****

**Neighborhood of Rhode Island - CMS Interoperability Project**

**Guide for FHIR Compliant API Data mining**

Table of Contents:

[1.0 Background and Summary 2](#_Toc78496389)

[2.0 Nature of the Neighborhood Data 2](#_Toc78496390)

[3.0 Use Cases Details 3](#_Toc78496391)

[3.1 Use Case List 3](#_Toc78496392)

[4.0 FHIR API Used by Neighborhood 4](#_Toc78496393)

[5.0 Authentication & Authorization Overview with Okta 4](#_Toc78496394)

[5.1 Pre-requisites 4](#_Toc78496395)

[5.2 How to Authenticate & Authorize 4](#_Toc78496396)

[5.3 How to leverage the JWT Token for API consumption 6](#_Toc78496397)

[5.4 How to Associate User Group to the Application 6](#_Toc78496398)

[5.5 OKTA Application, Group, Assign Application and Access Policy 7](#_Toc78496399)

[6.0 Best Practices for Payers and API Developers 8](#_Toc78496400)

[6.1 Best Practice for Payers: Multi-person Enrollment Groups 9](#_Toc78496401)

[6.2 Developing Third-Party Apps 9](#_Toc78496402)

[6.3 Privacy Notice 10](#_Toc78496403)

# 1.0 Background and Summary

The Centers for Medicare & Medicaid Services (**CMS)** is part of the Department of Health and Human Services (HHS). CMS recently introduced new interoperability mandates for health plans that must be implemented by July 1, 2021. This rule is designed to make health information more easily available to patients by implementing new industry standards like HL7 FHIR APIs and by deterring information blocking.

As part of the Trump Administration’s MyHealthEData initiative, the Interoperability and Patient Access final rule (CMS-9115-F) is focused on driving interoperability and patient access to health information by liberating patient data using CMS authority to regulate certain health plan issuers on the Federally facilitated Exchanges (FFEs). These new policies include:

* Patient Access API (applicable January 1, 2021, enforced July 1, 2021)
* Provider Directory API (applicable January 1, 2021, enforced July 1, 2021)
* Clinical Information (enforced July 1, 2021)
* Payer-to-Payer Data Exchange (applicable January 1, 2022)

Part D Medicare Advantage plans must also make formulary information available via the Patient Access API. And Medicaid and CHIP FFS and managed care must make preferred drug lists available.

Neighborhood has embarked on this project to comply with these CMS mandated requirements

# 2.0 Nature of the Neighborhood Data

CMS compliance rules mandate exposing all relevant data that is stored in various Neighborhood systems. Exposure will be through HL-7/FHIR compliant API as prescribed by CMS.

After the evaluation of data acquisition, data retention systems and the actual source data, the primary requirements are translated into the following “Use Cases” (UCs) under which the data will be made available to the prescribed enteritis.

Each use case is further decomposed into “User Stories”. These user storied are developed by comparing the data elements collected by Neighborhood and the partners source system/EMR with the practical scenarios for which a requester will frame the queries

The entire data is logically divided into seven **Use Cases**. Each Use Case is then associated with the expected queries by the requester. These queries are termed **User Stories**.

User Stories are mapped to the FHIR APIs that are based upon the HL7 formats. These APIs are prescribed by CMS and form the common data exchange and interoperability ecosystem.

# 3.0 Use Cases Details

Based upon the data that Neighborhood keep and maintain in their systems, following table describes the data associated with the user stories. These stories follow the recommendation by CMS.

## 3.1 Use Case List

|  |  |  |
| --- | --- | --- |
| **Use Case #** | **Use Case**  **Name** | **Description – User Stories** |
| **UC-1** | Providers Directory | Data exposure based upon the request for.   * Provider search based on name * Provider search based on specialty * Provider search based on address (City, State, Zip code) * Provider search based on NPI |
| **UC-2** | Patient Demographics | Data exposure based upon the request for.   * Search of pt demographics using name * Search of pt demographics using identifier * Search of pt demographics using combination of name & DOB * Search of pt demographics using combination of gender & name * Search of pt demographics using |
| **UC-3** | Access Historical Claims | Data exposure based upon the request for.   * Search for Adjudicated Claims by Member ID * Search for Adjudicated Claims using Identifier * Search for Adjudicated Claims using Provider |
| **UC-4** | Access Members Coverage Details | Data exposure based upon the request for.   * Search for Member Coverage Details using Status * Search for Member Coverage Details using unique Business Identifier * Search for Member Coverage Details using Members Name |
| **UC-5** | Access Drug Formulary | Data exposure based upon the request for.   * Search for Drug Coverage Plan specific for a member using Identifier * Search for drugs in Formulary specific to a plan identifier * Search for a drug in a specific Drug Coverage Plan using code |
| **UC-6** | Encounter and Clinical Information | Data exposure based upon the request for.   * Search for Encounter Information specific for a member using Identifier * Search for Encounter Information specific for a member using Date * Search for Procedure Information specific for a member using Identifier * Search for Procedure Information specific for a member using Date * Search for Medication request information specific to a member using Date * Search for Care Plan information specific for a member using Identifier * Search for Care Plan information specific to a member using Date |
| **UC-7** | Laboratory Reports and Observations | Data exposure based upon the request for.   * Search for Observation specific for a member using Member ID * Search for all Observations specific to Lab Test type using LOINC code * Search for all Diagnostic Reports specific to the Lab Test type using LOINC code |

# 4.0 FHIR API Used by Neighborhood

Each one of the user stories were carefully mapped with the appropriate FHIR APIs and when triggered by the requester, would produce and expose the desired results. Neighborhood will be utilizing the APIs that are cataloged in the following spreadsheet



# 5.0 Authentication & Authorization Overview with Okta

### 5.1 Pre-requisites

* User needs to be registered on the OKTA portal
* User needs to have credentials (UserName, Password)
* Using the Credentials, User can authenticate oneself on the portal

NOTE – If you are not registered or do not have credentials, reach-out to SUPPORT team

### 5.2 How to Authenticate & Authorize

Integrate the NHPRI Authentication and Authorization Code (see Okta [documentation](https://developer.okta.com/docs/guides/implement-auth-code/overview/))

* Redirect to Okta Authorize endpoint

**GET** <https://nhpri.oktapreview.com/oauth2/default/v1/authorize>?

state=123&

response\_type=code&

redirect\_uri=https://nhpri-web.pravici.com/authorization-code/callback&

scope=openid profile launch/patient patient/\*.read offline\_access& client\_id=0oax0xi8i9TiCCFQd1d6

Response pay load will contain the **{Code}**

* Leverage the {Code} in the Authorization endpoint. Redirect to callback URL with Authorization Code

[https://nhpri-web.pravici.com/authorization-code/callback?code=**{Code}**&state=123](https://nhpri-web.pravici.com/authorization-code/callback?code=%7bCode%7d&state=123)

* Exchange {Code} for {AccessToken} via token endpoint (using Client ID and Client Secret for auth):

**POST** <https://nhpri.oktapreview.com/oauth2/default/v1/token>

Content-Type: application/x-www-form-urlencoded

Authorization: Basic {Base64Auth}

grant\_type=authorization\_code&

redirect\_uri={Redirect URI}&

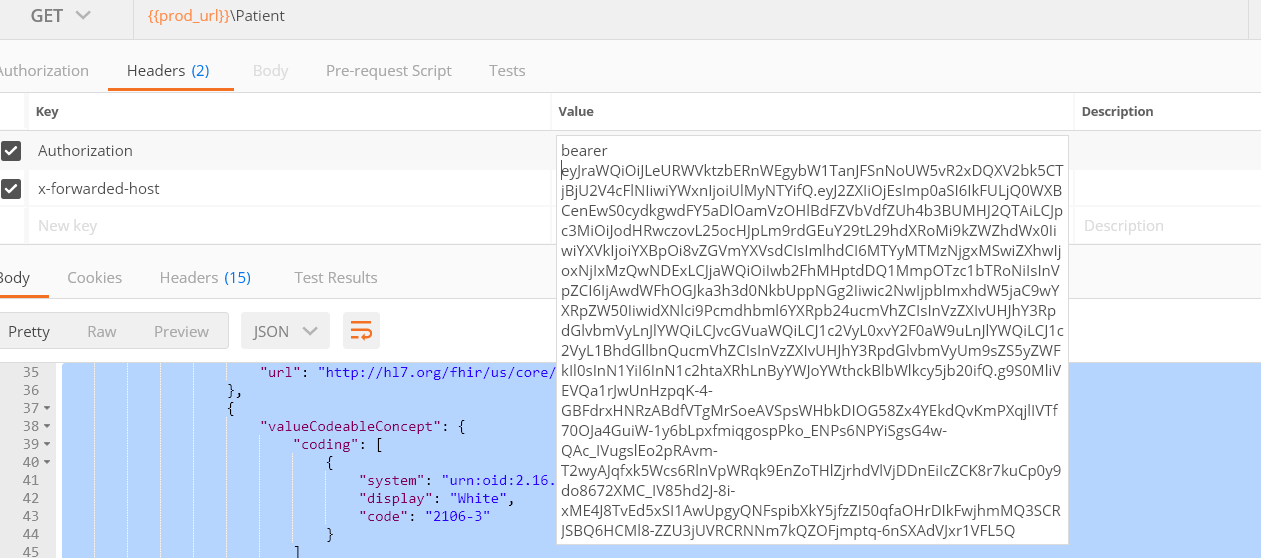
code={Code}

Authorization requests to the FHIR server are authenticated via Bearer Auth (Authorization: Bearer {AccessToken}) using the access token returned from Okta.

### 5.3 How to leverage the JWT Token for API consumption

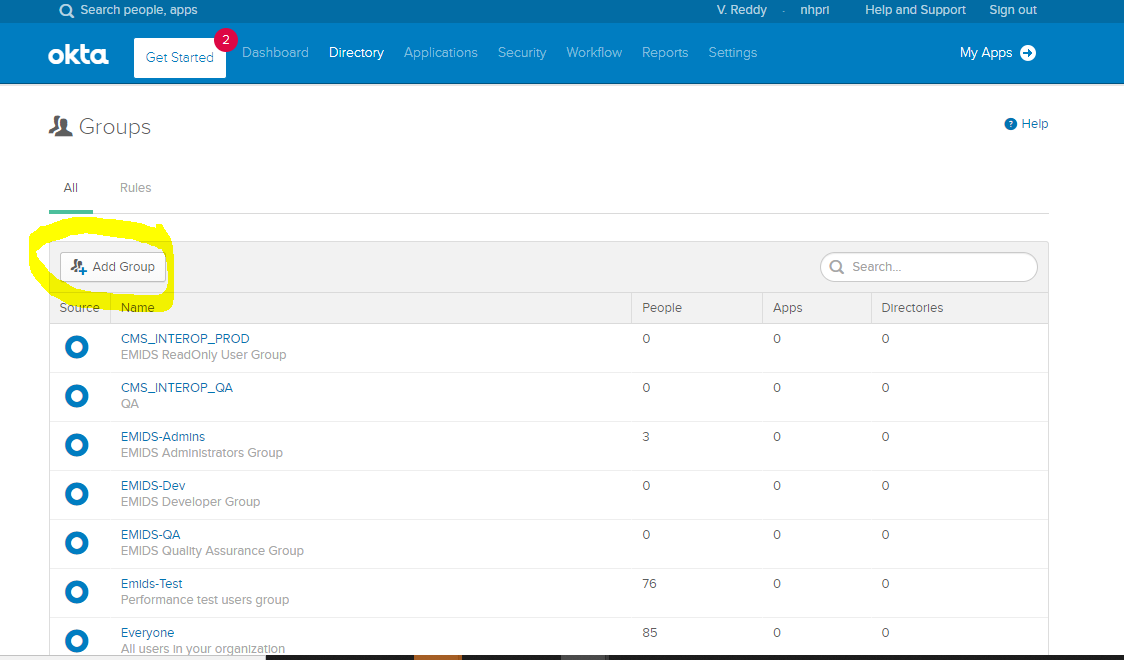
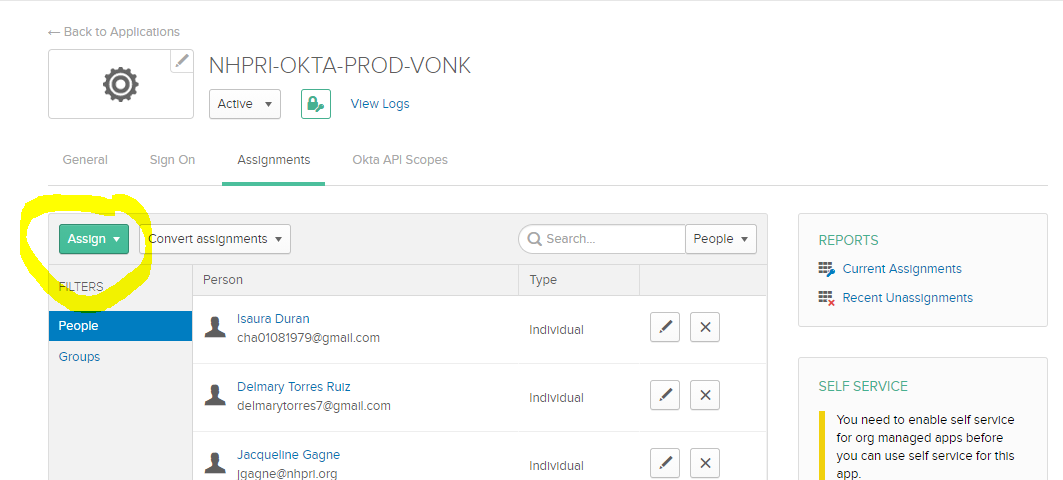
In Postman, while requesting a resource, the JWT Token needs to be leveraged to fetch a resource

* Open Postman, enter the resource that needs to be fetched viz., {baseURL}/{resource}
* In the Header section, add “Authorization” key
* Enter the JWT Token (obtained in previous step) as bearer {jwt token}



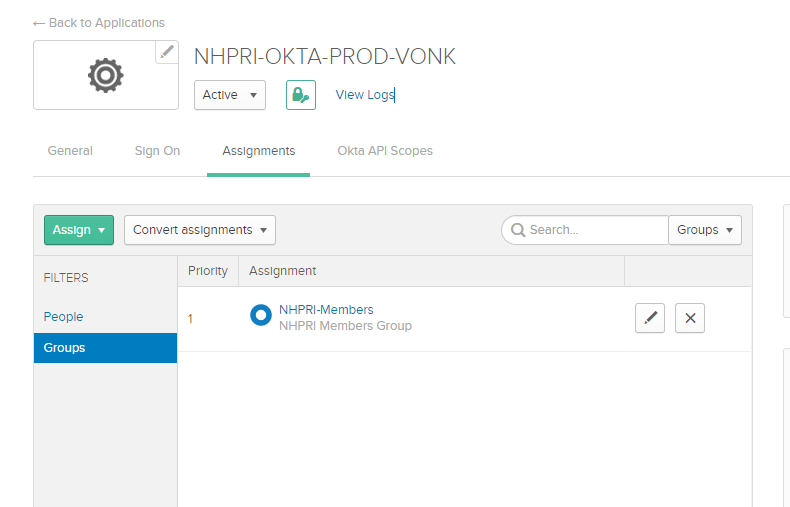
* Execute the request by clicking on Send
* The request will be validated for valid JWT Token. Upon successful validation, the requested data will be sourced to the requestor

### 5.4 How to Associate User Group to the Application

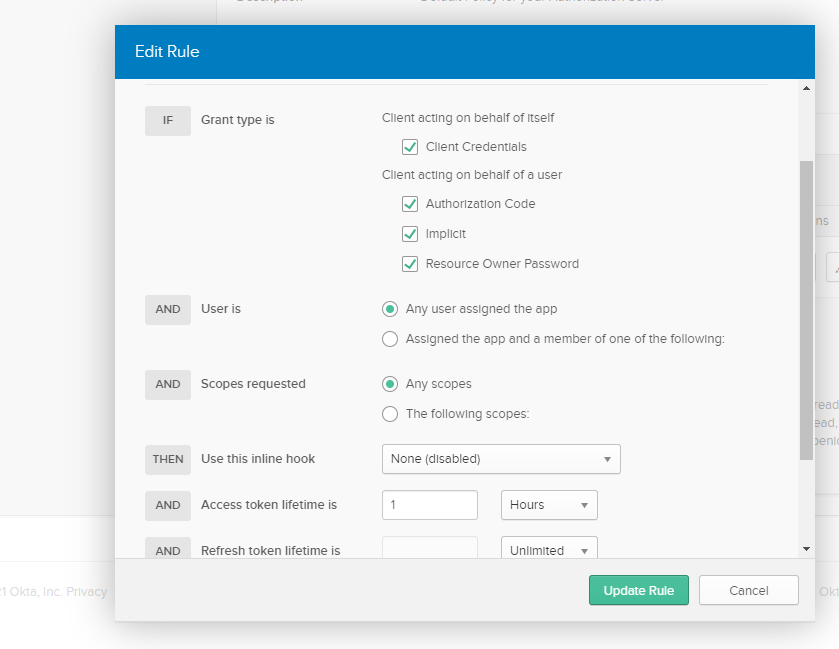
* Create user group using <https://nhpri-admin.okta.com/admin/groups> 
* For assign user group created to the Application, use <https://nhpri-admin.okta.com/admin/apps/active> and assign group using Assign group option 

### 5.5 OKTA Application, Group, Assign Application and Access Policy

In OKTA we have created Application called [NHPRI-OKTA-PROD-VONK](https://nhpri-admin.okta.com/admin/app/oidc_client/instance/0oaa0zmt452jNO75m4h6/) and user group [NHPRI-Members](https://nhpri-admin.okta.com/admin/group/00g88gykwqCd775nu4h6), all the users created/ create should be part of that user group and that user group has to be associated to application [NHPRI-OKTA-PROD-VONK](https://nhpri-admin.okta.com/admin/app/oidc_client/instance/0oaa0zmt452jNO75m4h6/).



We also have added Access policy created for any user that associated to application



# 6.0 Best Practices for Payers and API Developers

The Centers for Medicare and Medicaid Services (CMS) released the Interoperability and Patient Access final rule on March 9, 2020.

This final rule requires most CMS-regulated payers – specifically, Medicare Advantage (MA) organizations, Medicaid Fee-For-Service (FFS) programs, CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs), excluding issuers offering only Stand-alone dental plans (SADPs) and QHP issuers offering coverage in the Federally-facilitated Small Business Health Options Program (FF-SHOP) - to implement and maintain a secure, standards-based **Patient Access Application Programming Interface (API)** (using Health Level 7® (HL7) Fast Healthcare Interoperability Resources® (FHIR) Release 4.0.1) that allows patients to easily access their claims and encounter information, including cost (specifically, provider remittances and enrollee cost-sharing), as well as a defined sub-set of their clinical information through third-party applications of their choice.

This rule also requires MA organizations, Medicaid FFS programs, CHIP FFS programs, Medicaid managed care plans, and CHIP managed care entities to make provider directory information publicly available via a FHIR-based **Provider Directory API** accessible through a public-facing digital endpoint on the payer’s website.

In this section, you can find links to useful information and best practices to help you build and maintain a FHIR-based API, as well as best practices for payers and third-party app developers.

Please open the following spreadsheet.



## 6.1 Best Practice for Payers: Multi-person Enrollment Groups

The CMS Interoperability and Patient Access final rule applies to Qualified Health Plan (QHP) issuers on the individual market Federally facilitated Exchanges. We recommend that issuers explore ways to minimize the risk of the claims information of other members of an enrollment group from being unexpectedly shared with a third-party app when one member of an enrollment group requests that the payer share his or her claims information with an app. This could include storing and making accessible claims information for each non-minor member of an enrollment group separately.

## 6.2 Developing Third-Party Apps

The CMS Interoperability and Patient Access final rule provides app developers with an opportunity to find innovative ways to help patients access their health information and provider directory information. With this unprecedented opportunity comes an important responsibility. Here we provide information to help app developers give patients access to their health information in a way that protects their privacy and keeps their data secure.

Start by reviewing the standards payers will use to make these data available via APIs: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

Privacy and Security:

As a first step, it is important to know what laws may impact an app. A great place to start is the Federal Trade Commission’s (FTC’s) Mobile Health Apps Interactive Tool. Generally, once health information has been transmitted to a third-party app, it is no longer protected by the Health Insurance Portability and Accountability Act (HIPAA). To better understand an app’s relationship to HIPAA, see the Office for Civil Rights’ (OCR’s) HIPAA Q’s Portal for Health App Developers.

Third-party apps are subject to the FTC Act. Additional FTC resources developers may find helpful include:

• Start with Security: A Guide for Business

• Mobile Health App Developers: FTC Best Practices

In addition to these federal laws, state laws may also apply.

Beyond an app developer’s legal obligations, we strongly recommend app developers follow industry best practices to protect patient privacy and secure their health information.

## 6.3 Privacy Notice

Protecting patient privacy requires a strong privacy policy and an accessible, easy-to-read, comprehensive privacy notice. We strongly recommend that all third-party app developers clearly explain to patients that their data are no longer covered by HIPAA once the patient directs their data to be exchanged with most apps. Payers required to provide patients their data via the Patient Access API may also ask third-party developers to attest to having certain privacy provisions in place should a patient wish to use the developer’s app. For instance, they may ask if the app has a publicly available privacy policy, written in plain language, that has been affirmatively shared with the patient prior to the patient authorizing app access to their health information. When we say “affirmatively shared,” we mean that the patient had to take an action to indicate they viewed the privacy policy, such as click or check a box or boxes. Payers can ask if the privacy policy includes important information, such as, at a minimum:

* How a patient’s health information may be accessed, exchanged, or used by any person or other entity, including whether the patient’s health information may be shared or sold at any time (including in the future);
* A requirement for express consent from a patient before the patient’s health information is accessed, exchanged, or used, including receiving express consent before a patient’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 a similar transaction);
* If the app will access any other information from a patient’s device; or how a patient can discontinue app access to their data, and what the app’s policy and process is for disposing of a patient’s data once the patient has withdrawn consent.

We strongly urge developers to follow industry best practices when developing a privacy policy and consult relevant resources, such as:

CARIN Alliance Code of Conduct: https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/

ONC Model Privacy Notice: https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn

For more information visit https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index