Sevocity Certified FHIR API Public Technical Documentation

The purpose of this document, in its entirety, is to document the Sevocity FHIR API's implementation of the ONC Certification Criteria for Health IT Requirements. The Sevocity FHIR API, may include additional features beyond the standard US Core 6.1.0 Profile Requirements found here.

To express interest in non-certified FHIR features or non-FHIR capabilities, contact Sales@sevocity.com.

For how to engage with the ONC Certification Criteria for Health IT API Requirements, read this document and all listed references.

Terms of Use

Terms of Use

Introduction

Sevocity has created this API to encourage like-minded health IT vendors to partner with Sevocity to explore and promote interoperability opportunities to benefit providers and their patients.

This API supports the capabilities and industry standards as stated in ONC Certification Criteria for Health IT, 170.315(g)(10) Standardized API for patient and population services. As such, data available via the API includes USCDI v3 data elements and returns the data in the standard FHIR R4 format.

The documentation on this page provides a guide for any health IT vendors interested in engaging with Sevocity to leverage the capabilities of this API.

Software Requirements

Mandatory Software Components

In order to access the FHIR API, a REST client such as Postman, or a high-level language (Java, Python, etc) that can be used to make HTTP requests, is needed.

Mandatory Software Configuration

- Web applications MUST support the HTTPS 1.1 protocol.
- Application MUST use only port 443 for TLS.
- Application MUST support and prefer TLS 1.2 or higher.

- Application MUST read and parse FHIR-based JSON responses
- Application MUST utilize OAuth2.0 for client authentication and authorization.
- Target Sevocity customer MUST utilize Sevocity EHR 13.0 or higher
- For Patient Facing applications, participating patients MUST have an active Sevocity Patient Portal Account
- Application SHOULD have a valid, non-expired TLS certificate issued from a trusted authority.
- Application SHOULD use an OV or EV certificate, if possible, instead of a DV certificate.

Service Base URLS

Patient Facing Apps:

- FHIR API: https://api.sevocity.com/api/patients/v1/{Organization ID}
- Auth Base Endpoint: https://auth.sevocity.com/realms/portal

Clinic Provider Facing Apps:

- FHIR API: https://api.sevocity.com/api/sevocity/v1/{Organization ID}
- Auth Base Endpoint: https://auth.sevocity.com/realms/sevocity

Machine Readable Endpoints:

Clinic Provider Facing Apps:

Using a tool like Postman, make a GET request to https://api.sevocity.com/api/sevocity/v1/Endpoint

Patient Facing Apps:

Using a tool like Postman, make a GET request to https://api.sevocity.com/api/patients/v1/Endpoint

Errors

The FHIR server will return standard HTTP Error codes as listed and described in detail here.

For most errors the API will include a response body in the form of an OperationOutcome Resource.

{

"resourceType": "OperationOutcome"

"issue": [{ "code": "invalid", "details": { "text": "Not found" }, "severity": "error" }],

}

Getting Started with the API

Introduction

- This section contains information about how you can create third-party applications and use those applications to access the Sevocity FHIR API.

Registering a SMART APP with Sevocity

In order to have a client created for use with the Sevocity API please complete the online vendor request form here. The online form will prompt you to provide the following information:

- Name of your application
- A list of valid redirect URI's
- Is your application Patient or clinic provider facing?
  - Note: If your application is Patient-facing, eligible patients must have an active Sevocity Patient Portal Account.
- Is your application capable of securing a client secret?
- The scopes that your application will be requesting.
  - Example user/AllergyIntolerance.rs or patient/Condition.rs (See Scopes for more details)

Once Sevocity has approved your request you will receive an OAuth `client_id` to use on subsequent requests following the protocols specified in the official SMART App Authorization Guide and Bulk Data (Flat FHIR).

Authentication

The Sevocity FHIR APIs are authenticated using the OAuth 2.0 protocol. All API requests must include an Authorization header with an Access Token of the form:

Authorization: Bearer JWT_TOKEN

Sevocity supports the following OAuth Flows:

- **Client Credentials** - Mostly used for Machine-to-Machine authentication (e.g., CLIs, Daemons)
- **Authorization Code** - Usually used for web/native applications, since it requires a user to log in to the system.

Client Credentials

Confidential clients, such as web apps, which are capable of securely storing credentials will be issued a `client_secret` that may be used in conjunction with the `client_id` to form an authorization grant, which can be used to obtain refresh and access tokens. Our refresh tokens are long-lived and conform to Health IT criteria documented in 170.315(g)(10) (v)(A)(1)(ii),(iii) and (v)(A)(2)(ii) as documented here.

Authorization Code

Public applications, such as native apps, which are incapable of securely storing credentials will not be issued a `client_secret`. Instead, the `authorization_code` grant flow will be used to issue refresh tokens.

FHIR Resources

The documentation on the available Sevocity FHIR API resources is at Sevocity FHIR API Profiles and Operations