Technical Documentation

Carelogic API allows the external developer community to create applications that provide Patient engagement across the Internet of Things (IoT). Your apps will be able to make read only data requests for patient health information (specific data category or all data) for a specific date, date range or all data.

Our API feature is providing more options for electronic health information exchange for the consumer (patient). It will also serve as another option for consumer (patient), particularly those who will request information through a mobile device or tablet.

Get started today!

You can follow these steps to begin development of an application with the Carelogic Enterprise S3 API.

Step 1: Sign up

User onboarding

To use Carelogic API portal you must register an account.
Account registration requires:

- Company Name
- Company email address
- Company cell phone
- Application name
- Application/company URL
- Unique username
- Password
- List of IP Address(es) to be whitelisted

To register:

1. Send the required information to carelogiconcapirequest@qualifacts.com, with Subject: Registration for API access
2. Carelogic sends a confirmation email with Terms of Use attached.
3. Application developer replies indicating that accepts the Terms of Use
4. Carelogic register the application (OAuth credentials)
5. Carelogic sends API key & secret to developer

315 Deaderick Street, Suite 2300 Nashville, TN 37238 qualifacts.com

Note: The application name is editable after you accept registration.

No additional cost for accessing or using the ONC APIs.

Step 2: Authenticate using OAuth 2.0

Carelogic APIs use the OAuth 2.0 protocol for authentication and authorization, as explained below:

For running a test you need the following:

1. API Key and Secret: this is available after Step 1
2. OAuth Server
3. API Server
4. User's credentials

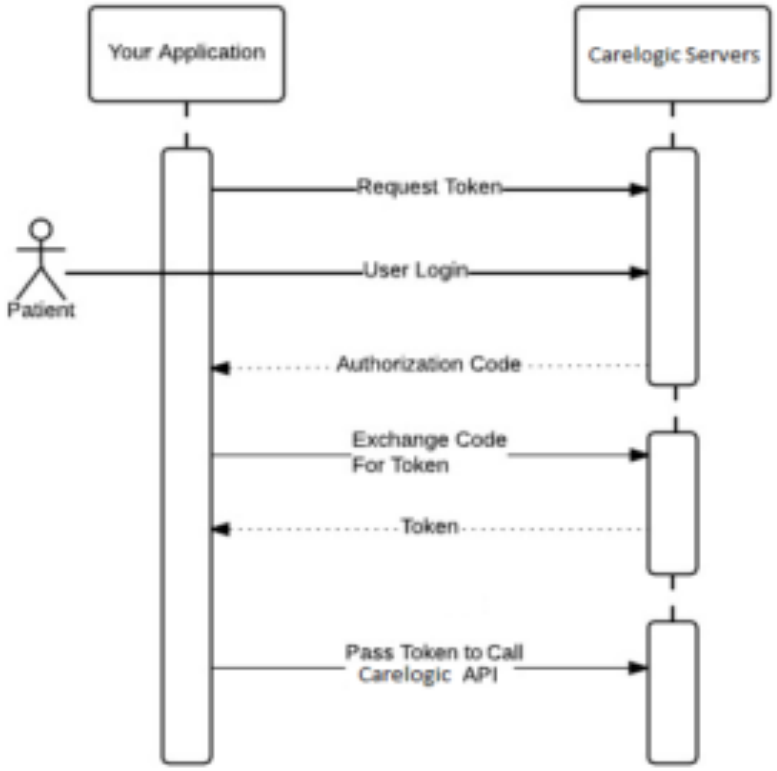
To get you started, here are some of the dummy user credentials that you can use with any of the following flows

Username: apidemo@dummy.com
Password: 1q#$%^
Test OAuth Server: https://login.qualifacts.org/authorization/oauth/authorize
Test API Server: https://login.qualifacts.org/api/gateway/fhir

Authorization code

In this flow, you get access to a refresh token (to generate a new access token) and the validity of the access token on behalf of the authenticated user.

Here's the flow diagram for obtaining the bearer access token using the authorization code grant type:



Listed below are the endpoints you need in order to get the authorization code, the access/refresh token, and token validity.

Relative endpoint paths

1. Authorize Code Endpoint: /oauth/authorize

- This endpoint gets you the authorization code (through the redirect URL registered during application creation) It needs to be called from a web interface (browser) in order to present the login page for the actual user for authenticating yourself. Then, the authorization code returns in the response using the redirect URL.
- Method: GET
- Request query parameters:

Parameter Name	Parameter Value
response_type	code
client_id	(associated with registered application)
redirect_uri	(associated with registered application)

2. Get Token Endpoint: /oauth/token

- This endpoint will return the bearer an access token for the authenticated user based on the input parameters (listed below), along with the refresh token, and access token validity (remaining in seconds).
- Method: POST
- Header:
- Content-Type: application/x-www-form-urlencoded
- Authorization:
  Basic 1M2YzOjVlZDU4YTQwYmNhZjRmNzM5YTNhMDIxNTU5NDJlZDkx
  "1M2YzOjVlZDU4YTQwYmNhZjRmNzM5YTNhMDIxNTU5NDJlZDkx" is Base64 encoded value of 'API Key:API Secret'
- Request body:

Parameter Name	Parameter Value
grant_type	authorization_code code
redirect_uri	(associated with registered application)
redirect_uri	(associated with registered application)

Note: It is recommended to always use HTTPS (secured) URL for the callback/redirect URL

Step 3: Access API

Note: We strongly recommend using this version of postman: https://dl.pstmn.io/download/version/5.3.0/windows64

Once the access token has been retrieved on behalf of the user from the OAuth server, all the secured APIs can be accessed subsequently on the API Server.

Pass the header information as listed below for authentication on each API:
Header:
Authorization:
Bearer

315 Deaderick Street, Suite 2300 Nashville, TN 37238 qualifacts.com

FHIR Services Documentation

Please refer to the following link for FHIR services documentation:
https://qualifacts-fhir.api-docs.io/v1

AllergyIntolerance API example:

1. Endpoint: /api/gateway/fhir/v1/AllergyIntolerance
2. HTTP Method: GET

Request headers:
Content-Type: application/json
Authorization: Bearer

Request format

GET https://qualifactserver/api/fhir/v1/AllergyIntolerance
[no cookies]
Request Headers:
Authorization: Bearer a310631c-29ae-4875-a6b5-9a550b008e12
Content-Type: application/json
Host: qualifactserver

Response format (application/json+fhir)


```
{
  "resourceType": "Bundle",
  "entry": [
    {
      "resource": {
        "resourceType": "AllergyIntolerance",
        "identifier": [
          {
            "system": "YCU",
            "value": "30080"
          }
        ],
        "onset": "2011-01-01T00:00:00+00:00",
        "patient": {
          "reference":
"Patient/565b1be3-45e1-4717-bb07-0ele5aed52ca"
        },
        "substance": {
          "coding": [
            {
              "system": "RXNorm",
              "code": "863538"
            }
          ],
          "text": "PENICILLIN G POTASSIUM"
        },
        "status": "active",
        "category": "medication",
        "lastOccurence": "2011-01-01T00:00:00+00:00",
        "reaction": [
          {
            "manifestation": [
              {
                "coding": [
                  {
                    "system": "SNOMED CT",
                    "code": "424988008"
                  }
                ],
                "text": "Anemia due to substance"
              }
            ]
          }
        ]
      }
    }
  ]
}
```


315 Deaderick Street, Suite 2300 Nashville, TN 37238 qualifacts.com

```
{
 “resourceType”: “Bundle”,
 “entry”: [
  {
   “resource”: {
    “resourceType”: “AllergyIntolerance”,
    “identifier”: [
     {
      “system”: “YCU”,
      “value”: “30080”
     }
    ],
    “onset”: “2011-01-01T00:00:00+00:00”,
    “patient”: {
     “reference”: “Patient/565b1be3-45e1-4717-bb07-0e1e5aed52ca”
    },
    “substance”: {
     “coding”: [
      {
       “system”: “RXNorm”,
       “code”: “863538”
      }
     ],
     “text”: “PENICILLIN G POTASSIUM”
    },
    “status”: “active”,
```

```
      “category”: “medication”,
      “lastOccurence”: “2011-01-01T00:00:00+00:00”,
      “reaction”: [
       {
        “manifestation”: [
         {
          “coding”: [
           {
            “system”: “SNOMED CT”,
            “code”: “424988008”
           }
          ],
          “text”: “Anemia due to substance”
         }
        ]
       }
      ]
     }
    }
  ]
}
```

Client Error Format/Structure

Here are the possible error codes, which can come up due to an invalid request

Failing to send a required header/query parameter will result in a 400 Bad Request response.
HTTP/1.1 400 Bad Request

Requesting a secured API without valid credentials will result in a 401 Unauthorized response.
HTTP/1.1 401 Unauthorized

Requesting data from an unknown instance or an instance where the application is not authorized will result in a 403 Forbidden response.
HTTP/1.1 403 Forbidden