

ONC 2015 Edition Cures Update

Web Service API Documentation

PCE Care Management Version 9.4

Table of Contents

Introduction	4
Registration	4
How to Use the API	5
Security	6
Overview	6
Redirection	6
Token Refresh / Expiration	7
USCDI Data Classes	8
API Operations	9
Authorization	9
Access Token	11
Refresh Access Token	13
Allergy Intolerances	15
Bulk Export	17
Bulk Export Delete Request	18
Bulk Export File Request	19
Bulk Export Status Request	20
Bulk Patient Export	21
Bulk Patient Group Export	22
Care Plans	23
Care Teams	25
Claims	28
Conditions	30
Coverage	32

Devices	34
Diagnostic Reports	36
Document References.....	39
Encounters	42
Goals	44
Healthcare Services.....	46
Immunizations.....	47
Locations	50
Medication Requests	51
Observations	54
Organizations	57
Patients	58
Practitioners.....	60
Practitioner Roles.....	61
Procedures	62
Provenance	64
Data Elements	65
Address.....	65
AllergyIntolerance.....	65
CarePlan	66
CareTeam	66
Claim	67
Coded Element.....	67
Condition.....	68
Coverage	68
Device.....	68
Diagnostic Report.....	69
Document Reference	70
Encounter.....	70
Goal	71
Healthcare Service	71

Immunization	72
Location.....	73
Medication Request.....	73
Message	74
Observation.....	74
Organization.....	75
Patient.....	76
Practitioner	76
Practitioner Role	77
Procedure.....	77
Provenance	78
Failed Response Header.....	78
Appendix A – PCE API Access Request Form.....	80
Appendix B - Terms of Use.....	81
Appendix C - Costs	86
Revision History	87

Introduction

The public-facing Web Service API provides an interface into the PCE Care Management Version 9.4 system for the purposes of meeting criteria for ONC 2015 Edition Cures Update criteria test 170.315(g)(10). This API specification may be used “out of the box” upon approval of an API request by the appropriate parties. Alternatively, other APIs (using other standards, protocols, or customized APIs) are also available for implementation by contacting PCE Systems using the PCE API Access Request Form in Appendix A. Requests may be sent to apirequests@pcesystems.com. Use of this API and any other API is subject to the Terms of Use in Appendix B.

Registration

You may request access to the API by submitting a written request to PCE Systems using the PCE API Access Request Form in Appendix A. This form may be submitted by e-mail to apirequests@pcesystems.com.

Registered applications must be confidential and server-based. Security credentials and fixed end-point URLs (“Launch” URI and redirect URI(s)) are required from the registered application to receive authorization and access data.

Registered applications must support TLS 1.2 for all transactions and PKCE for authorization and authentication requests. An active email address, phone number, and contact information must be received for communications and error reporting going forward.

Upon granting of a request for access to the API, security credentials, including JWT secrets when applicable, will be issued and endpoint URLs will be shared with the registered application. This will include two “Base URLs”, one for production and one for testing purposes. The production URL will not be enabled until applicable testing is completed and the exchange partner is approved to move to production. Additionally an email address will be provided for further communications and error reporting.

How to Use the API

This API uses REST technology with OAuth2 for authorization and JWKS asymmetric authentication for client authentication.

Request operations are listed in the **API Operations** section. Each request operation has its own URL, which starts with the Base URL. Search criteria for each request operation are given via REST URL parameters, which are case-sensitive. Applicable URL parameters are outlined for each request operation in the **API Operations** section.

Clinical data returned by the API is formatted as JSON based on FHIR v4.0.1 §170.215(a)(4) Argonaut Data Query specification. The top level data element is always a Request object which contains the data requested, a version identifier for the data and data format returned, a status flag which determines whether the request passed validations, and informational Message Data Elements if the request does not pass validations.

JSON Data types returned by request operations are identified for each request operation in the **API Operations** section. Data types are defined in detail in the **Data Elements** section.

The API's capability statement can be found here: [\[Base URL\]/MUPIX/v2/Capability](#)

The API's SMART-configuration file can be found here: [\[Base URL\]/MUPIX/v2/.well-known/smart-configuration.json](#)

The API's public JWKS can be found here: [\[Base URL\]/MUPIX/v2/.well-known/jwks.json](#)

Security

Overview

This API uses SMART on FHIR OAuth2 to allow a pre-registered client to request authorization from a patient via PCE Care Management Version 9.4 Patient Portal (CEHR). All requests are required to be made through a secure, encrypted tunnel (e.g., TLS 1.2+ or VPN).

When authentication is required for individual HTTP requests, minimally HTTP Basic Authentication is supported. Additional authentication methods are supported upon request.

The end-point for requesting authorization to patient resources is [Base URL]/OAUTH/v2/Authorize. PKCE and a state parameter are used to prevent CSRF and authorization code injection attacks. If the request is not recognized then the patient is notified there is a problem without redirecting to the client's redirect URL. If the request is from a recognized client but there is a problem with the request, then the patient is redirected to the client's redirect URL with standard error handling parameters/codes.

Upon a successfully validated request, the patient is redirected to the login page for the CEHR patient portal using their personal credentials. Successful authentication allows the patient to grant or deny the client access to the requested resources. If access is granted then an authorization token is returned to the client's redirect URL along with a time-restricted authorization token and the original state parameter.

The client may then request access to the authorized resources via the [Base URL]/OAUTH/v2/Token end-point. This is accomplished by sending the authorization token along with pre-registered credentials. Again, PKCE and a state parameter are used to prevent CSRF and authorization code injection attacks. If the request is not from a recognized client, the authorization token is not recognized, the PKCE code verifier does not match the code challenge from the original authorization request, or there is any other problem with the request structure, then an "invalid request" response is returned. If the given authorization token is expired or revoked, or the client credentials are not authenticated successfully then an "unauthorized access" response is returned.

Upon receipt of a valid authentication token and valid client credentials, an access token is returned to the client's redirect URL along with the state parameter and an OpenID JWE. The JWE contains details/scope of the authorization RS256 encrypted with a previously registered private key; this allows the client to verify the identity of the patient. The JWE contains a nonce identifier to help prevent replay attacks.

Access to patient resources can only be achieved using a valid & active authentication token and only when a valid & active authorization for those resources is in place between the client and the patient.

Redirection

Outbound redirect URLs are secured via the following requirements. If any of these requirements is not in place then redirection will not occur:

1. URLs must precisely match pre-registered URLs.
2. Required parameters are in place; notably the state, response_type, and client_id parameters are present and the client_id is recognized and registered to the redirect URL.
3. TLS 1.2 secure channels.
4. Cookies are not used in the process.

5. PKCE challenge in place and validated prior to redirection.
6. When present scope parameters must be recognized, authorized, and pertinent to the launch type.

In addition to avoiding a redirection, failure to meet requirement 1 or 2 will result in the end-user being notified of a potential security issue.

Inbound redirect URLs are secured via the following requirements & mechanisms. If any of these requirements is not in place then redirection will not occur:

1. All parameters must be recognized and contain known values applicable to the request for redirection.
2. TLS 1.2 secure channels.
3. Cookies are not used in the process.
4. PKCE challenge in place and validated prior to further action.
5. Inputs are sanitized and then validated in memory first.
6. Inputs must contain recognized values, and must be applicable to the specific type of redirection request.
 - a. Total parameter list max length: 1024
 - b. The maximum number of allowed URL parameters is 5
7. Tokens must match a persisted token for the client_id in question and the token must be active.
8. Redirections are only accepted over VPNs or within internal networks when feasible

Failure to meet any requirement above will prevent further processing of the redirect request.

Token Refresh / Expiration

Tokens are persisted with a required expiration timestamp representing the point at which the token is no longer active. The expiration time is based on the type of token and the type of authorization granted to the data. For example authorization tokens are created with an expiration timestamp 3 months out from the time of authorization. All tests for valid/active tokens take into account this expiration date relative to the current time. If the current time is after the expiration timestamp then the token is considered expired/inactive and requests using that token are treated as invalid.

An authorization token granted by a patient via CEHR to the patient's resources may be expired / revoked at any time by the patient through CEHR. This action sets the token's expiration timestamp to the current time. A revoked token is inactive effective immediately; further requests using that token are treated as invalid.

Tokens may be refreshed via the "RefreshToken" end-point when a refresh token was given with a previous successful authentication. If refreshing of a token is allowed at the time of authentication then a separate refresh token is included in the authentication response; it can be swapped later for a new access token. The refresh token must match precisely the refresh token given with the previous authentication.

USCDI Data Classes

USCDI v1 Data Class	API Operation (FHIR Resource)	FHIR Resource Data Element
Allergies and Intolerances	Allergy Intolerances	AllergyIntolerance
Assessment and Plan of Treatment	Care Plans	CarePlan
Care Team Members	Care Teams	CareTeam
Clinical Notes	Diagnostic Reports Document References	Diagnostic Report Document Reference
Goals	Goals	Goal
Health Concerns	Conditions	Condition
Immunizations	Immunizations	Immunization
Laboratory	Diagnostic Reports Observations	Diagnostic Report Observation
Medications	Medication Requests Allergy Intolerances	Medication Request AllergyIntolerance
Patient Demographics	Patients	Patient
Problems	Conditions	Condition
Procedures	Procedures	Procedure
Provenance	Provenance	Provenance
Smoking Status	Observations	Observation
Unique Device Identifier(s) for Patient's Implantable Device(s)	Devices	Device
Vital Signs	Observations	Observation

API Operations

Authorization

URL: [Base URL]/OAUTH/v2_[id]/Authorize

This URL is used by the client to request authorization to patient resources using OAuth in the form of an authorization token. The token is valid for a limited amount of time.

Method: Get

URL Parameters:

Parameter	Title	Required	Description
client_id	Client Identifier	Yes	Used to identify the entity/app attempting to authorize
code_challenge	Code Challenge	Yes	Value of the "S256" encrypted PKCE code verifier.
code_challenge_method	Code Challenge Method	Yes	Type of encryption used to create the PKCE "code_challenge" value. Always set to "S256".
redirect_uri	Redirect URI	Yes	URI to redirect to after successful patient-approved authorization
response_type	Response Type	Yes	Type of response requested. Always set to "code"
scope	Scope	No	Scope of the authorization requested.
state	State	Yes	Random / non-guessable value unique to each request to mitigate CSRF and replay attacks. This value will be returned as-is in responses and redirect URLs when present.

Return Value:

Before returning a value, the user is redirected to the CEHR patient portal. Upon successful login by the patient, the patient may approve or deny the authorization request. Upon approval the client is redirected to the "redirect_uri" URL parameter from the original request. This redirect includes a URL parameter "code" with value set to the assigned the authorization token, along with a "state" parameter with value matching the value of the original request's "state" parameter. The authorization token is 36 characters in length and is valid for 90 days.

If authorization is not approved then a redirect to the URI given by parameter "redirect_uri" is still returned but with no "code" URL parameter.

If the request is not recognized then the patient is notified there is a problem without redirecting to the client's redirect URL. If the request is from a recognized client but there is a problem with the request, then the patient is redirected to the client's redirect URL with error handling parameters "error",

“error_description”, and “error_uri” when applicable, along with a “state” parameter with value matching the value of the original request’s “state” parameter.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Access Token

URL: [Base URL]/OAuth/v2/Token

This URL is used to authenticate and retrieve an access token via client credentials and/or valid authorization code. The access token is valid for 15 minutes. A valid access token is required as a URL parameter for all patient resource requests. Minimally, “Basic authentication” is supported for credentials.

Method: Post

Content-Type: application/x-www-form-urlencoded

URL Parameters:

Parameter	Title	Required	Description
Single-Patient Token			
code	Authorization code	Yes	Authorization token “code” returned as part of the redirection following patient authorization via the “Authorize” endpoint.
code_verifier	Code verifier	Yes	The PKCE code verifier value used to generate the “code_challenge” value in the original “Authorize” request.
grant_type	Grant type	Yes	Always set to “authorization_code”.
redirect_uri	Redirect URI	Yes	URI to redirect to after successful authentication.
state	State	No	Random / non-guessable value unique to each request to mitigate CSRF and replay attacks. This value will be returned as-is in responses and redirect URIs when present.
Multi-Patient Token (Bulk Export)			
client_assertion_type	Client assertion type	Yes	Always set to “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”.
grant_type	Grant type	Yes	Always set to “client_credentials”. E.g. use basic authentication in request header.
redirect_uri	Redirect URI	Yes	URI to redirect to after successful authentication.
state	State	No	Random / non-guessable value unique to each request to mitigate CSRF and replay attacks. This value will be returned as-is in responses and redirect URIs when present.

Return Value:

An HTTP “application/json” response containing an access token used for accessing authorized patient resources. The access token is 36 characters in length.

The response also contains a “token_type” property set to “Bearer”, an “expires_in” property set to the number of seconds until the access token expires, and an “id_token” parameter containing an RS256 encrypted OpenID JSON Web Token (JWE). The JWE contains details of the authorization encrypted with a previously registered private key. The JWE contains the following claims: issuer of the JWT “iss”, subject of the JWT “sub”, recipient of the JWT “aud”, time after which the JWT expires “exp”, time when the JWT was issued “iat”, nonce JWT identifier from the client “jti”, and the time when original authorization was granted “auth_time”. The public key for the JWT can be found here: [Base URL]/MUPIX/v2/.well-known/jwks.json.

The response may include a “refresh_token” parameter, which can be used to obtain a new access token (“refresh the token”) later, prior to the current access token expiring or being revoked. Refresh tokens are only applicable when a patient agrees to “offline access” of their resources. Refresh tokens are valid for 3 months.

If the request is not from a recognized client, the authorization token is not recognized, the PKCE code verifier does not match the code challenge from the original authorization request, or there is any other problem with the request structure, then an “invalid request” Message Data Element is returned. If the given authorization token is expired or revoked, or the client credentials are not authenticated successfully then an “unauthorized access” response is returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Refresh Access Token

URL: [Base URL]/OAuth/v2/RefreshToken

This URL is used to refresh an existing OAuth access token through obtaining a new one via giving valid credentials and a valid “refresh token” from a previous Access Token request. The access token is valid for 30 minutes. A valid access token is required as a URL parameter for all patient resource requests. Minimally, “Basic authentication” is supported for credentials.

Method: Post

Content-Type: application/x-www-form-urlencoded

URL Parameters:

Parameter	Title	Required	Description
client_id	Client ID	Yes	Used to identify the entity/app attempting to authorize
code_verifier	Code Verifier	Yes	The PKCE code verifier value used to generate the “code_challenge” value from the original “Authorize” request.
grant_type	Grant type	Yes	Always set to “refresh_token”.
refresh_token	Refresh Token	Yes	The value of the “refresh_token” parameter from the original “Authorize” request. If a “refresh_token” value was not returned with the original request then refreshing the access token is not possible.
scope	Scope	No	Scope of the authorization requested. This may be the same scope as the original authorization or narrower.
state	State	No	Random / non-guessable value unique to each request to mitigate CSRF attacks. This value will be returned as-is in responses and redirect URIs when present.

Return Value:

An HTTP “application/json” response containing an access token used for accessing authorized patient resources. The access token is 36 characters in length.

The response also contains a “token_type” property set to “Bearer”, an “expires_in” property set to the number of seconds until the access token expires, and an “id_token” parameter containing an RS256 encrypted OpenID JSON Web Token (JWE). The JWE contains details of the authorization encrypted with a previously registered private key; this allows the client to verify the identity of the patient. The JWE contains the following claims: issuer of the JWT “iss”, subject of the JWT “sub”, recipient of the JWT “aud”, time after which the JWT expires “exp”, time when the JWT was issued “iat”, and the time when original authorization was granted “auth_time”. The public key for the JWT can be found here: [Base URL]/MUPIX/v2/.well-known/jwks.json.

The response may include a “refresh_token” parameter, which can be used to obtain a new access token (“refresh the token”) later, prior to the current access token expiring or being revoked. A new refresh token will only be sent if a patient has granted “offline access” to their resources. Refresh tokens are valid for 3 months.

If the request is not from a recognized client, the refresh token is not recognized, the PKCE code verifier does not match the code challenge from the original authorization request, or there is any other problem with the request structure, then an “invalid request” Message Data Element is returned. If the authorization token behind the refresh token is expired or revoked, or the client credentials are not authenticated successfully then an “unauthorized access” Message Data Element is returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Allergy Intolerances

URL: [Base URL]/MUPIX/v2_[id]/AllergyIntolerance

This URL is used to retrieve patient allergy intolerance data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the allergy intolerance record with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
enddate	End Date	No	Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
exactdate	Exact Date	No	Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.

Return Value:

A JSON-formatted response containing a list of Allergy Intolerance Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Allergy Intolerances match the request criteria then only the first 250 Allergy Intolerances will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Bulk Export

URL: [Base URL]/MUPIX/v2_[id]/\$export

This URL is used to start a system level export. [id] represents a public identifier of the EHR being accessed.

Method: GET

Parameters:

Parameter	Title	Type	Required	Description
bearer_token	Authentication Token	Header	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
accept	String	Header	Yes	Format of the optional OperationOutcome resource response to the export start request. Supported values include: “application/fhir+json”.
prefer	String	Header	Yes	Whether the response is immediate or asynchronous. Supported values include: “respond-async”.
_outputFormat	String	URL Parameter	No	Format for the requested bulk data files to be generated

Return Value:

A successful request will return an HTTP response code of 202 with “Content-Location” header set to the Bulk Data Status Request URL, which can be called periodically to retrieve the status of the export process. An unauthorized request will return an HTTP response code of 401. Any other error state will return an HTTP response code of 400.

Bulk Export Delete Request

URL: [Base URL]/MUPIX/v2_[id]/ExportProcess/[exportId]

This URL is used to delete data from an existing export or cancel & delete data from a currently running export. [id] represents a public identifier of the EHR being accessed. [exportId] represents the identifier of the export process. This URL is provided by each of the 3 Bulk Export end-points via the “Content-Location” header. Note that this URL is the same as the Bulk Export Status Request URL; the difference is the HTTP method.

Method: DELETE

Parameters:

Parameter	Title	Type	Required	Description
bearer_token	Authentication Token	Header	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.

Return Value:

A successful request will return an HTTP response code of 202. If the export data was previously deleted or canceled then an HTTP response code of 404 will be returned. An unauthorized request will return an HTTP response code of 401. Any other error state will return an HTTP response code of 400.

Bulk Export File Request

URL: [Base URL]/MUPIX/v2_[id]/ExportRetrieve/[exportId]/[fileId]

This URL is used to retrieve data from a completed export. [id] represents a public identifier of the EHR being accessed. [exportId] represents the identifier of the export process. This URL is provided by the Bulk Export Status Request end-point once the export is completed.

Method: GET

Parameters:

Parameter	Title	Type	Required	Description
bearer_token	Authentication Token	Header	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
accept	String	Header	No	Expected data format. Must be “application/fhir+ndjson” if set.

Return Value:

A successful request will return an HTTP response code of 200. A “Content-Type” header will be included with a value of “application/fhir+ndjson”. The body will contain the export data for the file in the URL formatted as ndjson.

If the export data was previously deleted or canceled then an HTTP response code of 404 will be returned. An unauthorized request will return an HTTP response code of 401. Any other error state will return an HTTP response code of 400.

Bulk Export Status Request

URL: [Base URL]/MUPIX/v2_[id]/ExportProcess/[exportId]

This URL is used to get the status of an existing export. [id] represents a public identifier of the EHR being accessed. [exportId] represents the identifier of the export process. This URL is provided by each of the 3 Bulk Export end-points via the “Content-Location” header. Note that this URL is the same as the Bulk Export Delete Request URL; the difference is the HTTP method.

Method: GET

Parameters:

Parameter	Title	Type	Required	Description
bearer_token	Authentication Token	Header	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.

Return Value:

When the requested export is in progress, a successful request will return an HTTP response code of 202. An “X-Progress” header will also be included containing information about the progress of the export. The same URL should be called again later to check the status again.

When the requested export is complete, a successful request will return an HTTP response code of 200. A “Content-Type” header is included with value “application/json”. An “Expires” header is included to identify the time when the export data will no longer be available. This is normally 7 days from the start of the export. The body of the response is a JSON-formatted string containing the following properties:

transactionTime: Time of the original export start

request: URL of the original export request

requiresAccessToken: Whether an access token is required to access the exported data. The value is always “true”.

output: A list of URLs identifying the files containing the export data that may be downloaded. Each file is comprised of a type, which identifies the type of resources contained within the file and the URL for accessing the file. Export data is contained within the files and is formatted as ndjson. This URL can be called to retrieve the ndjson file containing the exported data.

error: A list of ndjson files containing any errors that occurred during the export.

If the export data was previously deleted or canceled then an HTTP response code of 404 will be returned. An unauthorized request will return an HTTP response code of 401. Any other error state will return an HTTP response code of 400.

Bulk Patient Export

URL: [Base URL]/MUPIX/v2_[id]/Patient/\$export

This URL is used to start an export of all FHIR resources of diverse resource types pertaining to all patients. [id] represents a public identifier of the EHR being accessed.

Method: GET

Parameters:

Parameter	Title	Type	Required	Description
bearer_token	Authentication Token	Header	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
accept	String	Header	Yes	Format of the optional OperationOutcome resource response to the export start request. Supported values include: “application/fhir+json”.
prefer	String	Header	Yes	Whether the response is immediate or asynchronous. Supported values include: “respond-async”.
_outputFormat	String	URL Parameter	No	Format for the requested bulk data files to be generated

Return Value:

A successful request will return an HTTP response code of 202 with “Content-Location” header set to the Bulk Data Status Request URL, which can be called periodically to retrieve the status of the export process. An unauthorized request will return an HTTP response code of 401. Any other error state will return an HTTP response code of 400.

Bulk Patient Group Export

URL: [Base URL]/MUPIX/v2_[id]/Group/[groupId]\$/export

This URL is used to start an export of all FHIR resources of diverse resource types pertaining to all patients within the specified group. [id] represents a public identifier of the EHR being accessed. [groupId] represents the identifier of the group of patients to export.

Method: GET

Parameters:

Parameter	Title	Type	Required	Description
bearer_token	Authentication Token	Header	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
accept	String	Header	Yes	Format of the optional OperationOutcome resource response to the export start request. Supported values include: “application/fhir+json”.
prefer	String	Header	Yes	Whether the response is immediate or asynchronous. Supported values include: “respond-async”.
_outputFormat	String	URL Parameter	No	Format for the requested bulk data files to be generated

Return Value:

A successful request will return an HTTP response code of 202 with “Content-Location” header set to the Bulk Data Status Request URL, which can be called periodically to retrieve the status of the export process. An unauthorized request will return an HTTP response code of 401. Any other error state will return an HTTP response code of 400.

Care Plans

URL: [Base URL]/MUPIX/v2_[id]/CarePlan

This URL is used to retrieve patient care plan data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the care plan record with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
category	Category	No	Limit resources to those with the given category. When the category’s system is included it must precede the value and be separate with a bar. See http://hl7.org/fhir/us/core/CodeSystem/careplan-category

date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd.</p> <p>An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd.</p> <p>An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date.</p> <p>Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Care Plan Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Care Plans match the request criteria then only the first 250 Care Plans will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Care Teams

URL: [Base URL]/MUPIX/v2_[id]/CareTeam

This URL is used to retrieve patient care plan team data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the care team with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
category	Category	No	Limit resources to those with the given category. When the category’s system is included it must precede the value and be separate with a bar. See

			http://hl7.org/fhir/ValueSet/care-team-category
status	Status	No	<p>Limit resources to those with the given status. When the status's system is included it must precede the value and be separate with a bar. Multiple statuses may be included separated with a comma. See http://hl7.org/fhir/ValueSet/care-team-status</p>
date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to "lt" then only resources with a date less than the given date will be returned; If the operator is set to "gt" then only resources with a date greater than the given date will be returned; If the operator is set to "le" then only resources with a date less than or equal to the given date will be returned; If the operator is set to "ge" then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with "error" value "INVDT".</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with "error" value "INVDT".</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with "error" value "INVDT".</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with "error" value "INVDT".</p>

Return Value:

A JSON-formatted response containing a list of Care Team Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Care Teams match the request criteria then only the first 250 Care Teams will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Claims

URL: [Base URL]/MUPIX/v2_[id]/Claim

This URL is used to retrieve claim data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the claim with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Claim Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Claims match the request criteria then only the first 250 Claims will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Conditions

URL: [Base URL]/MUPIX/v2_[id]/Condition

This URL is used to retrieve patient condition data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the condition with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Condition Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Conditions match the request criteria then only the first 250 Conditions will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Coverage

URL: [Base URL]/MUPIX/v2_[id]/Coverage

This URL is used to retrieve claim coverage data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the coverage with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Coverage Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Coverages match the request criteria then only the first 250 Claims will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Devices

URL: [Base URL]/MUPIX/v2_[id]/Device

This URL is used to retrieve patient device data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the device with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Device Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Devices match the request criteria then only the first 250 Devices will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Diagnostic Reports

URL: [Base URL]/MUPIX/v2_[id]/DiagnosticReport

This URL is used to retrieve patient diagnostic report data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the diagnostic report with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
code	Code	No	Limit resources to those with the given code. When the code’s system is included it must precede the value and be separate with a bar.

			Multiple codes may be included separated with a comma. See http://loinc.org
category	Service Category	No	Limit resources to those with the given category. When the category's system is included it must precede the value and be separate with a bar. See http://hl7.org/fhir/DiagnosticReport-category
date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
enddate	End Date	No	Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
exactdate	Exact Date	No	Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.

Return Value:

A JSON-formatted response containing a list of Diagnostic Report Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Diagnostic Reports match the request criteria then only the first 250 Diagnostic Reports will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Document References

URL: [Base URL]/MUPIX/v2_[id]/DocumentReference

This URL is used to retrieve patient document reference data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the document reference with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient. *This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”. If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.
type	Type	No	Limit document references to those with a type matching this value. See

			http://hl7.org/fhir/us/core/ValueSet/us-core-documentreference-type for valid values.
category	Category	No	Limit document references to those with a category matching this value. See http://hl7.org/fhir/ValueSet/document-classcodes for valid values.
Status	Status	No	Limit document references to those with a status matching this value. See http://hl7.org/fhir/document-reference-status for valid values.
date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
enddate	End Date	No	Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
exactdate	Exact Date	No	Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An

		invalid date value will result in a Message Data Element with “error” value “INVDT”.
--	--	--

Return Value:

A JSON-formatted response containing a list of Document Reference Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Document References match the request criteria then only the first 250 Document References will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Encounters

URL: [Base URL]/MUPIX/v2_[id]/Encounter

This URL is used to retrieve patient encounter data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the encounter with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Encounter Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Encounters match the request criteria then only the first 250 Encounters will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Goals

URL: [Base URL]/MUPIX/v2_[id]/Goal

This URL is used to retrieve patient goal data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the goal with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>

Return Value:

A JSON-formatted response containing a list of Goal Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Goals match the request criteria then only the first 250 Goals will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Healthcare Services

URL: [Base URL]/MUPIX/v2_[id]/HealthcareService

This URL is used to retrieve Healthcare Service Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
_id	Identifier	No	Limit to the Healthcare Service with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.

Return Value:

A JSON-formatted response containing a list of Healthcare Service Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Healthcare Services match the request criteria then only the first 250 Healthcare Services will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Immunizations

URL: [Base URL]/MUPIX/v2_[id]/Immunization

This URL is used to retrieve patient immunization data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the resource with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
status	Status	No	Limit to resources with status matching the given value. See http://hl7.org/fhir/ValueSet/immunization-status .

date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	<p>Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
enddate	End Date	No	<p>Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>
exactdate	Exact Date	No	<p>Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.</p>

Return Value:

A JSON-formatted response containing a list of Immunization Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Immunizations match the request criteria then only the first 250 Immunizations will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Locations

URL: [Base URL]/MUPIX/v2_[id]/Location

This URL is used to retrieve Location Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
_id	Identifier	No	Limit to the Location with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
name	Location Name	No	Limit to Locations having a name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVNM".

Return Value:

A JSON-formatted response containing a list of Location Data Elements in the data field matching any given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Locations match the request criteria then only the first 250 Locations will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Medication Requests

URL: [Base URL]/MUPIX/v2_[id]/MedicationRequest

This URL is used to retrieve patient medication request data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the resource with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse Include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
_include	Include	No	Set the value to “MedicationRequest:medication” to include related Medication resources for any Medications referenced by the returned Medication Requests.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>

status	Status	No	Limit the returned Medication Requests to those with this status code. See http://hl7.org/fhir/ValueSet/medicationrequest-status for valid values.
intent	Intent	No	Limit the returned Medication Requests to those with this intent code. See http://hl7.org/fhir/ValueSet/medicationrequest-intent for valid values.
date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
enddate	End Date	No	Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
exactdate	Exact Date	No	Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.

Return Value:

A JSON-formatted response containing a list of Medication Request Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Medication Requests match the request criteria then only the first 250 Medication Requests will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Observations

URL: [Base URL]/MUPIX/v2_[id]/Observations

This URL is used to retrieve patient observation report data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” endpoint. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the observation with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
code	Observation Code	No	Limit to observations with a code value matching the given value. See https://hl7.org/fhir/valueset-observation-codes.html for valid values.

category	Observation Category	No	Limit to observations with a category value matching the given value. See https://hl7.org/fhir/valueset-observation-category.html for valid values.
date	Date	No	<p>Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.</p> <p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
enddate	End Date	No	Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
exactdate	Exact Date	No	Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.

Return Value:

A JSON-formatted response containing a list of Observation Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Observations match the request criteria then only the first 250 Observations will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Organizations

URL: [Base URL]/MUPIX/v2_[id]/[Organization](#)

This URL is used to retrieve Organization Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
_id	Identifier	No	Limit to the Organization with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
name	Organization Name	No	Limit to organizations having a name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVNM".
address	Address	No	Limit to resources with the given address characteristics.
type	Organization Type	No	Limit to organizations having a type "code" that contains this parameter's value. http://hl7.org/fhir/us/davinci-pdex-plan-net/CodeSystem/OrgTypeCS

Return Value:

A JSON-formatted response containing a list of Organization Data Elements in the data field matching any given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Organizations match the request criteria then only the first 250 Organizations will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Patients

URL: [Base URL]/MUPIX/v2_[id]/[Patient](#)

This URL is used to retrieve Patient Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Access Token	Yes	Access token from a successful response to either the "Token" or "RefreshToken" URL. If this parameter is missing or is invalid or the token has expired then a Message Data Element with "error" "NOAUTH" will be returned.
_id	Reference Identifier	No	Limit to the Patient with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the Patient with system and identifier matching the given value.
_revinclude	Reverse include	No	Set the value to "Provenance:target" to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with "error" value "INVREV".
firstname	First Name	No	Limit to patients having a first name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVFN".
family	Family	No	Limit to patients having a family name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVLN".
name	Name	No	Limit to patients having a first and or last name that matches this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVLN".
birthdate	Birth Date	No	Limit to patients having a date of birth that matches this parameter's value. Formatted as yyyyMMdd or yyyy-MM-dd. Invalid dates/formats will result in a Message Data Element with "error" value "INVDT".

gender	Gender	No	Limit to patients having a gender at birth that matches the given value. See http://hl7.org/fhir/administrative-gender .
--------	--------	----	--

Return Value:

A JSON-formatted response containing a list of Patient and optional corresponding Provenance Data Elements in the data field matching any given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Patients match the request criteria then only the first 250 Patients will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Practitioners

URL: [Base URL]/MUPIX/v2_[id]/[Practitioner](#)

This URL is used to retrieve Practitioner Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
_id	Identifier	No	Limit to the Practitioner with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
firstname	First Name	No	Limit to practitioners having a first name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVFN".
lastname	Last Name	No	Limit to practitioners having a last name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVLN".

Return Value:

A JSON-formatted response containing a list of Practitioner Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Practitioners match the request criteria then only the first 250 Practitioners will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Practitioner Roles

URL: [Base URL]/MUPIX/v2_[id]/[PractitionerRole](#)

This URL is used to retrieve Practitioner Role Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
_id	Identifier	No	Limit to the Practitioner Role with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
name	Name	No	Limit to practitioners having a first or last name that contains this parameter's value. Values less than two characters in length will result in a Message Data Element with "error" value "INVNM".

Return Value:

A JSON-formatted response containing a list of Practitioner Role Data Elements in the data field which match the given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Practitioner Roles match the request criteria then only the first 250 Practitioner Roles will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Procedures

URL: [Base URL]/MUPIX/v2_[id]/Procedure

This URL is used to retrieve patient procedure data based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Authentication Token	Yes	Access token from a successful response to either the “Token” or “RefreshToken” end-point. If this parameter is missing or is invalid or the token has expired then a Message Data Element with “error” “NOAUTH” will be returned.
_id	Identifier	No	Limit to the procedure with unique identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No	Limit to the resource with logical identifier matching the given value.
_revinclude	Reverse include	No	Set the value to “Provenance:target” to include related Provenance resources for resources returned in the response. If this parameter is not valid then the response will include a Message Data Element with “error” value “INVREV”.
patient	Patient Identifier	Varies*	<p>Identifier of the patient to which returned resources will be limited. This may be set to the identifier of a patient or a relative URL reference to a patient.</p> <p>*This parameter is required for all requests except “Multi-Patient” requests. If this parameter is missing when required then the response will include a Message Data Element with “error” value “MISPAT”.</p> <p>If the patient has not granted access to this resource then the response will include a Message Data Element with “error” value “UNAUTH”.</p>
date	Date	No	Limit resources based on this date. Formatted as [Operator]yyyyMMdd or [Operator]yyyy-MM-dd.

			<p>The operator is optional; If not given the date will be matched exactly; If the operator is set to “lt” then only resources with a date less than the given date will be returned; If the operator is set to “gt” then only resources with a date greater than the given date will be returned; If the operator is set to “le” then only resources with a date less than or equal to the given date will be returned; If the operator is set to “ge” then only resources with a date greater than or equal to the given date will be returned.</p> <p>The date parameter may be included in the URL multiple times to provide more than one date filter.</p> <p>An unrecognized value will result in a Message Data Element with “error” value “INVDT”.</p>
startdate	Start Date	No	Limit resources to those effective on or after this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
enddate	End Date	No	Limit resources to those effective on or prior to this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.
exactdate	Exact Date	No	Limit to resources effective on this date. Formatted as yyyyMMdd or yyyy-MM-dd. An invalid date value will result in a Message Data Element with “error” value “INVDT”.

Return Value:

A JSON-formatted response containing a list of Procedure Data Elements and optional corresponding Provenance Data Elements in the data field which match the given parameters. Problems with the request will result in the Response’s Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Procedures match the request criteria then only the first 250 Procedures will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Provenance

URL: [Base URL]/MUPIX/v2_[id]/[Provenance](#)

This URL is used to retrieve Provenance Data Elements based on given search criteria. [id] represents a public identifier of the EHR being accessed.

Method: GET or POST

Parameters:

Parameter	Title	Required	Description
token	Access Token	Yes	Access token from a successful response to either the "Token" or "RefreshToken" URL. If this parameter is missing or is invalid or the token has expired then a Message Data Element with "error" "NOAUTH" will be returned.
_id	Reference Identifier	No*	Limit to the Patient with unique resource identifier matching the given value. Alternatively the identifier may be appended to the URL prefixed with a forward slash, prior to URL parameters.
identifier	Identifier	No*	Limit to the Patient with system and identifier matching the given value.

*An identifier is required in some form, either via _id, identifier, or at the end of the URL.

Return Value:

A JSON-formatted response containing a list of Provenance matching any given parameters. Problems with the request will result in the Response's Data field being empty and the Messages field containing one or more Message Data Elements.

If more than 250 Provenance elements match the request criteria then only the first 250 Patients will be returned.

A successful request will return an HTTP response code of 200. An unauthorized request will return an HTTP response code of 401. A request with insufficient scope will return an HTTP response code of 403. Any other error state will return an HTTP response code of 400.

Data Elements

Address

Represents address information

Attribute	Data Type	Description
line	List	First & optional second address lines
city	String	City
period:start	DateTime	When the address is effective as of
period:end	DateTime	When the address is no longer effective as of
postalCode	String	Zip code
stateCode	String	State
telecom	Contact Point	Phone number associated with this address
use	Code	Address use
type	Code	Address type

AllergyIntolerance

Represents an allergy or intolerance resource for a specific patient. Conforms to the [US Core AllergyIntolerance Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "AllergyIntolerance"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
clinicalStatus	Coded Element	Clinical status of the allergy or intolerance.
verificationStatus	Coded Element	Verification status of the allergy or intolerance.
type	String	Whether the resource represents an allergy or an intolerance
code	Coded Element	Identifier of the allergy or intolerance
patient:reference	Reference	Unique identifier of the Patient to which this resource belongs represented as a relative URL
asserter:reference	Reference	Unique identifier of the asserter of this resource represented as a relative URL
reaction:manifestation:coding	Coded Element	Clinical symptoms/signs associated with the Event when recorded as SNOMED
reaction:manifestation:text	String	Clinical symptoms/signs associated with the Event when not recorded as SNOMED
reaction:severity	Code	Severity of the event

CarePlan

Represents plan of treatment information for a specific patient/subject. Conforms to the [US Core CarePlan Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "CarePlan"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	Status of the plan
category:coding	Coded Element	Type of plan
intent	Code	Intent of the plan
title	String	Name of the plan
subject:reference	Reference	Unique identifier of the subject to which this resource belongs represented as a relative URL
period:start	Date	Date on which the plan begins
period:end	Date	Date on which the plan ends
careTeam:reference	Reference	Unique identifier of the Care Team responsible for this resource represented as a relative URL
goal	List	List of goals associated with this plan
goal:reference	Reference	Unique identifier of a Goal associated with this plan represented as a relative URL
text:div	XHTML	XHTML Text summary of the resource, for human interpretation
text:status	Code	The status of the narrative - whether it is generated or human authored / may contain additional data.

CareTeam

Represents a care team for a specific patient/subject. Conforms to the [US Core CareTeam Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "CareTeam"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
category:coding	Coded Element	Care team category
status	Code	Status of the care team
subject:reference	Reference	Unique identifier of the subject to which this resource belongs represented as a relative URL
participant	List	List of care team participants
participant:role	Coded Element	The participant's role within the care team
participant:member:reference	Reference	Unique identifier of a care team member participating in this care team represented as a relative URL

Claim

Represents a claim for a specific patient

Attribute	Data Type	Description
resourceType	String	Always "Claim"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	Status of the claim
type	Coded Element	Category or discipline of the claim
use	Code	Use of the claim
patient:reference	Reference	Unique identifier of the Patient associated with this claim represented as a relative URL
billablePeriod:start	Date	Timeframe in which the claim is effective
billablePeriod:end	Date	Timeframe in which the claim is effective
created	DateTime	When the claim was created
provider:reference	Reference	Unique identifier of the party responsible for the claim represented as a relative URL
priority	Coded Element	Process priority of the claim
insurance:sequence	Integer	Insurance instance identifier
insurance:focal	Boolean	Coverage to be used for adjudication
insurance:coverage:reference	Reference	Unique identifier of the claim insurance represented as a relative URL
item:sequence	Integer	Item instance identifier
item:productOrService	Coded Element	Billing/service code
item:modifier	Coded Element List	Service billing modifiers
item:servicedDate	Date	Date of service delivery
item:encounter:reference	Reference	Unique identifier of the Encounter responsible for the claim represented as a relative URL
paid:value	Decimal	The total of the claim paid in US dollars
total:value	Decimal	The total cost of the claim in US dollars

Coded Element

Represents a machine readable codified value and its coding system.

Attribute	Data Type	Description
coding:system	String	Identifier of the coding system to which the code belongs
coding:code	String	Machine readable identifier of the value represented by this coded element
coding:display	String	Human readable title for the code

text	String	Human readable description of the codified value
------	--------	--

Condition

Represents a condition for a specific patient. Conforms to the [US Core Condition Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Condition"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
category	Coded Element	Category of the condition
clinicalStatus	Coded Element	Clinical status of the condition
verificationStatus	Coded Element	Verification status of the condition
code	Coded Element	Identification of the condition, problem or diagnosis
subject	Coded Element	Coded value representing the status of the problem
recordedDate	Date	Date when the condition was first recorded
recorder:reference	Reference	Unique identifier of the resource that recorded this condition represented as a relative URL

Coverage

Represents coverage for a claim

Attribute	Data Type	Description
resourceType	String	Always "Coverage"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	Status of the coverage
beneficiary:reference	Reference	Unique identifier of the Patient associated with this coverage represented as a relative URL
period:start	Date	Timeframe in which the coverage is effective
period:end	Date	Timeframe in which the coverage is effective
payor:reference	Reference	Unique identifier of the Payor associated with this coverage represented as a relative URL

Device

Represents an implanted device for a specific patient. Conforms to the [US Core Implantable Device Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Device"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
udiCarrier:deviceIdentifier	String	Fixed portion of the UDI
udiCarrier:issuer	String	UDI Issuing Organization

udiCarrier:carrierAIDC	Base64	UDI machine readable barcode string. Base64 encoded binary
udiCarrier:carrierHRF	String	UDI Human Readable Barcode String
udiCarrier:entryType	Code	UDI type
status	Code	Status of the device
distinctIdentifier	String	Distinct identifier of the device
manufacturer	String	Name of the device manufacturer
manufacturerDate	DateTime	Date when the device was made
expirationDate	DateTime	Date when the device expires
lotNumber	String	Lot number of the manufacturer
serialNumber	String	Device serial number assigned by the manufacturer
deviceName:name	String	Name of the device
deviceName:type	Code	Device name type
modelNumber	String	Model number of the device
type	Coded Element	Type of the device
note:text	String	Notes/comments about the device
patient:reference	Reference	Unique identifier of the Patient to whom the device is affixed represented as a relative URL.

Diagnostic Report

Represents a diagnostic report for a specific patient. Conforms to the [US Core DiagnosticReport Profile for Laboratory Results Reporting](#) (version 4.0.0) and the [US Core DiagnosticReport Profile for Report and Note exchange](#) (version 4.0.0), as applicable.

Attribute	Data Type	Description
resourceType	String	Always "DiagnosticReport"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
category	Coded Element	Classification of the clinical discipline, department or diagnostic service that created the report
code	Coded Element	Name/code for this diagnostic report
effectiveDateTime	DateTime	Effective time of the report
encounter:reference	Reference	Unique identifier of the Encounter to which the report is applicable to represented as a relative URL.
issued	Instant	DateTime the version of the report was made
performer:reference	Reference	Unique identifier of the performer of this report represented as a relative URL
presentedForm:url	String	URL to the report data
presentedForm:contentType	Code	Mime type of the report data
presentedForm:data	Base64	Base64 encoded binary data representing the report
presentedForm:size	Integer	Size of the data representing the report

status	Code	Status of the report
subject:reference	Reference	Unique identifier of the subject to whom the report is applicable to represented as a relative URL

Document Reference

Represents a document reference for a specific patient. Conforms to the [US Core DocumentReference Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "DocumentReference"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
author:reference	Reference	Unique identifier of the author of the document represented as a relative URL
category	Coded Element	High-level kind of document
content:attachment:contentType	String	Type of data encoded in the data attribute
content:attachment:data	Base64	Base64 encoded data representing the document
content:attachment:url	String	URL to the document data
content:format	Coded Element	Structure of the data representing the document
context:encounter:reference	Reference	Unique identifier of the encounter to which the document belongs represented as a relative URL
context:period:start	DateTime	Start time of the service
context:period:end	DateTime	End time of the service
custodian:reference	Reference	Unique identifier of the custodian of the document represented as a relative URL
date	Date	The document's date
status	Code	Status of the document reference
subject:reference	Reference	Unique identifier of the subject of the document represented as a relative URL
type	Coded Element	Type of document

Encounter

Represents an encounter for a specific patient. Conforms to the [US Core Encounter Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Encounter"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	Status of the encounter
class	Coded Element	Classification of the patient encounter
type	Coded Element	Specific type of encounter

subject:reference	Reference	Unique identifier of the subject of the encounter represented as a relative URL
period:start	DateTime	Start time of the encounter
period:end	DateTime	End time of the encounter
reasonCode	Coded Element	Coded reason for why the encounter took place
hospitalization:dischargeDisposition	Coded Element	Coded discharge disposition
participant:type	Coded Element	Role of the participant in the encounter
participant:period:start	DateTime	Time during the encounter when the participant started participating
participant:period:end	DateTime	Time during the encounter when the participant stopped participating
participant:individual	Reference	Unique identifier of the encounter's participants represented as relative URLs
location:location:reference	Reference	Unique identifier of the service provider responsible for the encounter represented as a relative URL

Goal

Represents a goal for a specific patient. Conforms to the [US Core Goal Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Goal"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
lifecycleStatus	Code	Current status of the goal. See http://hl7.org/fhir/ValueSet/goal-status
status	Code	Current status of the goal. See http://hl7.org/fhir/ValueSet/goal-status
subject:reference	Reference	Unique identifier of the subject of the goal represented as a relative URL
description:text	String	Description of the goal
target:dueDate	Date	The goal's targeted due date
statusDate	Date	When the goal's status took effect

Healthcare Service

Represents information about a specific Healthcare Service

Attribute	Data Type	Description
resourceType	String	Always "HealthcareService"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id

providedBy:reference	Reference	Unique reference to the Organization that provides this service represented as a relative URL.
location:reference	Reference List	Unique reference to the Locations where this service may be provided represented as relative URLs
category	Coded Element	Broad category of service being performed or delivered
name	String	Description of the service as presented to a consumer
comment	String	Additional description of the service as presented to a consumer
availableTime:daysOfWeek	Code List	Days of the week when the practitioner is available
availableTime:availableStartTime	Time	Start time when the practitioner is available on the given daysOfTheWeek
availableTime:availableEndTime	Time	End time when the practitioner is available on the given daysOfTheWeek

Immunization

Represents information about a specific Immunization. Conforms to the [US Core Immunization Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Immunization"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	The current status of the immunization. See http://hl7.org/fhir/medication-admin-status
statusReason	Coded Element	Reason why the immunization was not performed when applicable
primarySource	Boolean	Whether the content of the record is based on information from the person who administered the vaccine
vaccineCode	Coded Element	Vaccine product administered
patient:reference	Reference	Unique reference to the immunized Patient represented as a relative URL.
occurrenceDateTime	DateTime	When the vaccine was administered
manufacturer:display	String	Manufacturer of the vaccine
lotNumber	String	Vaccine lot number
site	Coded Element	Body site at which the vaccine was administered
route	Coded Element	How the vaccine entered the body
doseQuantity:value	Decimal	Amount of vaccine administered
doseQuantity:comparator	Code	How to understand the value

doseQuantity:unit	String	Unit representation of the amount
doseQuantity:system	String	System that defines the coded unit form
doseQuantity:code	Code	Coded form of the unit
note:text	String	Additional immunization notes

Location

Represents information about a specific Location. Conforms to the [US Core Location Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Location"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	The location's status
type	Coded Element	Type of location
mode	Code	Whether the resource represents a specific location or a class of locations
name	String	The location's name
telecom:	Contact Point	The location's phone number
address	Address	The location's address
hoursOfOperation	List	List of available days/times when the Practitioner is available in this role
hoursOfOperation:daysOfWeek	Code List	Day(s) of the week when the location is operating
hoursOfOperation:openingTime	Time	Start time when the location is operating on the given day(s)
hoursOfOperation:closingTime	Time	End time when the location is operating on the given day(s)
managingOrganization	Reference	Unique reference to the organization resource that is responsible for provisioning and upkeep of the location

Medication Request

Represents information about a specific Medication Request. Conforms to the [US Core MedicationRequest Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "MedicationRequest"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
status	Code	State of the prescribing event
intent	Code	The kind of medication order
medicationCodeableConcept	Coded Element	Medication to be taken

subject:reference	Reference	Unique reference to the Patient to which the medication was prescribed represented as a relative URL
authoredOn	DateTime	When the request was initially authored
requester:reference	Reference	Unique reference to the resource that made the request represented as a relative URL.
reportedBoolean	Boolean	Whether the request is reported vs the primary record
encounter:reference	Reference	Unique reference to the Encounter at which the medication request occurred represented as a relative URL
dispenseRequest:numberOfRepeatsAllowed	Integer	Number of refills authorized
dosageInstruction:sequence	Integer	The order of the dosage instructions
dosageInstruction:text	String	Free text dosage instructions
dosageInstruction:doseAndRate :doseQuantity:value	Decimal	Strength of medication
dosageInstruction:doseAndRate :doseQuantity:unit	String	Strength of medication units

Message

Message returned when a URL call cannot be completed due to a problem. For example a parameter validation error will result in an Error Message being returned.

Attribute	Data Type	Description
error	String	Machine readable identifier of the message type
error_description	String	Human readable message text
error_uri	String	URI to a resource that gives additional details about the error
state	String	Value of the "state" parameter from the originating request when present. This property is not set when a Message Data Element is wrapped in a Response Header Data Element; in this case the state property is set on the Response Header Data Element instead.

Observation

Represents an observation for a specific patient. Conforms to the following US Core Profiles (version 4.0.0) as applicable:

- [US Core Vital Signs Profile](#)
 - [US Core Blood Pressure Profile](#)
 - [US Core BMI Profile](#)
 - [US Core Body Height Profile](#)
 - [US Core Body Temperature Profile](#)
 - [US Core Body Weight Profile](#)

- [US Core Head Circumference Profile](#)
- [US Core Heart Rate Profile](#)
- [US Core Pediatric BMI for Age Observation Profile](#)
- [US Core Pediatric Head Occipital-frontal Circumference Percentile Profile](#)
- [US Core Pediatric Weight for Height Observation Profile](#)
- [US Core Pulse Oximetry Profile](#)
- [US Core Respiratory Rate Profile](#)
- [US Core Smoking Status Observation Profile](#)

Attribute	Data Type	Description
resourceType	String	Always “Observation”
identifier	Coded Element	The resource’s identifiers
id	Code	The resource’s logical id
category	Coded Element	Classification of the type of observation
code	Coded Element	Type of observation
issued	Instant	DateTime this version of the observation was made
status	Code	Status of the observation
subject:reference	Reference	Unique identifier of the subject to whom the observation is applicable to represented as a relative URL
value:valueCodeableConcept	Coded Element	Actual result
value:range	Range	Actual result as a range of values
component:code	Coded Element	Type of component observation (code / type)
component:valueQuantity	Quantity	Actual component result
component:valueCodeableConcept	Coded Element	Actual component result
component:valueCodeableConcept:unit	String	Units for actual component result
component:valueRange	Range	Actual component result as a range of values
effectiveDateTime	DateTime	Clinically relevant time/time-period for the observation

Organization

Represents information about a specific Organization. Conforms to the [US Core Organization Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always “Organization”
identifier	Coded Element	The resource’s identifiers

id	Code	The resource's logical id
identifier:NPI:value	String	National Provider Identifier (NPI)
identifier:NPI:system	URI	Always http://hl7.org/fhir/sid/us-npi when NPI is present
identifier:CLIA:value	String	Clinical Laboratory Improvement Amendments (CLIA) Number for laboratories
identifier:CLIA:system	URI	Always "urn:oid:2.16.840.1.113883.4.7" when CLIA is present
type	Coded Element	Type of organization
active	Boolean	Whether the resource is active
name	String	The organization's name
telecom	Contact Point	The organization's phone number
address	Address	The organization's address

Patient

Represents basic identifying information about a specific patient. Conforms to the [US Core Patient Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Patient"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
name:family	String	Patient's family name
name:given	String	Patient's given name
name:period:start	DateTime	When the name was/is effective as of
name:period:end	DateTime	When the name was/is no longer effective as of
name:suffix	String	Parts that come after the patient's name
name:use	Code	Intended use of this name. See http://hl7.org/fhir/valueset-name-use.html .
gender	Code	Patient's gender
birthDate	DateTime	Patient's date of birth
address	Address	Address element representing the patient's home address
extension:us-core-birthsex	Code	Patient's sex identified at birth
extension:us-core-ethnicity	Coded Element	Patient's ethnicity
extension:us-core-race	Coded Element	Patient's race
communication:language	Coded Element List	Patient's spoken language(s)

Practitioner

Represents information about a specific Practitioner. Conforms to the [US Core Practitioner Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Practitioner"

identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
name:family	String	Practitioner's last name
name:given	String	Practitioner's first name
telecom	Contact Point	Practitioner's phone number
email	String	Practitioner's email address
address	Address	Practitioner's address
communication:language	Coded Element	Practitioner's spoken language(s)
qualification	List	List of the practitioner's qualifications
qualification:code	Coded Element	Identifier of a qualification
qualification:period:start	DateTime	When the qualification is effective as of
qualification:period:end	DateTime	When the qualification is no longer effective as of

Practitioner Role

Represents information about a specific Practitioner Role. Conforms to the [US Core PractitionerRole Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "PractitionerRole"
identifier	Coded Element	The resource's identifiers
id	Code	The resource's logical id
practitioner:reference	Reference	Unique reference to the Practitioner to which this role belongs represented as a relative URL
organization:reference	Reference	Unique reference to the Organization where this role is available represented as a relative URL.
code	Coded Element List	Role(s) which the Practitioner may perform
acceptingNewPatients	Boolean	Whether the Practitioner is accepting new patients in this role
availableTime	List	List of available days/times when the Practitioner is available in this role
availableTime:daysOfWeek	Code List	Day(s) of the week when the practitioner is available
availableTime:availableStartTime	Time	Start time when the practitioner is available on the given day(s)
availableTime:availableEndTime	Time	End time when the practitioner is available on the given day(s)

Procedure

Represents information about a specific Procedure. Conforms to the [US Core Procedure Profile](#) (version 4.0.0).

Attribute	Data Type	Description
resourceType	String	Always "Procedure"
identifier	Coded Element	The resource's identifiers

<code>id</code>	<code>Code</code>	The resource's logical id
<code>status</code>	<code>Code</code>	Status of the procedure
<code>code</code>	<code>Coded Element</code>	Identification of the procedure
<code>performedPeriod:start</code>	<code>DateTime</code>	When the procedure started
<code>performedPeriod:end</code>	<code>DateTime</code>	When the procedure ended
<code>subject:reference</code>	<code>Reference</code>	Unique reference to subject of the procedure represented as a relative URL

Provenance

Represents provenance information for a Data Element. Conforms to the [US Core Provenance Profile](#) (version 4.0.0).

Attribute	Data Type	Description
<code>resourceType</code>	<code>String</code>	Always "Provenance"
<code>target:reference</code>	<code>Reference</code>	The resource's unique identifier represented as a relative URL
<code>occurredDateTime</code>	<code>DateTime</code>	Time when the provenance action occurred
<code>recorded</code>	<code>Instant</code>	Time when the provenance action was recorded
<code>agent:type</code>	<code>Coded Element</code>	Role of the resource identified by the agent:who field
<code>agent:who</code>	<code>Reference</code>	Reference to the resource that performed the provenance action represented as a relative URL.
<code>agent:onBehalfOf</code>	<code>Reference</code>	Unique reference to the Organization of the resource that performed the provenance action represented as a relative URL
<code>agent[ProvenanceAuthor]:type</code>	<code>Coded Element</code>	Role of the resource identified by the agent[ProvenanceAuthor]:who field
<code>agent[ProvenanceAuthor]:who</code>	<code>Reference</code>	Unique reference to the resource that authored the provenance represented as a relative URL.
<code>agent[ProvenanceTransmitter]:type</code>	<code>Coded Element</code>	Role of the resource identified by the agent[ProvenanceTransmitter]:who field
<code>agent[ProvenanceTransmitter]:who</code>	<code>Reference</code>	Unique reference to the resource that transmitted the provenance represented as a relative URL

Failed Response Header

Top level wrapper Data Element returned when calling any MUPIX request URL fails to return expected results. Requested Data Elements or related error messages are contained within this wrapper.

Attribute	Data Type	Description
<code>messages</code>	<code>List</code>	A list of Message Data Elements. One or more Messages will be present when the status is zero
<code>status</code>	<code>Integer</code>	0 = failed; When the status is zero the data property will be empty and one or more messages will be present within the

		messages element. For example zero will be returned when parameter values have failed validation.
--	--	---

Appendix A – PCE API Access Request Form

PCE API Access Request Form

To request API Access to a PCE system, please complete this document and send to apirequests@pcesystems.com. A representative will contact the requester to establish a requirements gathering conference call within five (5) business days of receipt of a request.

Contact Name: _____

Contact E-mail Address: _____

Contact Phone: _____

Requesting Agency: _____

Requesting Agency's EHR / Health IT Vendor: _____

Exchange Partner / System: _____

Brief Description of Desired Use Case(s):

Desired Transactions: _____

API Protocols / Standards (check all that apply)

- We wish to use the API documentation as published
- We wish to use the following standards / protocols: _____
- We wish to use a custom API (briefly describe): _____

Appendix B - Terms of Use

Access to the PCE Care Management Version 9.4 ONC 2015 Edition Cures Update Web Service API is predicated on your agreement to the following Terms of Use. Please note that the use of the Service is also subject to separate legal agreements dictating additional terms, costs (as described in Appendix C – Costs), conditions, and acceptable use that will be necessary between or among you, PCE, and any PCE clients or other entities whose systems / information may be accessed through the Service. PCE cannot guarantee that PCE clients or third party entities will agree to allow such access. In addition, PCE reserves the right to deny any request for access to the Service for any reason. All access is subject to applicable privacy and security considerations including, without limitation, those that are necessary to comply with HIPAA, 42 C.F.R. Part 2, and any other federal, state, or local laws and regulations. To the extent that access to the Service is granted, the following Terms and Conditions apply.

Terms of Use

Please read these Terms of Use (the "Agreement") carefully before using the PCE Care Management Version 9.4 ONC 2015 Edition Cures Update Web Service API (the "Service") operated by PCE Systems ("PCE").

Your access to and use of the Service is conditioned on your acceptance of and compliance with these Terms. These Terms apply to all visitors, users, customers, contracted entities, downstream entities, and others who access or use the Service.

By accessing or using the Service you agree to be bound by these Terms. If you disagree with any part of the terms then you may not access the Service.

1. Access and Use. You are provided access to the Service for the sole purpose of aiding you in your professional healthcare job responsibilities. When you access a certain patient's PHI through the Service, you represent and warrant that you have an active treatment relationship with that patient and that you are accessing such PHI only to the extent permissible under applicable law regarding the privacy of PHI for one of the following reasons: (1) for treatment of the patient within the scope of your existing treatment relationship, (2) to conduct authorized healthcare operations. The terms "treatment" and "healthcare operations" shall have those meanings attributed to them as defined in HIPAA and its related regulations. You understand that credentials used for access to The Service are unique to you and may not be shared with or viewed by others. You agree that you will not share credentials with anyone.

2. Compliance with Applicable Law / Privacy. You understand that you are responsible for abiding by and compliance with all applicable laws and regulations relating to your access of all PHI, including SPHI. These laws and regulations include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. Parts 160 and 164 Subparts C and E and 42 C.F.R. Part 2.

3. Data Quality / Independent Medical and Professional Judgment. You understand that you are responsible for all decisions, acts, and omissions of any persons in connection with the delivery of medical care or other services to any patients within the exercise of your independent medical and/or professional judgment. It is your responsibility to review and test all software and associated workflows and other content, as implemented, make independent decisions the use of the system based upon your needs, practices, standards

and environment, and reaches your own independent determination that they are appropriate for use. You understand that the Service provides data routing, transmission, and display of data from various sources across the healthcare community. You agree that PCE is not responsible for the content, completeness, reliability, or quality of any data transmitted. You further understand that anomalies may occur at numerous points throughout the process, including data quality from sources, service availability, source system availability, transmission issues, or other data issues. You understand that any data you receive or that is omitted should be independently verified by you using your medical and/or professional judgment, regardless of whether the information received appears anomalous or otherwise inconsistent with other information you obtain. You understand and acknowledge that the Service is merely one of a variety of sources of information to be used in providing care to your patient. All data that is made available through the Service is subject to change arising from numerous factors, including without limitation, changes to patient health information made at the request of the patient, changes in the patient's health condition, the passage of time and other factors. The Service may not initiate the transmission of any data, and does not monitor the specific content of data being transmitted. Without limiting any other provision under this Agreement, PCE SHALL HAVE NO RESPONSIBILITY FOR OR LIABILITY RELATED TO THE ACCURACY, CONTENT, CURRENCY, COMPLETENESS, CONSENT, OR DELIVERY OF ANY DATA PROVIDED BY A PARTICIPANT TO THE SERVICE.

4. **Prohibition on Redisclosure.** Except as specifically set forth herein or as provided by law, you may not make further disclosures of patient information you obtain from the Service, including SPHI, unless further disclosure is permitted by the written consent of the person to whom it pertains or as otherwise permitted by federal and/or state laws and regulations. You agree not to remove any confidentiality tags or other indications of confidentiality on any data that you obtain from the Service. You take responsibility for the safekeeping and protection of the privacy of any PHI you obtain from the Service.

5. **Availability.** Access to the Service or other source systems with the Service's network may be limited during periods of high volume, system upgrades, maintenance, or for unanticipated reasons. PCE shall not be liable if you or another user is unable to access the Service or any resources connected to the Service or if you or another user is unable to complete transactions through the Service.

6. **Consent to Monitoring.** By using this system, you consent to the monitoring and auditing of all of your activity by the Service system.

7. **License.** Upon granting access to the Service, PCE is granting you a non-exclusive, non-transferable, non-sub-licensable, and limited right to use the Service. The Service shall only be used through direct access through the web portal, and shall not be used for any other purpose whatsoever, and shall not be copied or incorporated into any other computer program, hardware, firmware, or product without the express written consent of PCE.

8. **DISCLAIMER OF WARRANTY: THE SERVICE AND ANY SERVICES RELATED TO THE SERVICE PROVIDED BY PCE ARE PROVIDED UNDER THIS AGREEMENT ON AN "AS IS", "WHERE IS", AND "AS AVAILABLE" BASIS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE SERVICE OR RELATED SERVICES ARE FREE OF DEFECTS, IMPLIED WARRANTY OF**

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, OR THAT THE OPERATION OF THE SERVICE OR SERVICES WILL BE UNINTERRUPTED, TIMELY, OR ERROR-FREE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SERVICE ARE WITH YOU. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT AND THE LICENSE GRANTED HEREUNDER. NO USE OF THE SERVICE OR RELATED SERVICES IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER, THIS AGREEMENT DOES NOT OBLIGATE PCE TO PROVIDE ANY SERVICES RELATED TO THE SERVICE OR ANY UPDATES TO YOU AND ANY SUCH SERVICES OR UPDATES, IF PROVIDED, WILL BE AT THE SOLE DISCRETION OF PCE.

9. LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, CONTRACT, OR OTHERWISE, SHALL PCE BE LIABLE TO YOU OR ANY PERSON FOR ANY LOSS OR DAMAGE OF ANY KIND ARISING FROM THE SOFTWARE, OR YOUR USE OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, HARM, INJURY, OR DEATH OF A PATIENT, EVEN IF SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. Indemnification. In consideration for PCE's granting you permission to use the Service, you expressly release and hold harmless PCE, as well as its trustees, officers, directors, employees, agents and affiliates from any and all claims, liabilities, demands, causes of action, costs, expenses, and damages of every kind and nature, in law, equity, or otherwise, arising out of or in any way related to your use of the Service, or any of the data or other content obtained by using the Service, whether or not arising from any acts or omissions by PCE or its trustees, officers, directors, employees, agents or affiliates. In addition, you shall indemnify and hold harmless PCE, its officers, directors, agents, affiliates, and employees, against all actual and direct losses, liabilities, damages, claims, costs or expenses (including reasonable attorney's fees) they may suffer as the result of third-party claims, demands, actions, investigations, settlements or judgments against it arising from or in connection with any breach of this Agreement, or from any claim of any nature or any wrongful acts or omissions, by you or your other employees, officers or agents. These provisions shall survive any termination of this Agreement.

11. Term and Termination. This agreement shall take effect at the time you first access the Service and will remain in effect until it is terminated. Either party may terminate this Agreement at any time, with or without cause, upon ten (10) days' prior notice. Users who wish to terminate this Agreement must do so in writing by contacting the following:

PCE Systems
Attn: Corporate Counsel
28530 Orchard Lake Road
Farmington Hills, MI 48334

In addition, the PCE may terminate this Agreement immediately if: (i) you breach the terms of this Agreement;

(ii) in the PCE's good faith judgment, audit results demonstrate unusual use of the Service from your account (provided, however, that nothing contained herein shall require PCE to perform monitoring of such use); or
(iii) you have not used the Service at all for a period of three (3) months. In the event of Termination for any reason, your rights to use the Service shall end immediately and you must destroy all copies of relevant software on your computer or in your possession.

12. Prohibited Uses. You acknowledge that the Software is the valuable proprietary, intellectual property and trade secret information of PCE. You may not except as specifically permitted in this Agreement do any of the following. (These items will survive termination of this Agreement.)

- a. Attempt to (or permit another in his or her attempts to) reverse engineer, disassemble, or de-compile the Service or to remove any product identification, copyright notices, or other notices or proprietary restrictions from PCE;
- b. Use, copy, modify, transfer, create derivative works of, publicly display or distribute the Service or any component thereof. Use the data obtained from the Service for your own benefit or for the benefit of a third party other than the patient;
- c. Transmit or provide any data or other content you obtain from the Service to a third party except in accordance with applicable law; or
- d. Incorporate any data or other content you obtain through use of the Service platform (e.g., screenshots, workflows, etc.) in a product design, developed, marketed, sold, or licensed to you, on your behalf, or on your employer's behalf.

In addition, you agree, through your use of and access to the Service:

- a. not to disrupt or interfere with the security of, or otherwise abuse, the Service, or any services, system resources, accounts, servers or networks connected to or accessible through the Service;
- b. not to disrupt or interfere with any other user's enjoyment of the Service;
- c. not to upload, post, or otherwise transmit through or on the Service any viruses or other harmful, disruptive or destructive files;
- d. not to use or attempt to use another's account, service, or system without authorization from PCE, or create or use a false identity on this Service;
- e. not to divulge any security credentials, tokens, or other security-related information (including endpoint information) to others; and
- f. not to attempt to obtain unauthorized access to the Service or any service, system, or resource linked thereto.

13. PCE is the owner or licensor of all rights in the Service, its content, software, and services, unless expressly and prominently specified otherwise in the Service content. You have no rights to such content, software or services except as expressly granted in this Agreement. The name "PCE Care Management", system names, and the logos or other proprietary marks of PCE and belong to PCE, its licensors, and / or partners. No right, title or interest in that intellectual property is granted to you in this Agreement.

14. No waiver of any term of this Agreement will be valid unless in writing and acknowledged in writing by the waiving party. If any portion of this Agreement is adjudged invalid or unenforceable by a court of competent jurisdiction, such provision will be enforced to the maximum permissible extent to effect the intent of the parties, and the remaining portions will remain in full force and effect. No joint venture, partnership, franchise, employment, or agency relationship exists between you and PCE, or any other party participating in the Service as a result of this Agreement or your use of the Service. This Agreement constitutes the entire agreement between the parties regarding its subject matter; provided, however, that you will also be subject to any additional terms and conditions of which you are notified and to which you manifest consent by continued use of the Service. These terms are subject to change; any updated terms will be available at https://w3.pcesecure.com/staticPages/PCM/PIX_9_4_API_Documentation.pdf. This EULA is governed by the laws of the State of Michigan, and you consent to jurisdiction and venue for any dispute relating to this Agreement within the courts located in Oakland County, Michigan without regard to choice of law / venue provisions in your jurisdiction.

Appendix C - Costs

The Web Service API is subject to a one-time setup fee to be charged to exchange partners (vendors, technical platforms, endpoints, etc.). This setup fee will be due prior to the initial kick-off call with the exchange partner and includes (1) provisioning and deployment of a test environment, (2) initial setup, configuration, and activation of the exchange partner within the test environment, (3) up to 5 hours of non-production testing with a PCE engineer and the exchange partner, (4) setup, configuration, and activation of the exchange partner within the production environment upon successful testing, and (5) up to two hours of production testing and validation with a PCE engineer.

Additional testing time, assistance, and support, including ongoing support, troubleshooting or other partner-required maintenance post-launch, can be purchased in 10-hour pre-paid increments. Please contact PCE at apirequests@pcesystems.com for the current fee schedule.

Use of the API assumes an appropriate level of technical experience and expertise with the technologies described in the Web Service API Documentation. PCE reserves the right to unilaterally terminate an API setup project in the event that an API cannot be successfully tested and approved for production within 25 testing hours (excluding any time spent addressing issues originating from PCE's platform or services).

All costs are non-refundable.

Revision History

Date	Author	Description
2025-01-06	Jeff Chang	Terms and Costs Updates
2022-11-10	Jeff Chang	Initial Release