DEVELOPER SANDBOX

Outlined below are steps to try our API using the developer sandbox and retrieve member data for sample Patient ID.

Step 1: Generate an Authorization Code

To test out the BlueCross NC API, you must first generate an authorization code and a sample token that represents a member granting consent.

Below are few details you will need for generating the code

Client ID: `AJMP7iHHEfegyn2PMzTj`

Client Secret: `OHBJ8Pl9I2ilDZ5gRY74`

RedirectURL: `https://oidcdebugger.com/debug`

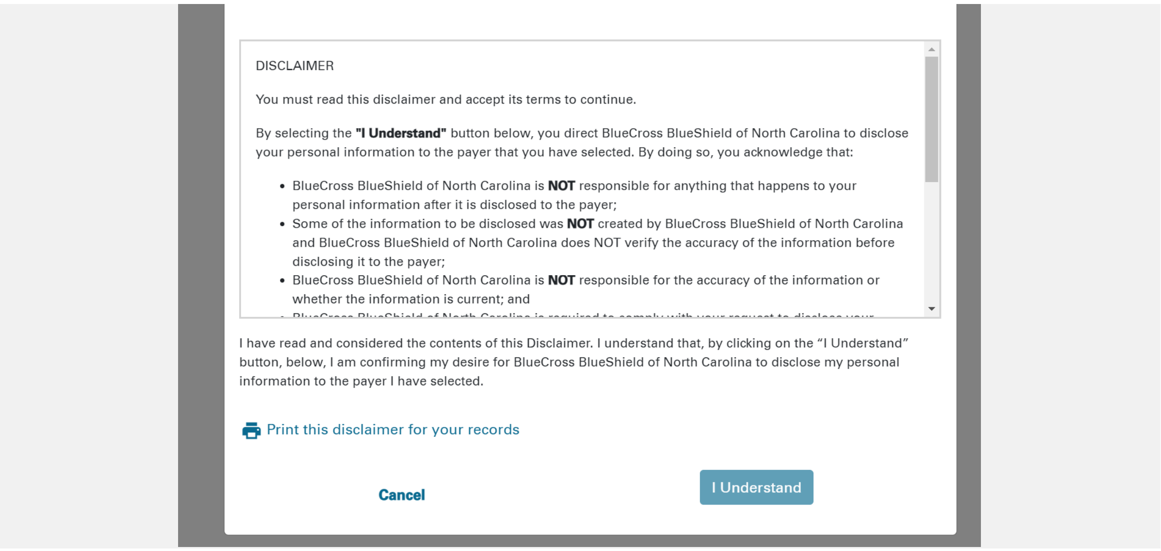
Scope:

```
clinical openID FHIRUser
```

1. Invoke the “Authorization Code” request from a browser using below syntax

```
https://oauthp2psb.bcbsnc.com/CMSP2PMemberSB/sps/oauth/oauth20/authorize?response_type=code&client_id=AJMP7iHHEfegyn2PMzTj&redirect_uri=https://oidcdebugger.com/debug&scope=openid%20read%20profile%20clinical&state=test123
```

2. You will be redirected to a disclaimer page. Review and click “I Understand” if you wish to proceed.



DISCLAIMER

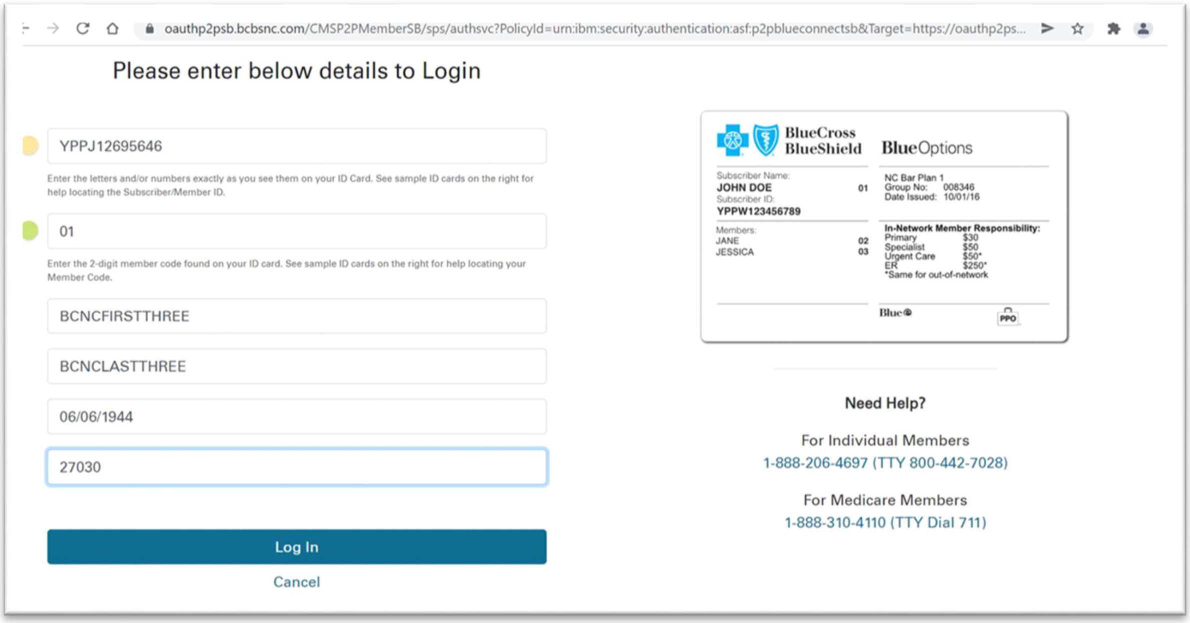
You must read this disclaimer and accept its terms to continue.

By selecting the **"I Understand"** button below, you direct BlueCross BlueShield of North Carolina to disclose your personal information to the payer that you have selected. By doing so, you acknowledge that:

- BlueCross BlueShield of North Carolina is **NOT** responsible for anything that happens to your personal information after it is disclosed to the payer;
- Some of the information to be disclosed was **NOT** created by BlueCross BlueShield of North Carolina and BlueCross BlueShield of North Carolina does NOT verify the accuracy of the information before disclosing it to the payer;
- BlueCross BlueShield of North Carolina is **NOT** responsible for the accuracy of the information or whether the information is current; and
- BlueCross BlueShield of North Carolina is required to comply with your request to disclose your

I have read and considered the contents of this Disclaimer. I understand that, by clicking on the “I Understand” button, below, I am confirming my desire for BlueCross BlueShield of North Carolina to disclose my personal information to the payer I have selected.

3. You will be redirected to a BlueCross login screen. Login with one of the synthetic beneficiary accounts



oauthp2psb.bcbsnc.com/CMSP2PMemberSB/sps/authsvc?PolicyId=urn:ibm:security:authentication:asf:p2pblueconnectsb&Target=https://oauthp2ps...

Please enter below details to Login

YPPJ12695646

Enter the letters and/or numbers exactly as you see them on your ID Card. See sample ID cards on the right for help locating the Subscriber/Member ID.

01

Enter the 2-digit member code found on your ID card. See sample ID cards on the right for help locating your Member Code.

BCNCFIRSTTHREE

BCNCLASTTHREE

06/06/1944

27030

Need Help?

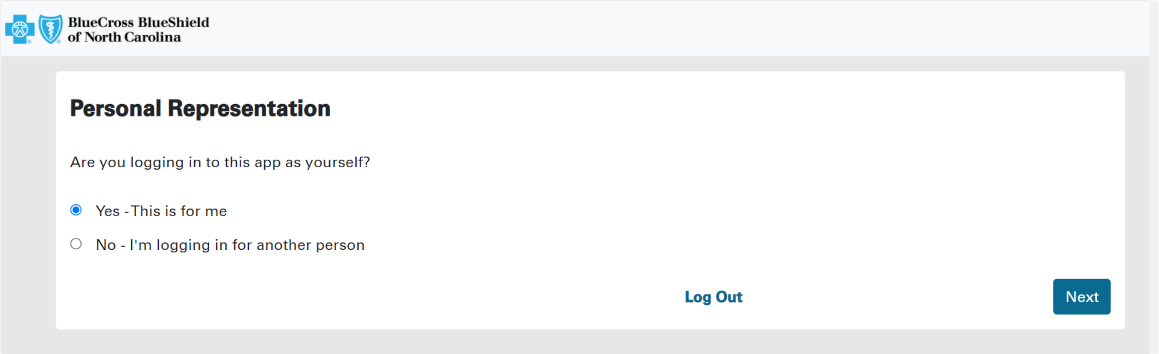
For Individual Members
1-888-206-4697 (TTY 800-442-7028)

For Medicare Members
1-888-310-4110 (TTY Dial 711)

4. **Synthetic Beneficiary Accounts**
The following test user accounts can be used for authentication and authorization:

SubscriberID	MemberCode	FirstName	LastName	DOB	Zipcode
YPPJ12695646	01	BCNCFIRSTTHREE	BCNCLASTTHREE	06/06/1944	27030

5. After successful member authentication, you are presented with a screen to indicate if you are accessing data for "Self" or as a "Personal Representative".



Personal Representation

Are you logging in to this app as yourself?

● Yes -This is for me

○ No - I'm logging in for another person

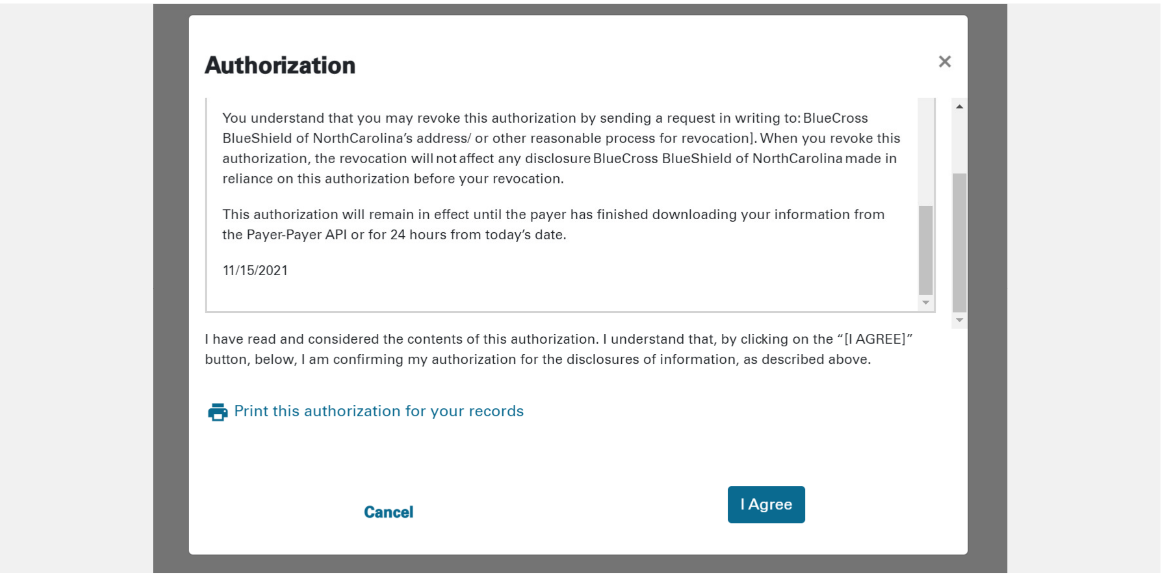
6. You are redirected to the "Authorization / Consent page".

   - If Personal Representative option is selected, you will need to choose from one of the options below in order to proceed to the "Authorization / Consent page"

a. Parent or Guardian of a minor
b. Active Healthcare Power of Attorney
c. Court ordered guardianship
d. Other

- You will be presented a text field entry to enter the full name
- If the option "Other" is chosen, you are presented with a text field entry to enter the relationship to the member
- Click “Next” to proceed to the “Authorization / Consent page”

7. Need to review the “Authorization / Consent page” and scroll to the bottom of the screen to click “I Agree” in order to “Authorize”



Authorization

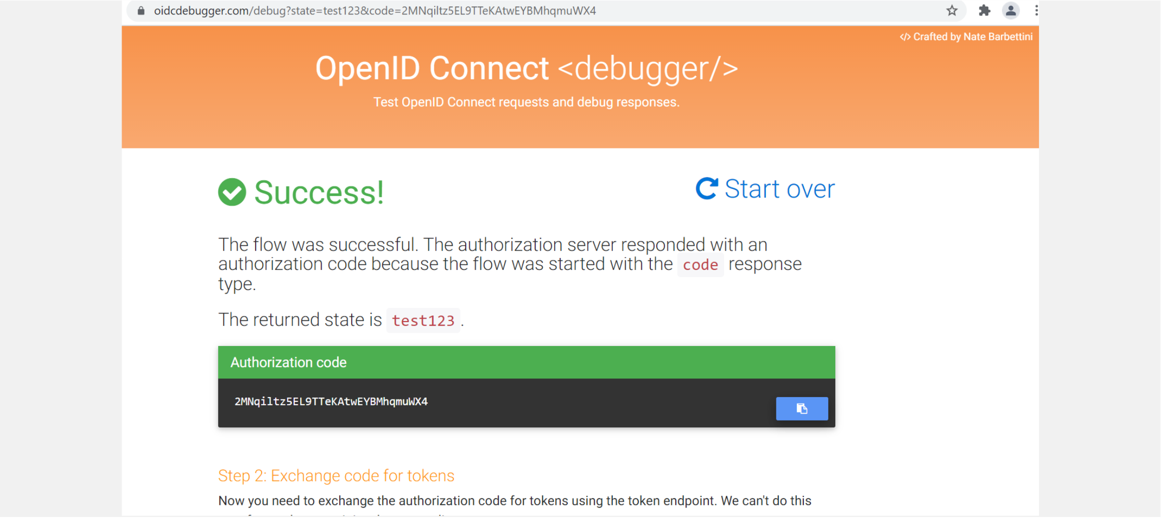
You understand that you may revoke this authorization by sending a request in writing to: BlueCross BlueShield of NorthCarolina’s address/ or other reasonable process for revocation]. When you revoke this authorization, the revocation will not affect any disclosure BlueCross BlueShield of NorthCarolina made in reliance on this authorization before your revocation.

This authorization will remain in effect until the payer has finished downloading your information from the Payer-Payer API or for 24 hours from today’s date.

11/15/2021

I have read and considered the contents of this authorization. I understand that, by clicking on the “[I AGREE]” button, below, I am confirming my authorization for the disclosures of information, as described above.

8. You will be redirected to your app’s redirect screen and the “Authorization code” will be sent in the response URL. The “Authorization code” is valid for 1 hour



oidcdebugger.com/debug?state=test123&code=2MNqiltz5EL9TTeKAtwEYBMhqmuWX4

Crafted by Nate Barbettini
OpenID Connect <debugger/>
Test OpenID Connect requests and debug responses.
Success!
Start over

The flow was successful. The authorization server responded with an authorization code because the flow was started with the `code` response type.

The returned state is `test123`.

Authorization code

```
2MNqiltz5EL9TTeKAtwEYBMhqmuWX4
```

Step 2: Exchange code for tokens

Now you need to exchange the authorization code for tokens using the token endpoint. We can't do this

Step 2: Generate a sample token

Access Token URL:

```
https://oauthp2psb.bcbsnc.com/CMSP2PMemberSB/sps/oauth/oauth20/token
```

Example using curl syntax

```
curl -v -k -H "Content-Type: application/x-www-form-
urlencoded;charset=UTF-8" -d
"grant_type=authorization_code&code=[Insert_Auth_Code]&redirect_uri=[In
sert_Redirect_URL]&client_id=[Insert_Client_Id]&client_secret=[Insert_C
lient_Secret]&state=test" https://oauthp2psb.bcbsnc.com/CMSP2PMemberSB/
sps/oauth/oauth20/token
```

State: An optional value that you may use in your app

Response

```
{
  "access_token":
"eyJraWQiOiJ3QThGR3hrM3pWa1FrYU9qUW11aWxTTlJGUWp2bHNzaTJna",
  "patient": "2657",
  "scope": "clinical read openid profile",
  "id_token": "eyJraWQiOiJ3QThGR3hrM3pWa1FrYU9qU",
  "token_type": "bearer",
  "expires_in": 86399
}
```

The response will contain a “Patient ID” that needs to be used as a search criteria for API data requests.

Step 3: Try a sample API

Try this out in Postman:

1. From the Postman app, open a new tab
2. Paste the Request URL:

   With the access token, you can use Curl to make queries as follows:

```
curl --header "Authorization: Bearer YOUR TOKEN HERE"
https://apiservicessb-ext.bcbsnc.com/fhir/sb/R4/payer-to-
payer/Patient/<FHIRPatientId>/$everything
```

NOTE: When a beneficiary is authorizing your application, they will not be presented the choice to select any scope**. Only the app has the ability to choose what scope is required when making a request for the token.**

3. Click “Send” and see the synthetic beneficiary’s personal health information as a Patient FHIR Resource display under “Body” in Postman

Step 4: Configure your app to enable connectivity to BlueCross NC with the following Authorization endpoint and the set of static ClientId and ClientSecret

Auth URL:

```
https://oauthp2psb.bcbsnc.com/CMSP2PMemberSB/sps/oauth/oauth20/authorize
```

Client ID: `AJMP7iHHEfegyn2PMzTj`

Client Secret: `OHBJ8Pl9I2ilDZ5gRY74`

Step 5: Accessing Synthetic Data In order to access the full synthetic dataset for an individual synthetic beneficiary, you can do the following:

1. Set up your sandbox application

   Access the authorization url at

```
https://oauthp2psb.bcbsnc.com/CMSP2PMemberSB/sps/oauth/oauth20/authorize/
```

   Note: The last backslash is important. Also remember to append `?client_id={your client_id assigned to the application you registered}`

2. You will be redirected to the BlueCross authentication screen. DO NOT ACCESS THIS PAGE DIRECTLY.

3. The following test user account can be used for authentication and authorization

   Synthetic Beneficiary Accounts

SubscriberID	MemberCode	FirstName	LastName	DOB	Zipcode
YPPJ12695646	01	BCNCFIRSTTHREE	BCNCLASTTHREE	06/06/1944	27030

4. Approve access for your application, which will now receive an access token, which can be used in the requests described above.

5. The authorization completes when you are redirected back to the Redirect_URI you specified when you registered your application.

FAQs

Authorization

To use the BlueCross NC OAuth 2 a developer must **register** their application.

A registered application is given a client ID and a client secret. The secret should only be used if it can be kept confidential, such as communication between your server and the BlueCross NC API. Otherwise the **Client Application Flow** may be used.

NOTE : For sandbox environment, static clientId, clientSecret will be shared. This is registered by BlueCross team internally with a static redirect URL and will need to be configured by the client in order to initiate authorization request.

Scopes

Access tokens have a scope, which defines what the access token can do and what resources it can access. For our purposes, scopes are primarily utilized to give beneficiaries more granular choice over what data they would like to share with applications. The BlueCross NC API has implemented **a default scope** to restrict read & write access to only the clinical resources as defined by HL7

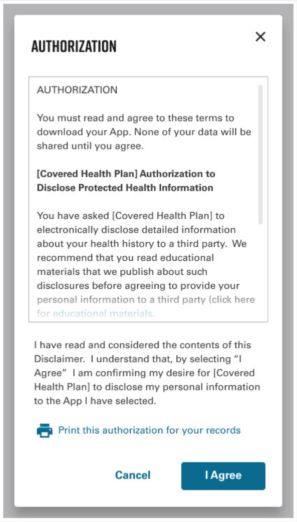
```
Clinical/*.*
```

From the OpenID Connect specification we support:

```
profile
```

This gives access to the fhir/sb/R4/payer-to-payer/UserInfo Endpoint.

Our implementation gives apps the ability to choose OpenID scope.



AUTHORIZATION

AUTHORIZATION

You must read and agree to these terms to download your App. None of your data will be shared until you agree.

[Covered Health Plan] Authorization to Disclose Protected Health Information

You have asked [Covered Health Plan] to electronically disclose detailed information about your health history to a third party. We recommend that you read educational materials that we publish about such disclosures before agreeing to provide your personal information to a third party (click here for educational materials.

I have read and considered the contents of this Disclaimer. I understand that, by selecting "I Agree" I am confirming my desire for [Covered Health Plan] to disclose my personal information to the App I have selected.

If the beneficiary declines to share information that your application needs to function, you may display a message explaining why that information is needed and request reauthorization or handle the collection of that information elsewhere within your application.

The default selection when a beneficiary reaches the authorization screen will be to share all clinical data, including demographic data, with your application. If a beneficiary makes a selection as to whether or not they want to share demographic data with your application and later decides they want to change that selection, they'll need to be taken through the authorization flow again to make a different choice from the OAuth screen.

Native Mobile App Support

Native Mobile App Support follows the RFC 8252 - OAuth 2.0 for Native Apps authentication flow utilizing the PKCE extension and enables a custom URI scheme redirect.

The implementation of the RFC 8252 specification enables developers to build mobile applications without requiring a proxy server to route redirect calls to their mobile app.

The PKCE extension provides a technique for public clients to mitigate the threat of a "man-in-the-middle" attack. This involves creating a secret that is used when exchanging the authorization code to obtain an access token.

PKCE uses a code challenge that is derived from a code-verifier. The standard supports two styles of code challenge:

- plain
- S256

Redirect_URI

When registering an Application, a redirect URI is required. This is the API endpoint on *your* system that receives the callback from the BlueCross NC API after a beneficiary is passed to the BlueCross NC API to authorize your application.

Web Application Flow

To use this flow your application should be registered with `Client Type` set to `confidential` and `Grant Type` set to `authorization-code`.

Core Resources

Base Request URL:

```
https://apiservicessb-ext.bcbsnc.com/fhir/sb/R4/payer-to-payer
```

FHIR Resources:

- All Clinical resources as defined in DaVinci IG - http://hl7.org/fhir/us/davinci-pdex/toc.html

  Note : Patient/<FHIRID>/$everything is supported and will need to be used by clients to initiate data request and receive a bundle response. Individual FHIR resources are not supported.

UserInfo:

- Get User Profile from an Authorization Token

FHIR Resource Bundle

```
/fhir/sb/R4/payer-to-payer/Patient/2657/$everything
```

The above URL returns all of the beneficiary’s clinical records as an FHIR Resource Bundle.

```
curl --header "Authorization: Bearer AUTHORIZATION TOKEN"
"https://apiservicessb-ext.bcbsnc.com/fhir/sb/R4/payer-to-payer/Patient/2657/$everything"
```

That API call will return a bundle that contains many FHIR resources and is typically thousands of lines long.

```
{
    "resourceType": "Bundle",
    "id": "989f6d15-43e9-429f-97a5-93de5dc1e89b",
    "meta": {
        "lastUpdated": "2021-11-22T20:24:03.946-05:00"
    },
    "type": "searchset",
    "link": [
        {
            "relation": "self",
            "url": "https://apiservicessb-ext.bcbsnc.com/fhir/sb/R4/payer-to-payer/Patient/2657/$everything"
        }
    ],
    "entry": [
        {
            "fullUrl": "https://apiservicessb-
ext.bcbsnc.com/fhir/sb/R4/payer-to-payer/Patient/2657",
            "resource": {
                "resourceType": "Patient",
                "id": "2657",
                "meta": {
                    "versionId": "2",
                    "lastUpdated": "2021-11-22T14:53:07.885-05:00",
                    "source": "#PuvVum8uEowtNfhY",
                    "profile": [
                        "http://hl7.org/fhir/us/carin-
bb/StructureDefinition/C4BB-Patient",
                        "http://hl7.org/fhir/us/core/StructureDefinition/us-
core-patient"
                    ]
                },
                "identifier": [
                    {
                        "type": {
                            "coding": [
                                {
                                    "system":
"http://terminology.hl7.org/CodeSystem/v2-0203",
                                    "code": "MB"
                                }
                            ]
                        },
                        "system":
"http://bluecrossnc.com/fhir/memberidentifier",
                        "value": "J1269564601"
                    }
                ],
                "name": [
                    {
                        "family": "BCNCLASTTHREE",
                        "given": [
                            "BCNCFIRSTTHREE"
                        ]
                    }
                ],
                "gender": "female",
                "birthDate": "1944-06-06",
                "address": [
                    {
                        "line": [
                            "23 WESTERN ST"
                        ],
                        "city": "MOUNT AIRY",
                        "state": "NC",
                        "postalCode": "27030"
                    }
                ]
            },
            "search": {
                "mode": "match"
            }
        },
        {
            "fullUrl": "https://apiservicessb-
ext.bcbsnc.com/fhir/sb/R4/payer-to-payer/Provenance/4e44a0f0-e723-3f1b-a6de-
a3f5023630d0",
            "resource": {
                "resourceType": "Provenance",
                "id": "4e44a0f0-e723-3f1b-a6de-a3f5023630d0",
                "meta": {
                    "versionId": "1",
                    "lastUpdated": "2021-08-04T08:58:05.801-04:00",
                    "source": "#sAN2NtgMboFqXbTd",
                    "profile": [
                        "http://hl7.org/fhir/us/core/StructureDefinition/us-
core-provenance"
                    ]
                },
                "target": [
                    {
                        "reference": "Patient/2657",
                        "identifier": {
                            "type": {
                                "coding": [
                                    {
                                        "system":
"http://terminology.hl7.org/CodeSystem/v2-0203",
                                        "code": "MB"
                                    }
                                ]
                            },
                            "value": "J1269564601"
                        }
                    },
                    {
                        "reference": "Condition/26efcfd2-acfb-31bb-b2fe-
b48574ff188f"
                    },
                    {
                        "reference": "Procedure/6dac3a0e-283b-3a37-a1aa-
b98214efa5ef"
                    }
                ],
                "recorded": "2018-10-10T00:00:00.000-04:00",
                "agent": [
                    {
                        "type": {
                            "coding": [
                                {
                                    "system":
"http://terminology.hl7.org/CodeSystem/provenance-participant-type",
                                    "code": "author"
                                }
                            ]
                        },
                        "who": {
                            "reference": "Organization/BCBSNC"
                        }
                    }
                ]
            },
            "search": {
                "mode": "match"
            }
        }

        ...this is only a subset of the entire output...
```

Get User Profile for an Authorization Token

```
HTTP GET /connect/userinfo
```

The UserInfo Endpoint is an OAuth 2.0 Protected Resource.The above URL fetches the fictitious beneficiary's basic account information given an Authorization Token. This is most often used when creating an account within your application. An HTTP GET is called and the response is returned as JSON.

```
curl --header "Authorization: Bearer AUTHORIZATION TOKEN"
"https://apiservicessb-ext.bcbsnc.com/v1/connect/userinfo"
{
  "sub": "fflinstone",
  "prefered_username": "fflinstone",
  "given_name": "Fred",
  "family_name:, "Flinstone,
  "name": "Fred Flinstone",
  "email": "pebbles-daddy@example.com",
  "created": "2017-11-28",
  "patient": "123456789",
}
```