InterOp Station®

Third-Party Developer Portal

User Guide

Version 6
January 27th, 2026

Document History

Date	Version	Sections Revised	Description	Modifier
1/30/2025	v5	All	Updated to current template and format. Updated Security Attestation and Debug and Validate an OAuth Connection sections	M. Allen, M. Smith
2/19/2025	v5	Acronyms and Definitions	Updated information on several acronyms and definitions that were missing.	M. Allen, M. Smith
6/18/2025	V5	All	Updated spacing, grammar, acronyms, and spelling	T. Fite
8/18/2025	V5	All	Rewrote most sections for clarity and accuracy.	M. Allen
9/29/2025	V5	All	General editing	S. Denhof
10/8/2025	V5	All	Application of Review Edits and finalization of draft.	M. Allen
1/27/26	V6	All	General editing of format and removal of tenants	M. Smith

```
```

Table of Contents

1. Introduction

1.1 Purpose of this Guide

The purpose of this guide is to help third-party developers register an application (app) as a client of the InterOp Station®. This guide focuses on connecting, testing, and/or adding a developer's privacy policy and security attestation documents.

1.2 Additional Information and Resources

If developers or other users of the InterOp Station® require additional information or need assistance with the use of this application, they can contact the MiHIN Help Desk by email at help@mihin.org.

Additionally, users should contact the MiHIN Help Desk if they experience any of the following issues while connecting to their app:

- An inability to submit a security attestation
- An inability to get credentials in development
- Tests that are conducted are failing in the development environment
- An inability to get credentials for production.
- Tests that are conducted are failing in the production environment

2. InterOp Station® Third-Party Developer Accounts

2.1 Creating an Account

New Interop Station® users will first need to create an account before using the InterOp Station® tools. The creation of a new account is accomplished through the following steps:

1. Users should navigate to https://www.interopstation.com/login.
2. Upon navigating to the above URL, users will find the login and account creation interface as shown in **Figure 1**. To create a new account, users should click the **Sign Up** link, as shown in **Figure 1**.

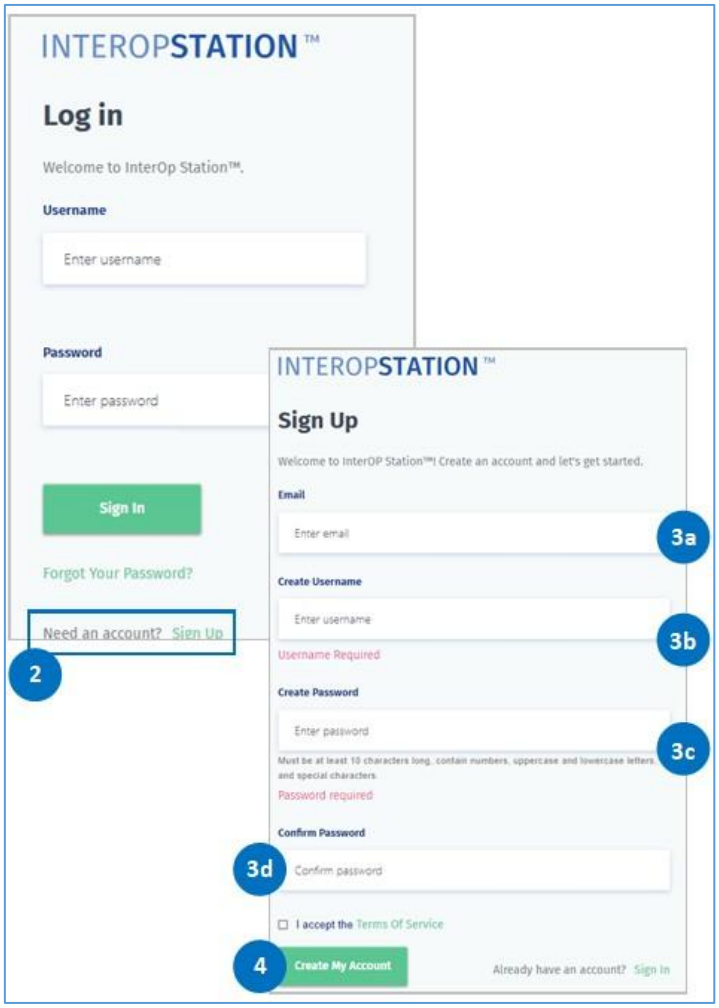

Figure 1. InterOp Station® Account Creation UI

3. On the following pop-up screen, the user should fill out the following fields, as shown in **Figure 1**.
    a) Email
    b) Create Username
    c) Create Password
    d) Confirm Password

    Please note: The chosen password must conform to the following specifications:

    - Minimum password length: 10 characters
    - Must contain numbers, uppercase and lowercase letters, and special characters

4. Once the fields have been entered, the user will click the **I accept the Terms of Service** check box and then click the **Create My Account Button,** as shown

in **Figure 1**. A confirmation pop-up as shown in **Figure 2** will display showing that the account has been successfully created.

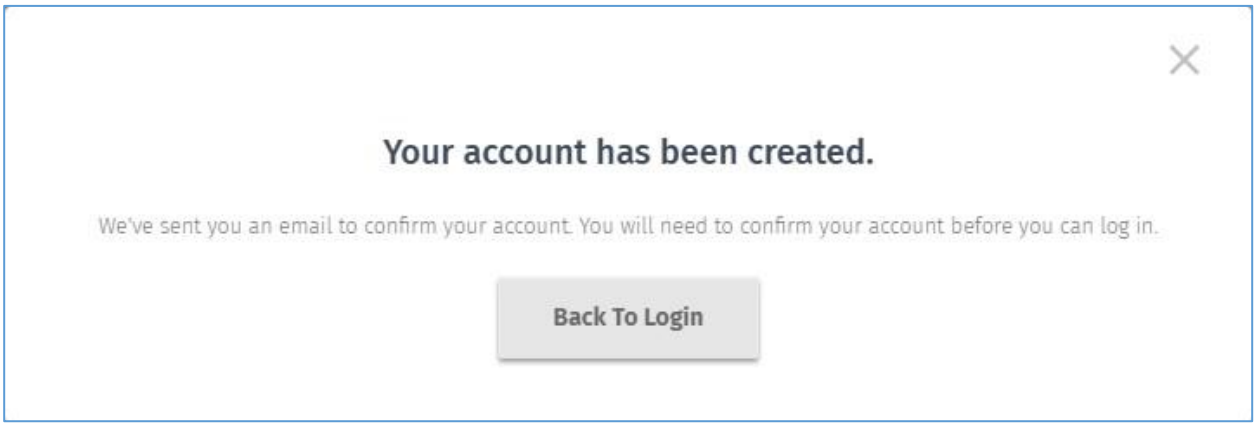

Figure 2. Account Creation Confirmation Screen

5. Once created, an email will be sent to the email address provided to confirm the user's account. This is accomplished by clicking the Verify Email link in the body of the email, as shown in **Figure 3**. Clicking this will take them to a page confirming that the user's account has been verified.

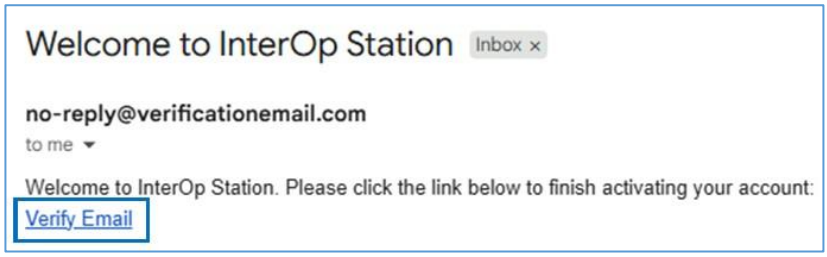

Figure 3. Email Account Verification

6. Once confirmed, the user can sign in with their username and password by returning to the login screen and filling in the appropriate fields.
7. Once the user has signed in on the login screen, to proceed, they will need to click the **I Accept** button to agree to the InterOp Station® Terms of Service, pictured in **Figure 4**.

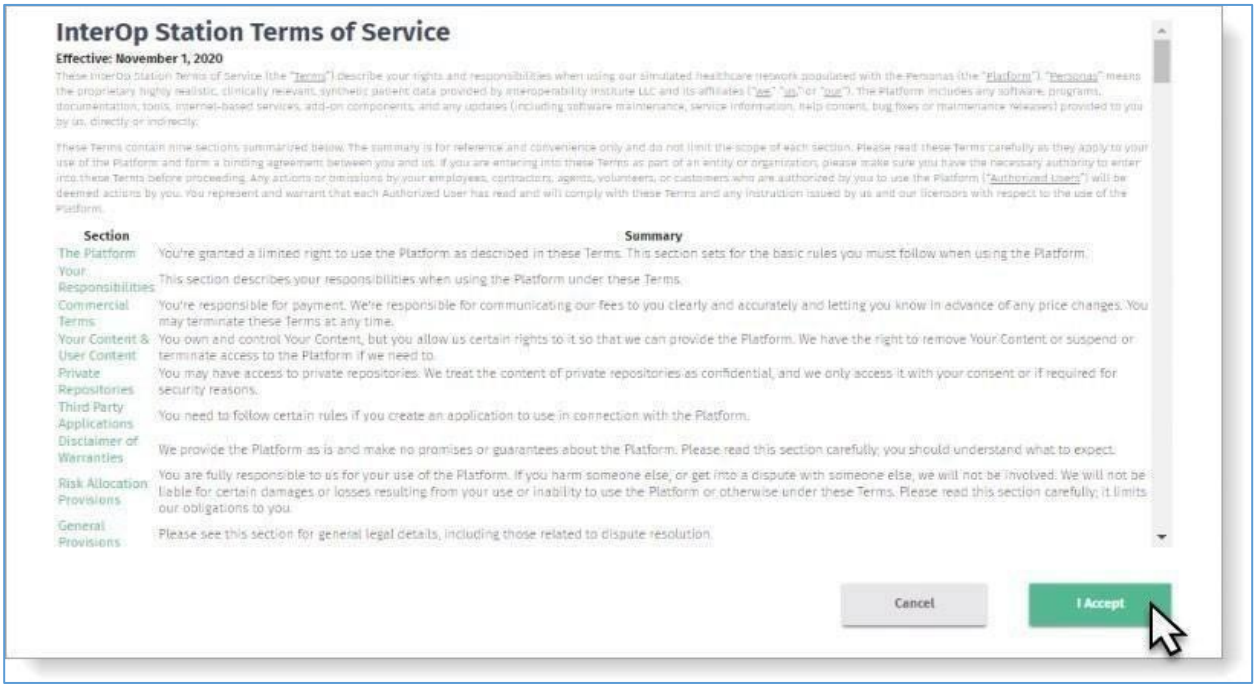

Figure 4. InterOp Station® Terms of Service Screen

Please Note: Clicking the **Cancel** button will return the user to the login window, as failure to agree to MiHIN's terms of service will put the user in breach of the privacy and security policies that dictate InterOp Station®'s use.

2.2 Login Issues

In the event a user has followed the above steps and sign in still fails, they should contact the MiHIN Help Desk at help@mihin.org.

3 Connecting a Third-Party Developer Application to InterOp Station®

3.1 Welcome Page Navigation

Upon successfully logging into the portal, users will find themselves on the main **Welcome Page,** shown in **Figure 5**. The main Welcome Page contains links that allow a user to register their applications (apps), configure details regarding their registered app, and view supporting information from the Document Library.

The Welcome Page contains links to the following:

a. Application Dashboard
b. Developer Attestation
c. Document Library
d. Specific document summaries and links

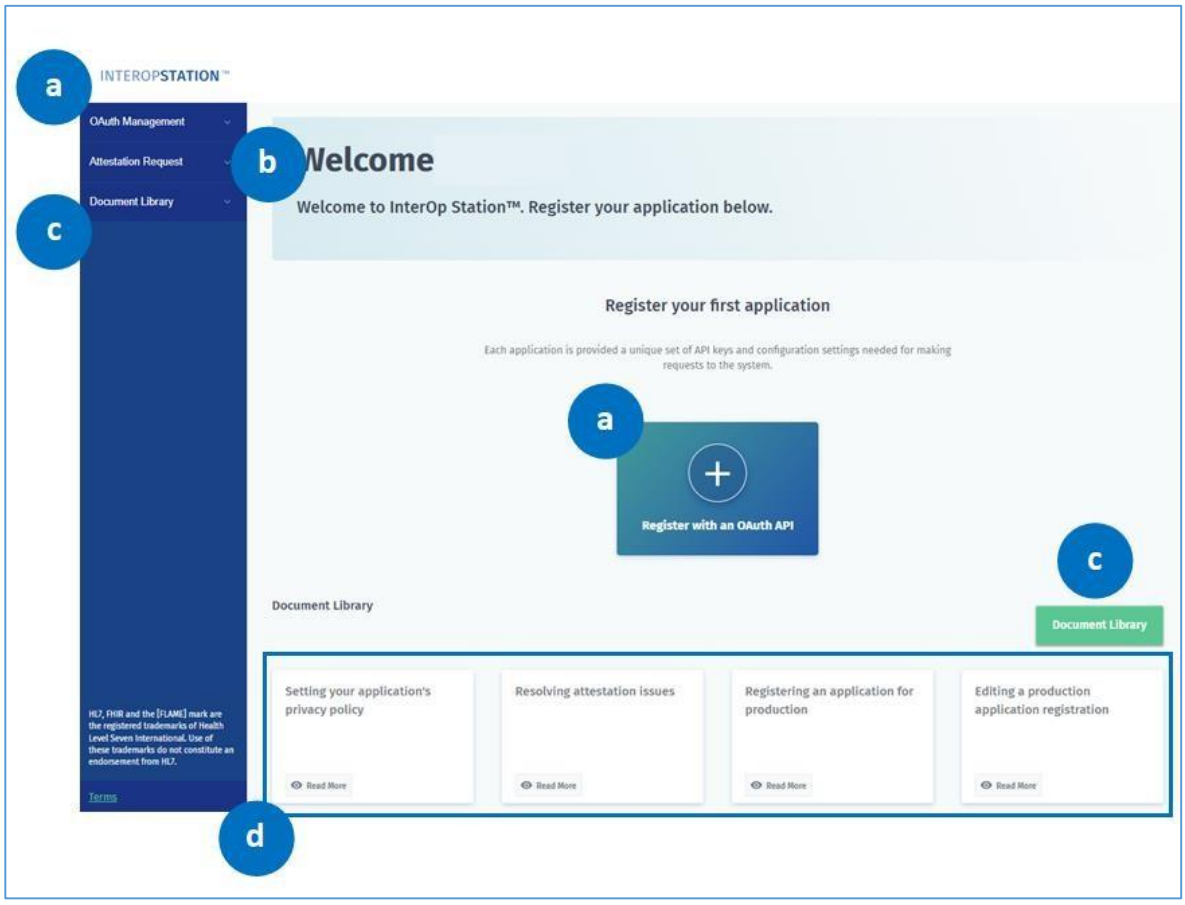

Figure 5. Welcome Page User Interface

Please note that some of these links are both located on the Welcome Page, as well as on the sidebar along the left-hand side of the page. Clicking on either link will take users to the same page.

If at any point a user would like to navigate back to the Welcome Page, they may do so by clicking on the **INTEROPSTATION™** title located above the sidebar navigation.

3.2 Registering a SMART Application with the OAuth API Tool

Developers that would like to register their applications in the InterOp Station® Third-Party Developer Portal will need to first register with the OAuth API Tool. This can be accessed either by clicking the **Register with an OAuth API** link on the main Welcome Page, as shown in **Figure 6a**, or by clicking on the OAuth Management link in the sidebar menu and then clicking the **Register an App** button on the resulting page, as illustrated in **Figure 6b**.

Figure 6a. Register with an OAuth API Link on Main Welcome Page

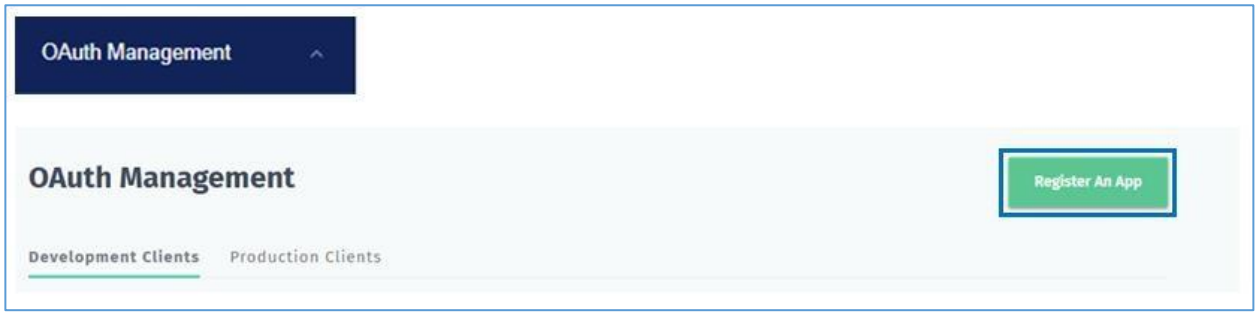

Figure 6b. OAuth Management Side Menu Link

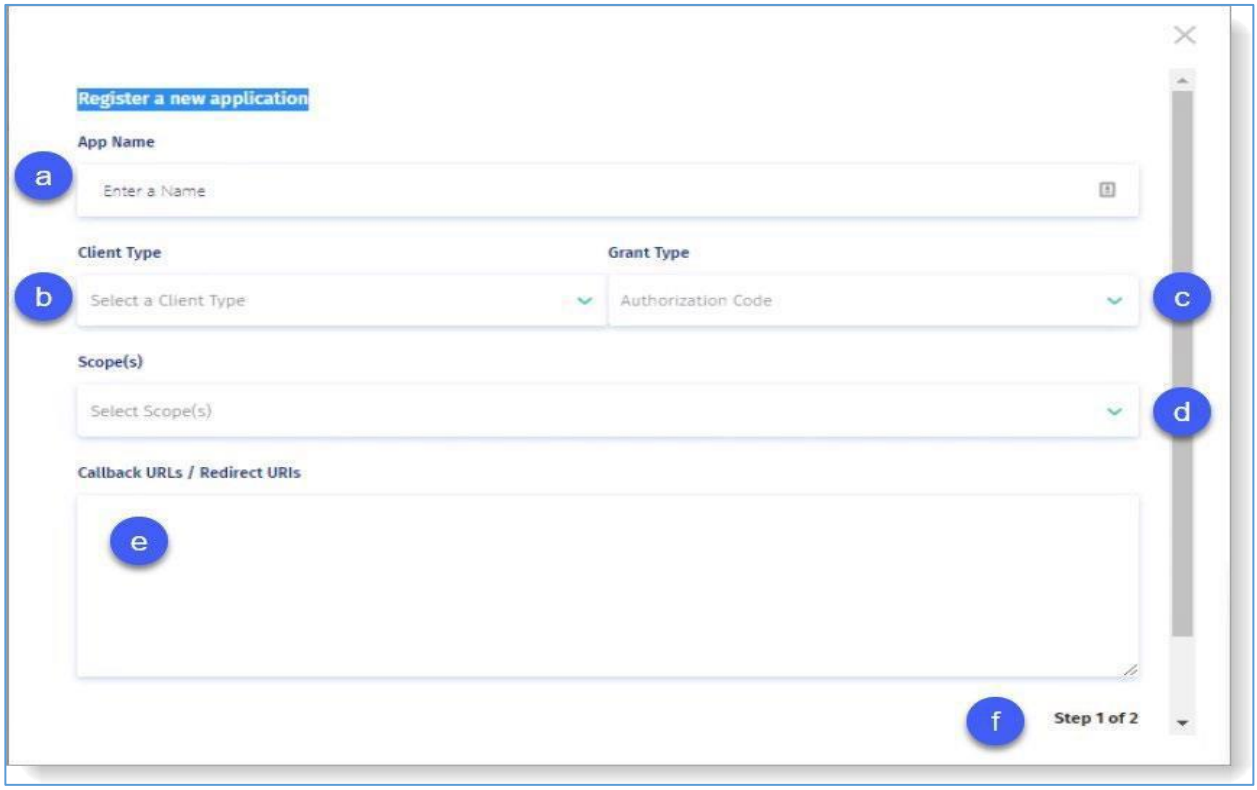

Figure 7. Register a New Application Form and Fields

Regardless of which link the user chooses, users will arrive at the Register a New Application pop-up window, as shown below in **Figure 7**.

1. On the resulting registration form for the new application, the user enters the required information as follows:

    a. **App Name** – Chosen name that identifies the user's Substitutable Medical Applications, Reusable Technologies (SMART) App.

    b. **Client Type** – From drop down, the user will select how they will be configuring calls to the token endpoint from the following options:

        - Public
        - Confidential – Forms Auth
        - Confidential – Basic Auth

The Client ID (username) and secret (password) generated by MELD™ (Formerly Interoperability Land™) will be passed to the endpoint via this selection. **Confidential - Basic Auth** is considered the default setting and should work unless another form of authentication is used by the app.

c. **Grant Type** – The user will select how their app will request and receive the authorization token. The Authorization Code option is considered the default and is the only option available.

d. **Scope(s)** – The user will select the scope of resources they are requesting for access from the drop-down list. If a user has multiple scopes that need to be called out, they will need to manually select and add them to the list, as there is no multi-selection option for this field.

   For reference, HL7™ identifies the allowed scopes for a user's resources.

   - For more information on allowed scopes, visit http://www.hl7.org/fhir/smar t-applaunch/scopes-and- launch- context/.
   - The list of scopes accepted are specified in the Metadata/Capability Statement located in the following link: https://api.interopstation.com/{tenant}/fhir/metadata (select the appropriate tenant's name to get a tenant-specific list).

e. **Callback URIs / Redirect URI** – The user will list all Callback and Redirect Uniform Resource Identifiers (URI) for the application they are connecting.

Note: To test this application with oauthdebugger.com, the user will need to list application's redirect URI and oauthdebugger.com/debug here separated by commas.

Example:

https://yourapphere.com,https://oauthdebugger.com/debug

More information about the OAuth 2.0 Debugger will be covered in section 3.4.

f. Once the above fields have been completed, the user will need to click the **Next** button to move onto and complete the second step of registration.

g. Once the **Next** button is clicked the **Step 2 of 2** popup, shown in **Figure 8**, will prompt the user to upload a PDF of the user's privacy policy. This is completed by selecting the **Upload Now** button, selecting the desired Policy PDF and then clicking **Save Application**.

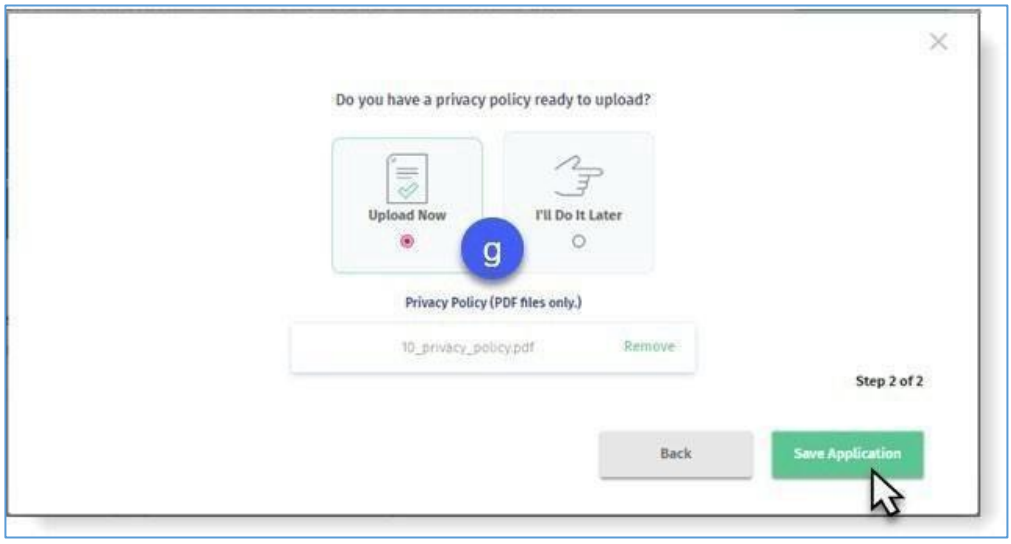

Figure 8. Step 2 Pop-Up Prompt

The app will then be connected with the selected policy.

Note: If the user is not yet ready to upload their policy, they may select the **I'll Do It Later** option and then click **Save Application**. However, a privacy policy must be uploaded before the app can go into the Production environment.

3.3 Navigating the Application Dashboard Page

Once the application has been registered with the OAuth API, the App Dashboard page will become available, as pictured in **Figure 9**.

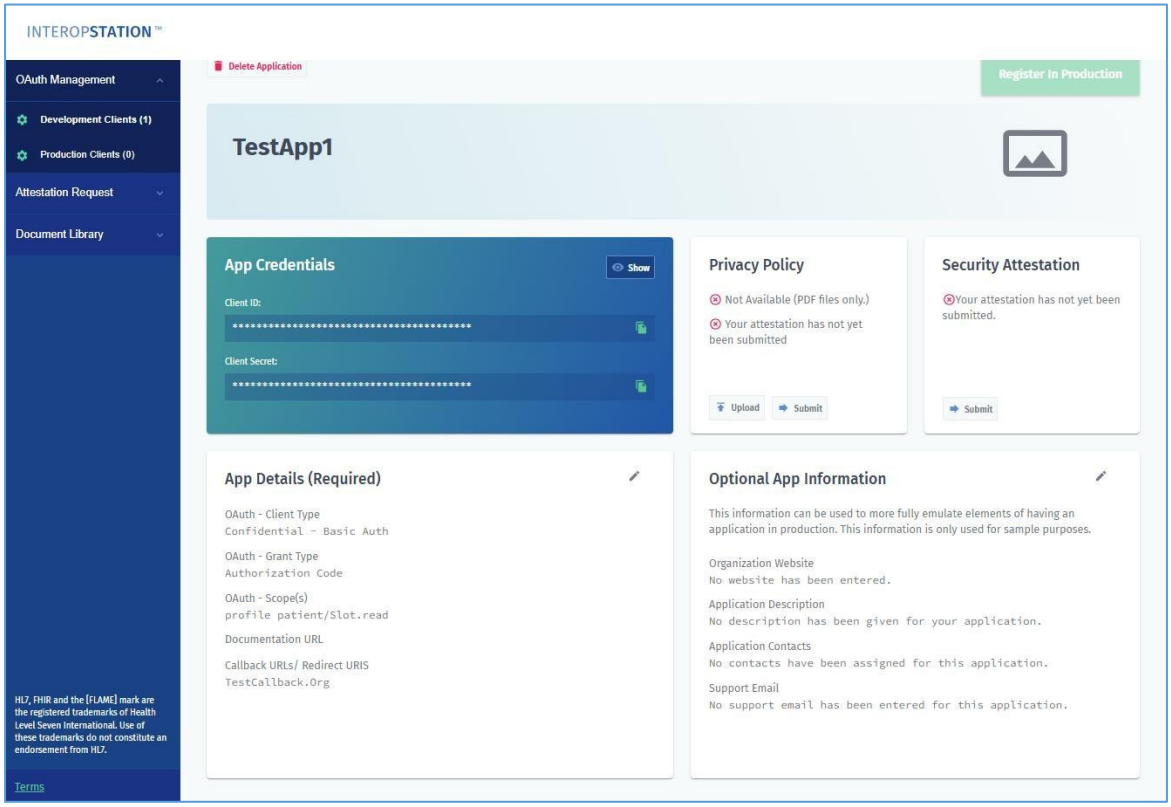

Figure 9. Application Dashboard Layout

From this page, a user can do the following:

- Modify the **App Details**, which are the details that were selected during the registration process.
- Upload and review a **Privacy Policy**.
- Complete or review a **Security Attestation**.
- Add **Optional App Information** such as the organization's website, a description of the application, a point of contact, and an email address.

- Obtain app credentials, specifically the **Client ID** and **Client Secret**, to complete the connection to the InterOp Station®. The Client ID and Secret are also obtainable from the OAuth Credentials section of the Welcome page.

These processes will be described in more detail in the following sections.

Please Note: This page can be navigated back to at any time by choosing the **OAuth Management** option on the sidebar navigation menu and then selecting **Edit**.

3.3.1 Uploading a Privacy Policy

Privacy Policies can be uploaded from the Privacy Policy section of the Application Dashboard, pictured in **Figure 10**.

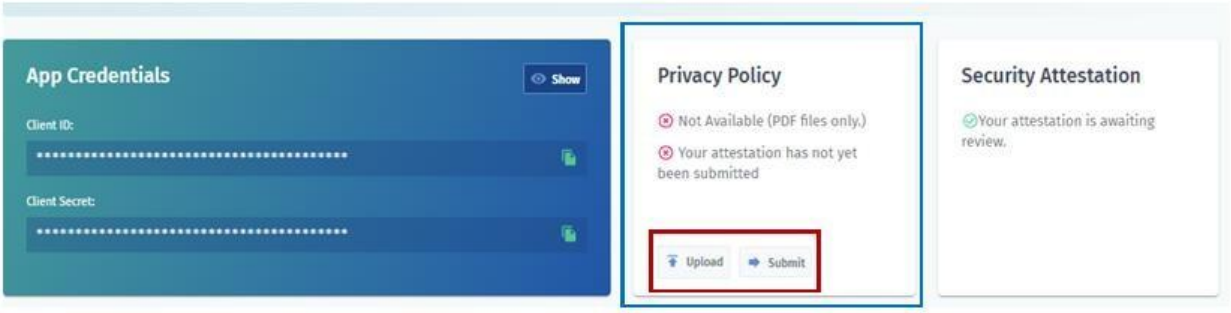

Figure 10. Privacy Policy UI on the Application Dashboard

To submit a privacy policy, a user should adhere to the following steps:

1. On the **Privacy Policy** section on the Application Dashboard, the user will select the Upload button and select the Policy PDF they would like to submit.
2. When the PDF file successfully uploads, the options on the Privacy Policy tile change to either View or Remove as shown in **Figure 11**.

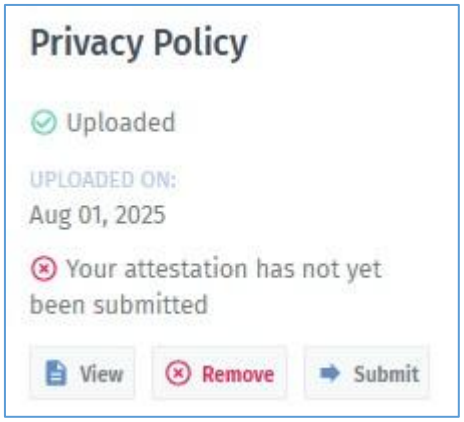

Figure 11. Privacy Policy Section after Policy Upload

3. **Note**: Selecting View will allow the user to view their policy or they may select Remove if they are not ready to submit their policy.
4. Once ready, the user will click **Submit** to complete their upload.

The privacy policy must be in PDF format. If the submitted privacy policy is in PDF format and does not upload successfully, please contact the MiHIN Help Desk at help@mihin.org.

3.3.2 Privacy Policy Attestation

When the **Privacy Attestation** page displays, illustrated in **Figure 12**, the user should respond to each question, and then click **Submit**.

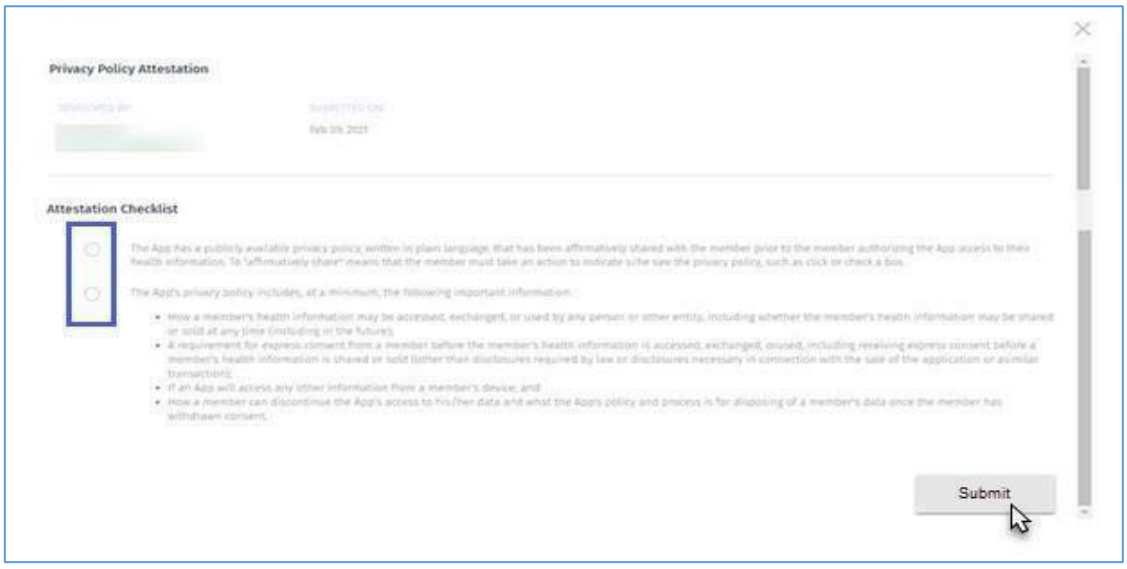

Figure 12. Privacy Policy Attestation Page

Please Note: How questions are answered on this attestation does not affect whether an application to register with InterOp Station® is accepted.

3.3.3 Submitting a Security Attestation

Developers are required to submit a security attestation for their app. An automated MiHIN Help Desk ticket is generated after a security attestation is completed and submitted. The MiHIN Security Team will review the third-party developer ticket and determine whether the submitted Security Attestation is accepted or needs to be resubmitted.

Users can submit a security attestation for their registered application through the following process.

1. Security Attestations can be submitted from the Application Dashboard page by choosing the **Submit** option located on the user's **Security Attestation** tool, illustrated in **Figure 13**

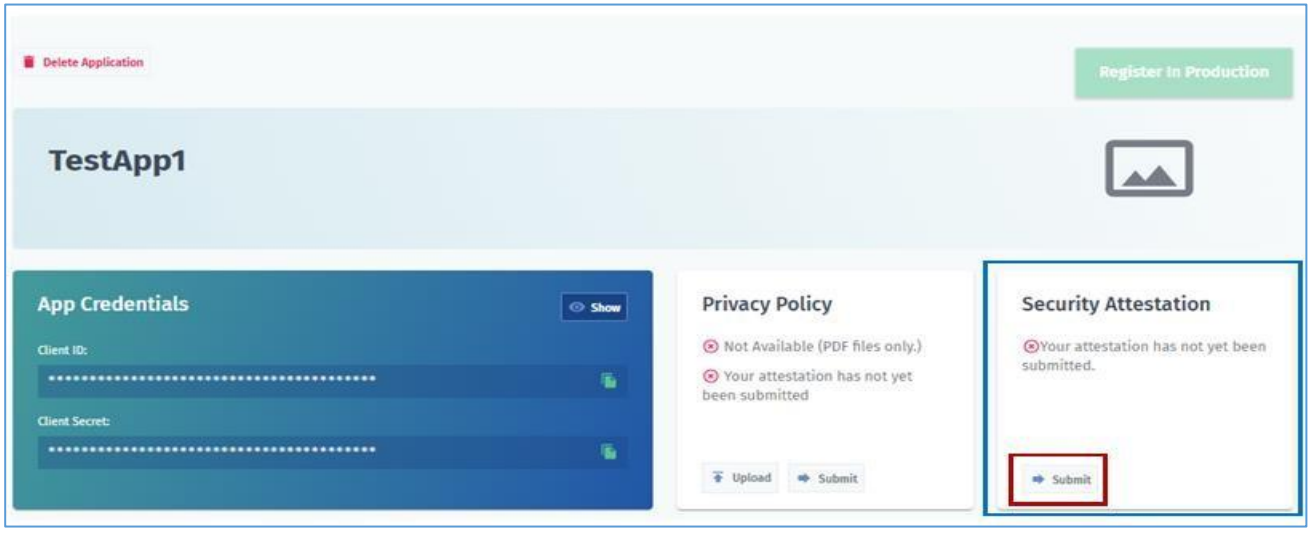

Figure 13. Security Attestation Interface on Application Dashboard

2. When the **Application Attestation** page appears, illustrated in **Figure 14**, the user will need to respond to each question and then click **Submit** to send the information to the MiHIN Security Team for review.

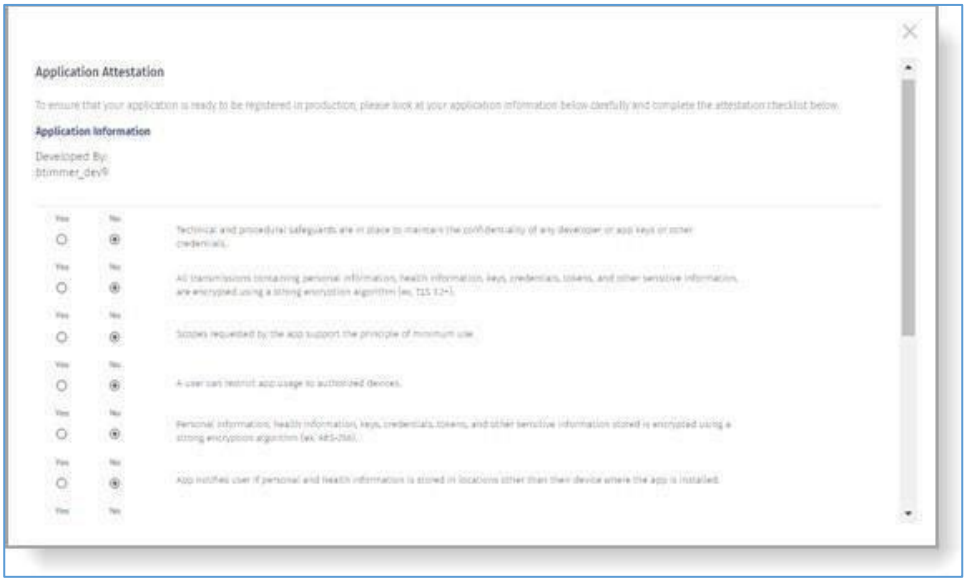

Figure 14. Application Attestation Page

3. A user may check on the status of their Security Attestation by navigating to the Welcome page and looking under the **Attestation Requests** dashboard or by clicking **Attestation Requests** located on the Sidebar Navigation Menu, as shown in **Figures 15 and 16.**

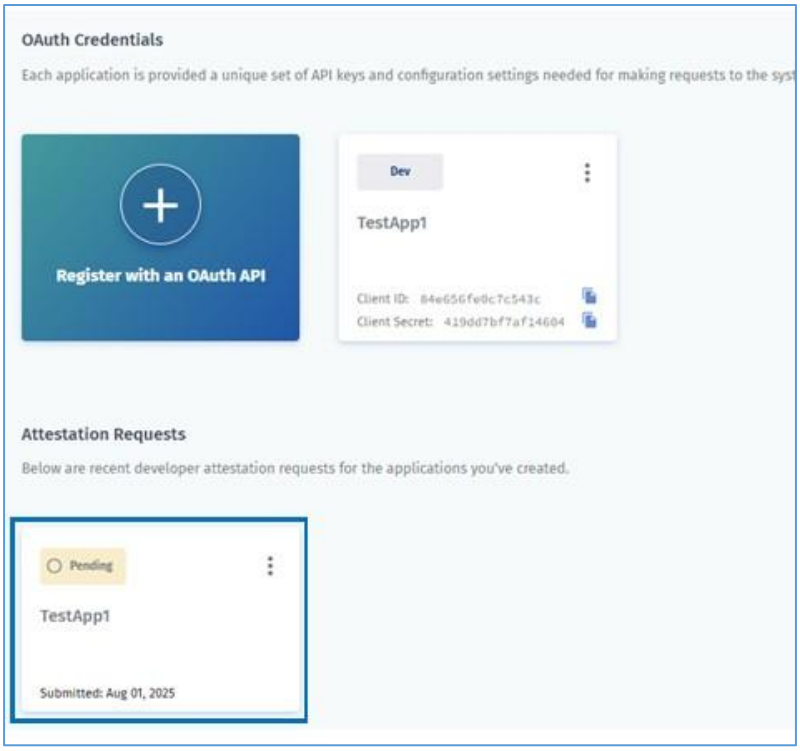

Figure 15. Security Attestation Status Location on Welcome Page

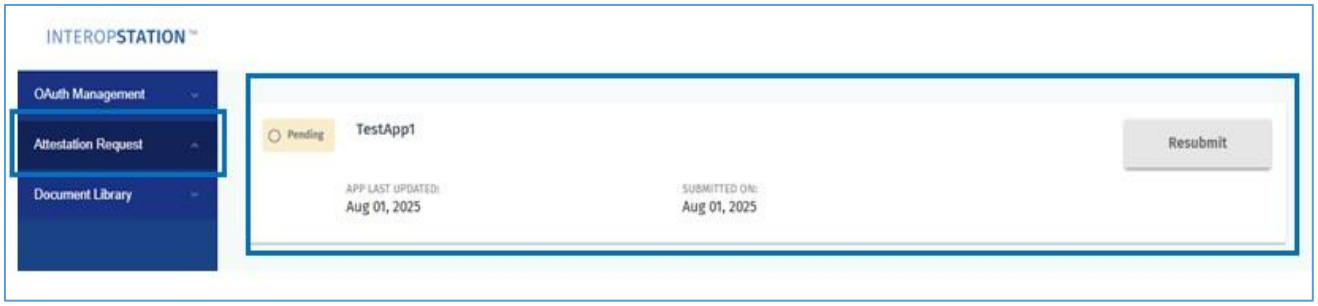

Figure 16. Security Attestation Status Location on Menu Bar

4. Attestation Requests can have one of the following statuses:
    a. **Approved**. The security attestation has been accepted by the MIHIN Security Team.
    b. **Pending**. The MIHIN security attestation has been submitted and is awaiting review.
    c. **Issue**. The security attestation has been denied by the MiHIN

        Security Team, who will notify the third- party developers via email. The user will need to update their security attestation and resubmit for approval.

Please Note: To resubmit security attestation, select either Attestation Requests on the Sidebar navigation menu or by clicking the **More** vertical ellipses tool on the Security Attestation tile, pictured in **Figure 17.**

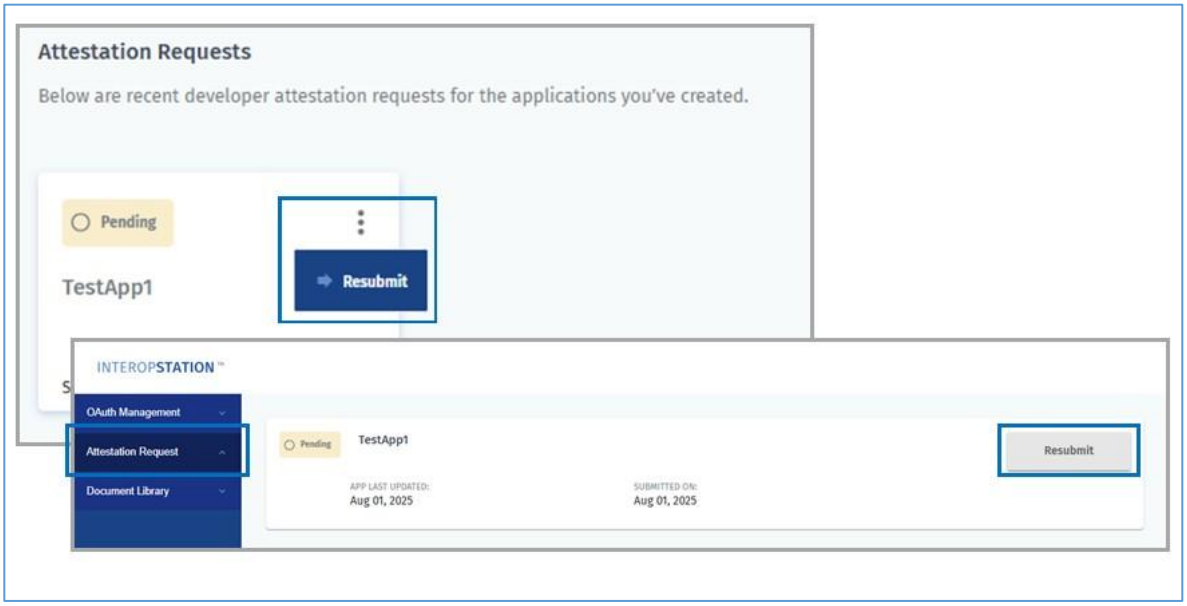

Figure 17. UI Options to Resubmit Security Attestations

For more information, please review Section 3.3.3 Upload a Privacy Policy.

3.4 Validation of OAuth Connections

To complete the connection between a user's application and InterOp Station®, the Client ID and Client Secret will need to be used with the application to connect. This information can be found on the Welcome page or on the Application Dashboard, as shown in **Figures 18 and 19**.

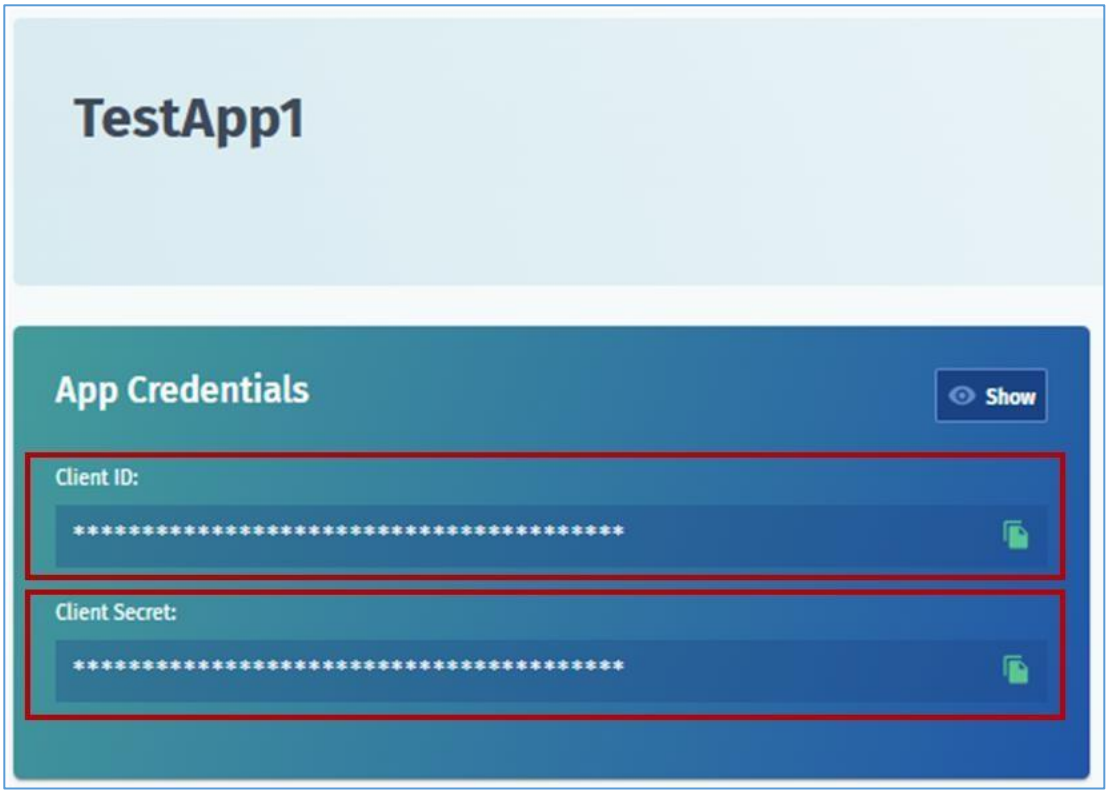

Figure 18. Client ID and Secret Access Location on Application Dashboard

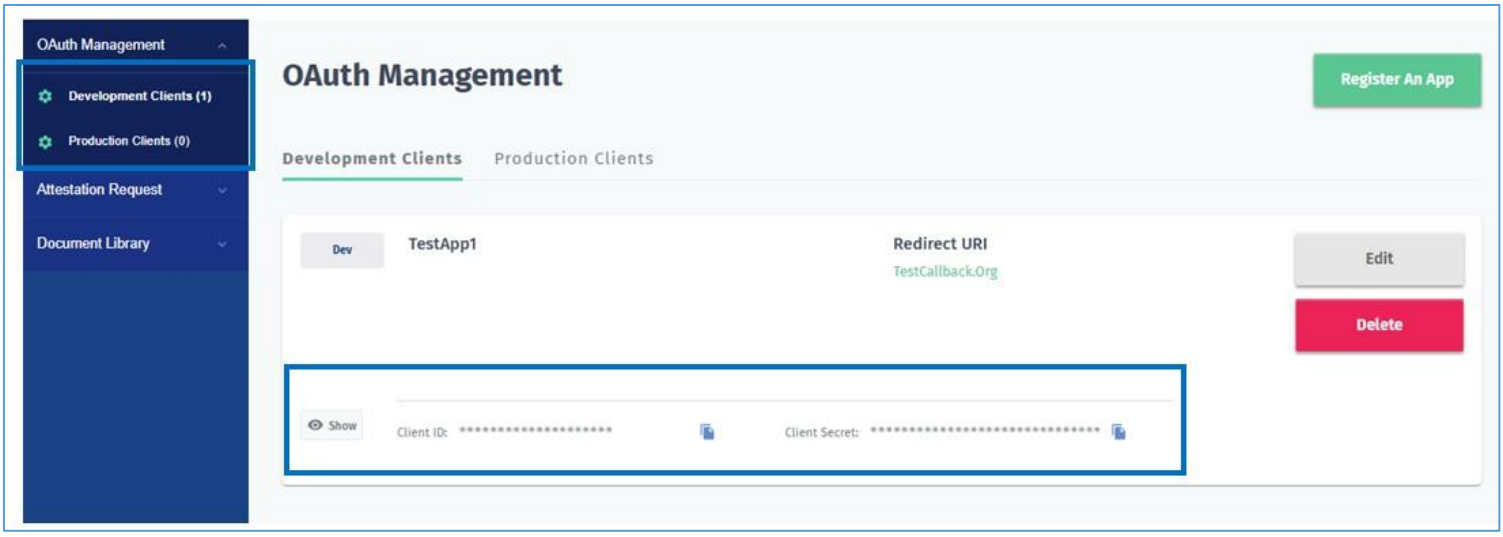

Figure 19. Client ID and Secret Access Location from Welcome Page

The process of validating a user's OAuth connection is the same whether the app is set up in a development or production environment. The connection points for development and production vary, as noted in the third-party developer portal document library.

Due to the varying nature of user applications, the open-source OAuth 2.0 Debugger application will be used to demonstrate an example of how an OAuth 2.0 connection is made with calls via an API. The address of the OAuth 2.0 Debugger can be found here: https://oauthdebugger.com.

Tip: User's will have to update their application to authenticate to interopstation.com by using OAuth 2.0 and then performing API requests based on their application's scope.

1. As mentioned above, this example will use the OAuth 2.0 Debugger to demonstrate the process of entering a user's required app information as well as their Client ID and Scope, but a user's situation may vary based on the specification of their application. The Debugger interface is illustrated in **Figure 20**.

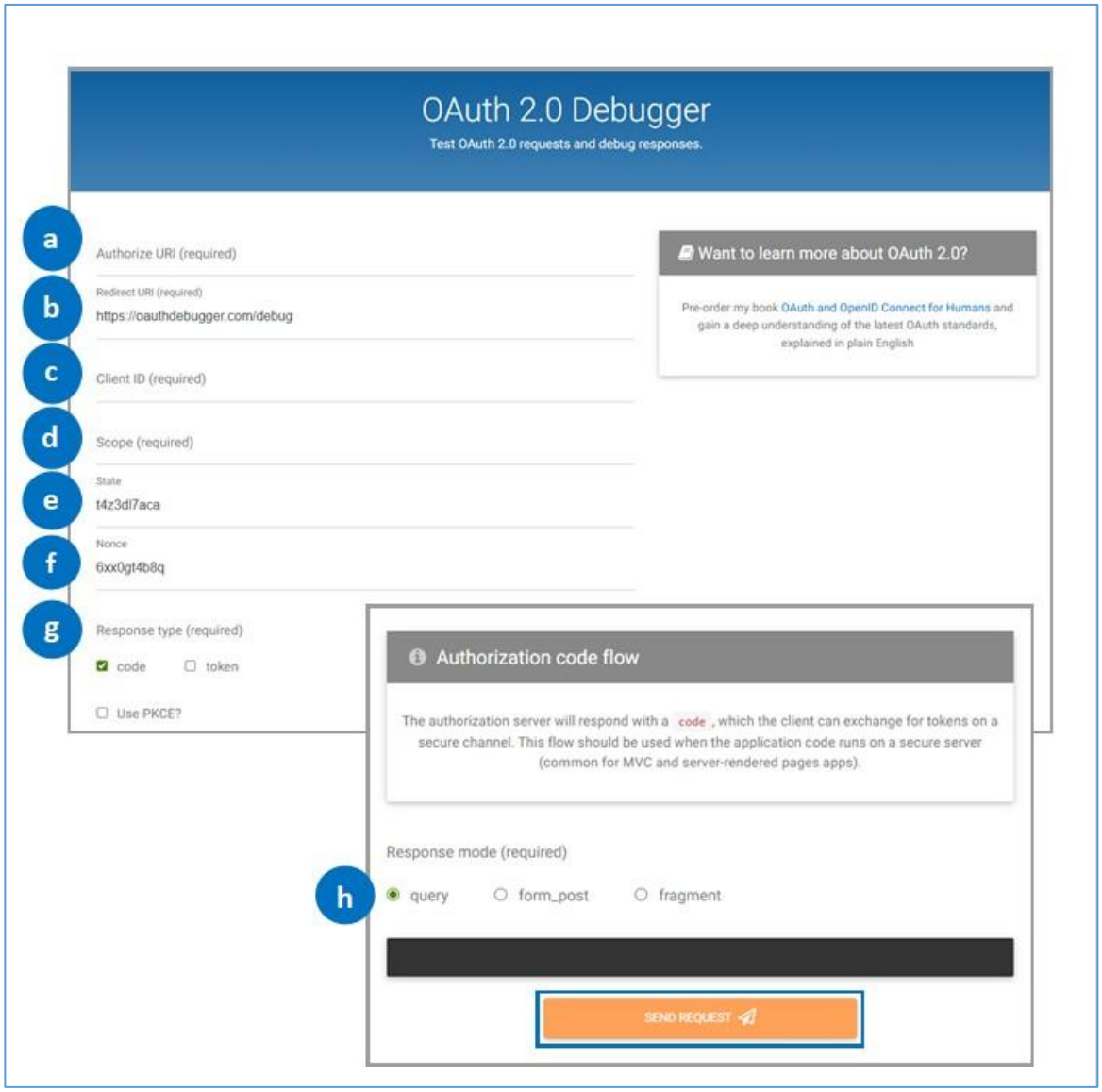

Figure 20. OAuth Debugger Interface

The image shown is an example of how a tool like OAuth Debugger could display after a user enters their information. Each field is described below. An example of code follows this section.

Note: The names of the parameters listed below must be entered as shown, as they are case sensitive. All fields are required.

a) **Authorize URI**. Authorized URIs can be found on interopstation.com, in the Document Library, at the InterOp Station® API Endpoints, and at the OAuth 2 URL for the environment for which the user is trying to connect.

b) **Redirect URI**. From the application or from oauthdebugger.com/debug, the user should select **Redirect URI**. In their code, they should use the variable: **redirect_uri**

c) **Client ID**. In their code, the user should use the variable: **client_id**. The Client ID can be copied from the application's page on InterOp Station® under App Credentials.

d) **Scope**. In their code, the user should use the variable: **scope.** This is the application scope they chose while registering their application.
Note: The scopes can be copied from the list that was selected while registering the app.

e) **State**. In their code, the user should use the variable: **state.**
Note: The value for state is auto generated, should not be changed, and cannot be left blank.

f) **Nonce**. In the code, the user should use the variable: **nonce**
Note: This value must be unique for each request. It is auto generated, should not be changed, and cannot be left blank.

g) **Response type**. In the code, the user should use the variable: **response_type.** The default value is **code**. If there is a Response Type, the user should select **token**.

h) **Response mode**. In the code, the user should use the variable: **response_mode=query**
Note: An example of the URL after the parameters above have been updated can be found in Section 5.2: Appendix B.

2. Once the user has entered in the requisite information, they should submit the request. In the OAuth 2.0 Debugger example, this is accomplished by clicking the **Send Request** button, as shown in **Figure 21**.

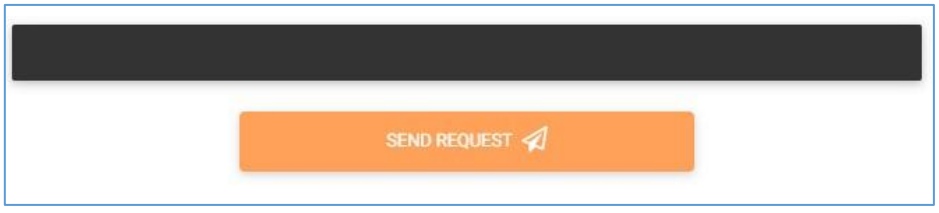

Figure 21. Send Request Button in OAuth Debugger

3. After the application connects, the user will be redirected to the MELD™ User Login pictured in **Figure 22**. The username and password for the development account are prefilled. The user should click **Sign In.**

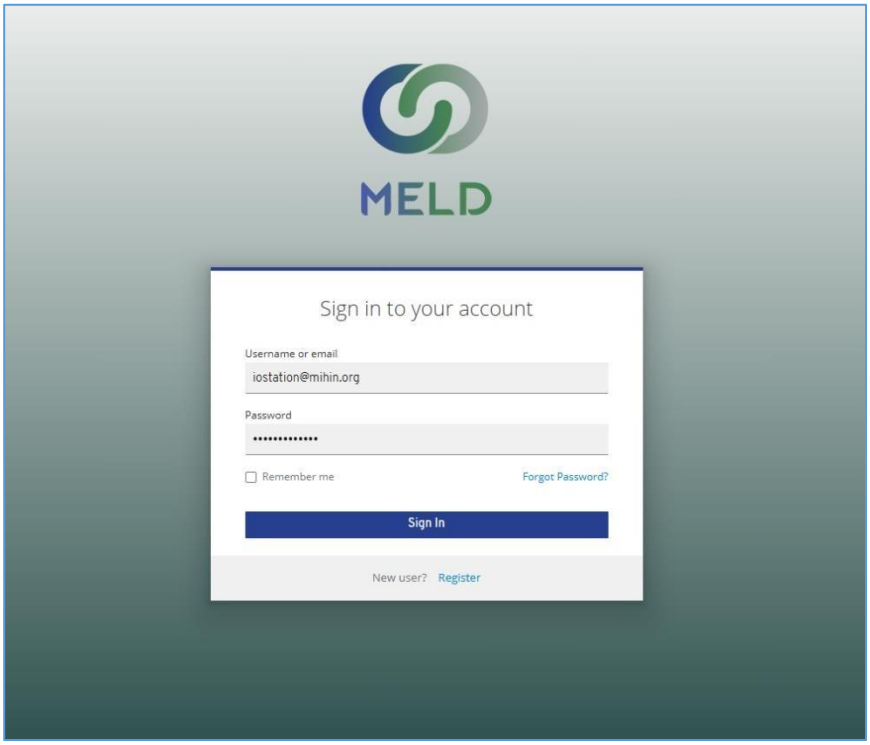

Figure 22. MELD™ User Login Interface

Note: This step does not occur in production. It occurs because there is a test patient in the development environment with the following demographics:

- Name: Rose Tammy Beltran
- Date of Birth: 03/21/1997
- Identifier: smart-15716

4. Upon signing in, notifications pop-ups will display as illustrated in **Figures 23 and 24.** The legal language that is used here can be customized by the user to indicate that the patients using the app will be providing their personal health information (PHI) to a third party.

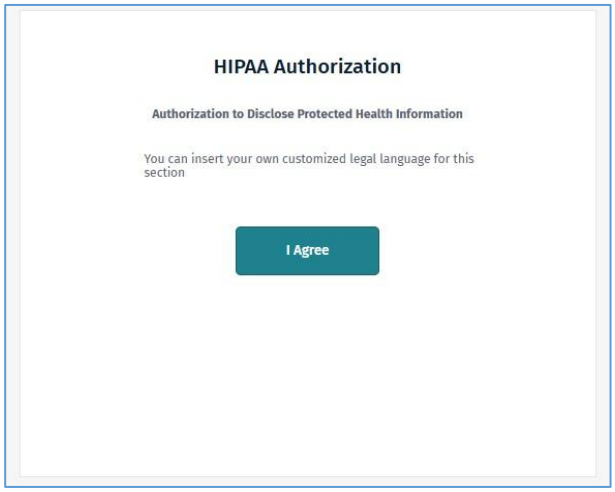

Figure 24. HIPAA Authorization Agreement Pop-Up

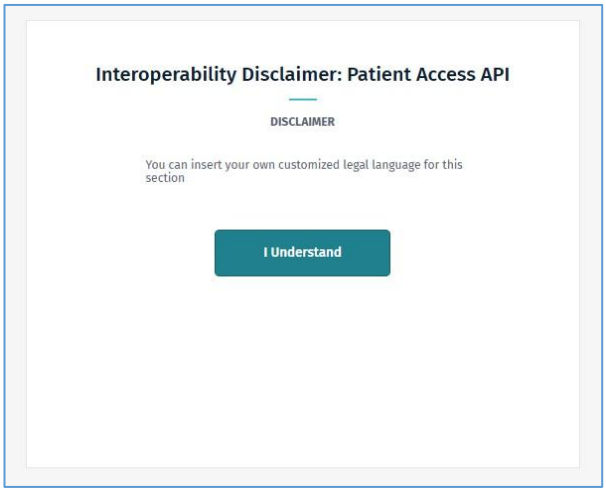

Figure 23. Interoperability Disclaimer Pop-Up

5. After confirming the two pop-ups, a Success! message, pictured in the OAuth 2.0 Debugger in Figure 25 will display with the user's Authorization Code for Postman.

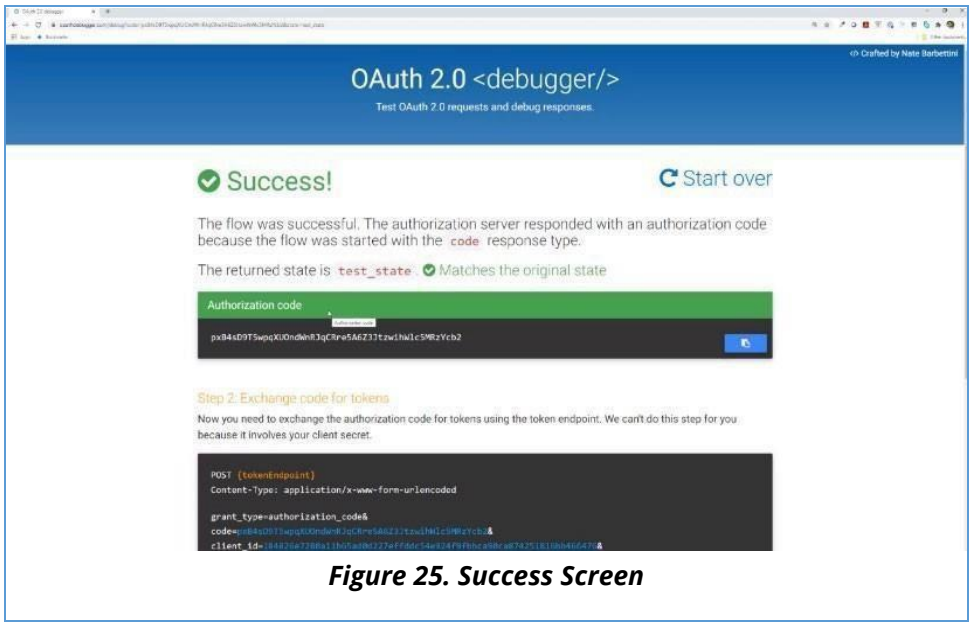

Figure 25. Success Screen

3.5 Connecting to InterOp Station®

Once the user has acquired their Postman Authorization Code, they will need to proceed through the following steps to fully connect with the InterOp Station®.

1. The user will copy their token and navigate to and open **Postman**.

Note: The Postman Demo bundle is available to download at: https://mihin.org/wp-content/uploads/2021/02/IOS-Demo.postman_collection.json_.zip

2. Using the Body tab, shown in Figure 26, the user should proceed with the following steps:
    a. The user will enter their **Client ID** and **Client Secret** which can be obtained from the Application Dashboard.
    b. The user enters their **grant_type** key value (default value to be given as: **authorization_code.**
    c. The user enters their **redirect_uri** key value (default value to be given as: https://oauthdebugger.com/debug).
    d. The user will then paste their authorization code as their **code** value. This is the Authorization Code described in Section 3.4.

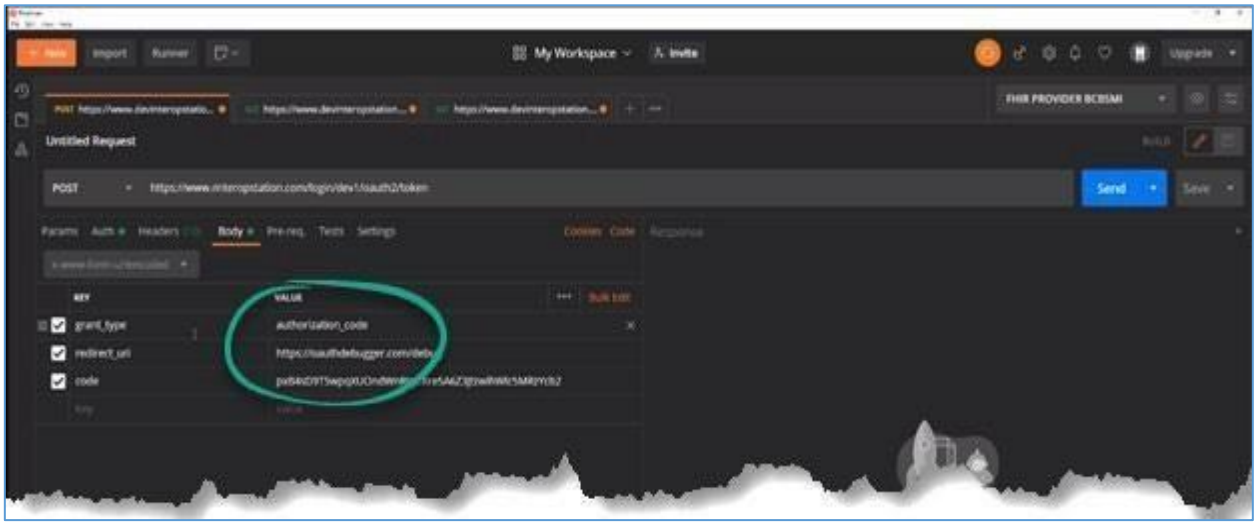

Figure 26. Body Tab Interface with Values

3. Once complete, the user will copy the access token string in the response window, as pictured in **Figure 27**.

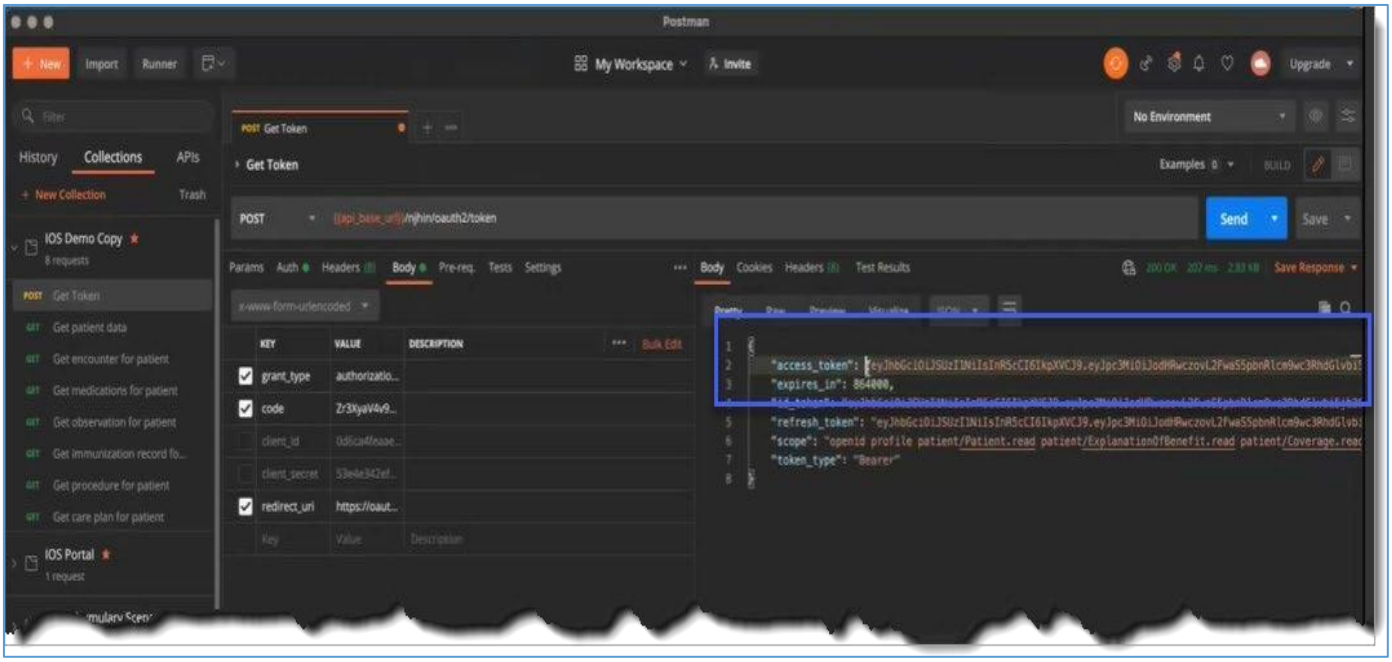

Figure 27. Access Token String in Response Window Interface

4. On the left navigation menu, the user should click on the **More** button, represented as the **three dots** button shown in **Figure 28,** for options to manage their collection.
5. From here, the user should click on **Edit** to bring up the **Edit Collection** form.

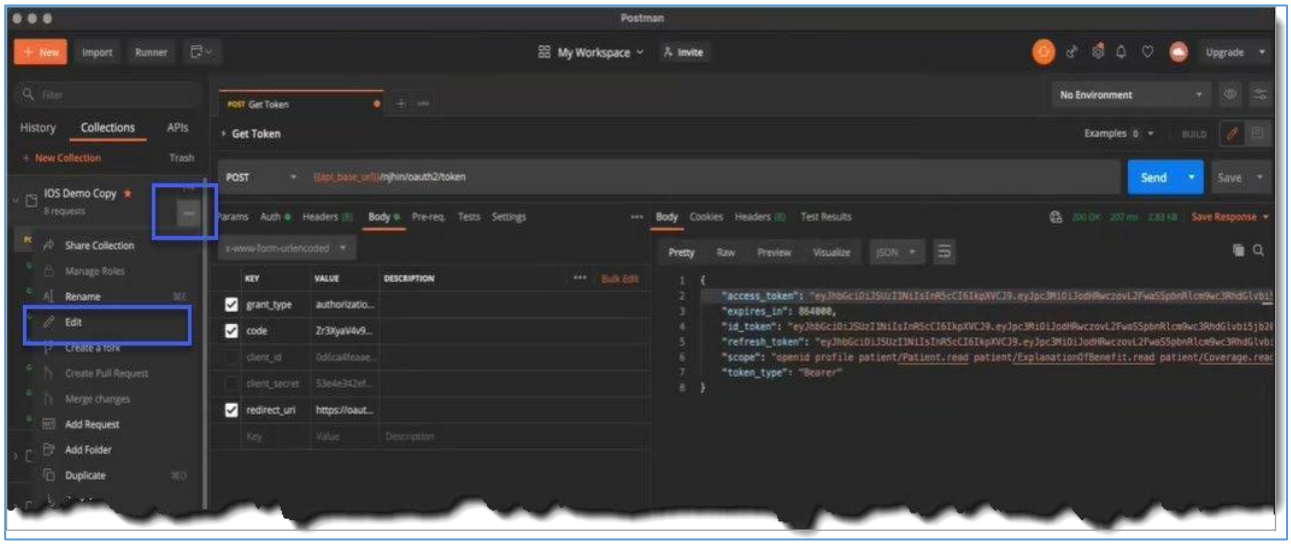

Figure 28. "More" and "Edit" Options in Navigation Menu

6. On the **Edit Collection** form, the user should click on the **Authorization** tab and paste the token in the **Token** field, and then click **Update,** as shown in **Figure 29**.

   Note: The **Type** should be set to **Bearer Token**.

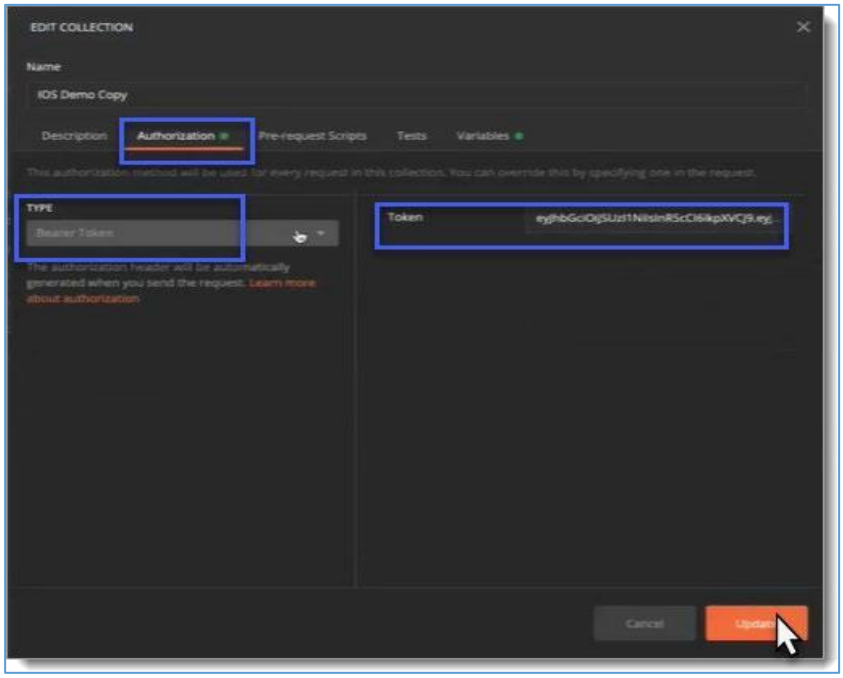

Figure 29. Authorization Tab with Token Field Filled In

3.6 Testing a Third-Party Application Connection to the InterOp Station® for Development

Once a user has successfully connected their application with the InterOp Station® in the development environment, the user will be able to test whether they will be able to connect and test data using the following information.

1. On the left side menu, the user will click **Get Patient Data** to open the **Get Patient Data** form.
2. On the resulting screen the user will select the **Auth** tab, and then select **Inherit Auth from Parent** in the **Type** dropdown menu, as shown in **Figure 30.**

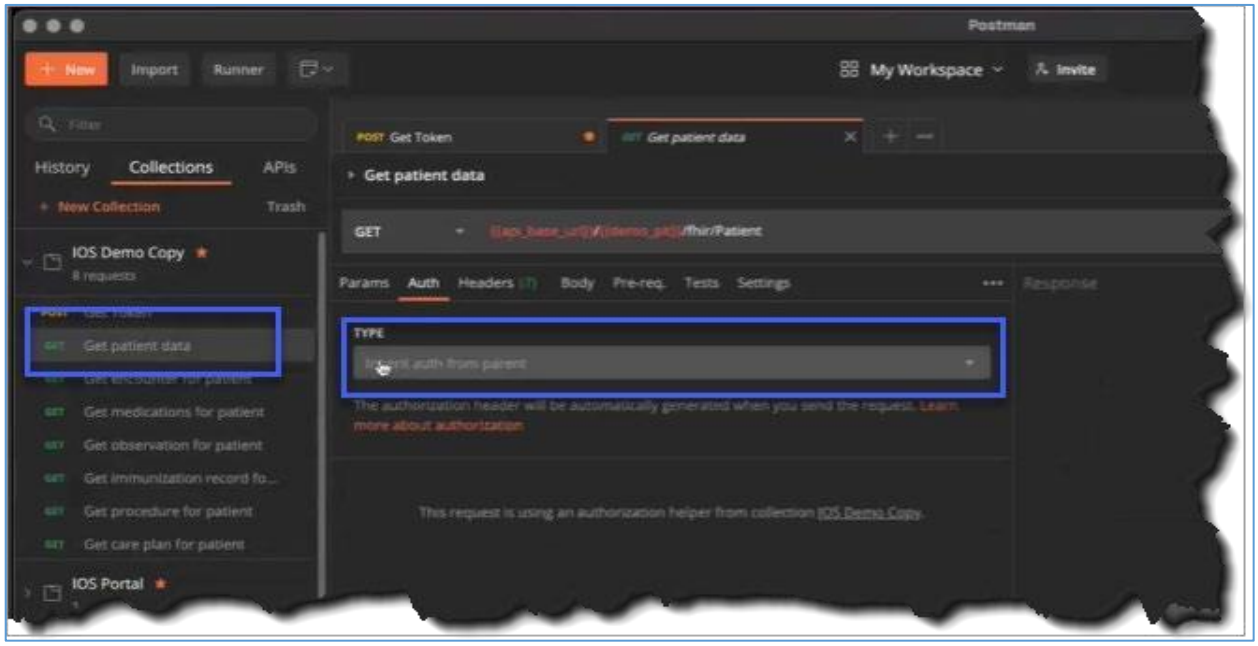

Figure 30. Auth Tab Navigation and Entered Values

3. The user will click on the **More** button for options to manage their collection.
4. From the resulting options, the user will click on **Edit** and the **Edit Collection** form will appear, as shown in **Figure 31**.
   Note: Confirm **Bearer Token** is the selected token type on the Auth tab.

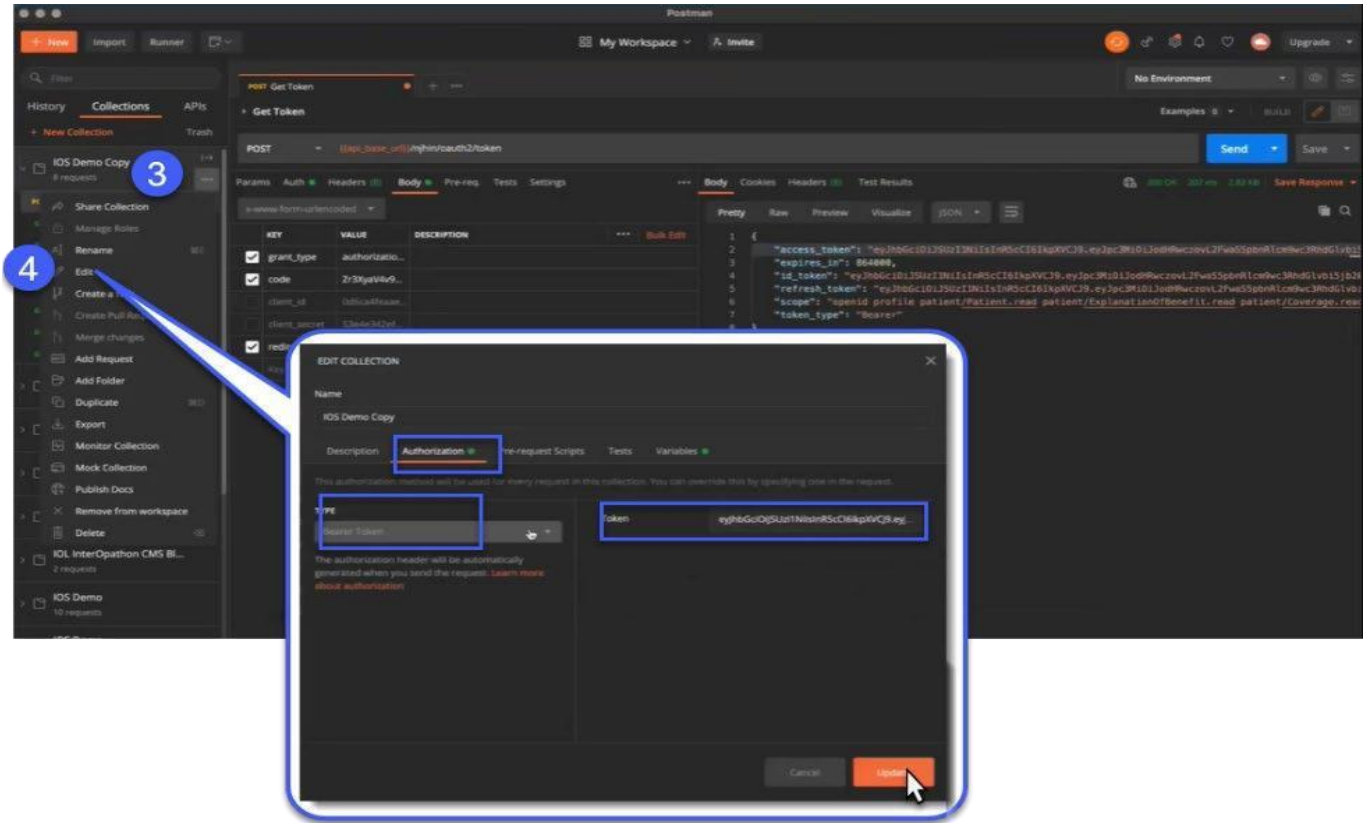

Figure 31. Edit Collection Navigation

5. From here, the user will click **Get Patient Data** on the left side menu.
6. On the **Get Patient Data** form, the user will click **Send** to retrieve patient data, as shown in **Figure 32**.

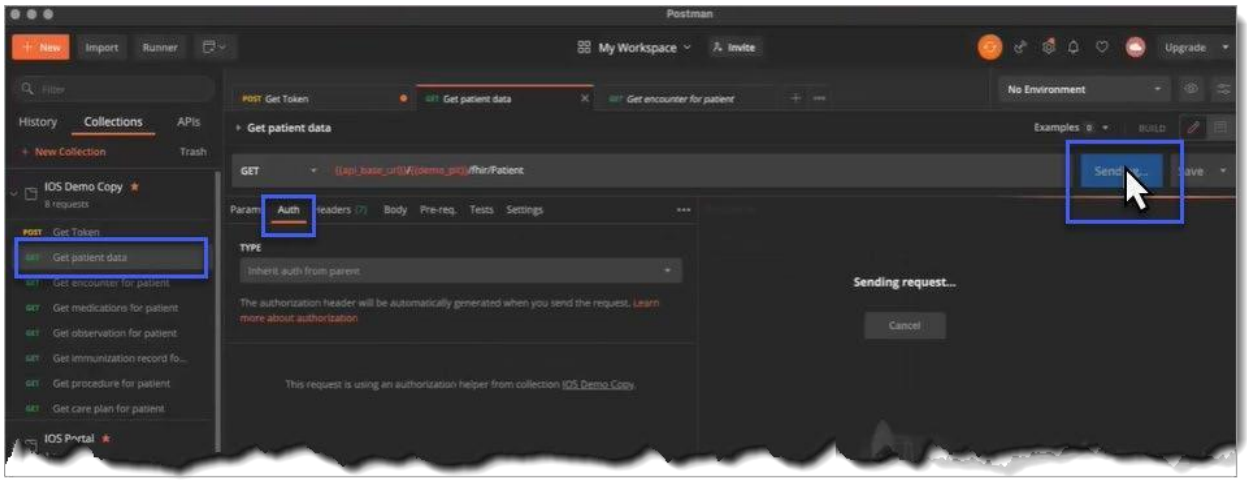

Figure 32. UI Navigation to Retrieve Patient Data

7. On the resulting screen, patient data will be displayed in the **Response** section of the **Get Patient Data** form, as shown in **Figure 33**.

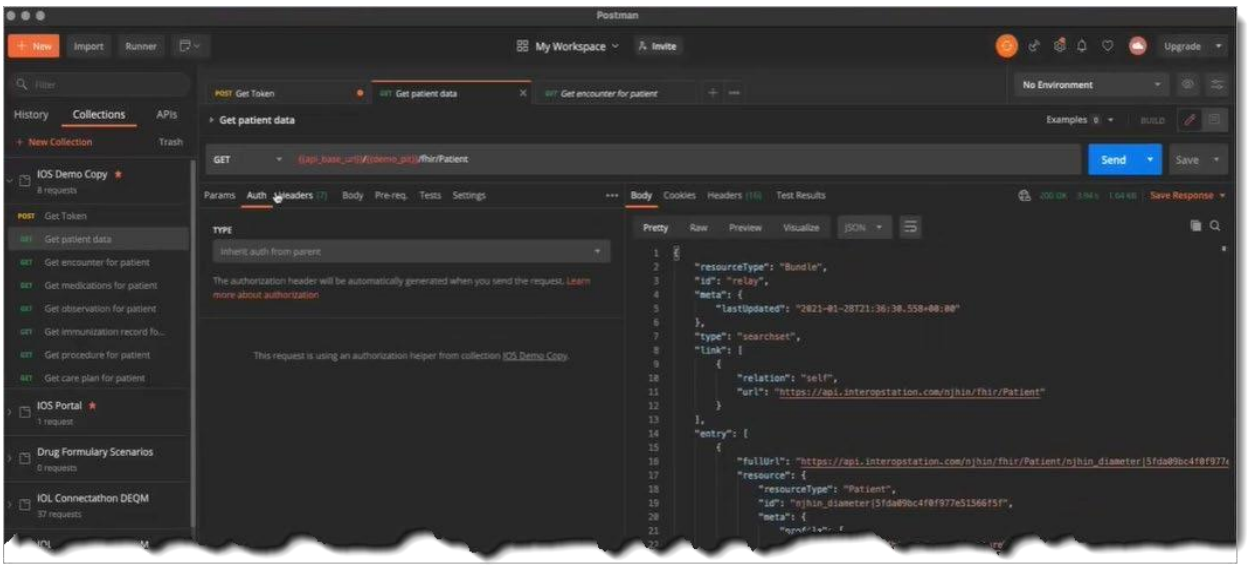

Figure 33. Patient Data Display

8. The user should repeat **Steps 1-7** to retrieve other patient data categories from the collection.

3.7 Third-Party Application Connections for Production Clients in the InterOp Station®

In addition to connecting applications in the development environment, a user may also register and connect applications in the production environment. This process has some similarities with the previous process, but there are some notable differences. The following two sections will describe the registration and connection process.

Caution! When a user registers an application in production, they will be accessing HIPAA-protected data.

3.7.1 Registering a Third-Party App for Production Clients

After a user successfully uploads their security attestation and privacy policy, they can navigate to the **Application Dashboard** and proceed through the following steps to register their application in production:

1. Users must first click **Register in Production**, as shown in **Figure 34**.

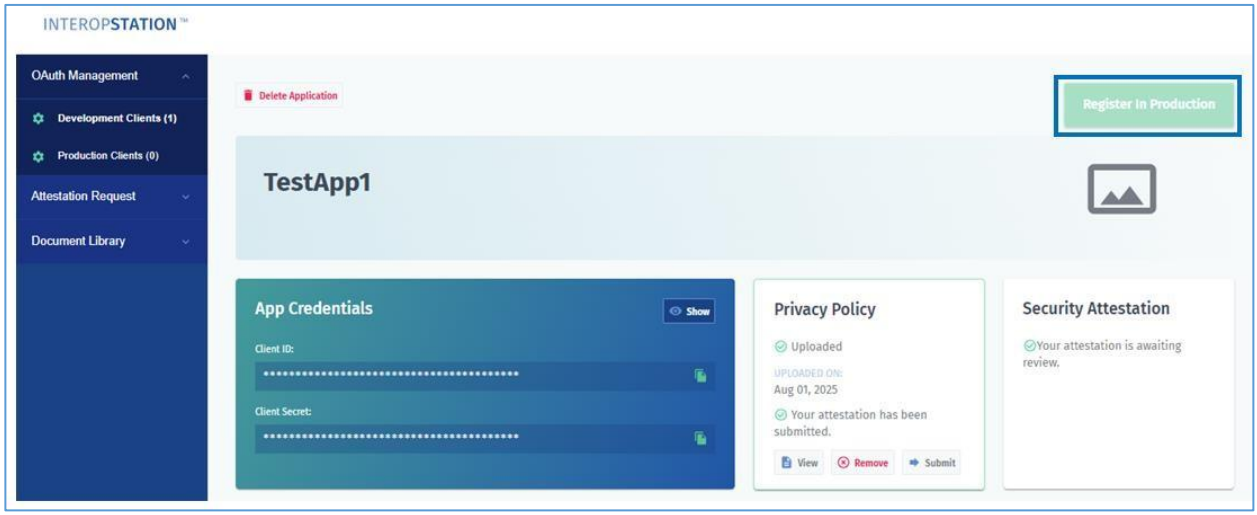

Figure 34. "Register in Production" Option Location in Application Dashboard

2. On the resulting **Register Your Application in Production** form, the user will need to type the **Callback URLS/Redirect URIs** for each application, as shown in **Figure 35**.

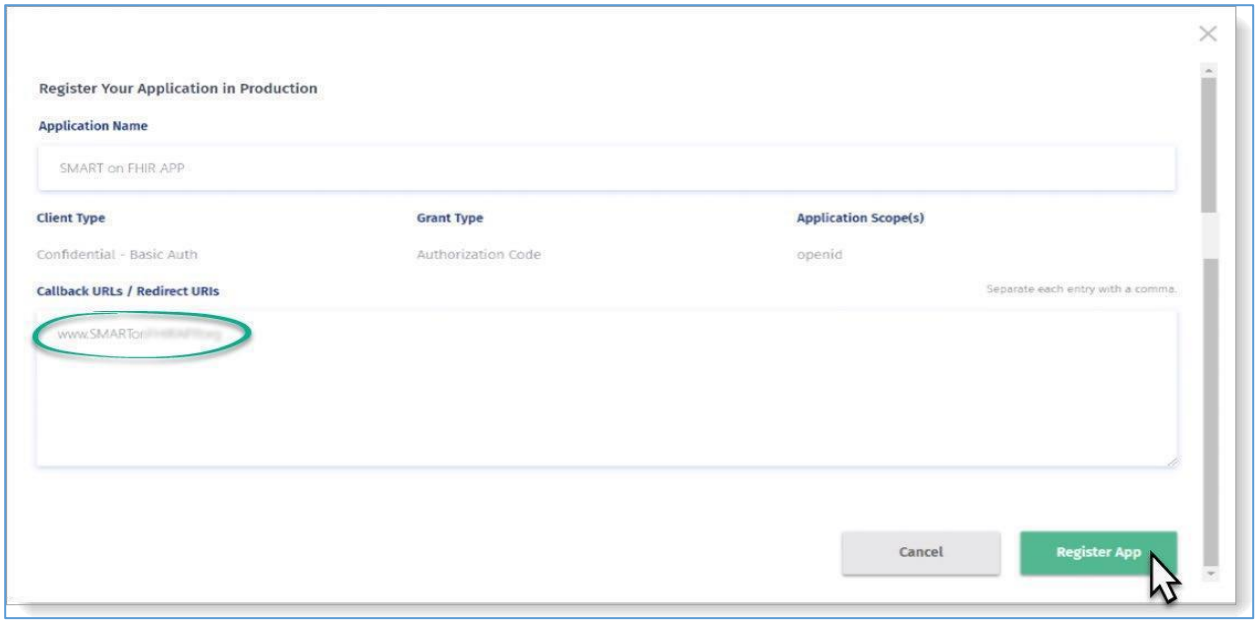

Figure 35. Register Your Application in Production Form and Entries

3. Once all fields have been completed, the user will click the **Register App** option, as shown in **Figure 35**.

4. In **OAuth Management**, the user will have the following options in the **Production Clients** option, as shown in **Figure 36**.

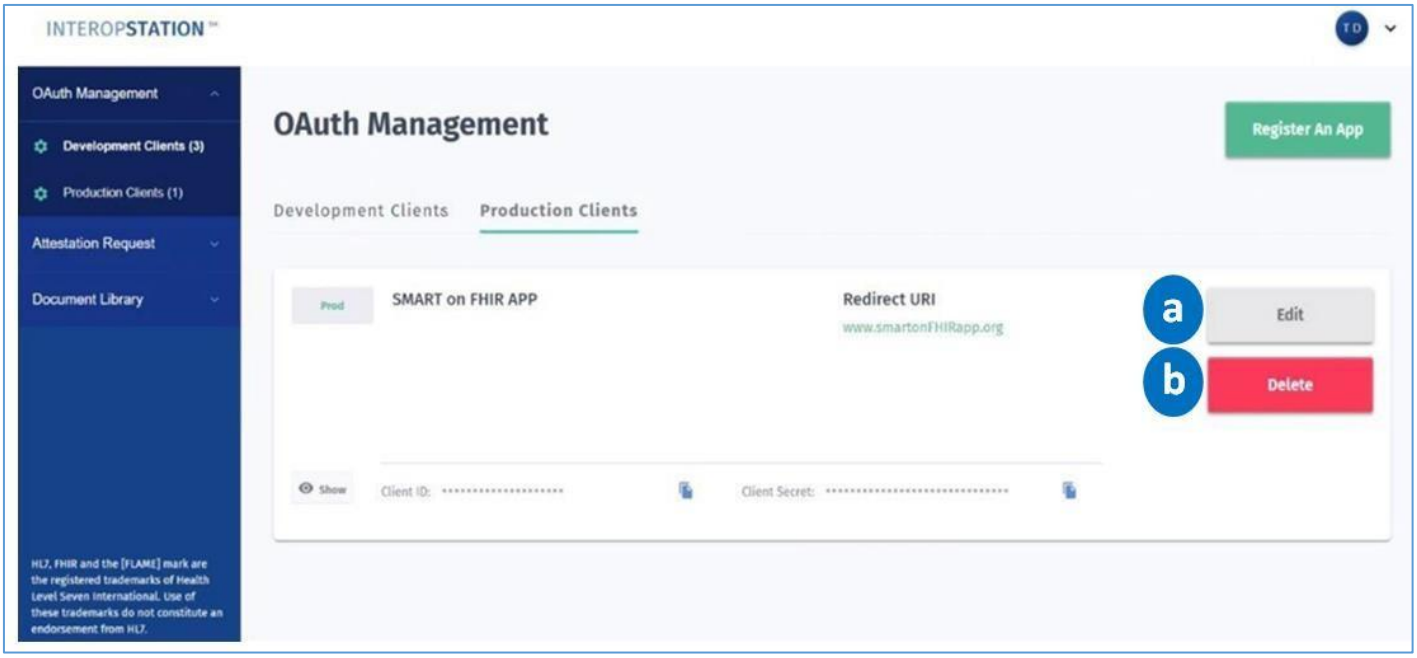

Figure 36. OAuth Management Screen and Production App Options

a) Using the **Edit** tool as noted in the Development Clients section above, the user can make updates to their registered application.

b) Using the **Delete** tool, the user can remove an application from production. If they choose to delete their sandbox version, they must navigate to the **Development Clients** tab and delete it there as well.

Tip: A best practice is to query test records to confirm a user's application is registered correctly. They can then use the Postman App for querying records. To query the test payer record, they must have an associated test patient record.

5. When the **Are you sure you want to delete this application?** message displays, as shown in **Figure 37**, the user will click the **Delete** option to remove their application from production.

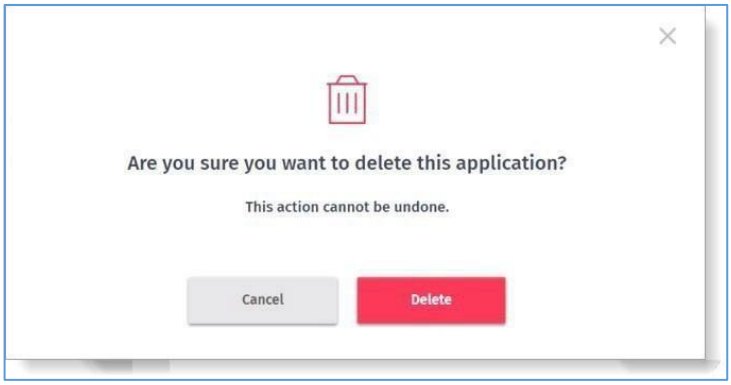

Figure 37. Application Deletion Confirmation Pop-Up

3.7.2 Testing a Third-Party App Connection in Production

3.7.2.1 Patient Access API

To test an application's connection in production, users must follow the same steps as outlined in Section 3.6 Testing a third-party app Connection to InterOp Station® for Development.

However, instead of a patient name and password as shown in **Step 2**, they will need to use the credentials for a synthetic user.

Note: Production testing uses credentials for a synthetic user. The development environment will only connect to Development client third party applications in the InterOp Station®. The production environments, such as Blue Cross Blue Shield of Michigan (BCBSM), will only connect to production client third-party applications in the InterOp Station®.

The synthetic user credentials for testing are:

- **Environment:** Development
- **Username:** MarianBenton
- **Password:** [Autofilled in UI]

Note: If the user needs test credentials for the production environment, they should contact the MiHIN Help Desk at help@mihin.org.

3.7.2.2 Provider Directory API

Third-party app developers should use the following provider directory endpoints to connect to the InterOp Station® production environment:

- https://api.interopstation.com/[tenant]/fhir/Endpoint
- https://api.interopstation.com/[tenant]/fhir/HealthcareService
- https://api.interopstation.com/[tenant]/fhir/InsurancePlan
- https://api.interopstation.com/[tenant]/fhir/Location
- https://api.interopstation.com/[tenant]/fhir/OrganizationAffiliation
- https://api.interopstation.com/[tenant]/fhir/Organization
- https://api.interopstation.com/[tenant]/fhir/PractitionerRole
- https://api.interopstation.com/[tenant]/fhir/Practitioner

Where [tenant] is the tenant/payer that is being queried.

Users should refer to the following table for the tenant's name for each customer.

Customer Name	Tenant
Blue Cross Blue Shield of Michigan	bcbsm
McLaren Health Plan	mhp
McLaren MDwise	mdw
Michigan Department of Health and Human Services	mdhhs

4. Production Support

	Severity Levels			
	1	***2***	***3***	***4***
Description	***Critical Impact/ System Down:*** Business critical software is down or critical interface has failed. The issue is impacting all production systems, causing all participating organizations' or other organizations' ability to	***Significant Business Impact:*** Software component severely restricted. Entire organization is unable to continue business functions, causing all communications and transfer of messages to be halted.	**Partial Failure or Downtime:** Program is useable and less significant features unavailable. The service is online, though may not working as intended or may not currently working as intended or may not currently be accessible, though other systems are currently available.	**Minimal Business:** A non-critical software component is malfunctioning, causing minimal impact, or a test system is down.

	function to be unusable.			
Example	All messages to and from MiHIN are unable to be sent and received, let alone tracked	MiHIN cannot communication (send or receive) messages between single or multiple participating organizations, but can still successfully communicate with other organizations.	Messages are lost in transit; messages can be received but not sent.	Additional feature requested.
Primary Initiation Method	***Phone:*** (517) 336-1430	***Phone:*** (517) 336-1430	Web form at http://mihin.org/requesthelp	Web form at http://mihin.org/requesthelp
Secondary Initiation Method	Web form at http://mihin.org/requesthelp	Web form at http://mihin.org/requesthelp	Email to help@mihin.org	Email to help@mihin.org
Tertiary Initiation Method	Email to help@mihin.org	Email to help@mihin.org	N/A	N/A
Initial Response	Within 2 hours	Within 2 hours	1 business day	1 business day
Resolution Goal	24 hours	24 hours	3 business days	7 business days

A list of common questions regarding the (Name of Data exchange solution) data exchange solution can be found at:

(Link to the MiHIN webpage that contains documentation supporting this data exchange solution)

If you have questions, please contact the MiHIN Help Desk:

- www.mihin.org/requesthelp
- Phone: (517) 336-1430
- Monday – Friday 8:00 AM – 5:00 PM (Eastern)

5. Appendices

5.1 Appendix A – Frequently Asked Questions

Q: Where is the Refresh Token?

A: The refresh token is located below the access token in the response. This token expires after 30 minutes. The user can obtain another access token using the same refresh token for its duration.

Q: What is an Access Token?

A: An access token expires 5 minutes after the time it was issued. Thereafter, the user must obtain a new access token (using the same refresh token) once it expires.

Q: What is a Capability Statement?

A: The types of resources available can be found in metadata for the respective tenant when searched for the meta data in FHIR™. Below is the sample query that can be used to do the same: https://api.interopstation.com/{tenant}/fhir/metadata

The general capability statement is also located at: https://mihin.org/wp-content/uploads/2021/04/IOSCapabilityStatementtypical.zip

Q: What are the requirements of Nonce being a unique value?

A: Nonce is auto generated and nothing needs to be done.

Q: What is the required "Response_mode=query" used for?

A: This is set to get the response back as a query.

Q: Is the patient ID in the Authorization Token for the response?

A: Yes.

Q: How are we able to get the FHIR patient ID and patient data without an ID?

A: A third-party application cannot have direct access to the patient data without an authorization token, which is prompted by the member/enrollee. Once an authorization token is obtained, it already has the patient ID in it; it gives back the respective data when queried. There is no need to insert the patient ID separately.

Q: Why don't all organization resources have Type 2 NPIs?

A: In the InterOp Station® Provider Directory, organizations have an OID (Object Identifier) as their primary and unique identifiers. Hence, NPI is not a required field here. MiHIN suggests using an OID when querying for an organization.

Q: Does MiHIN support Bulk API Queries?

A: Although Bulk API Queries are on MiHIN's road map, they are not currently supported by the InterOp Station®.

5.2 Appendix B – Debugging and Validating an OAuth Connection

Here is an example of the URL after the parameters above have been updated:

```
https://api.interopstation.com/dev1/oauth2/authorize?
redirect_uri=https://oauthdebugger.com/debug
&client_id=client_id&scope=openid profile patient/Patient.read
patient/ExplanationOfBenefit.read patient/Encounter.read
patient/Procedure.read patient/Observation.read patient/Condition.read
patient/Immunization.read patient/DiagnosticReport.read
patient/ServiceRequest.read&state=test&nonce=kbbuk9mhz2n
&response_type=code&response_mode=query
```

Note: dev1 is an example tenant. Users should the tenant they are targeting, if not dev1.

6. Acronyms and Abbreviations

ACRONYM	Meaning
API	Application Program Interface
App	Application
InterOp	InterOp Station®
FHIR	Fast Healthcare Interoperability Resources
MiHIN	Michigan Health Information Network
NPI	National Provider Identifier

OAuth	Open Authorization
OID	Object Identifier
SMART	Substituable Medical Applications, Reusable Technologies
PHI	Protected Health Information
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

7. Definitions

Access Token. A type of security token used to grant an application (like a SMART app) permission to access healthcare data stored in a FHIR server.

Application. A program or piece of software designed and written to fulfill a particular purpose of the user.

Application Attestation. The page in InterOp Station® where a user answers the prompted questions and inputs their application information to determine if their application is Production ready.

Application Programming Interface (API). A set of rules and protocols that allow software applications to communicate with each other.

Authorization Token. A type of OAuth 2.0 token used in the context of SMART on FHIR to authorize an application to access healthcare data from a FHIR server. This token serves as proof that the application has been authorized by the user to access their healthcare data, ensuring security and privacy in the process.

Bearer Token. Specific type of OAuth 2.0 access token used to authorize an application to access healthcare data from a FHIR server. The bearer token is the primary means for proving that the app has been authorized to access protected health information (PHI) in a FHIR server.

Callback Uniform Resource Identifier (URI). A specific URL used in the OAuth 2.0 authorization flow. This URL is where the authorization server will send the authorization code or tokens (such as the access token and refresh token) after the user grants permission for an app to access their healthcare data.

Capability Statement. The types of resources available can be found in metadata for the respective tenant when searching for the meta data in FHIR.

Electronic Address. A string that identifies the transport protocol and end point address for communicating electronically with a recipient. A recipient may be a person, organization, or other entity that has designated the electronic address as the point at which it will receive electronic messages. Examples of an electronic address include a secure email address (Direct via secure SMTP) or secure URL (SOAP / XDR / REST / FHIR). Communication with an electronic address may require a digital certificate or participation in a trust bundle.

Electronic Medical Record or Electronic Health Record (EMR/EHR). A digital version of a patient's paper medical chart.

Electronic Service Information (ESI). All information necessary to define an electronic destination's ability to receive and use a specific type of information (e.g., discharge summary, patient summary, laboratory report, or query for patient/provider/healthcare data). ESI may include the type of information (e.g. patient summary or query), the destination's electronic address, the messaging framework supported (e.g., SMTP, HTTP/SOAP, XDR, REST, FHIR), security information supported or required (e.g., digital certificate), and specific payload definitions (e.g., CCD C32 V2.5). In addition, ESI may include labels that help identify the type of recipient (e.g., medical record departments).

Environment. The infrastructure, hardware, software, and systems that a business relies on every day while using information technology.

End Point. An instance of an electronic address or ESI.

Fast Healthcare Interoperability Resources (FHIR). A standard for exchanging health information between systems. It is an application programming interface (API) that uses internet standards to represent and share electronic health records (EHR).

Health Information. Any information, including genetic information, whether oral or recorded in any form or medium, that (a) is created or received by a health

provider, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Information Network (HIN). An organization or group of organizations responsible for coordinating the exchange of protected health information (PHI) in a region, state, or nationally.

InterOp Station®. Product that intakes a wide range of claims and clinical data types from various sources and converts them to FHIR resources housed in a cohesive, secure cloud environment. From there, a patient may request their own data using a third-party app of their choice. Authorized payers may also exchange historical data with other payers. The InterOp Station® provides a foundational platform for housing all clinical and claims data to be made available in one format, representing a giant leap forward in health information exchange and interoperability.

InterOp Station® Provider Directory. Service that provides a centralized listing of healthcare providers, their credentials, and other relevant details. This directory enables organizations and applications to search, retrieve, and manage information about healthcare professionals, facilities, and organizations.

MELD™. An open-source healthcare sandbox populated with fully synthetic FHIR® data. It provides a safe space for creation, development, testing and validation of healthcare applications and APIs. The fully synthetic data existing in MELD™ allows for users to "fail forward" when working with the data, as there is no risk of PHI or PII exposure.

Michigan Health Information Network Shared Services. The state-designated HIE, serving as a consolidated, statewide, public-private partnership.

MiHIN Infrastructure Service. Certain services that are shared by numerous use cases. MiHIN infrastructure services include, but are not limited to, Active Care Relationship Service (ACRS), Health Directory, Statewide Consumer Directory (SCD), and the Medical Information Direct Gateway (MIGateway®).

MiHIN Services. The MiHIN infrastructure services and additional services and functionality provided by MiHIN allowing the participating organizations to send,

receive, find, or use information to or from MiHIN as further set forth in an exhibit.

National Provider Identifier (NPI). A 10-digit number that identifies health care providers in administrative and financial transactions.

Object Identifier (OID). A globally unique ISO (International Organization for Standardization) identifier. This identifier is required to uniquely identify HIE participants.

Open Authorization (OAuth). An open standard that allows users to grant third-party access to their information without sharing their passwords.

Patient Data. Any data about a patient or a consumer that is electronically filed in a participating organization or participating organization participant's systems or repositories. The data may contain protected health information (PHI), personal credit information (PCI), and/or personal identifiable information (PII).

Postman. Popular API testing tool that allows developers to send requests to APIs, view responses, and automate tests for API endpoints. It is widely used for interacting with RESTful APIs, making it a useful tool for developers working with APIs like FHIR (Fast Healthcare Interoperability Resources).

Protected Health Information (PHI). Under HIPAA, PHI is an individual's health, treatment, and payment information, and any further information maintained in the same designated record set that could identify the individual or be used with other information in the record set to identify the individual.

Privacy Policy. The page in the InterOp Station® where users answer the prompted questions and input their application information to determine if their application is Production ready from a policy standard.

Redirect Uniform Resource Identifier (URI). URI to which the authorization server sends the authorization code (or tokens) after the user has authenticated and granted the application permission to access their data. used during the OAuth 2.0 authorization flow when the app is trying to access protected healthcare data from a FHIR server.

Refresh Token. A special token used in the OAuth 2.0 authentication and authorization framework. It allows an application to obtain a new access token without requiring the user to reauthenticate. Refresh tokens are often used

when access tokens expire, enabling a seamless user experience by allowing the app to keep access to the protected resources without requiring the user to log in again.

Security Attestation. The page in the InterOp Station® where a user answers the prompted questions and inputs their application information to determine if their application is Production ready, interchangeable term with "Application Attestation."

Substituable Medical Applications, Reusable Technologies (SMART). Provides a framework for building healthcare applications that can work across different EHRs and healthcare systems. The **SMART app** in the context of FHIR (Fast Healthcare Interoperability Resources) refers to a type of healthcare application that interacts with FHIR-based systems using the SMART on FHIR specification.

User Interface (UI). The means by which the user and a computer system interact, in particular the use of input devices and software.

Uniform Resource Locator (URL). A unique address for a resource on the internet. URLs are used to locate web pages, images, videos, and other files.

Uniform Resource Identifier (URI). A formal system for identifying resources and consisting of two types: URLs (Uniform Resource Locator) and URNs (Uniform Resource Name)