

## Table of Contents

Purpose of InterOp Station Third-Party Portal User Guide .....	1
Creating an InterOp Station third-party developer portal account .....	2
Sign in issues after creating an account.....	3
Connecting a Third-Party Developer App to InterOp Station .....	4
Welcome page navigation.....	4
Register a SMART Application with the OAuth API tool .....	5
Navigating the application dashboard page.....	6
Security Attestation requirement.....	7
Submitting a Security Attestation .....	7
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
Patient Access API.....	20
Provider Directory API .....	21
Splash page .....	21

## 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 who may experience issues connecting, testing, and adding their privacy policy and security attestation documents.

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

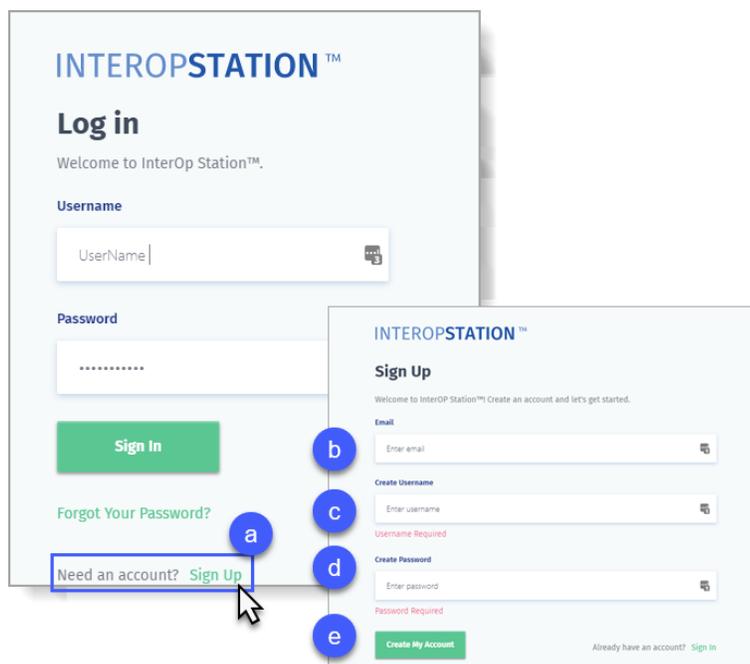
Contact the [MiHIN Help Desk](#) if you experience any of the following issues while connecting your app:

- 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) Select **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 select **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 sign in 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 Log in 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.

## Sign in issues after creating an account

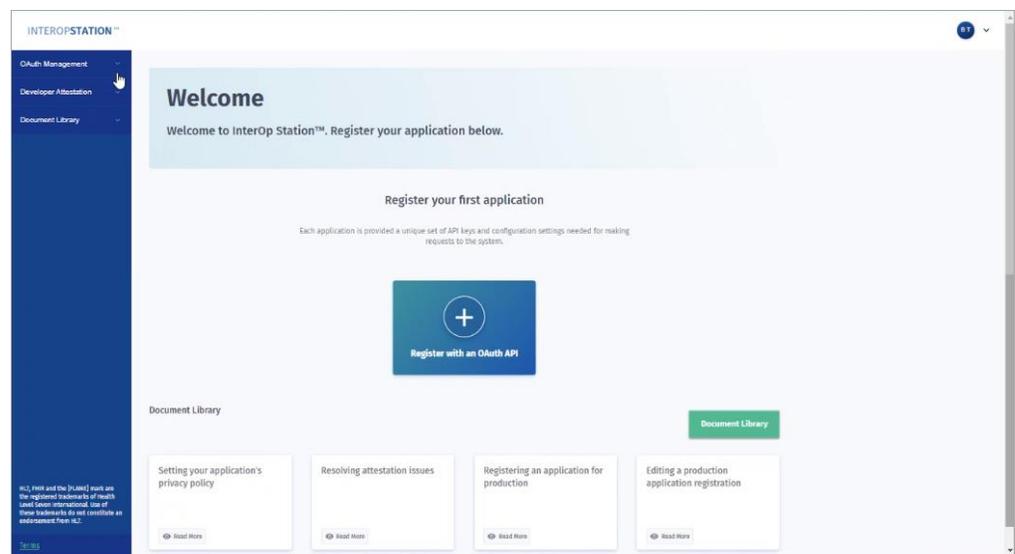
If a third-party developer has followed the steps appropriately and sign in still fails, refer to the [MiHIN Help Desk](#).

# 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



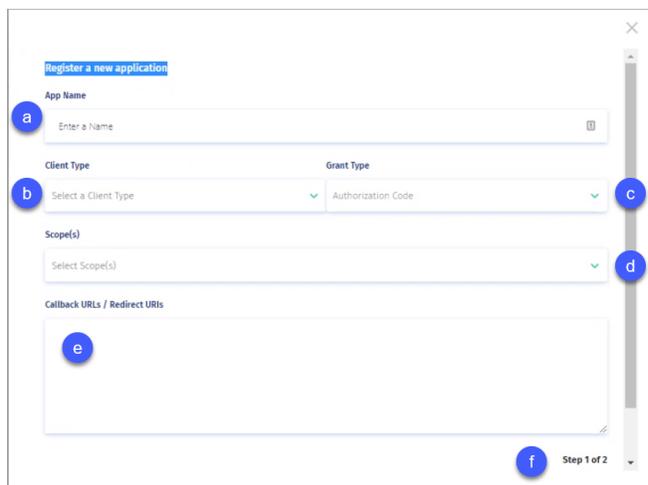
**INTEROPSTATION™** located above the Sidebar Navigation Menu you will return to the Welcome page.

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 select this tool you will be redirected to the **Register a new application** form.

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 select 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. Select your **Scope(s)** arrow to scroll to and select the scope of resources you are requesting for access, for example, 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.



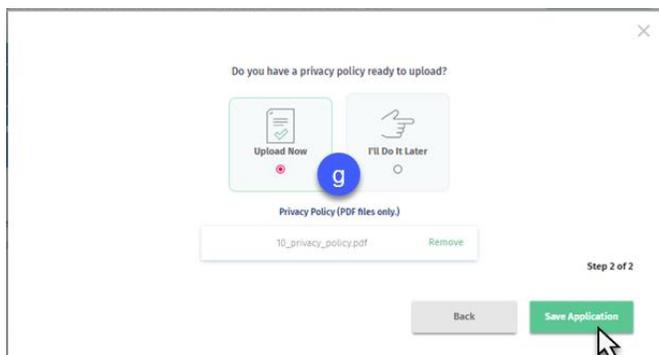
The screenshot shows a web form titled "Register a new application". It contains several fields: "App Name" with a text input and a trash icon; "Client Type" and "Grant Type" dropdown menus; "Scope(s)" with a scrollable list; and "Callback URIs / Redirect URIs" with a large text area. Callouts a-f are placed over the form: 'a' is over the App Name input; 'b' is over the Client Type dropdown; 'c' is over the Grant Type dropdown; 'd' is over the Scope(s) dropdown; 'e' is over the Callback URIs text area; and 'f' is over the "Step 1 of 2" indicator at the bottom right.

**Note:** To test this application with the [oauthdebugger.com](https://oauthdebugger.com), list your application's redirect URI and [oauthdebugger.com/debug](https://oauthdebugger.com/debug) here separated by commas, for example: [https://\[yourapphere.com/\]](https://[yourapphere.com/]) or <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. Select **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, select **I'll Do It Later** and then click **Save Application**. However, your privacy policy must be uploaded before your app can go to Production.*

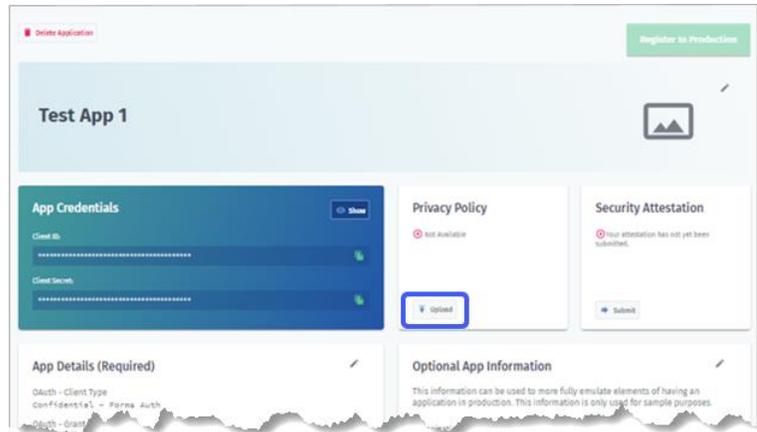


### Navigating the application dashboard page

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

- Modify the **App Details** you selected during the registration process.
- Upload and review your **Privacy Policy**.
- Complete or review your **Security Attestation**.
- Add **Optional App Information** such as your organization website, a description of the application, a point of contact, and an email address.
- Obtain your app credentials, for example, 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.

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

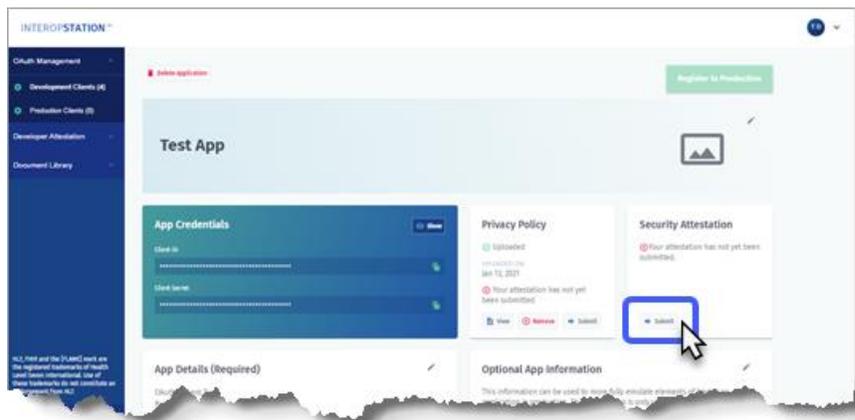


## Security Attestation requirement

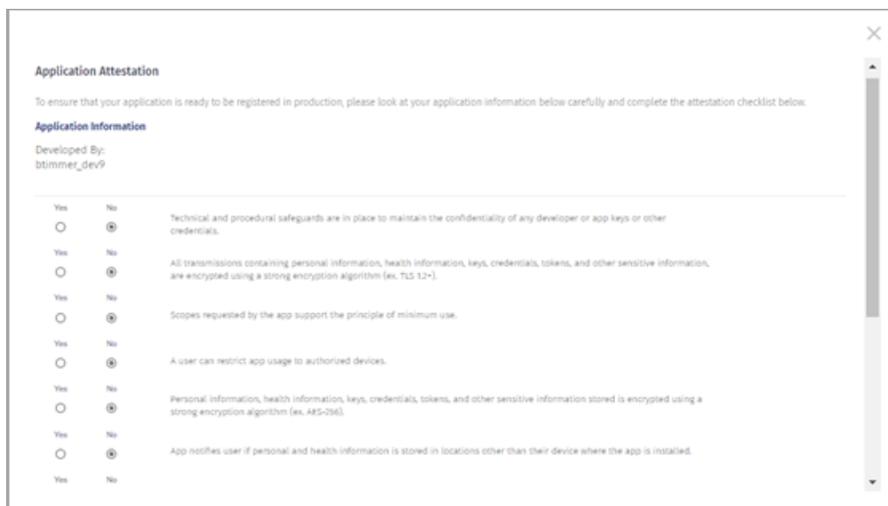
Developers are required to submit a Security Attestation for their app. An automated MiHIN Help Desk ticket is generated after a Security Attestation review is completed. The MiHIN Security Team will review the third-party developer ticket and determine whether the submitted Security Attestation is accepted 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.
3. Navigate to and select your **Security Attestation** which will be like the example shown below.



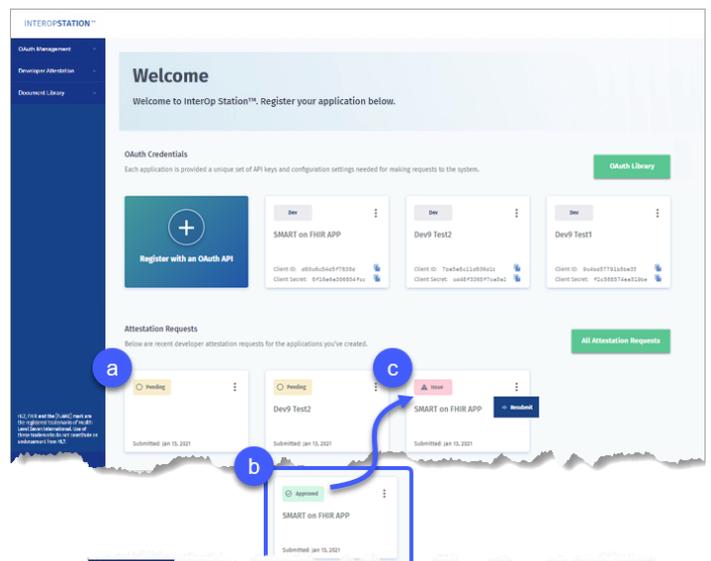
The screenshot shows a web form titled "Application Attestation". Below the title is a sub-heading "Application Information" and the text "Developed By: btimmer\_dev9". The form contains a checklist of seven items, each with "Yes" and "No" radio buttons. The "No" button for each item is selected, and each has a small blue icon to its right. The items are:

Yes	No	Question
<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 type="radio"/>	

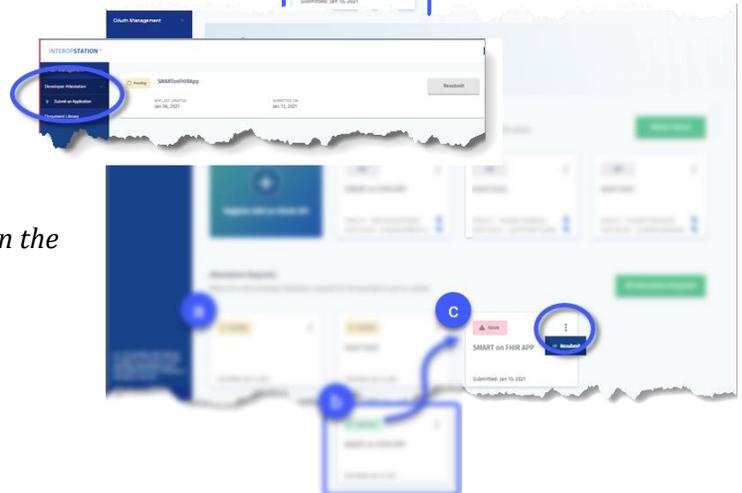
- The status of your Security Attestation can be found on the **Welcome** page **Attestation Requests** dashboard or by clicking Attestation Requests located on your Sidebar Navigation Menu.

*Note: The Security Attestation must be in PDF format. If your Security Attestation is in PDF format and does not upload successfully, escalate to the MiHIN Help Desk 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.



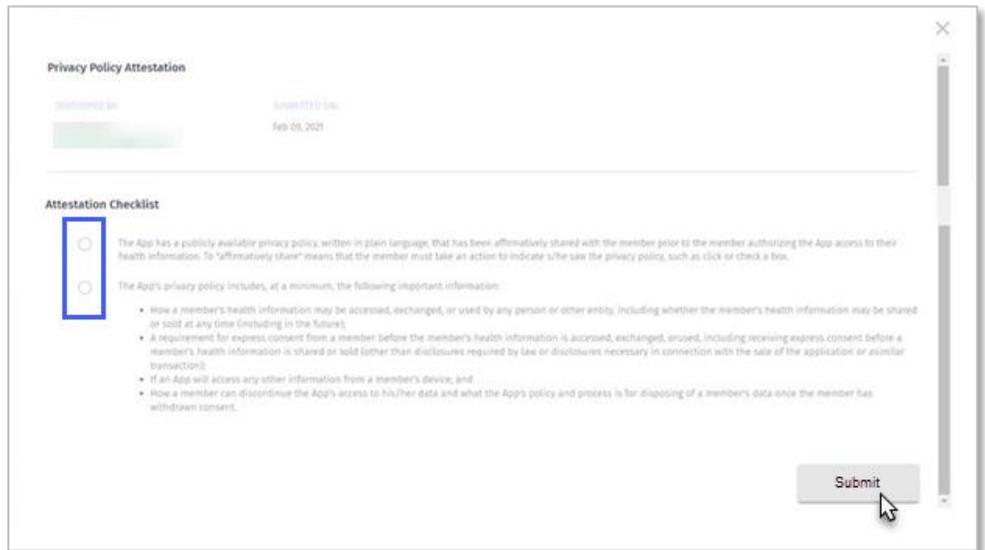
*Note: To resubmit, select either **Attestation Requests** on the Sidebar Navigation menu or by clicking your **More** vertical ellipses tool on the Security Attestation tile. Additional information can be found in the [Upload a Privacy Policy](#) section.*



## 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.

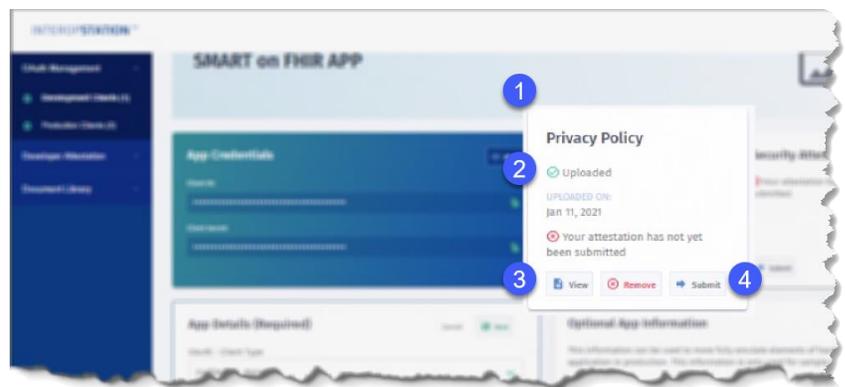
**Note:** The Privacy Policy must be in PDF format. If your Privacy Policy is in PDF format and does not upload successfully, escalate to the MiHIN Help Desk at [help@mihin.org](mailto:help@mihin.org).



1. Navigate to your **SMART on FHIR APP** dashboard, **Privacy Policy** tile.
2. Click **Upload** (📄).
3. Navigate to and select 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 select **View** to preview your policy or select **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 InterOp Station is accepted.*

## 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 and making calls via an API.*

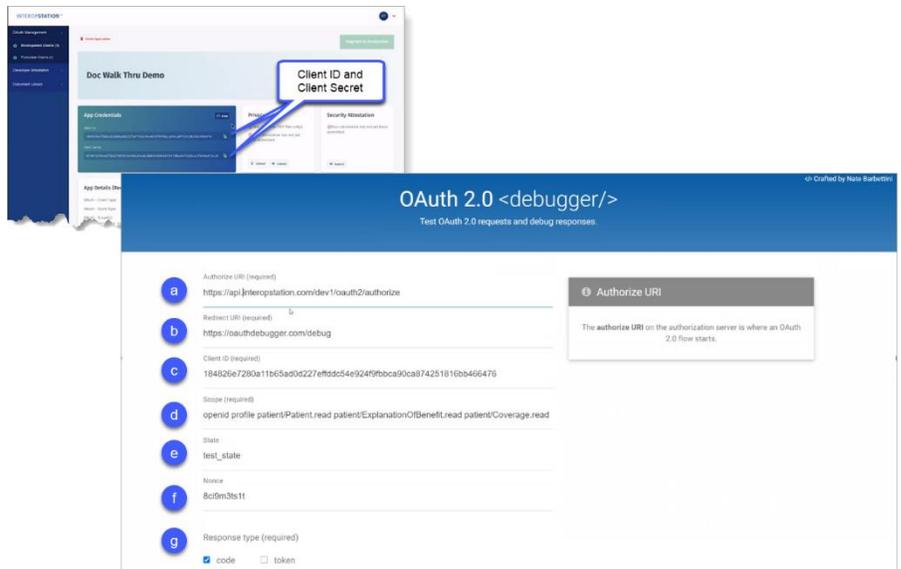
***Tip:** You will have to update your application to authenticate to interopstation.com using OAuth 2.0 and then API requests based on your application's scope.*

1. The OAuth debugger shown here is used to demonstrate how to 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.

***Note:** The names of the parameters listed below must be entered as shown because they are case sensitive.*

- a. **Authorize URI** (required). 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** (required). From your application or the oauthdebugger.com/debug select **Redirect URI**.

- c. Enter the **Client ID** (required) from your App Credentials.
- d. **Scope** (required). This is the application scope, you chose during registration.
- e. **State**. Type a text string.
- f. **Nonce**. This value must be unique for each request.
- g. **Response type** (required). The default value is **code**. Select **token** if you have a Response type.
- h. **Response mode** equals query.



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

```
https://api.interopstation.com/[dev1]/oauth2/authorize?client_id=client_id&redirect_uri=https://oauthdebugger.com/debug&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&response_type=code&response_mode=query&nonce=kbbuk9mhz2n
```

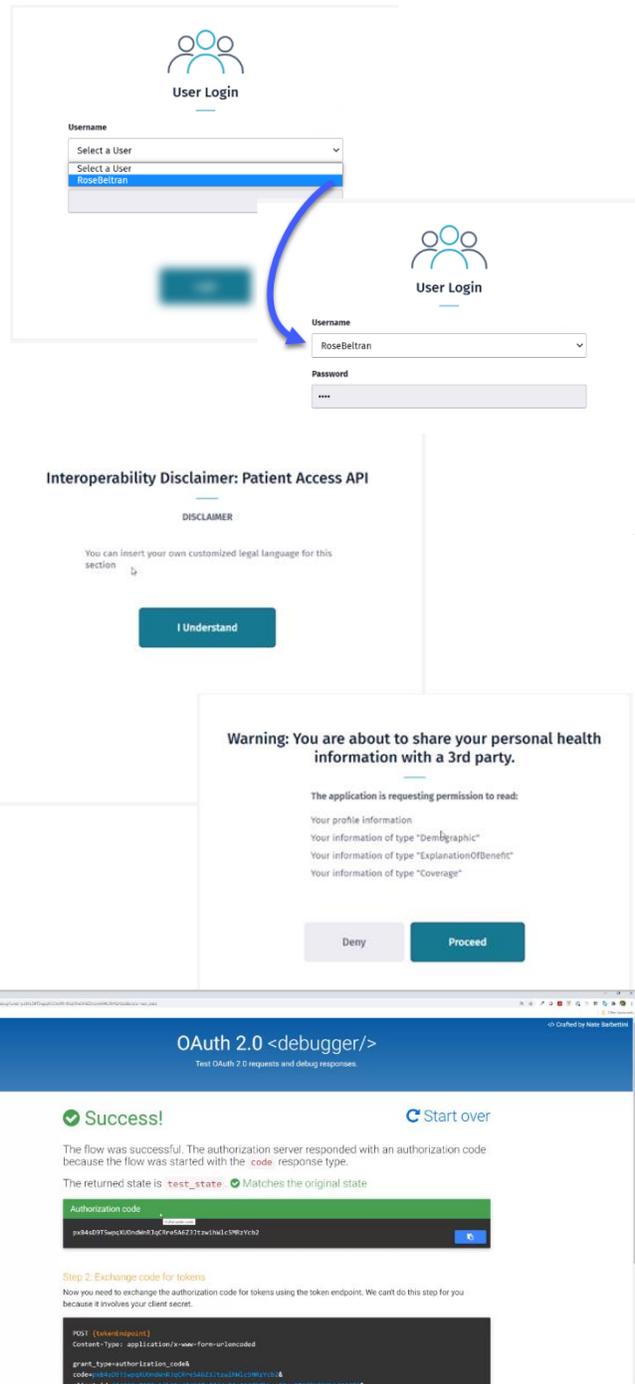
**Note:** It should be noted that **dev1** is an example environment. Please use the environment you are actually targeting, if not **dev1**.

- After the application connects, you will be redirected to the patient **User Login**. Once you log in, 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, for example, Development or Production.*

- 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.



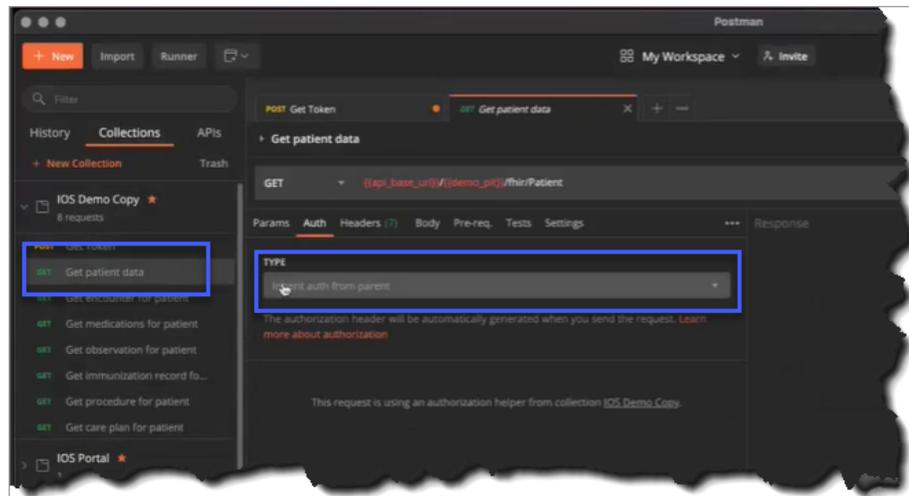




## Testing a third-party app connection to InterOp Station for development

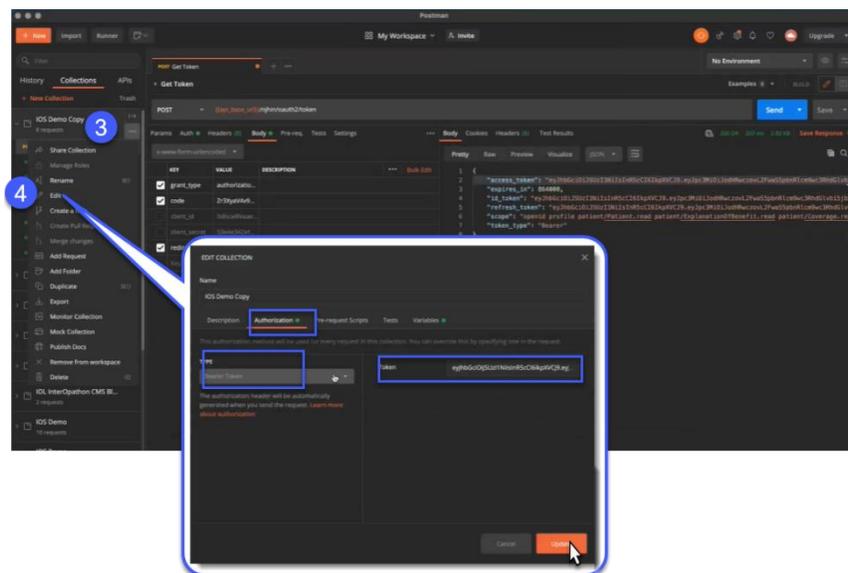
Using the information below, you will be able to test whether you can connect and test for data.

1. On the left side menu, click **Get patient data** to open the **Get patient data** form.
2. On the **Auth** tab, select **inherit auth from parent** in **Type** dropdown menu.

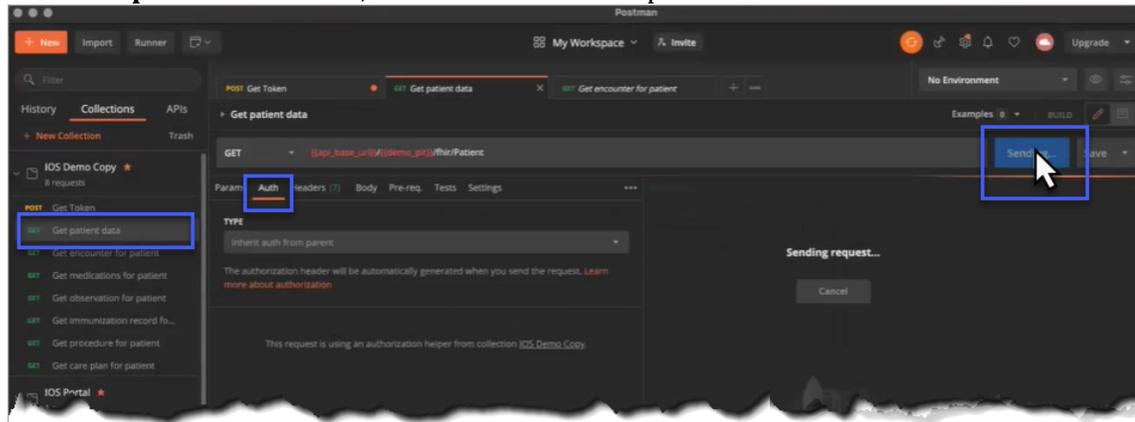


3. Click on the **More** horizontal ellipses for options to manage your collection.
4. Click on **Edit**. The **Edit Collection** form appears.

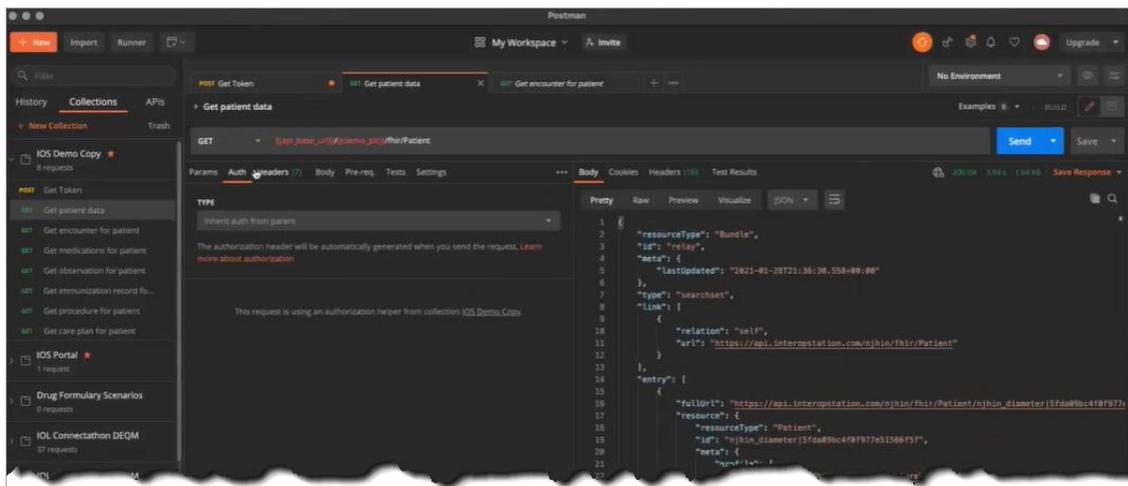
*Note: Confirm **Bearer Token** is the selected token type on the **Auth** tab.*



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 displays in the **Response** section of the **Get patient data** form.



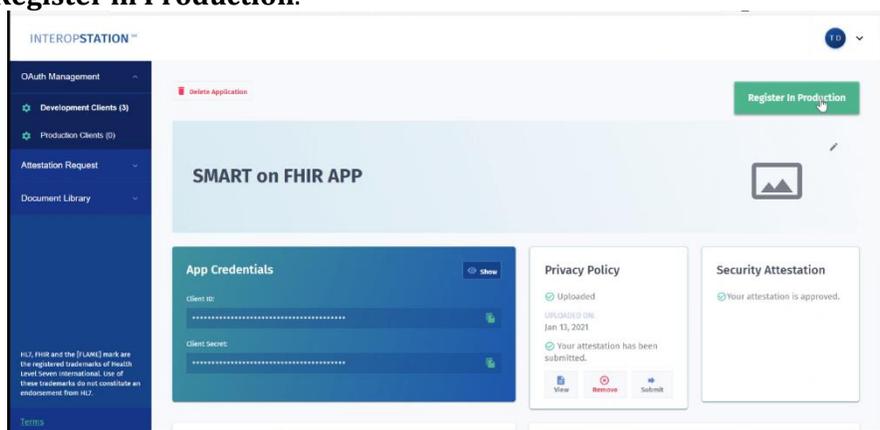
8. Repeat Steps 1 through 7 to retrieve other patient data categories from your collection.

## Registering a third-party app for production clients in InterOp Station

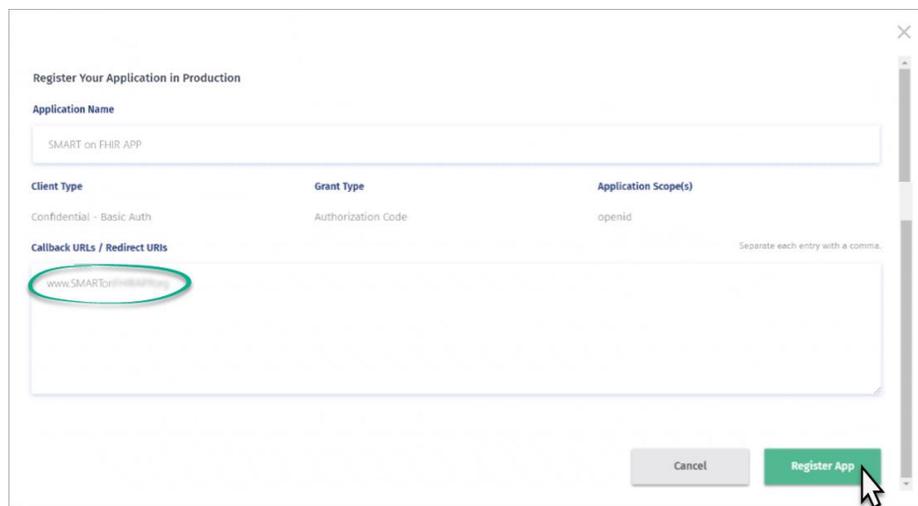
**Caution!** When you register an app in Production you will be accessing HIPAA-protected data.

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

1. Click **Register in Production**.



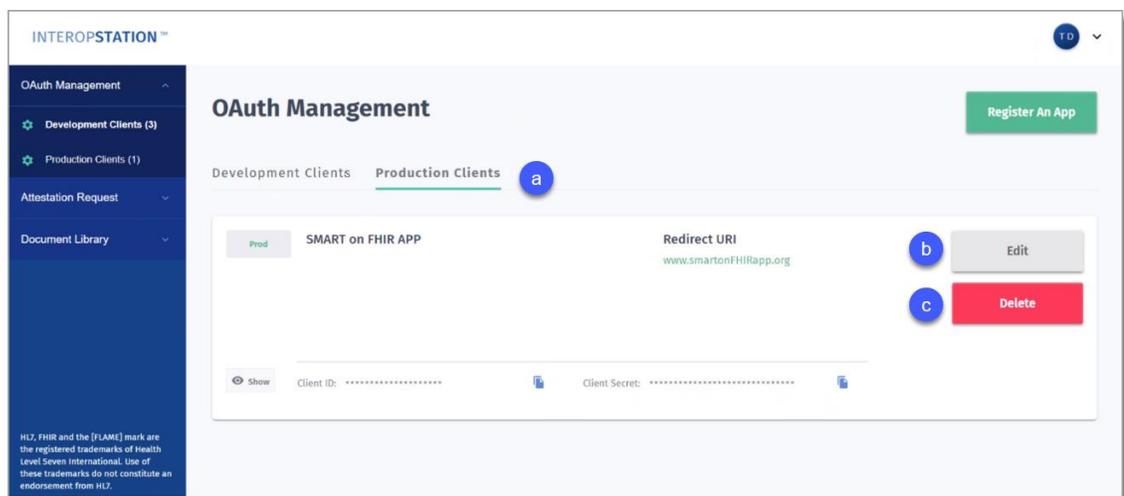
2. In the **Register Your Application in Production** form, type the **Callback URLs / Redirect URIs** for each application as shown in the example.

The screenshot shows the 'Register Your Application in Production' form. It includes fields for 'Application Name' (filled with 'SMART on FHIR APP'), 'Client Type' (Confidential - Basic Auth), 'Grant Type' (Authorization Code), and 'Application Scope(s)' (openid). The 'Callback URLs / Redirect URIs' field contains 'www.SMARTonFHIR.org' and is circled in green. At the bottom right, there are 'Cancel' and 'Register App' buttons, with a mouse cursor pointing to the 'Register App' button.

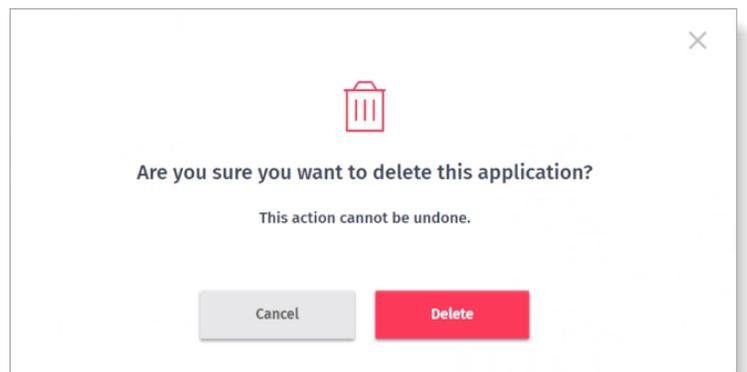
3. Click **Register App**.

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 Clients* 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 Clients** 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 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** to remove your app from Production.



## Testing a third-party app connection in InterOp Station production

### *Patient Access API*

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, for example, 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

### Provider Directory API

Third-party app developers should use the following Provider Directory endpoints to connect to the IO Station production environment:

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

Where [tenant] is the tenant/payer that is being queried. See the following table for the tenant name for each customer.

Customer Name	Tenant
Blue Cross Blue Shield of Michigan	bcbsm
McLaren Health Plan	mhp
McLaren MDwise	mdw
Upper Peninsula Health Plan (UPHP)	uphp
Michigan Department of Health and Human Services	mdhhs
New Jersey Medicaid / Family Care	njios

### Splash page

Here is an image of the splash page that New Jersey Medicaid / Family Care is requiring to appear in the third-party app. The splash page shown here **must** be included in the user interface. When the user clicks on **Link Data Provider** in the **New Jersey Medicaid / Family Care** section, the splash page must display. To close the splash, click the **Close** button (X) in upper right corner.

