



# InterOp Station Third-party Developer Portal User Guide

---

## Contents

Purpose of InterOp Station Third-party Portal User Guide .....	2
Creating an InterOp Station Third-party Developer Portal Account.....	3
Logon issues after creating an account .....	4
Connecting a Third-party Developer App to InterOp Station .....	5
Welcome Page Navigation .....	5
Register a SMART Application with the OAuth API tool .....	6
Navigating the Application Dashboard Page .....	7
Security Attestation Requirement .....	8
Submitting a Security Attestation .....	8
Upload a Privacy Policy .....	10
Privacy Policy Attestation .....	11
How to Debug and Validate an OAuth Connection .....	11
Connecting to InterOp Station .....	14
Testing a Third-party App Connection to InterOp Station for Development .....	16
Registering a Third-Party App for Production Clients in InterOp Station .....	18
Testing a Third-Party App Connection in InterOp Station Production .....	20





# InterOp Station Third-party Developer Portal User Guide

---

## Purpose of InterOp Station Third-party Portal User Guide

The purpose of this guide is to assist Third-party developers with registering an Application (App) as a client of the InterOp Station. This guide targets activity by the following users.

- Third-Party App developers that may have issues involved with connecting, testing, and adding their privacy policy and security attestation documents.

**Note:** *Third-party Developers can contact the MiHIN helpdesk for assistance by email at [help@mihin.org](mailto:help@mihin.org).*

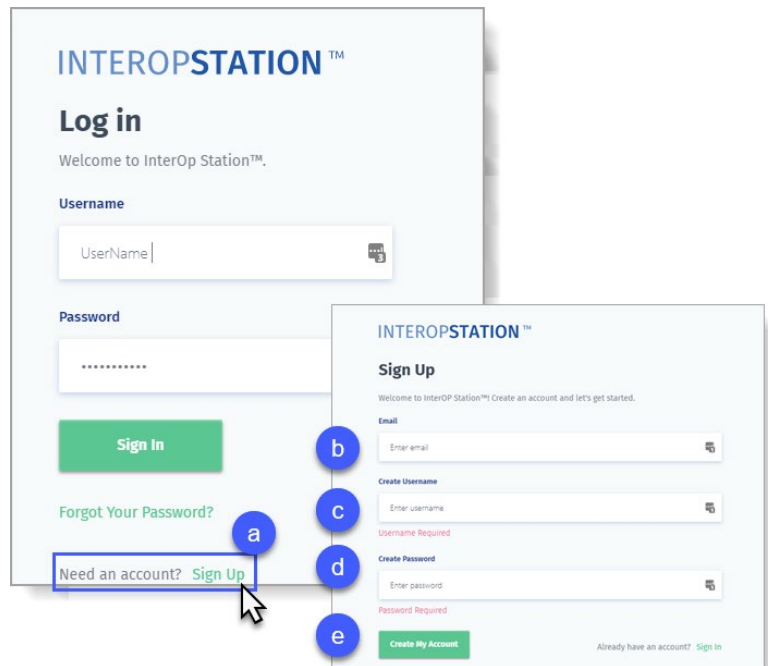
If while connecting your App you encounter any of the issues below, contact the [MiHIN Helpdesk](#).

- Can't submit a security attestation.
- Can't get credentials in development.
- Tests are failing in development.
- Can't get credentials for production.
- Tests are failing in production.



## Creating an InterOp Station Third-party Developer Portal Account

1. Navigate to <https://www.interopstation.com/login>
2. When your **Log in** menu displays:
  - a) Choose **Sign Up**.



- b) Type your **Email** address.
- c) Create and type your **Username**.
- d) Create and type your **Password** using the password policy as shown here.

Minimum password length	8
Password policy	uppercase letters, lowercase letters, special characters, numbers
User sign ups allowed?	Users can sign themselves up

- e) Then choose **Create My Account**.



3. An email will be sent to the email address provided to confirm your account.
4. Once confirmed the Third-party Developer can log on with the Username and password created.
5. Click **I Accept** to agree to the **InterOp Station Terms of Service** to proceed.

**Note:** Clicking **Cancel** returns you to the logon window.

### InterOp Station Terms of Service

**Effective: November 1, 2020**

These InterOp Station Terms of Service (the "Terms") describe your rights and responsibilities when using our simulated healthcare network populated with the Personas (the "Platform"). "Personas" means the proprietary highly realistic, clinically relevant, synthetic patient data provided by Interoperability Institute LLC and its affiliates ("us", "we", or "our"). The Platform includes any software, programs, documentation, tools, internet-based services, add-on components, and any updates (including software maintenance, service information, help content, bug fixes or maintenance releases) provided to you by us, directly or indirectly.

These Terms contain nine sections summarized below. The summary is for reference and convenience only and do not limit the scope of each section. Please read these Terms carefully as they apply to your use of the Platform and form a binding agreement between you and us. If you are entering into these Terms as part of an entity or organization, please make sure you have the necessary authority to enter into these Terms before proceeding. Any actions or omissions by your employees, contractors, agents, volunteers, or customers who are authorized by you to use the Platform ("Authorized Users") will be deemed actions by you. You represent and warrant that each Authorized User has read and will comply with these Terms and any instruction issued by us and our licensors with respect to the use of the Platform.

Section	Summary
<b>The Platform</b>	You're granted a limited right to use the Platform as described in these Terms. This section sets for the basic rules you must follow when using the Platform.
<b>Your Responsibilities</b>	This section describes your responsibilities when using the Platform under these Terms.
<b>Commercial Terms</b>	You're responsible for payment. We're responsible for communicating our fees to you clearly and accurately and letting you know in advance of any price changes. You may terminate these Terms at any time.
<b>Your Content &amp; User Content</b>	You own and control Your Content, but you allow us certain rights to it so that we can provide the Platform. We have the right to remove Your Content or suspend or terminate access to the Platform if we need to.
<b>Private Repositories</b>	You may have access to private repositories. We treat the content of private repositories as confidential, and we only access it with your consent or if required for security reasons.
<b>Third Party Applications</b>	You need to follow certain rules if you create an application to use in connection with the Platform.
<b>Disclaimer of Warranties</b>	We provide the Platform as is and make no promises or guarantees about the Platform. Please read this section carefully; you should understand what to expect.
<b>Risk Allocation Provisions</b>	You are fully responsible to us for your use of the Platform. If you harm someone else, or get into a dispute with someone else, we will not be involved. We will not be liable for certain damages or losses resulting from your use or inability to use the Platform or otherwise under these Terms. Please read this section carefully. It limits our obligations to you.
<b>General Provisions</b>	Please see this section for general legal details, including those related to dispute resolution.

## Logon issues after creating an account

If a Third-party Developer has followed the steps appropriately and logon still fails, refer to the [MiHIN Helpdesk](#).



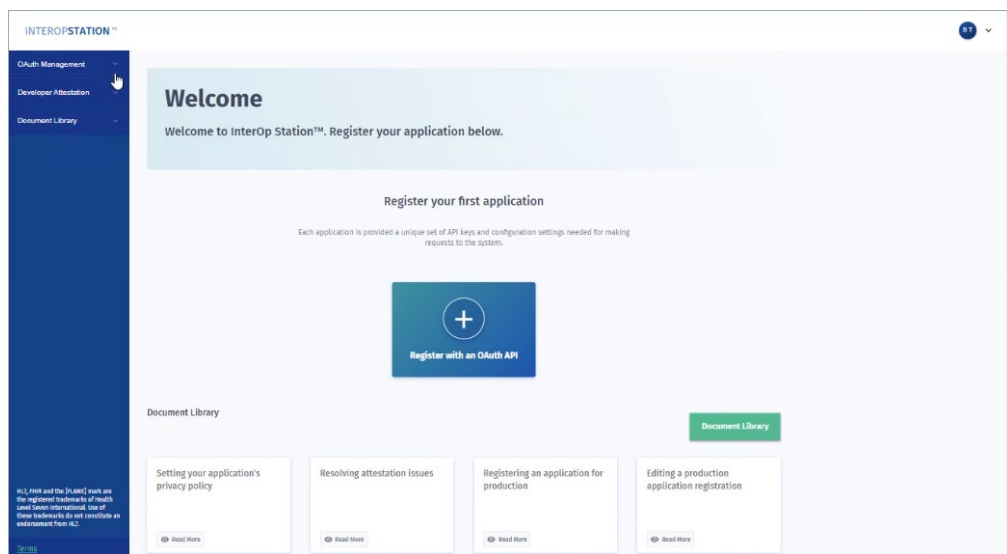
## Connecting a Third-party Developer App to InterOp Station

### Welcome Page Navigation

The Welcome page allows you to register your App and view supporting information from the Document Library.

When you click **INTEROPSTATION™** located above the Sidebar Navigation Menu you will return to the Welcome page.

The left **Sidebar Navigation** menu provides links to view your **OAuth Management** including your Application Dashboard, **Developer Attestation**, and the **Document Library**. Choosing one of these links from any page will redirect you.

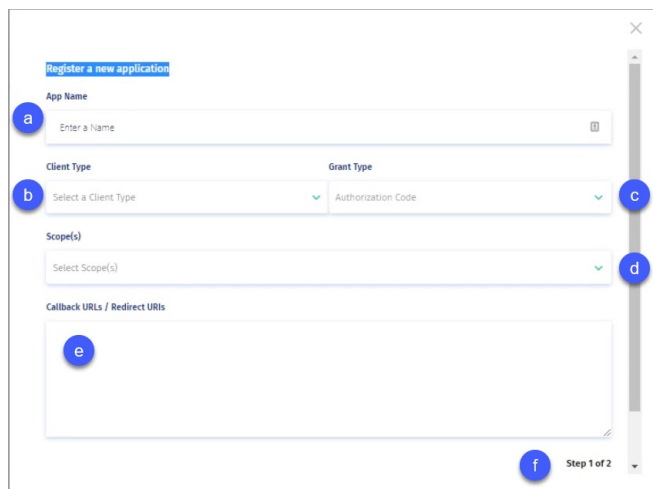


## Register a SMART Application with the OAuth API tool

In the OAuth Credentials section of the Welcome page the **Register with an OAuth API** tool displays and when you choose this tool you will be redirected to the **Register a New Application** page.

1. Using the **Register a new application** form, enter the required information as follows:
  - a. Type the **App Name** which identifies your SMART App.
  - b. Use your **Client Type** arrow to choose how you are configuring calls to the token endpoint. The Client ID (username) and secret (password) generated by IOL will be passed to the endpoint via this selection. **Confidential-Basic Auth** is your default and should work unless you know that another form of authentication is used by the App.
  - c. Use your **Grant Type** arrow to choose how your app will request and receive the authorization token.

- d. HL7 identifies the allowed scopes for your resources. Choose your **Scope(s)** arrow to scroll to and choose the scope of resources you are requesting for access e.g., CARIN Blue Button® FHIR Smart authorization. For more information on allowed Scopes visit <http://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context/>
- e. Type your **Callback URIs / Redirect URI** for the application you are connecting.



The screenshot shows a web form titled "Register a new application". It contains several input fields and dropdown menus. Callouts a-f are placed on the form: 'a' points to the "App Name" input field; 'b' points to the "Client Type" dropdown; 'c' points to the "Grant Type" dropdown; 'd' points to the "Scope(s)" dropdown; 'e' points to the "Callback URIs / Redirect URIs" text area; and 'f' points to the "Next" button at the bottom right. The form is labeled "Step 1 of 2".

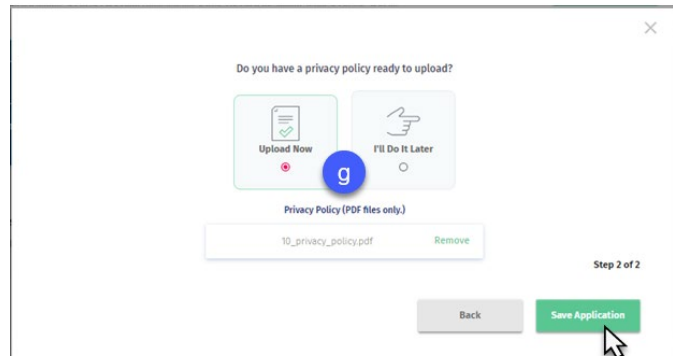
**Note:** To test this application with the *oauthdebugger.com*, list your application's redirect URI and *oauthdebugger.com/debug* here separated by commas  
EX 'https://yourapphere.com/, https://oauthdebugger.com/debug'

- f. Click **Next** to complete **Step 1 of 2**.



- g. The **Step 2 of 2** pop-up prompts you to upload a PDF of your Privacy Policy. Choose **Upload Now** if your privacy policy is ready for upload and then click **Save Application**. The App is now connected with your policy.

**Note:** *If you are not yet ready to upload your policy, choose **I'll Do It Later** and then click **Save Application**. However, your privacy policy must be uploaded before your App can go to Production.*

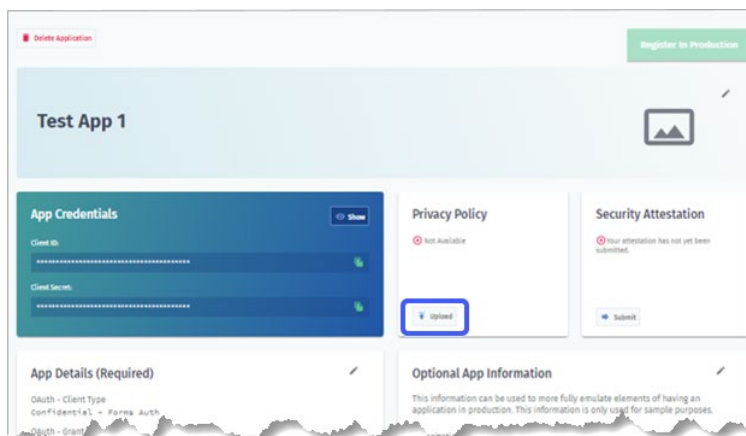


## Navigating the Application Dashboard Page

Once the application has been registered with the OAuth API the Application Dashboard page will display. From this page you can:

- Modify the Application Details you selected during the registration process.
- Upload and review your Privacy Policies.
- Complete or review your Security Attestations.
- Add Optional Application Information such as your organization website, a description of the application, a point of contact and an email for contact.
- Obtain your App credentials e.g., Client ID and Client Secret, to use on the application side 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.

**Note:** You can navigate back to this page at any time via **OAuth Management** on the sidebar Navigation Menu and then choose **Edit**

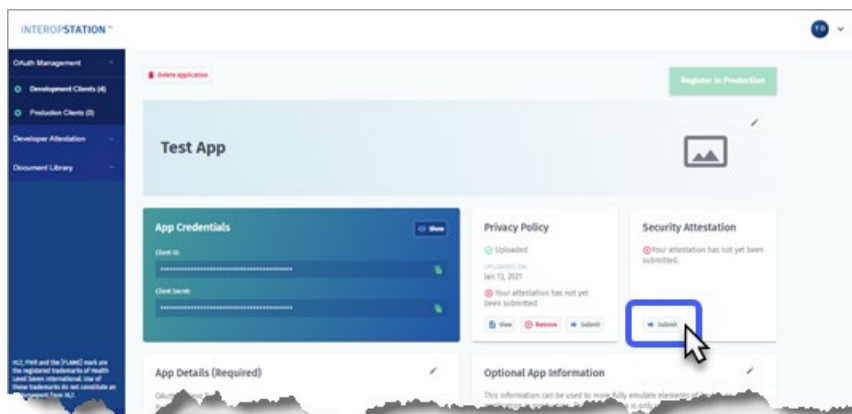


## Security Attestation Requirement

Developers are required to submit a Security Attestation for their App. An automated MiHIN Helpdesk ticket is generated after a Security Attestation review is completed. 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.

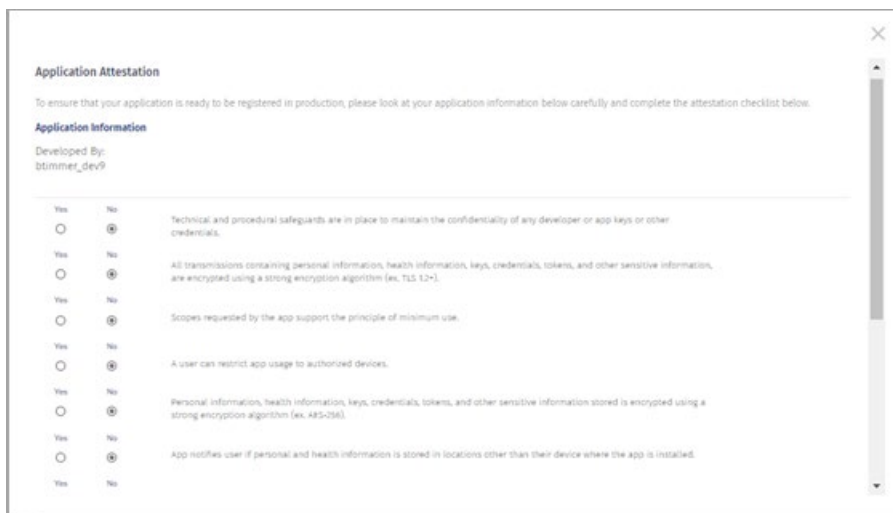
### Submitting a Security Attestation

1. Security Attestations can be submitted from the Application Dashboard page by choosing **Submit** located on your **Security Attestation** tool.





2. When the **Application Attestation** page displays, respond to each question and then click **Submit** to send to the MiHIN Security Team for review.



**Application Attestation**

To ensure that your application is ready to be registered in production, please look at your application information below carefully and complete the attestation checklist below.

**Application Information**

Developed By:  
btimmer\_dev9

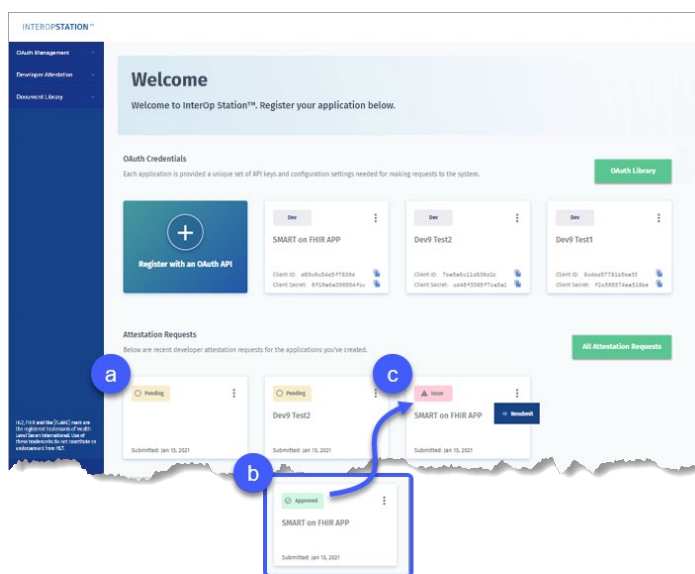
Yes	No	
<input type="radio"/>	<input checked="" type="radio"/>	Technical and procedural safeguards are in place to maintain the confidentiality of any developer or app keys or other credentials.
<input type="radio"/>	<input checked="" type="radio"/>	All transmissions containing personal information, health information, keys, credentials, tokens, and other sensitive information, are encrypted using a strong encryption algorithm (ex. TLS 1.2+).
<input type="radio"/>	<input checked="" type="radio"/>	Scopes requested by the app support the principle of minimum use.
<input type="radio"/>	<input checked="" type="radio"/>	A user can restrict app usage to authorized devices.
<input type="radio"/>	<input checked="" type="radio"/>	Personal information, health information, keys, credentials, tokens, and other sensitive information stored is encrypted using a strong encryption algorithm (ex. AES-256).
<input type="radio"/>	<input checked="" type="radio"/>	App notifies user if personal and health information is stored in locations other than their device where the app is installed.
<input type="radio"/>	<input checked="" type="radio"/>	
<input type="radio"/>	<input checked="" type="radio"/>	

3. Navigate to and choose your **Security Attestation** which will be like the example shown below.

4. The status of your Security Attestation can be found on the **Welcome** page **Attestation Requests** dashboard or by clicking Attestation Requests located on your Sidebar Navigation Menu.

**Note:** The Security Attestation must be in PDF format. If your Security Attestation is in PDF format and does not upload successfully, escalate the MiHIN Helpdesk at [help@mihin.org](mailto:help@mihin.org)

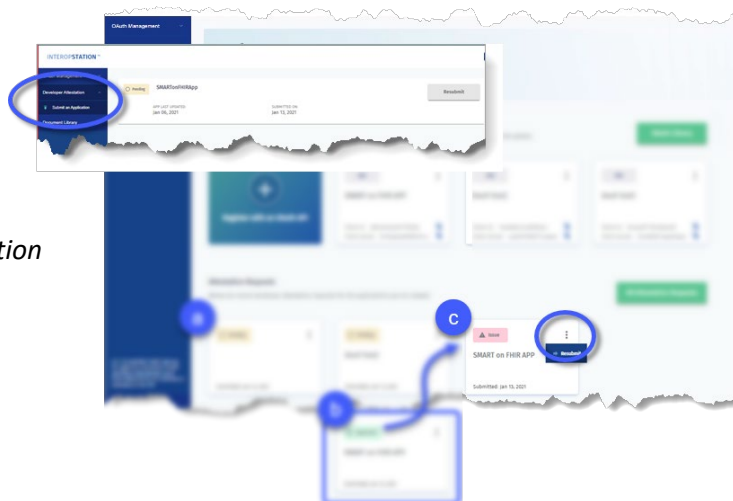
- Approved. The Security Attestation has been accepted by the MiHIN Security Team.
- Pending. The MiHIN Security Attestation has been submitted and is awaiting review.
- Issue. The Security Attestation has been denied by the MiHIN Security Team which will notify the Third-party Developers via email. Update your Security Attestation and resubmit for approval.



The screenshot shows the 'Welcome' page of the InterOp Station developer portal. It includes sections for 'OAuth Credentials' with a table of application keys, and 'Attestation Requests' showing a list of requests with their status (Approved, Pending, Issue). Three callouts labeled 'a', 'b', and 'c' point to specific elements: 'a' points to the 'Register with an OAuth API' button, 'b' points to the 'Approved' status of the 'SMART on FHIR APP' request, and 'c' points to the 'Issue' status of the 'SMART on FHIR APP' request.



**Note:** To resubmit choose either **Attestation Requests** on the Sidebar Navigation menu or by clicking your **More** vertical ellipses tool on the Security Attestation tile. Additional information can be found in the [Upload a Privacy Policy](#) section



## Upload a Privacy Policy

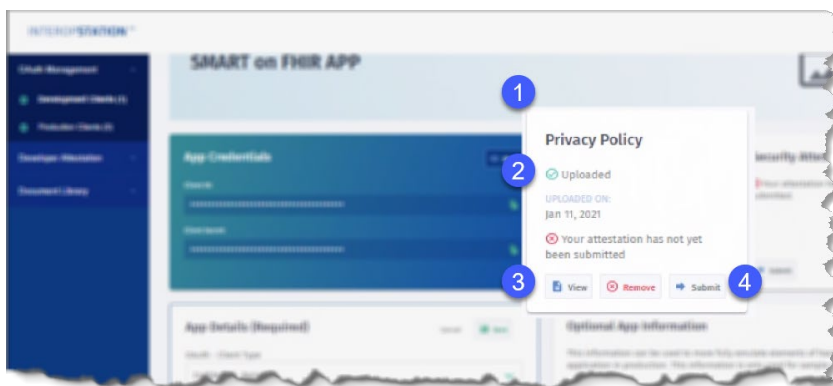
If you chose, *I'll Do It Later* on the *Do you have a privacy policy to upload?* pop up, you can upload it using your SMART on FHIR APP dashboard.

**Note:** The Privacy Policy must be in PDF format. If your Privacy Policy is in PDF format and does not upload successfully, escalate to the MiHIN Helpdesk at [help@mihin.org](mailto:help@mihin.org).

1. Navigate to your **SMART on FHIR APP** dashboard, **Privacy Policy** tile.
2. Click **Upload** (📄).
3. Navigate to and choose your Privacy Policy. When your PDF file successfully uploads, the options on the Privacy Policy tile change to either *View* or *Remove*.

**Note:** Now you can choose **View** to preview your policy or choose **Remove** if you are not ready to Submit your policy.

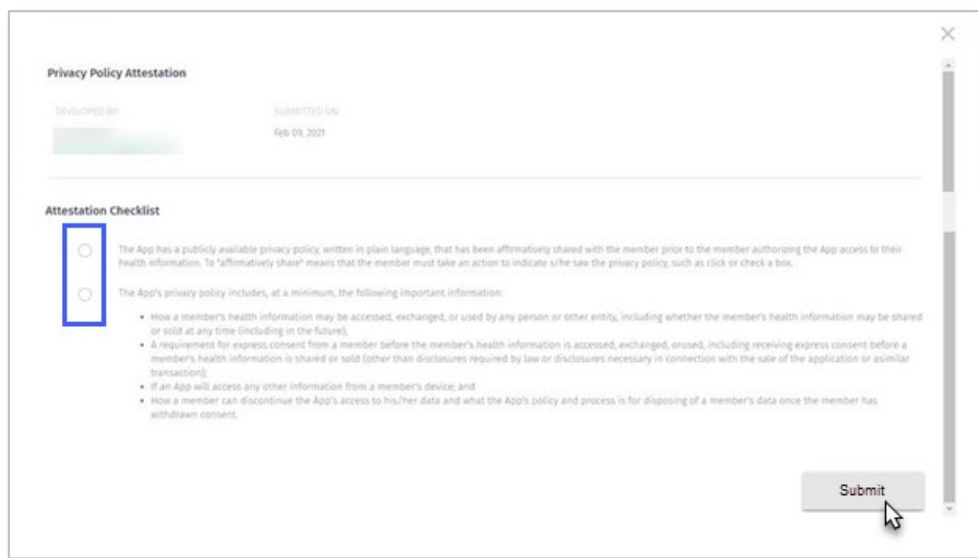
4. Click **Submit** to complete your upload.



## Privacy Policy Attestation

When the **Application Attestation** page displays, respond to each question, and then click **Submit**.

**Note:** How you answer questions on this attestation does not affect whether your application to register with IO station is accepted.



The screenshot shows a web form titled "Privacy Policy Attestation". At the top, it displays "DEVELOPED BY" with a blurred name and "SUBMITTED ON" with the date "Feb 09, 2021". Below this is an "Attestation Checklist" with two radio button options. The first option is selected and highlighted with a blue box. The second option is unselected. A "Submit" button is located at the bottom right of the form.

**Privacy Policy Attestation**

DEVELOPED BY: [Redacted] SUBMITTED ON: Feb 09, 2021

**Attestation Checklist**

- The App has a publicly available privacy policy, written in plain language, that has been affirmatively shared with the member prior to the member authorizing the App access to their health information. To "affirmatively share" means that the member must take an action to indicate s/he saw the privacy policy, such as click or check a box.
- The App's privacy policy includes, at a minimum, the following important information:
  - How a member's health information may be accessed, exchanged, or used by any person or other entity, including whether the member's health information may be shared or sold at any time (including in the future);
  - A requirement for express consent from a member before the member's health information is accessed, exchanged, or used, including receiving express consent before a member's health information is shared or sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or similar transaction);
  - If an App will access any other information from a member's device; and
  - How a member can discontinue the App's access to his/her data and what the App's policy and process is for disposing of a member's data once the member has withdrawn consent.

Submit

## How to Debug and Validate an OAuth Connection

The Client ID and Client Secret are displayed on the Application Dashboard or on the Welcome page. Copy the credentials and enter on them in the appropriate area of the Third-party Application to complete the connection to the InterOp Station.

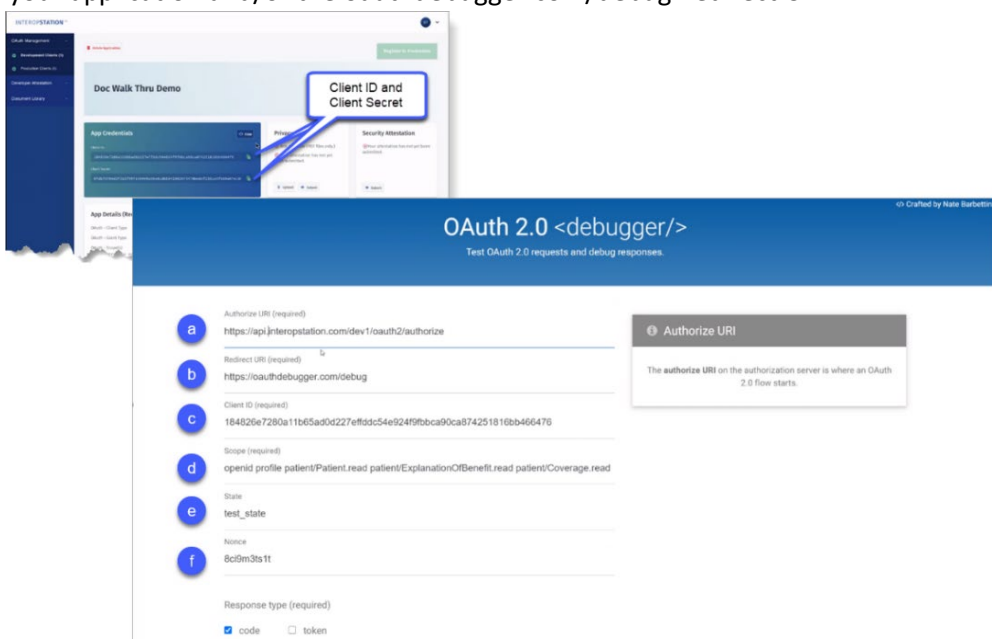
The process to validate your OAuth connection is the same whether you are setting up in a Development or Production environment. The connection points for Development and Production vary as noted in the third-party developer portal document library.

**Note:** The example below demonstrates how to simulate the OAuth 2.0 connection using the open source [oauthdebugger.com](http://oauthdebugger.com) and making calls via an API.

**Tip:** You will have to update your application to authenticate to [interopstation.com](http://interopstation.com) using OAuth 2.0 and then API requests based on your application's scope.

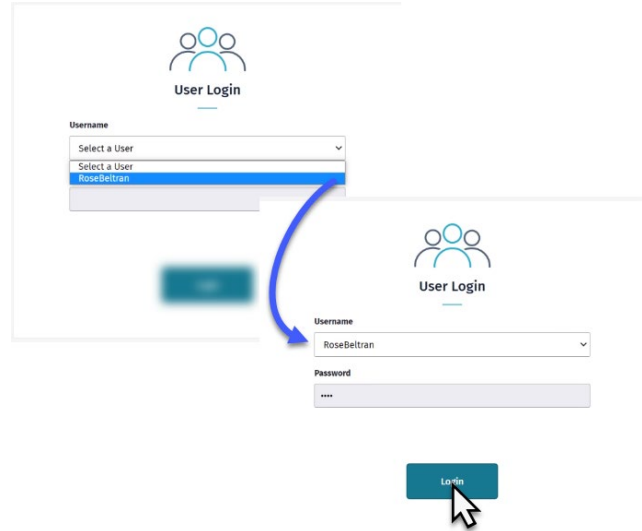


1. The OAuth debugger shown here is used to demonstrate how you could enter your required App information such as Client ID and Scope. The image shown here is an example of how a tool similar to OAuth Debugger could display after you enter your information.
  - a. **Authorize URI.** Authorize URIs can be found on interopstation.com -> Document Library -> InterOp Station API Endpoints -> OAuth 2 URL for the Environment for which you are trying to connect.
  - b. **Redirect URI.** From your application and/or the oauthdebugger.com/debug Redirect URI.
  - c. **Client ID** from your App Credentials.
  - d. **Scope.** This is the application scope, you chose during registration.
  - e. **State.** Use any text string.
  - f. **Nonce.** This value must be unique for each request.
  - g. **Response type (required).** The default value is **code**. Choose **token** if you have a Response type.



- After the application is connected you will be redirected to the Logon as a patient. Once you logon, your test patient will display along with the password.

**Note:** Rose Beltran is a patient in the Development environment. Verify the username and password match the environment you are working in e.g., Development or Production.



### Interoperability Disclaimer: Patient Access API

DISCLAIMER  
You can insert your own customized legal language for this section

I Understand

### Warning: You are about to share your personal health information with a 3rd party.

The application is requesting permission to read:

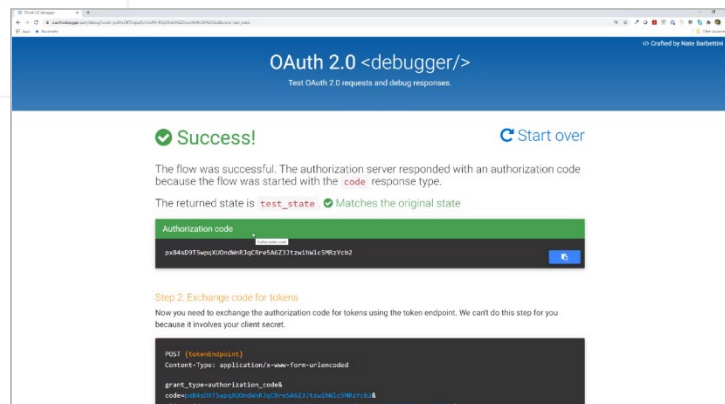
Your profile information  
Your information of type "Demographic"  
Your information of type "ExplanationOfBenefit"  
Your information of type "Coverage"

Deny

Proceed

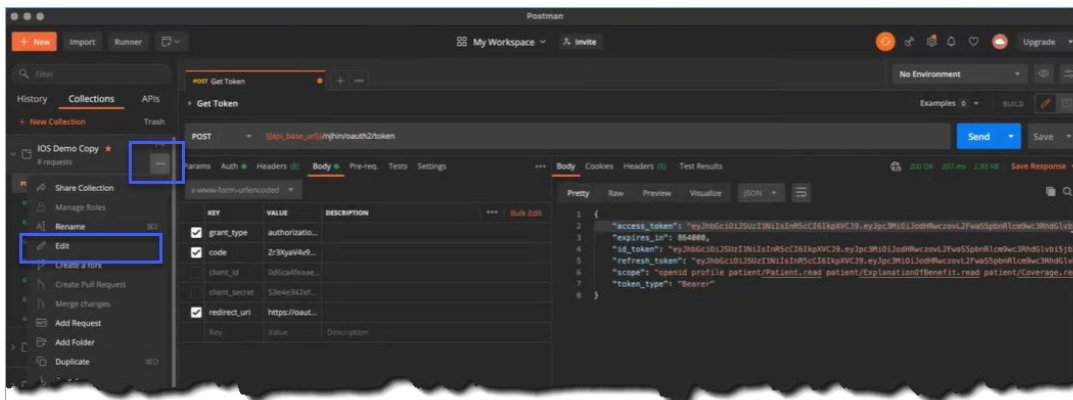
- The following notifications display using the language that the Payer inserts indicating that the patient will be providing their personal health information (PHI) to a third-party.

- The **Success!** message will display with your **Authorization code** for Postman.





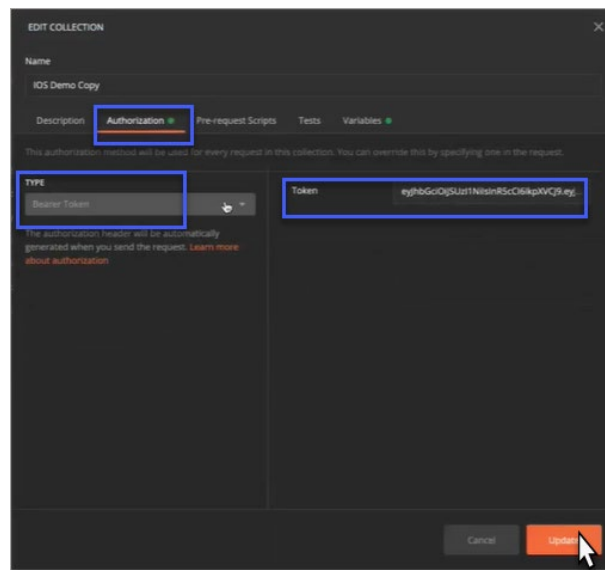
- On the left navigation menu, click on the **More** horizontal ellipses for options to manage your collection.
- Click on **Edit** to bring up the **Edit Collection** form.



- Click on the **Authorization** tab and paste the token in the **Token** field.

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

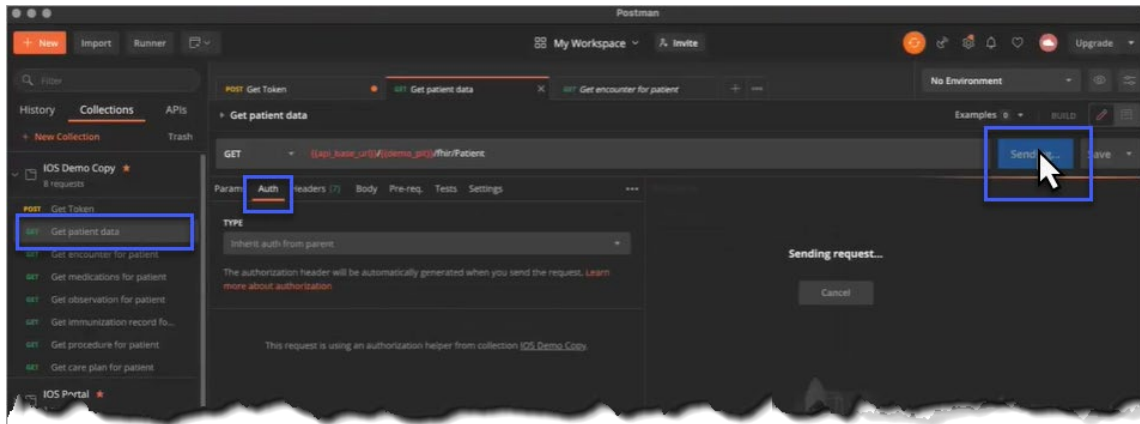
- Click **Update**.



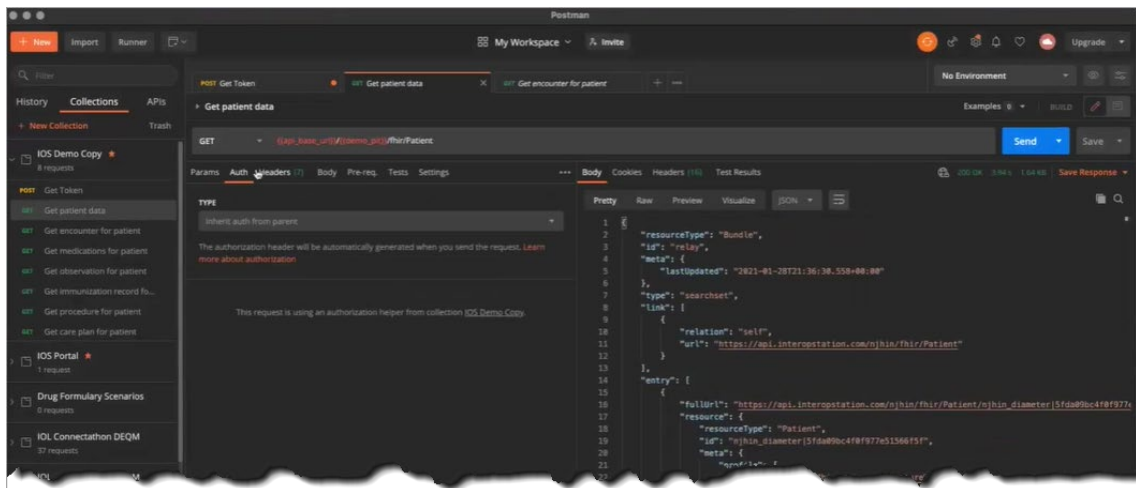




5. On the left side menu, click **Get patient data**.
6. On the **Get patient data** form, click **Send** to retrieve patient data.



7. Patient data appears in the Response section of the **Get patient data** form.



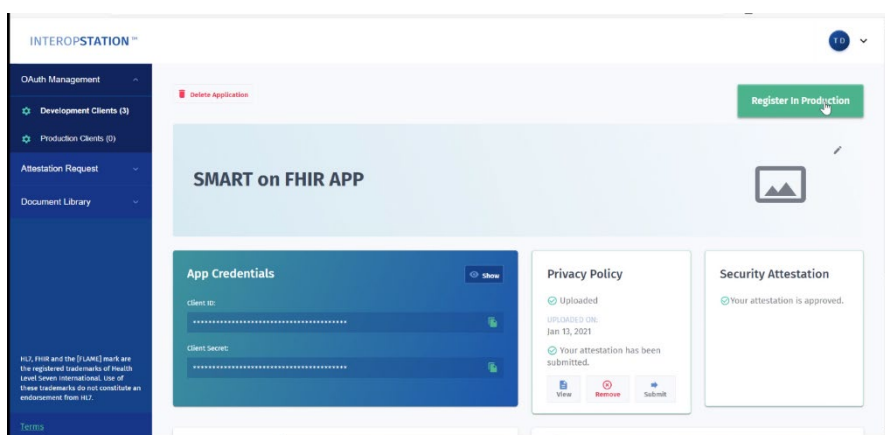
8. Repeat Steps 1-7 to retrieve other patient data categories from your collection.

## Registering a Third-Party App for Production Clients in InterOp Station

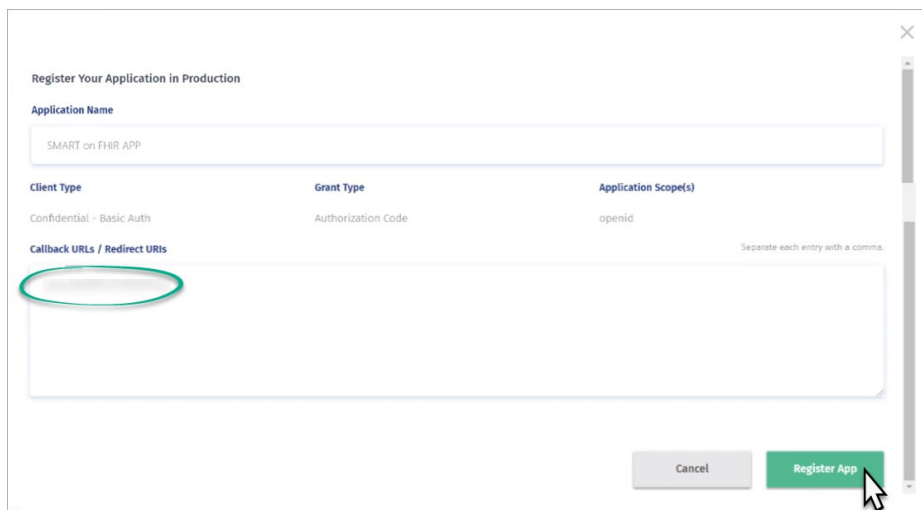
**Caution!** When you register an App in Production you will be accessing HIPAA protected data.

After successfully uploading your Security Attestation and Privacy Policy, navigate to the **Application Dashboard**.

1. Click **Register in Production**.



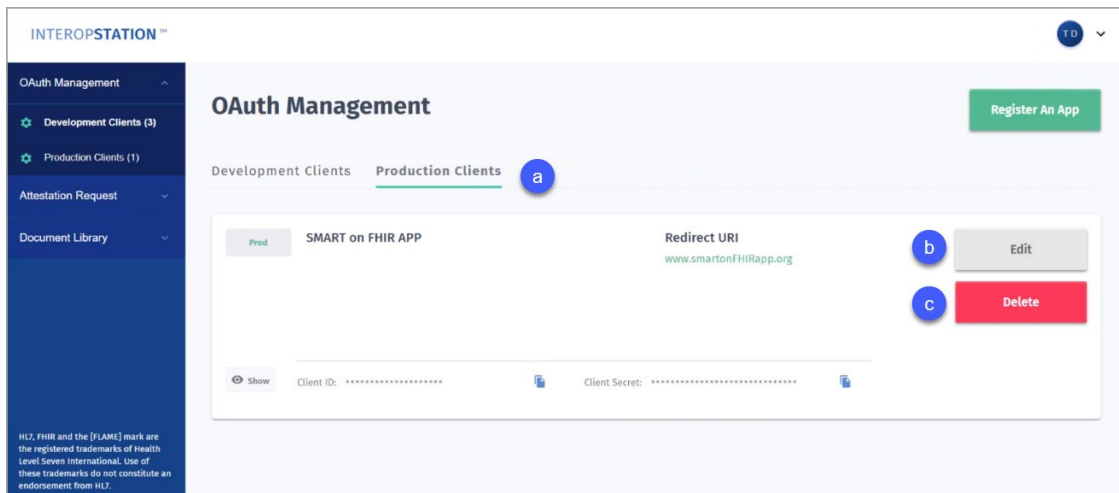
2. In the **Register Your Application in Production** form, type the **Callback URLs / Redirect URIs** for each application.



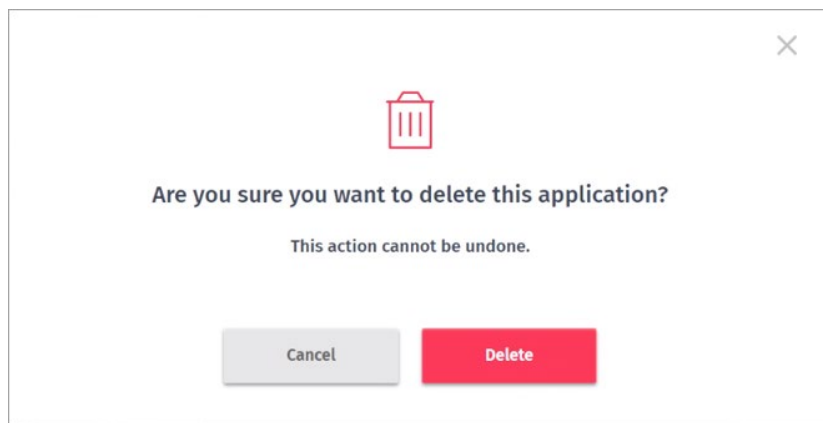
3. Click **Register App**.

4. In **OAuth Management**, click **Production Clients** on your Sidebar Navigation Menu.
  - a. Click the **Production Clients** tab to view a list of your registered apps in production.
  - b. Use your **Edit** tool as noted in the *Development Client* section above.
  - c. Use your **Delete** tool to remove an App from Production. If you choose to delete your Sandbox version, you must navigate to the **Development Client** tab and delete it there as well.

*Tip: A best practice is to query test records to confirm your App is registered correctly. Use the Postman App described below for querying records. To query the test Payer record, you must have an associated test patient record.*



5. When the **Are you sure you want to delete this application?** message displays, click **Delete** remove your App from Production.





# InterOp Station Third-party Developer Portal User Guide

---

## Testing a Third-Party App Connection in InterOp Station Production

Follow the same steps as outlined in the section [Testing a Third-party App Connection to InterOp Station for Development](#) above. Instead of a patient name and password as shown in Step 2, you 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 InterOP Station. The Production environments e.g., BCBSM and NJHIN, will only connect to Production client Third-party applications in InterOP Station.*

The synthetic user credentials for testing are:

**Environment:** Development

**Username:** RoseBeltran

**Password:** <Autofilled in UI>

**Environment:** BCBSM (Production)

**Username:** mihintest1

**Password:** 5Y^&!blp

**Environment:** NJHIN (Production)

**Username:** mihintest@protonmail.com

**Password:** 5kPt6Ridj83PiVm

