FHIR@VITALINK COOKBOOK

Version 0.3

FHIR@VITALINK Cookbook

Contents

1. Document management

1.1. History

Version	Date	Description
0.1	25/08/2023	First draft
0.2	28/08/2023	Added security labels
0.3	11/01/2024	New URL for HVA environment & fix typo's

1.2. Purpose

This cookbook is for developers, analysts and software producers involved in the integration into their software solution of the services delivered by Vitalink, specifically for the FHIR data.

Fast Healthcare Interoperability Resources (FHIR) is a next generation standards framework created by HL7. Solutions are built from a set of modular components called "Resources". These resources can easily be assembled into working systems that can solve clinical and administrative problems. More about FHIR can be read on the FHIR website: http://hl7.org/fhir/.

FHIR has defined general, international definitions of resources. Nevertheless, within the standard, it is possible to create a local variant based on those international resources. In a co-creation with the industry, the healthcare-sector, HL7 and the different governments involved eHealth has created a Belgian version of international resources. These Implementation Guides can be retrieved on the eHealth website: https://www.ehealth.fgov.be/standards/fhir/index.html.

The goal of the cookbook is to document how a software can accomplish a technical integration with Vitalink in FHIR.

The business use cases and data models themselves are not part of this cookbook.

This document is composed of two sections:

- Section Principles explains the architectural principles as authentication, authorization and security.
- Section FHIR interactions provides an overview of the used resources.

2. Principles

2.1. Architectural principles

Vitalink has selected some specifications in order to guarantee the regulations on the data shared in the ecosystem.

2.1.1. Pseudonymisation

To ensure privacy regulation Vitalink has chosen to use pseudonyms for identifiers of patients in order to guarantee security around the medical data of each patient that is stored in the database of Vitalink.

To accomplish pseudonymisation eHealth's pseudo service, as trusted party, will be used to pseudonymize, convert and identify data.

Vitalink will expect incoming data to contain pseudonyms of specific data elements (see chapter 3). A software will need to onboard with eHealth to be able to pseudonymize data using the pseudo service. Access needs to be granted for the software package so it can pseudonymize, identify and/or convert to the Vitalink domain.

More details can be found on the eHealth documentation: NL, FR.

2.1.2. Authentication

Vitalink expects tokens from the authentication service of eHealth: I.AM Connect.

More information about I.AM Connect can be found here: NL, FR. A client should register itself in a realm so that it can connect to the services of I.AM Connect. The client registration document on the website should be filled out and sent to eHealth to get access.

It uses the OpenID Connect (https://openid.net/connect/) layer on top of the OAuth2.0 protocol (https://oauth.net/2/), where it provides a JWT token for the client who can use it to identify itself at the vaults. The granted access token should be put in the Authentication header of each REST request to Vitalink as a Bearer token.

More details about what users, roles and organizations can have access will be part of the onboarding phase.

2.1.3. Authorization

The JWT token that the client should provide will contain the necessary information to authorize itself. Based on the information provided in the JWT token the necessary authorization checks are performed.

Patient's consent, exclusions, therapeutic relations and 'access matrix' are also verified according to the regulations. Vitalink uses an integration for this with the Attribute Authority service of eHealth. More information can be found here: NL, FR.

2.1.4. Security Labels

As Vitalink is used for the storage of medical data of multiple business owners which could be using the same FHIR resource type, it is chosen to protect resource instances with security labels. The decision engine of Vitalink will decide to which security label(s) certain actors and software have access to (http://hl7.org/fhir/R4/security-labels.html).

The declaration of what security labels can be used, is part of the onboarding phase at Vitalink.

The usage of security labels is described in the chapter below.

3. FHIR interactions

Like mentioned before we follow the FHIR standards. It provides default resource definitions, created by HL7. In Belgium, eHealth (together with all parties stated above) defined specific FHIR profiles according to the Belgian requirements. The implementation guide for these profiles can be found here: https://www.ehealth.fgov.be/standards/fhir/index.html.

Vitalink supports only FHIR R4 as this is also the version used in the implementation guide.

3.1. CapabilityStatement

The server's capabilities of Vitalink will always be exposed on the CapabilityStatement like how it's specified in FHIR. This contains both the supported operations as the supported profiles of the implementation guides.

- ACC: https://apps-acpt.vitalink-services.be/vault/api/r4/metadata
- PROD: not available yet

3.2. OpenAPI

Vitalink also exposes an OpenAPI for testing. Authorization is necessary beforehand. Once a software got a client-id from eHealth it can be filled in depending on the configuration. The next step is to login as a user to have an access token. The usage of a Bearer token is also supported.

- ACC: https://apps-acpt.vitalink-services.be/vault/api/r4/swagger-ui/
- PROD: no testing done in PROD

3.3. Use of pseudonyms

SSIN identifier

As Vitalink we expect the incoming SSIN (INSZ/NISS) identifiers of patients to be pseudonymized.

By pseudonymizing the patients identifier the medical data can be used in the clear as it's not possible to know which data is linked to which patient.

For the usage of pseudonyms in FHIR, eHealth defined an extension to be used on FHIR elements. This extension can be found here: https://www.ehealth.fgov.be/standards/fhir/infsec/StructureDefinition-be-ext-pseudonymization.html.

For each identifier of a patient Vitalink expects a pseudonym in transit as a string in the value of the identifier, like follows:


```
"identifier":
        {
          "system": "https://www.ehealth.fgov.be/standards/fhir/core/NamingSystem/ssin",
          "value":
        "ewogICJpZCIgOiAiOWFhNDE2Y2ItNTg2Yy00YmJjLWI3MGQtMTE5N2RkN2JmODczIiwKICAiY3J2IiA6ICJQLTUy
        MSIsCiAgIngiIDogIkFNNDNMcXcxTVVTV016eFVQVW9HME9HOUNST0VXdUE5akNMTTc5TGU1OUdGWkJ4UjRHK1lPO
        Hl6Z3JxWHFNM2RwQXdEM0xWU1hrdGNMc3pLWnJEMk5QQ3ciLAogICJ5IiA6ICJBVGNTREZTYno3QVRoMkxWWHRCak
        RHSHVndnFkaFB5S2hhSVptREJ5QXdtNzFUeis0dGM4Q2Q0d0FUMFJST3JCNjFTR1BaOTBreDFqTjhXZkcvTHgyUHE
        4IiwKICAiZG9tYWluIiA6ICJ2aXRhbGlua192MSIsCiAgImlhdCIgOiAxNzA0OTY5NjMyLAogICJleHAiIDogMTcw
        NDk3MDIzMiwKICAidHJhbnNpdEluZm8iIDogImV5SmhkV1FpT2lKb2RIUndjem92TDJGd2FTMWhZM0IwTG1Wb1pXR
        nNkR2d1Wm1kdmRpNWlaUzl3YzJWMVpHOHZkakV2Wkc5dFlXbHVjeTkyYVhSaGJHbHVhMTkyTVNJc0ltVnVZeUk2SW
        tFeU5UWkhRMDBpTENKaGJHY2lPaUprYVhJaUxDSnJhV1FpT2lJM1pXSTFNbUZsTlMweE5qVXhMVFEwT0dRdE9UWmt
        ZeTAxTkdSbE5XRmxZbU01TlRVaWZRLi5RcDZLUVZMOFVhazZMZTdBLklsWHkwWUVMRmVfbkRzU2h1SEhEUElCOXMw
        NTVFSmYyY3VUYWpUUmZPci1ueEQzTnl0ZmIzZEpUVllwT0R3bkl5LVFNRnowSFZiUmVYakFpdDhuQy1WMWZnWHFVc
        3RSa0czNnl6RVJGdDdOajJLclZRWTFVcHJFZ2dpVG5LUVVLel9abTlQVjVWWWxaRWRwdjNTNFJmNTJPTGwzTjRLT2
        16TkJzNFl1eGx3MjhhdGFXZjM1RS5SMm16SGVfVnlOX05GVkp1OWdOY1F3Igp9",
          "_value": {
            "extension": [
              {
                "url": "https://www.ehealth.fgov.be/standards/fhir/infsec/StructureDefinition/be-
        ext-pseudonymization",
                "extension": [
                  {
                    "url": "marker",
                    "valueBoolean": true
                  }
                ]
              }
            ]
          }
        }
```

3.4. Use of patient references

The FHIR resource for Patient is managed by Vitalink itself. In order to create, update or search data for a patient a software should only use a logical reference in the property of the FHIR resource where it is expected to use the patient reference. This needs to be like following:


```
{
  "resourceType": "ResourceType",
  "subject": {
    "type": "Patient",
    "identifier":
        {
          "system": "https://www.ehealth.fgov.be/standards/fhir/core/NamingSystem/ssin",
          "value":
        "ewogICJpZCIgOiAiOWFhNDE2Y2ItNTg2Yy00YmJjLWI3MGQtMTE5N2RkN2JmODczIiwKICAiY3J2IiA6ICJQL
        TUyMSIsCiAgIngiIDogIkFNNDNMcXcxTVVTV016eFVQVW9HME9HOUNST0VXdUE5akNMTTc5TGU1OUdGWkJ4UjR
        HK1lPOHl6Z3JxWHFNM2RwQXdEM0xWU1hrdGNMc3pLWnJEMk5QQ3ciLAogICJ5IiA6ICJBVGNTREZTYno3QVRoM
        kxWWHRCakRHSHVndnFkaFB5S2hhSVptREJ5QXdtNzFUeis0dGM4Q2Q0d0FUMFJST3JCNjFTR1BaOTBreDFqTjh
        XZkcvTHgyUHE4IiwKICAiZG9tYWluIiA6ICJ2aXRhbGlua192MSIsCiAgImlhdCIgOiAxNzA0OTY5NjMyLAogI
        CJleHAiIDogMTcwNDk3MDIzMiwKICAidHJhbnNpdEluZm8iIDogImV5SmhkV1FpT2lKb2RIUndjem92TDJGd2F
        TMWhZM0IwTG1Wb1pXRnNkR2d1Wm1kdmRpNWlaUzl3YzJWMVpHOHZkakV2Wkc5dFlXbHVjeTkyYVhSaGJHbHVhM
        TkyTVNJc0ltVnVZeUk2SWtFeU5UWkhRMDBpTENKaGJHY2lPaUprYVhJaUxDSnJhV1FpT2lJM1pXSTFNbUZsTlM
        weE5qVXhMVFEwT0dRdE9UWmtZeTAxTkdSbE5XRmxZbU01TlRVaWZRLi5RcDZLUVZMOFVhazZMZTdBLklsWHkwW
        UVMRmVfbkRzU2h1SEhEUElCOXMwNTVFSmYyY3VUYWpUUmZPci1ueEQzTnl0ZmIzZEpUVllwT0R3bkl5LVFNRno
        wSFZiUmVYakFpdDhuQy1WMWZnWHFVc3RSa0czNnl6RVJGdDdOajJLclZRWTFVcHJFZ2dpVG5LUVVLel9abTlQV
        jVWWWxaRWRwdjNTNFJmNTJPTGwzTjRLT216TkJzNFl1eGx3MjhhdGFXZjM1RS5SMm16SGVfVnlOX05GVkp1OWd
        OY1F3Igp9",
          "_value": {
            "extension": [
              {
                "url":
        "https://www.ehealth.fgov.be/standards/fhir/infsec/StructureDefinition/be-ext-
        pseudonymization",
                "extension": [
                  {
                    "url": "marker",
                    "valueBoolean": true
                  }
                ]
              }
            ]
          }
        }
  }
}
```

3.5. Use of security labels

Each FHIR resources sent to Vitalink should have a security label. This way Vitalink can ensure the correct usage of the resource instance based on the rules behind the security label defined by the business owner.

```
{
  "resourceType": "ResourceType",
  "meta": {
    "security": [
      {
        "system": "https://www.apps.vitalink-services.be",
        "code": "PATIENT_HEALTH_RECORD",
        "display": "Patient Health Record"
      }
    ]
  }
}
```

The example above uses a fictive security label.

For search queries the _security search parameter can be used to filter resources based on security labels: https://hl7.org/fhir/R4/search.html#security. This parameter is optional in the server. If it's not used the user will only receive the resources matching the security labels the user is allowed to access.