Pega FHIR APIs User Guide

Installation

- Download the FHIR®© API component
- Import the component into your Pega application
- Under the "Built on application(s)" or "Enabled component(s)" section of your Application, add the FHIR®© API component
- Save the changes

FHIR Source System

- In order to make use of this component, you will need to connect to a source clinical data system that has a FHIR®© server. Pega used two publicly available sandbox environments for testing the APIs:
- HAPI FHIR®© - http://fhirtest.uhn.ca – This is a public test server available for testing FHIR®© APIs
- Epic FHIR®© - https://open.epic.com – This is an open source light weight access layer made available for Epic.

How to use this component

Once you have successfully installed the component; then you are ready to use the FHIR APIs in your Pega application.

Begin by looking at Data on the "Cases & Data" tab of the component's application rule. These are the business data assets available for use in your application. You should add the ones you want to use as data types on your own application.

To use the data in your application's cases, decision strategies, business rules, etc. you should create your own data pages that reference the FHIR connectors. Use the data pages included in the component only as an example, as they are defined at the Integration class and are representative of the API's physical data model, In order to future-proof your application from changes that may occur in the FHIR API and allow your application to more easily account for those changes, you should create a normalized (logical) data model where your application's data pages are defined. For an overview of data pages, how to use them and where to use them please visit the PDN (https://pdn.pega.com/understanding-data-pages/understanding-data-pages). For an overview of Pega's recommended best practice for data virtualization, see here: https://pdn.pega.com/data-virtualization-prpc.

Authentication with EHR

Patient-facing applications must secure and protect the privacy of patients and their data. EHR systems support the OAuth 2.0 framework to authenticate and authorize public applications, which requires your application to ask for and receive the appropriate permission from the EHR organization before accessing patient data.

Using the credentials:

Once you register your application with the EHR, you will need to create an appropriate authentication profile to associate with the REST Connect rules. A placeholder authentication profile called **FHIRAuthentication** has been created ad packaged with the application. Copy this profile into your ruleset and update it with the details of the Client ID, security token etc. as appropriate with the EHR requirements.

This authentication profile is already referenced in all the CONNECT REST rules for each FHIR Resource API.