

Patient Access API Version 3.0

This document discusses Patient Access API Version 3.0 and its methods to connect and query patient data from EHRs, in the context of meeting the ONC 2015 certification criteria.

Overview

This document discusses Patient Access API Version 3.0 and its methods to access the Common Clinical Data Set via an API. APIs enable patients to view, download, or transmit their health information using any application of their choice that is configured to meet the technical specifications of the API in the provider's CEHRT.

Terms and Conditions of Use

This section discusses the terms and conditions of using the Patient Access API. The Patient Access API documentation, access link, and materials have been made available to developers for development and testing. The documentation and materials are provided to developers as-is with no other warranties expressed or implied.

Developers may use the Materials with adherence to the below terms and conditions:

1. Use of Patient Access API and access to the material it contains is subject to the following Legal Terms and Conditions as well as to applicable laws. Your access to and browsing of this Web API constitutes your full acceptance of these Legal Terms and Conditions. We reserve the right, at our sole discretion, to update or revise these Legal Terms and Conditions. Please check the Terms and Conditions periodically for changes. Your continued use of this site following the posting of any changes to the Legal Terms and Conditions constitutes acceptance of those changes.
2. Developers are responsible for maintaining the confidentiality of your logon information, and are fully responsible for all activities that occur under your password or user name. You agree (a) to immediately notify Eye Care Leaders of any unauthorized use of your password or user name or any other breach of security, and (b) to ensure that you exit from your account at the end of each session.
3. Client applications using the service for API calls require an identifier to connect. Client identifier creation can be accomplished by vendors, in the case

of patient-facing applications, or organizations, in the case of provider-facing applications.

4. Applications must not contain any malware, malicious or harmful code, program, or other internal component (e.g., computer viruses, Trojan horses, “backdoors”) which could damage, destroy, or adversely affect the Patient Access API Platform, services, or other software, firmware, hardware, data, systems, services, or networks.

Introduction

This guide is written for third party developers, including patients, who are developing software applications for accessing Protected Health Information (PHI) based on this documentation of a Patient Access API. This documentation allows applications to query a public-facing API enabled by a data holder.

Patient Access API Configuration:

Detailed steps to begin development of an application with the Patient Access API.

Step 1: Connecting to the server

The server is accessed by clients through an https connection.

IMPORTANT: Local customer security policies must be in place to prevent unauthorized monitoring or eavesdropping of connections to the server.

Note: Only SSL/TLS connections (TLS 1.0 or higher) are accepted. All plaintext connections will be refused.

Note: Please limit your connection frequency to a value appropriate for your use case. Connection attempts which are more frequent than permitted by the bandwidth allocation for the data resource are not allowed.

Step 2: Patient Application Access

Patient application access can be performed using a Patient username, password, and ECL Account Number. The end user should obtain these credentials directly from the Patient. The Access information needs to be sent to body parameter in Json format specified here:

URL: <https://mobileapi.mycaresuite.com/token>

Parameters require:
grant_type:password
username:username@account_number
password:password
scope:app_type:PatientAccessApp

EXAMPLE:
grant_type:password
username:alice@qabeta
password:12345678
scope:app_type:PatientAccessApp

Step 3: API Details for accessing Patient PHI

After successful authentication of User credentials, now user can access PHI data for the patient, with the search criteria or input by the user through the Patient application. Data accessed can be downloaded in the form of CDA XML or HTML Human Readable Format. Date ranges and CDA Subsections may be queried individually or together.

For querying CDA Subsections, the Section Header must be specified in the API call.

For querying by Date Range, Technical documentation and specifications can be found here:

For a list of CDAs:

[https://mobileapi.mycare suite.com/Help/Api/GET-api-PatientAccessHealthSummaries-search_enteredOperator_entered1_entered2_doctorId\[0\]_doctorId\[1\]_type\[0\]_type\[1\]_page_itemsPerPage](https://mobileapi.mycare suite.com/Help/Api/GET-api-PatientAccessHealthSummaries-search_enteredOperator_entered1_entered2_doctorId[0]_doctorId[1]_type[0]_type[1]_page_itemsPerPage)

For CDA Subsections:

https://mobileapi.mycare suite.com/Help/Api/GET-api-PatientAccessHealthSummaries_cdaId_cdaSubSection_download

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/json object 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

Software Components

- Software must be capable of making HTTPS RESTful requests.

Intended audience

These APIs are intended to patient-facing applications via web and mobile in providing a higher quality of care. Patient should have access to an active patient portal account.