

## NextGen® Office Patient Access API Developer Guide

for NextGen® Office

Prepared by NextGen R&D May 31st, 2023

Confidential – Proprietary Information

Property of NextGen Healthcare Information Systems, LLC and its parent company NextGen Healthcare, Inc. (collectively "Company"). For Use By Authorized Company Clients Only.

NOTICE: This document contains information that is confidential and proprietary to Company and is intended for use solely by its authorized clients. This document may not be copied, reproduced, published, displayed, otherwise used, transmitted, or distributed in any form by any means as a whole or in any part, nor may any of the information it contains be used or stored in any information retrieval system or media, translated into another language, or otherwise made available or used by anyone other than the authorized client to whom this document was originally delivered without the prior, written consent of Company.

By retaining or using this document, you represent that you are a client or an authorized representative of a client of Company who is authorized to use this document under one or more agreements between you and Company now in force, and that you will use this document and the information it contains solely as and to the extent those agreements permit. Any other use or distribution of the contents of this document, as a whole or in any part, is prohibited. Although we exercised great care in creating this publication, Company assumes no responsibility for errors or omissions that may appear in this publication and reserves the right to change this publication at any time without notice.

© 2023 NXGN Management, LLC. All Rights Reserved.

NextGen® Office EHR – Pat. 8,947,374 and 9,791,999

NextGen® is a registered trademark of NXGN Management, LLC. All other names and marks are the property of their respective owners.

## Purpose of this document

This document is written for developers building client applications that connect to the NextGen® Office Patient API. These client applications give patients access to their health records in the application of their choosing, outside of access via YourHealthFile.com.

This document covers the following:

- 1. How to register as a client application and gain access credentials
- 2. A detailed walk-through of using the NextGen® Office Patient Access API

Page **2** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

# How to register your client application to access NextGen® Office Patient Access API

Send an email to nextgen-office-api@nextgen.com with the following information:

- Contact e-mail address
- Organization name
- Organization description
- Client application name
- Client application use-case description
- OAuth Callback URL (should not include query parameters)
- The NextGen® Office API team will issue client credentials and/or request additional information.

## Detailed walk-through of using the NextGen® Office Patient Access API

The following instructions are from an internal validation of the NextGen® Office Patient Access API. These instructions exercise API authentication & data retrieval process as would a 3<sup>rd</sup> Party Developer whose application Callback URL had been registered by NextGen® Office and had subsequently been issued the requisite application credentials (i.e., client ID & client secret) and test patient credentials (i.e., NextGen® Office Patient API username & password).

#### **Test Patients:**

- Smith, David HF428946492 (UN/PW: DavidFHIR/password)
- Smith, Anna HF428946523 (UN/PW: AnnaFHIR/Password01)
- Smith, Alex HF429119572 (UN/PW: AlexSmithFhir/Password01)
  - Grant Type: Authorization Code (With PKCE)
  - Callback URL: https://oauth.pstmn.io/v1/callback
  - Authorization URL: https://idp-

prod.prod.ngo.nextgenaws.net/auth/realms/nextgen/protocol/openid-

connect/auth?aud=https://fhir.meditouchehr.com/api/fhir/r4

Page **3** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

- Access Token URL: <a href="https://idp-prod.prod.prod.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/token">https://idp-prod.prod.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/token</a>
- Test Client ID: yourHealthFile
- Test Client Secret: P2uCnXestgMxmLWnlUXNDO8u98qPa4NZ
- Code Challenge Method: SHA-256
- Code Verifier: {RANDOM STRING WITH 43 TO 128 CHARS}
- **Scope:** {Add Allowed scopes}
- State: Blank
- Client Authentication: Send as Basic Auth header.
- Test Patient's NextGen® Office Patient Access API Credentials:

UN: DavidFHIRPW: password

### Validation Process Steps

The steps below can be performed either manually with a tool like **curl** or using **Postman** which automates steps like OAuth token generation.

Once we fill in the above authorization data, we can generate an authorization code by launching the URL generated in the Browser.

#### 1. Open Authorize URL in Browser:

The expected Authorize URL components are:

- a. Endpoint: <a href="https://idp-prod.prod.ngo.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/auth?aud=https://fhir.meditouchehr.com/api/fhir/r4">https://idp-prod.prod.ngo.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/auth?aud=https://fhir.meditouchehr.com/api/fhir/r4</a>
- b. **Parameters**:
- i. response\_type=code
- ii. client\_id={CLIENT\_ID\_ASSIGNED\_TO\_DEVELOPER}
- iii. redirect Uri={APP\_REDIRECT\_URL}
- iv. scope={APP\_REDIRECT\_SCOPE}
- v. Code Verifier={RANDOM STRING WITH 43 TO 128 CHARS}
- vi. code challenge method=SHA-256

#### Example Authorize URL Launched by 3<sup>rd</sup> Party App:

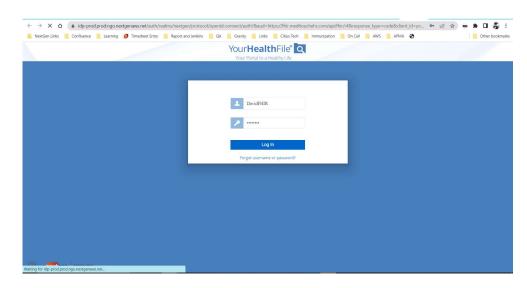
App

https://idp-prod.prod.ngo.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/auth?&aud=https://fhir.meditouchehr.com/api/fhir/r4&response\_type=code&client\_id =yourHealthFile&scope=openid%20patient%2FMedication.read%20patient%2FCondition.read%20patient%2FPatient.read%20offline\_access%20patient%2FAllergyIntolerance.read%20fhirUser%20patient%2FCareTeam.read%20patient%2FDevice.read%20launch%2Fpatient%20patient%2F

Page **4** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

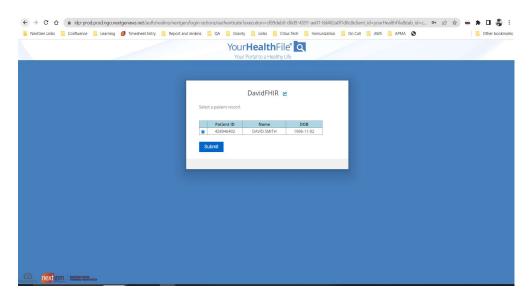
<u>DiagnosticReport.read%20patient%2FCarePlan.read%20patient%2FDocumentReference.read&redirect\_uri=https%3A%2F%2Foauth.pstmn.io%2Fv1%2Fcallback&code\_challenge=aXlhsuyOvsg282Uf4ltfGM6BnStnKKX\_kLyEbSWyud0&code\_challenge\_method=S256</u>

#### 2. Patient Enters their NextGen® Office Patient Access API Credentials:

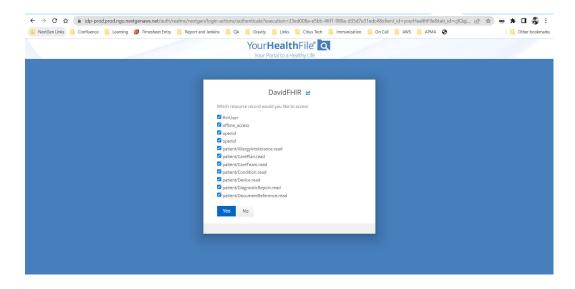


#### Note:

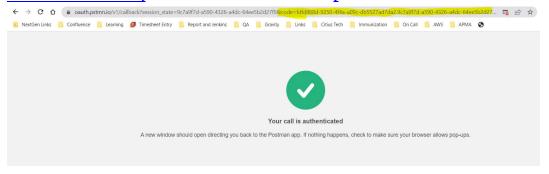
This screen will display only the Master patient if there aren't any dependent patients.



Page **5** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.



3. **Authorization Code is returned in URL** upon successful authentication (Example: <a href="https://oauth.pstmn.io/v1/callback?session\_state=e2f5354f-0c19-40ec-bf27-9f41fe6de65b&code={ISSUED AUTHORIZATION CODE}</a>



- 4. Exchange Authorization Code for Token:
  - a. The expected components of the request to the access token route are:

i. **Method**: POST

ii. **Endpoint**: <a href="https://idp-">https://idp-</a>

prod.prod.ngo.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/token

- iii. Authorization: Basic Auth: Enter Client ID and Client Secret
- iv. Headers:
  - 1. Content-Type = application/x-www-form-urlencoded
  - 2. A Basic Authorization header (Authorization=Basic {encoded string} using a base64 encoded representation of the following string: client\_id:client\_secret

#### Authorization Header Example:

Authorization= Basic {base64 encoded representation of client id: client secret}

Page **6** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

- v. **Body**: (x-www-form-urlencoded)
  - 1. grant type=authorization code
  - 2. code= {ISSUED AUTHORIZATION CODE}
  - 3. redirect\_uri={APP\_REDIRECT\_URL}
  - 4. Code Verifier= {Use the same code verifier as used while generating code}

#### Example Request to /access token (curl Format):

```
curl --location --request POST 'https://idp-prod.prod.ngo.nextgenaws.net/auth/realms/nextgen/protocol/openid-connect/token' \
---
header 'Authorization: Basic eW91ckhlYWx0aEZpbGU6VmpwN0RGVlJSVXl2UTU0QVVPS
XJqSjdNQW1ZSUtOSno=' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'grant_type=authorization_code' \
--data-urlencode 'code=c8b55047-2275-4570-8a30-c56bedaf2564.6fd6bfcf-55a5-47f7-b067-a233e178944c.52449374-f741-427d-859f-f88ca01dbea0' \
--data-urlencode 'redirect_uri=https://oauth.pstmn.io/v1/callback' \
--data-urlencode 'code_verifier=thisisasecretciodetotesttheauthorizationoforintegrationtesting'
```

- b. A successful call to /access token will produce a response that includes:
  - i. The access token
  - ii. expires in.
  - iii. refresh\_expires\_in;
  - iv. refresh\_token
  - v. token\_type
  - vi. id\_token
  - vii. not-before-policy
  - viii.session\_state
  - ix. scope
  - x. resource
  - xi. patient
  - xii. need\_patient\_banner
  - xiii.practice id
  - xiv.smart\_style\_url

Page **7** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

```
xv. client_type
xvi.subscription_type
```

#### Example Response from /access token

```
{
"access_token": "{access_token_value}",
"expires_in": (expressed in seconds),
"refresh_expires_in": (expressed in seconds),
"refresh_token": "{refresh_token_value}",
"token_type": "Bearer",
"id token": "{id token value}",
"not-before-policy": 1661487077,
"session state": 9c7a9f7d-a590-4326-a4dc-64ee5b2d27f9
"scope": "{assigned_scope}",
"resource": "Person/4007449",
"patient": " 428946492",
"need_patient_banner": "false",
"smart style url": "
https://fhir.meditouchehr.com/electronic/json/api/portalSmartStyleConfig.json ",
"client_type": "STANDALONE"
"subscription_type": "Indefinite"
```

#### 5. Request FHIR Resource: {FHIRurl}/Patient/{id}

Using the "Reference Value" URL from the prior request, obtain FHIR resource data from the {FHIRurl}/Patient/{id} endpoint.

- a. Method: GET
- b. **Endpoint**: https://fhir.meditouchehr.com/api/fhir/r4/Patient/428946492
- c. **Authorization: Bearer Token:**{Token generated in previous step}
- d. **Header**: An OAuth2 Authorization header with a value of Bearer {access\_token}
- e. Example Request to {FHIRurl}/Patient/{id}:
   curl --location --request GET
   'https://fhir.meditouchehr.com/api/fhir/r4/Patient/428946492'\
   --header 'Authorization: Bearer {access token value}'\
- f. Response from {FHIRurl}/Patient/{id}:

```
"resourceType": "Patient",
    "id": "428946492",
    "extension": [
        {
            "url": "http://hl7.org/fhir/us/core/StructureDefinition/us-core-race",
            "extension": [
                {
                    "url": "ombCategory",
                    "valueCoding": {
                         "system": "urn:oid:2.16.840.1.113883.6.238",
                         "code": "1002-5",
                         "display": "American Indian or Alaska Native"
                    }
                },
                    "url": "text",
                    "valueString": "American Indian or Alaska Native"
                }
            ]
        },
            "url": "http://hl7.org/fhir/us/core/StructureDefinition/us-core-
ethnicity",
            "extension": [
                {
                    "url": "ombCategory",
                    "valueCoding": {
                         "system": "urn:oid:2.16.840.1.113883.6.238",
                         "code": "2135-2",
                         "display": "Hispanic or Latino"
```

Page **9** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

```
},
                {
                     "url": "detailed",
                     "valueCoding": {
                         "system": "urn:oid:2.16.840.1.113883.6.238",
                         "code": "2138-6",
                         "display": "Andalusian"
                    }
                },
                {
                    "url": "text",
                     "valueString": "Hispanic or Latino"
                }
            ]
        },
            "url": "http://hl7.org/fhir/us/core/StructureDefinition/us-core-
birthsex",
            "valueCode": "M"
        }
    ],
    "identifier": [
        {
            "use": "official",
            "type": {
                "coding": [
                    {
                         "system": "http://terminology.hl7.org/CodeSystem/v2-0203",
                         "version": "1.0",
                         "code": "MR",
                         "display": "Medical record number"
                    }
                ],
                "text": "Unique Id for EHR"
            "system": "http://terminology.hl7.org/CodeSystem/v2-0203",
            "value": "428946492",
            "assigner": {
                "reference": "Organization/1673497"
            }
        }
    ],
    "active": true,
    "name": [
        {
            "use": "usual",
            "family": "SMITH",
            "given": [
                "DAVID"
```

Page **10** of **12** Confidential – Proprietary Information – For Use By Authorized Company Clients Only. Do Not Distribute.

```
],
    "telecom": [
        {
            "system": "phone",
            "value": "(621)654-6545",
            "use": "home"
        }
    ],
    "gender": "male",
    "birthDate": "1996-11-02",
    "address": [
        {
            "line": [
                "PUNE"
            "city": "SOLANA BEACH",
            "state": "TX",
            "postalCode": "73301",
            "period": {
                "start": "2023-04-18T22:48:58-07:00",
                "end": "2023-04-20T01:32:32-07:00"
            }
        }
    ],
    "communication": [
        {
            "language": {
                "coding": [
                    {
                         "system": "urn:ietf:bcp:47",
                         "code": "en",
                         "display": "English"
                    }
                ]
            },
            "preferred": true
        }
   ]
}
```

#### 6. Request Additional FHIR Resources

Please consult the full documentation at

https://petstore.swagger.io/?url=https://hfstatic.s3.amazonaws.com/swagger/swaggerR4.yaml to obtain the full set of available endpoints and details for calling those additional NextGen® Office Patient Access API routes using the obtained Patient {id}.

- a. Method: GET
- b. Base URL + Endpoint:

https://fhir.meditouchehr.com/api/fhir/r4/{endpoint}

c. **Header**: An OAuth2 Authorization header with a value of Bearer {access\_token}