender>
      <TertiaryIdentification>Insert WA Credential
      License</TertiaryIdentification>
    </Sender>
    <Receiver>
      <TertiaryIdentification>WA-OHP</TertiaryIdentification>
    </Receiver>
  </Security>
  <TestMessage>1</TestMessage>
  <TertiaryIdentifier>FIL</TertiaryIdentifier>
</Header>
<Body>
  <RxHistoryRequest>
    Content of PMP request
  </RxHistoryRequest>
</Body>
</Message>

```

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

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.

200	OK - DOH successful message submission response passed back by the API gateway.
400	<p>Bad Request</p> <p><b>Action:</b> Review response for additional detail for conformance errors. Make corrections and resubmit.</p>
401	<p>Unauthorized</p> <p><b>Action:</b> 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 <a href="#">form</a> to request a new OAuth 2.0 JWT token.</p> <p>If the 401 is related to the access token in the PMP 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><b>Action for vendor or partner when receiving a 403 response:</b></p> <p>Submit a OneHealthPort HIE Support Request <a href="#">form</a>.</p> <p>In the section of the form called, <i>Issue or Question area</i>, select the option called <b>HIE connectivity set-up</b>.</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 forbidden error and provide the content of the error message.
500	Internal Server Error  <b>Action:</b> 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.  <b>Action: The submitter needs to hold submissions until notified systems are online and operational.</b>
504	Timeout generated by the DOH system if processing is delayed.  <b>Action:</b> Resubmit messages that received this response.

## HTTP Successful Response

### Synchronous 200 OK response from DOH system that PMP file was accepted

```
HTTP/1.1 200 OK
Max-Forwards: 20
Via: 1.1 44dd03c67acbb2.cloudfront.net (CloudFront), 1.1 axwc-api-21-v2 ()
Connection: close
X-CorrelationID: Id-ee3c72695124a5602d6a05cc 0
Date: Thu, 22 Jan 2026 15:06:22 GMT
expires: Mon, 01 Jan 2000 00:00:00 GMT
x-request-id: 2285aeb2-14c7-4151-968a-7586a9733bbe
Content-Type: application/xml
<?xml version="1.0" encoding="UTF-8"?>
<Message xmlns="http://www.ncdpd.org/schema/SCRIPT" release="006" version="010">
  <Header>
    <To Qualifier="ZZZ">OHP HIE OrgID</To>
    <From Qualifier="ZZZ">WA-OHP</From>
    <MessageID>2256316</MessageID>
    <RelatesToMessageID>2256516</RelatesToMessageID>
    <SentTime>2026-01-22T15:06:22+00:00</SentTime>
  </Header>
  <Body>
    Response from DOH PMP system
  </Body>
</Message>
```

## 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 PMP 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 PMP 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 200.
- Maintenance schedules are posted on the OneHealthPort HIE [web page](#) under Maintenance Schedule.