A Personalised Integrated Care Platform

(Grant Agreement No. 689209)

D5.6 Second Integrated Data Management Subset in Public Cloud

Date: 2018-10-10

Version 1.0

Published by the PICASO Consortium

Dissemination Level: Confidential

Co-funded by the European Union's Horizon 2020 Framework Programme for Research and Innovation under Grant Agreement No 689209

Document control page

Document file: D5.6 Second Data Management Subset in Public Cloud.docx
Document version: 1.0
Document owner: TUK

Work package: WP5 – Private Enhanced Integrated Data Management
Task: T5.5 – Data Management Subset
Deliverable type: [DEM]

Document status: ☒ approved by the document owner for internal review
☒ approved for submission to the EC

Document history:

Version	Author(s)	Date	Summary of changes made
0.1	Marek Skokan (TUK)	09-07-2018	Structure of deliverable
0.2	Marek Skokan (TUK)	21-08-2018	Architecture diagram with description and description of TUK's components. Preparation for collection of partner's inputs
0.3	Matts Ahlsén, Tobias Brodén (CNET)	26-09-2018	Section on ODS added
0.4	Armanas Povilionis (INUIT)	27-09-2018	Section 5 Security and Privacy Managerment has been added
0.5	Marek Skokan	03-10-2018	Integration of the inputs. Section 8 added. Version for peer review created.
1.0	Marek Skokan	10-10-2018	Final version prepared based on peer review

Internal review history:

Reviewed by	Date	Summary of comments
Carlos A. Velasco	08-10-2018	Accepted with comments

Index:

1 Executive Summary

This document presents an overview of the status of the Integrated Data Management Subset components. These components are built on a federation of multiple external and internal cloud solutions, which match the needs of future care provision, while still respecting the legacy structure of today's health care systems. The implemented and deployed ICT solution based on this approach provide a data management backbone for the PICASO Trial. The integrated components building the Data Management Subset in PICASO are described from functional point of view and the dependencies between components are explained and demonstrated.

2 Introduction

The PICASO project aims at providing holistic view on health state of Patient with comorbidities. Such view means visualisation of integrated healthcare data available that are originated from various information sources. The ICT solution enabling management of healthcare data coming from available information sources was designed components were (and are being) developed and integrated. This deliverable describes integrated set of components that create PICASO Data Management Subset. By having deployed these components the PICASO trial could start. The status of the Data Management Subset which enabled PICASO trial to start is presented in this version of the deliverable. Note, there were significant changes in Data Management Subset when comparing it with the first version of deliverable (D5.4). Most notably, the secure access management of data was designed and deployed and ODS system was updated with some extra components.

2.1 Purpose, context and scope of this deliverable

In this deliverable the current "trial-ready" status of PICASO Data Management Subset is described. It is second version from the series of three deliverables that provide a "snapshot" on the evolution of Data Management Subset in the PICASO system. Note, even though the ODS system is not part of PICASO Public Cloud (explanation of architectural decisional why ODS is part of the PICASO Private Cloud can be found in D2.4 Section 6) it is integral part of the Data Management. The reason is that it integrates healthcare data from information sources into ODS and provides private interfaces (managed by Message Handler component) over such data. Thus, the description of ODS system is considered as being in scope of this deliverable.

2.2 Intellectual Property (IP)

The different components of the Data Management Subset are subject to open source and commercial licences, which are subject to the licences reflected in the IP repository being created for the project.

2.3 Content and structure of this deliverable

The deliverable is organized as follows:

- Chapter 3 – Architecture of Data Management Subset with description of components and references to the related content describing components in more details
- Chapter 4 – ODS system.
- Chapter 5 – Security and Privacy Management
- Chapter 6 – Shared Memory Manager.
- Chapter 7 – Data Resource Browser.
- Chapter 8 – Basic demonstration of Integrated Data Management
- demonstration of Integrated Data Management

3 Data Management Subset Architecture

The Architecture of Data Management Subset is a subset of the overall PICASO system Architecture. It defines components and their dependencies the way it enables management of healthcare data in PICASO system.

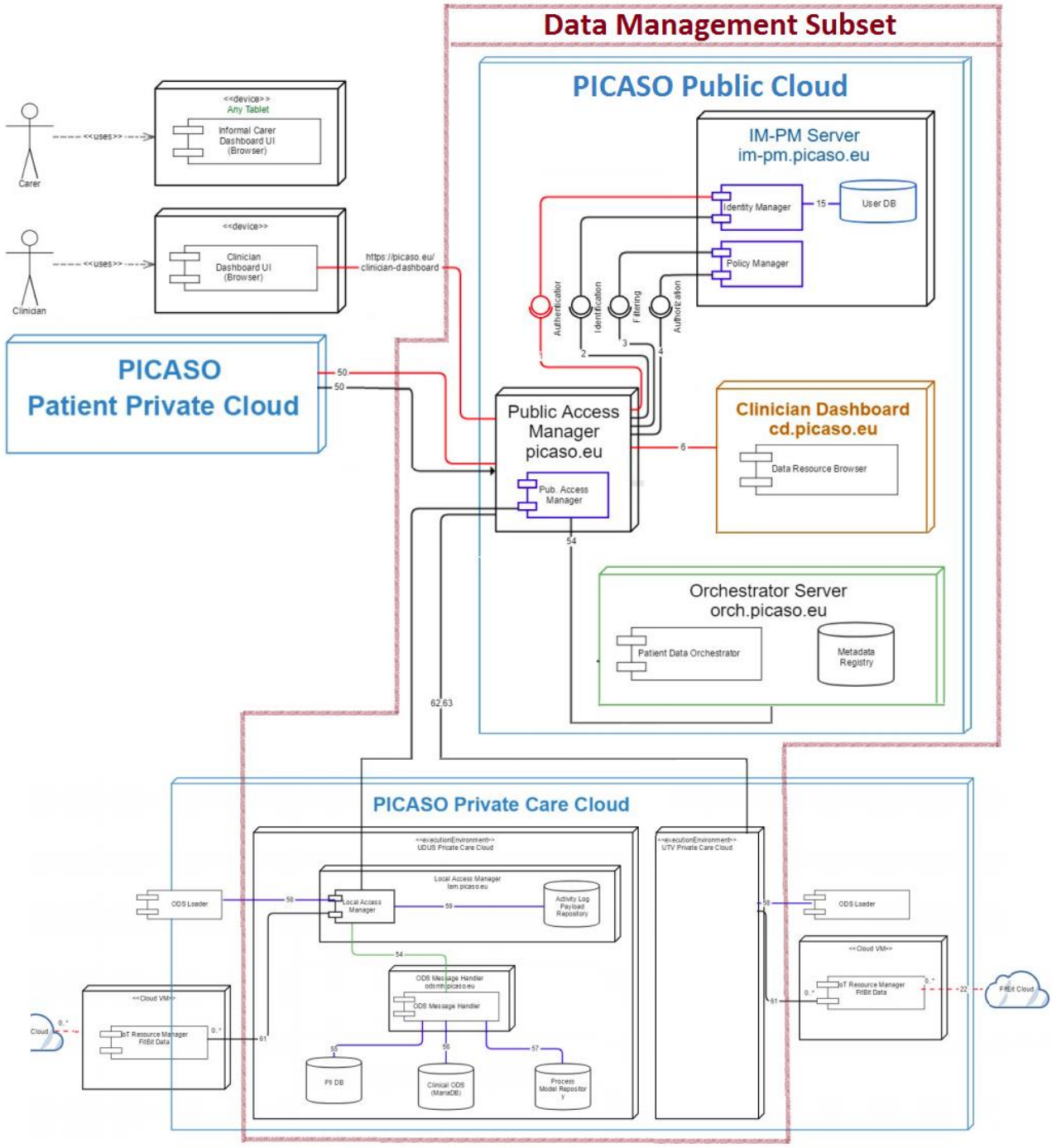


Figure 1: Data Management Subset architecture - components belonging to red polygon represent the Data Management Subset.

The integrated components of Data Management Subset depicted on the deployment view in Figure 1 enable secure data management of healthcare data fused from PICASO Private Care Cloud (hosted in hospitals) and Patient Private Cloud (Home monitoring and measurements). The Clinical ODS (Operational Data Store) has been developed based on a PICASO Common Information Model (output of T5.1). It is deployed in the hospitals - PICASO Private Care Cloud. The relevant healthcare data about patients involved in the PICASO trial from Hospital Information System (HIS) have been migrated into the ODSes. Also, the data from Patient Private Cloud (incl. FitBit Cloud) are fetched into the ODSes. Thus, each ODS serves as integration secure point for healthcare data available. Such implementation comes from architectural decision that has been done

after long discussions with all sides involved. There is one aspect on this design that allowed convincing of IT and legal departments in the hospitals as well as Patient involved about the maximum possible privacy and security of the data being stored like this. Namely, the data are stored in the hospital in the servers running by hospitals behind the hospital firewalls. This means, the data are protected by the same security standards the data already stored by original HISes. More information about the ODS as secure PICASO storage enabling data integration is provided in Section 4. Then, there is another feature needed to manage data - secure way of accessing them. As can be seen on the Figure 1, the Access Manager component is involved in every single connection between components from the Public Cloud and those components running in the Private Care Cloud. Shortly, the components communicating between these public and private clouds have to be registered in the Access Manager otherwise any attempt for communication will fail. It can be also seen that Identity Manager component and Policy Manager component as well as User databases are involved. They run on so-called IM-PM Server (see Figure 1), which is technically an independent server. These components support the process of secure access management in the PICASO system. More information about the PICASO Access Management solution is provided in Section 5. Even though data are integrated in ODS, the functionality that fuse data from all relevant ODSes is needed. This functionality is covered by the Patient Data Orchestration component (PDO) together with the Metadata Registry component (MDR). Both of these components represent so called Shared Memory Manager (Note, first version of Shared Memory Manager is described in D5.2 and the current version is its further evolution.) These components run in the independent server belonging to the Public Cloud. The PDO basically provides secure data access services for the Clinician Dashboard. It enables accessing of relevant data about the selected patient by user/clinician (e.g. currently examined patient by clinician) that are filtered by the authorisation rules applicable. Such data fusion functionality employees also Metadata registry. It is a registry containing patient UPIDs, data category with last modification date of this category and URI to the source - ODS. Based on architecture, this registry is being continually updated from ODSes, when there is any update of patient's healthcare data there. Using the information from the registry, the relevant ODSes are further queried for data by PDO and the rest ODSes are not queried. More details about the PDO and MDR are in Section 6.

The information sources about patient examined are visualised in Data Resource Browser (DRB). The DRB is part of Clinician Dashboard. It enables browsing of information using graph similar to Mind map where nodes represent same data categories that are recognised in Access management as well as in MDR. By selecting the node, its expansion with relevant nodes with sub-categories happened. Thus, navigation towards details selected is presented. In case no expansion is possible the list giving history of data relevant to the selected category is presented below the mind map. The navigation to the Patient Data Viewer is possible from this list (data are presented in the interactive charts and timelines there). The DRB is tool for end user/clinician that enable investigation of Data sources available for the patient. More information about the DRB is in Section 7.

The Data Management Subset components are responsible for secure retrieval of relevant patient information from information sources available. It is done based on request response according to actual context. In particular, steps of care plan execution and the decision support tools need very specific patient information relevant to the patient's actual context.

4 ODS system

4.1 Operational Data Store - ODS

4.1.1 Description

The Operational Data Store (ODS), implements persistent data storage for the PICASO platform. The ODS stores data extracted from the back-end clinical systems, in combination with data (observations) retrieved from remote patient monitoring. The ODS is used by the PICASO user interface components (Clinician and Patient Dashboards) and by any internal PICASO component requiring persistent storage.

The database schema is based on the CIM (Common Information Model) as defined by PICASO and conforms to subsets of HL7 and the FHIR model for care plans.

The ODS separates all Personally Identifiable Information (PII) which could identify an individual, from the related clinical data. This is supported by the use of pseudonymization in combination with separate physical storage of the corresponding database subsets.

The *clinical database subset* includes the following categories,

- Patients clinical data
- Diagnosis data
- Observations (remote monitoring data)
- Medications
- Questionnaires (data collected from patients)
- Care Plan Instances, including
    - Patient Dairy activities and schedules
- Meta data for monitoring devices

The *PII database subs*et stores personal and demographic data related to the patients, their informal carers and clinicians.

An ODS is deployed in the Private Carer Cloud (Hospital DMZ) in isolation from the back-end clinical systems, with no update dependencies between clinical systems and PICASO. However, clinical data extraction is performed periodically using specific ETL[1] tools interfacing the back-end clinical systems.

4.2 ODS Message Handler

4.2.1 Description

The ODS Message Handler is a service layer providing a controlled interface to underlying ODS database instances. It effectively encapsulates all ODS clinical and other patient generated data, thus forcing all PICASO client component requests to pass through this layer.

It provides a FHIR-based (Fast Healthcare Interoperability Resources) API for insertion and retrieval of care related data. The ODS MH supports the following functionality,

- Receives and submits updates to the ODS
- Forwards retrieval requests to the ODS
- Receives (update) triggers from the ODS
- Informs the Meta Data Registry component when patient data and care plans are added, updated or deleted.

The Message Handler API is structured in a number of controllers. Each controller manages a specific ODS data category, with the corresponding set of methods.

[1] Extract Transform Load

- **Careplan** // CRUD[2] for careplan and JSON BLOBs. Retrieval of Careplan activities .
- **Clinician** // Data on clinicians.
- **DataResourceBrowser** // Aggregation of data for the Data Resource Browser.
- **FollowUp** // POST of bookings of Follow-Up Appointments.
- **LeaveOfAbsence** // CRUD for Leave of Absence.
- **Medication** // CRU for medication intake confirmation.
- **Observation** // POST of home measurements including Fitbit data. Retrieval of data for the Patient Dashboard.
- **PatientDataOrchestrator** // Aggregation of all data for the Patient Data Viewer.
- **PushNotification** // POST of gateway info via tablet, POST of notifications, GET unsent notifications.
- **Questionnaire** // CRU for questionnaires.

The DataResourceBrowser and PatientDataOrchestrator are special purpose controllers for the corresponding components in the Clinician Manager user interface.

4.2.2 Dependencies

The ODS instances and the ODS Message Handler are deployed with the Private Care Cloud of PICASO.

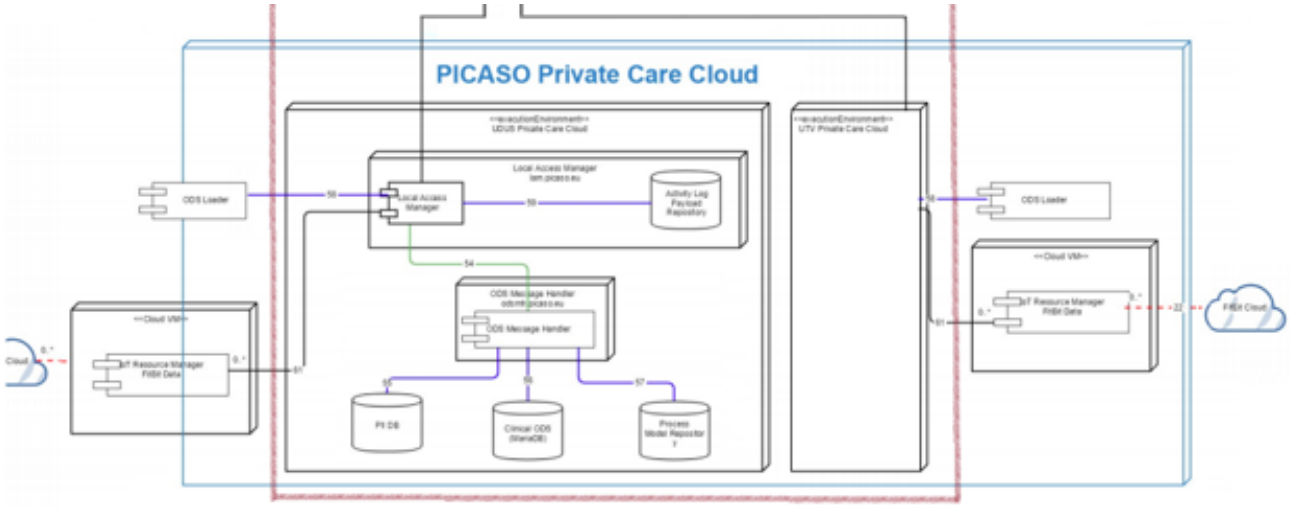


Figure 2: ODS Message Handler dependencies

4.3 ODS Message Broker

4.3.1 Description

The ODS Message Broker implements message validation, transformation and routing in the data management subset of the PICASO architecture. The message broker can receive messages from multiple destinations, determine the correct destination and route the message to the correct channel. The message broker also provides the means to manage scalability in a consistent manner. Thus, the general communication mechanism for PICASO is data-centric and messaging-based.

[2] Create Read Update Delete

The message broker component is implemented using the open source software RabbitMQ[3]. This is a widely used open source message broker with an extensible architecture. It implements the AMQP 0-9-1 protocol[4] and can through extension mechanisms, plugins, support the most common messaging protocols, e.g. MQTT, STOMP and XMPP. Extensions and adapters can be written to support other messaging patterns, protocols and security management solutions.

RabbitMQ implements AMQP 0-9-1 and the AMQP concepts of brokers, messages, producers, exchanges, queues and consumers. A publisher – an application that produces messages - sends a message to an exchange, where it is routed to one or more queues. The message is then pushed to (or pulled by) a consumer – an application that processes messages - for processing. Exchanges and brokers may reside on different brokers. The topology of the message routing is controlled by the publisher and consumer, which allows for a very flexible communication design. Exchanges and brokers are access-controlled via PICASO Public and Local Access Mangers (PAM/LAM), which allows for fine-grain security control over the communication.

The general-purpose applicability, plugin architecture and extension mechanisms will allow for built-in multiprotocol support.

In the overall solution the message broker does not perform any translations or transformation of the data and thus provides more of a message passing, queuing type functionality. In addition, it also maintains an Activity Log repository.

The extensions provided to RabbitMQ is an encapsulation layer for both inbound and outbound calls. Other PICASO components can call the Message Broker using standard REST calls and do not have to manage the RabbitMQ queues. In the same way the broker forwards message to recipients using standard REST calls. The Broker interface a Hospital Interoperability Layer for mapping incoming requests to the different hospital specific APIs that exists.

4.3.2 Dependencies

The ODS Message Broker is deployed in the PICASO Public Cloud. It relays all request/response messages for ODS instances deployed in Private Care Clouds on the PICASO platform. This is done via the Hospital Interoperability Layer, which provides adapter components for each Private Care Cloud.

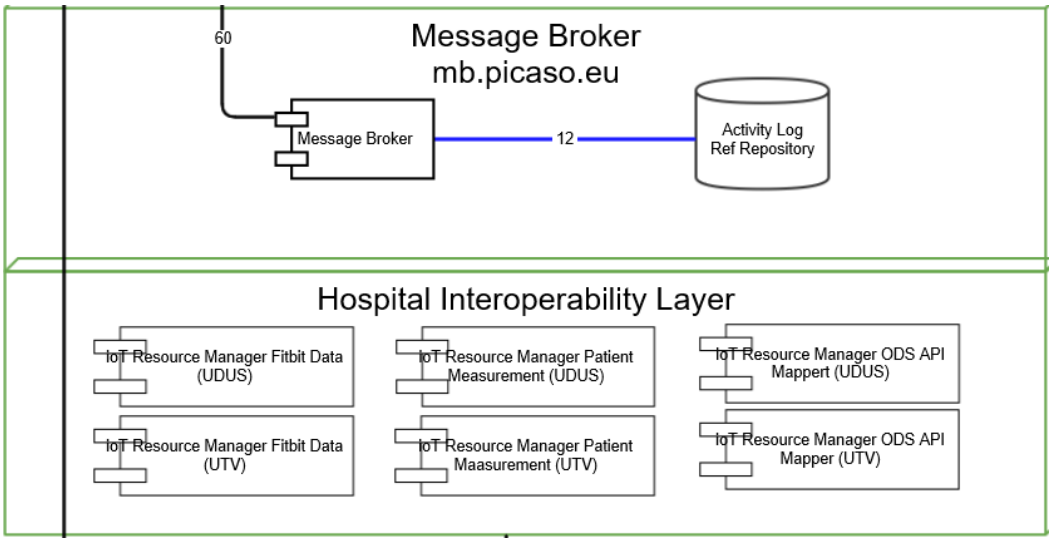


Figure 3: Message Broker dependencies

The Message Broker also maintains an Activity Log repository

[3] https://www.rabbitmq.com/
[4] http://www.amqp.org/sites/amqp.org/files/amqp0-9-1.zip

4.4 ODS Schema

Main pieces of ODS data schemas depicted in the following figures gives overview how data are stored in PICASO ODS. This storage is first step of PICASO data management process.

4.4.1 PII DB

The PII database holds separate tables storing PII for patients, clinicians and informal carers. The PII data storage is physically separated from the corresponding clinical data.

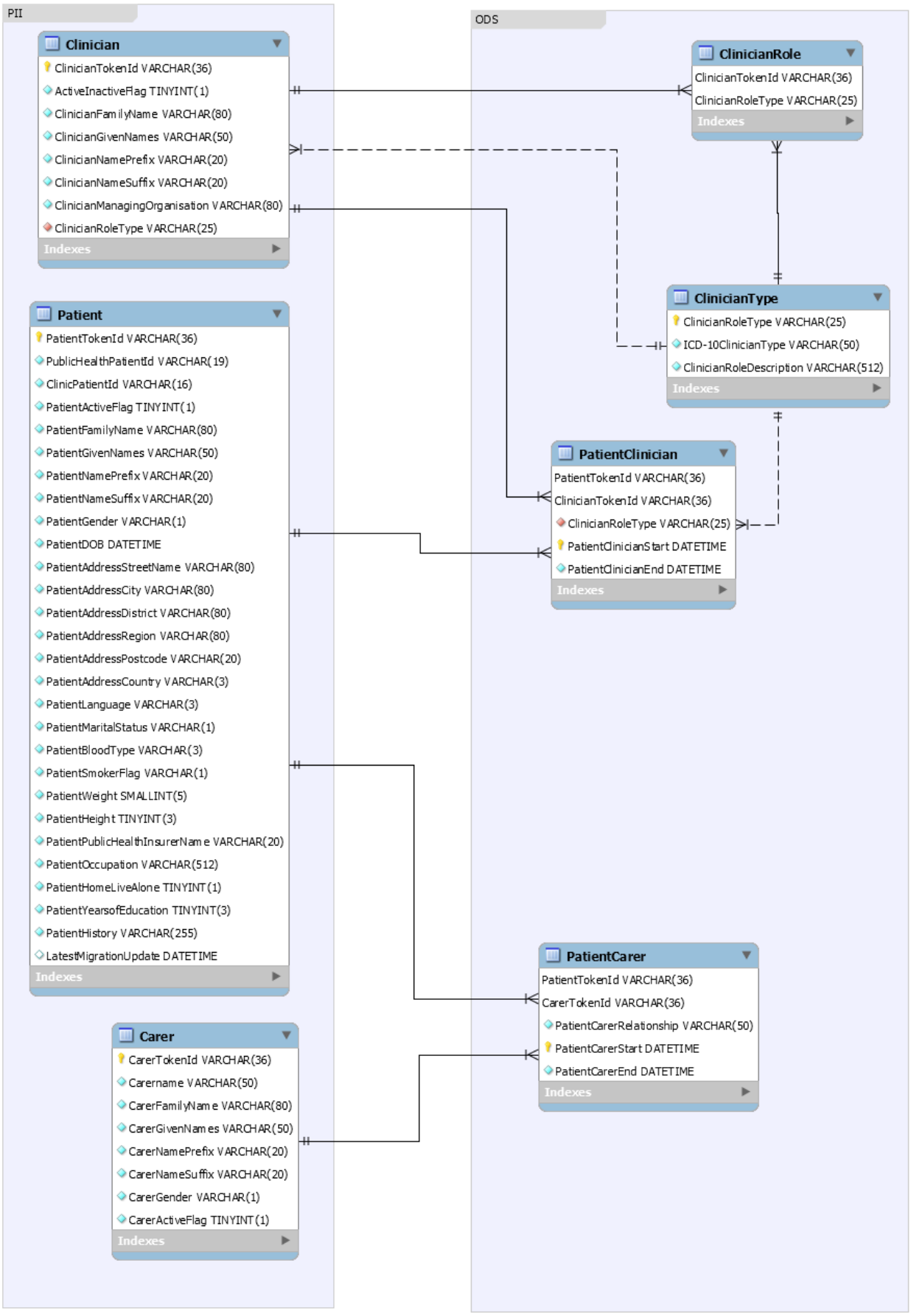


Figure 4: The PII database schema for storing data about patients, clinicians and informal carers

4.4.2 Care plan

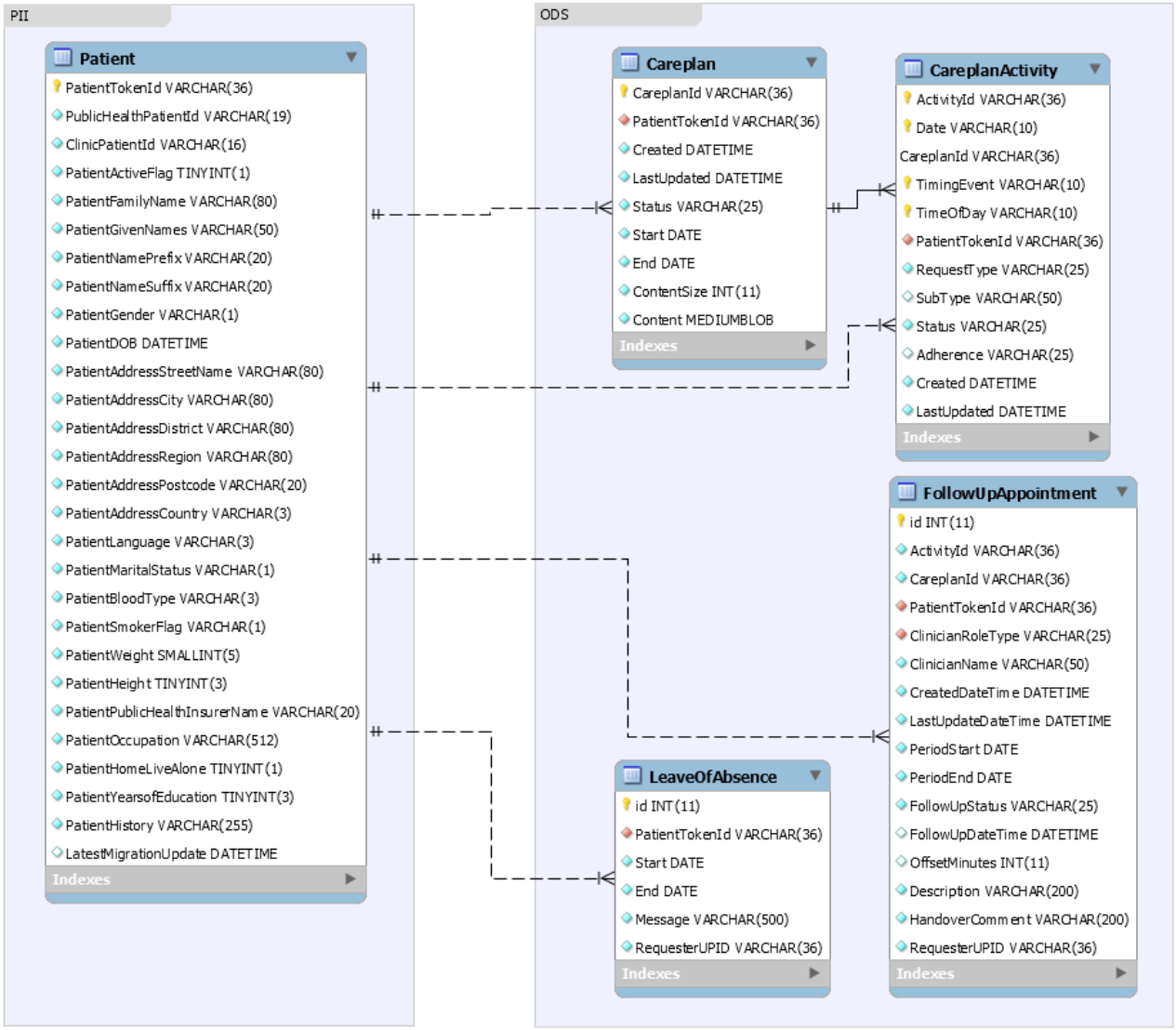


Figure 5: Database schema designed for storing data about Care Plans

Careplan and CareplanActivity relations hold the meta data for the FHIR care plans. The FHIR care plan JSON instances are stored as content BLOBs.

The FollowUpApointment is a result of a care plan activity and links a patient and a clinician.

The HL7 FHIR CarePlan resource definition can be found at: https://www.hl7.org/fhir/careplan.html

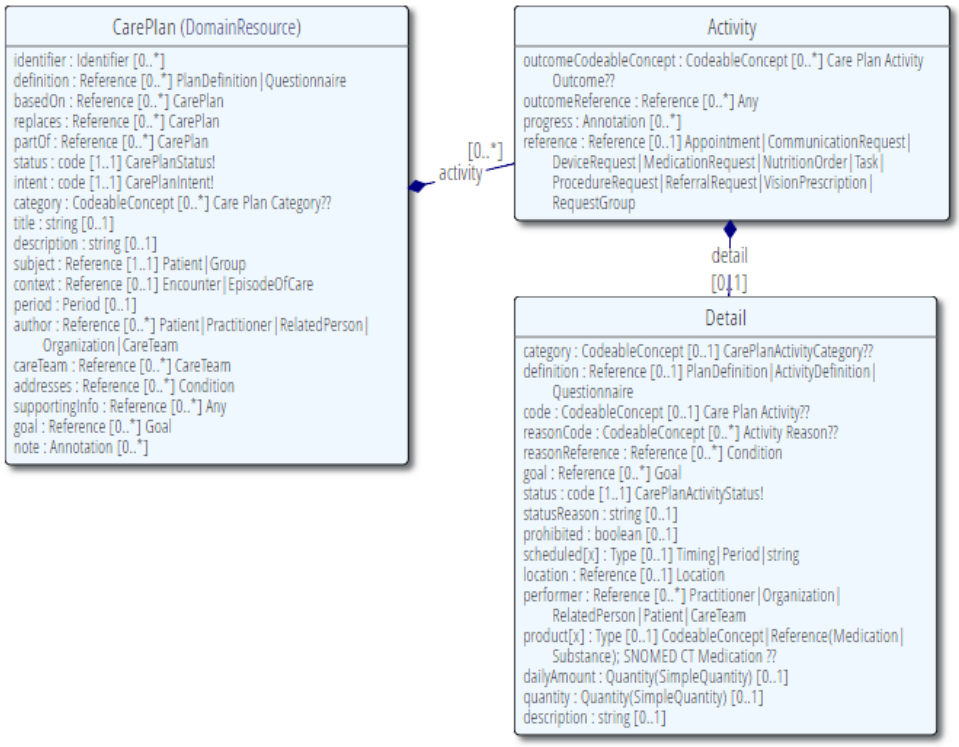


Figure 6: FHIR CarePlan resource

4.4.3 PICASO Observations

Figure 7 depict data schema for PICASO Observations. The observations come from devices installed at home.

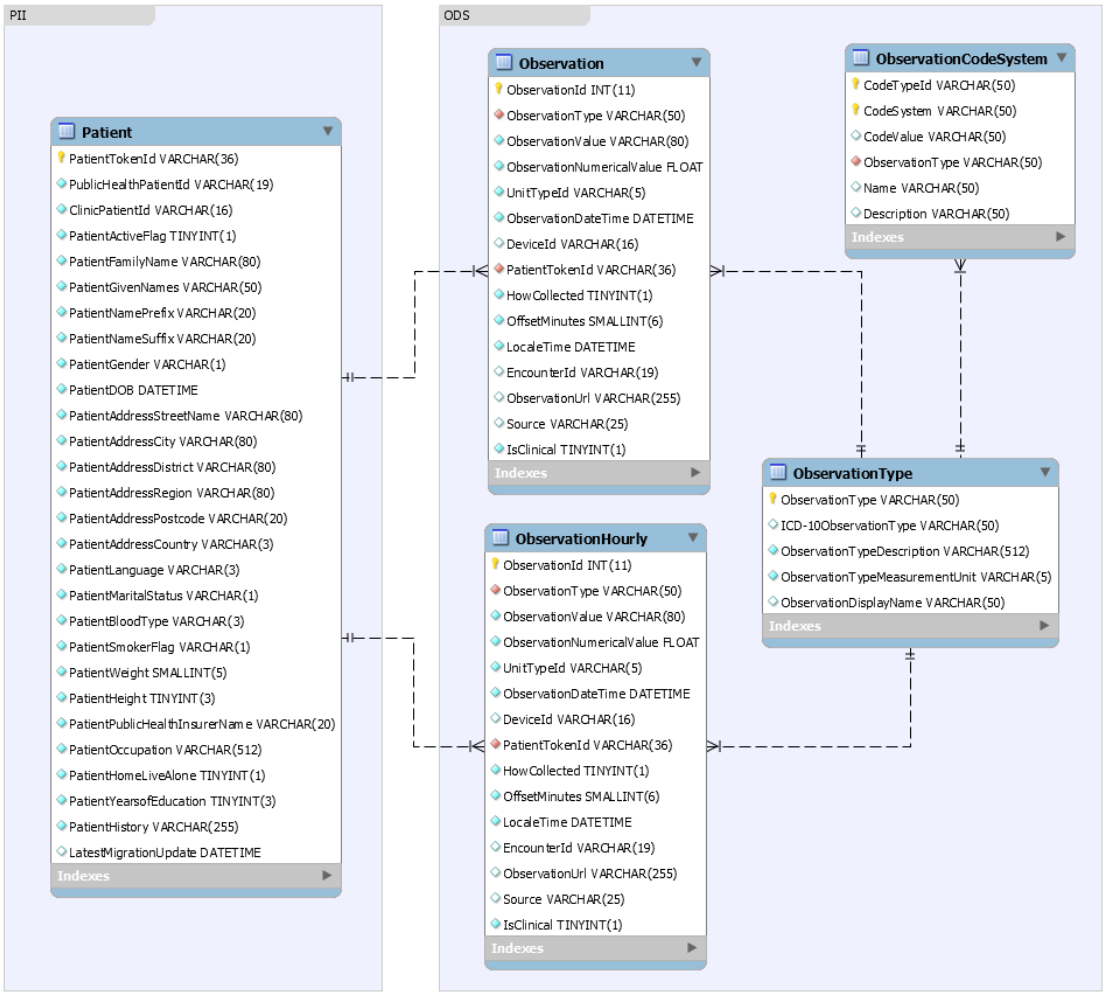


Figure 7: Database schema used for storing Observations

4.4.4 Encounters

Figure 8 depict data schema for PICASO Encounters.

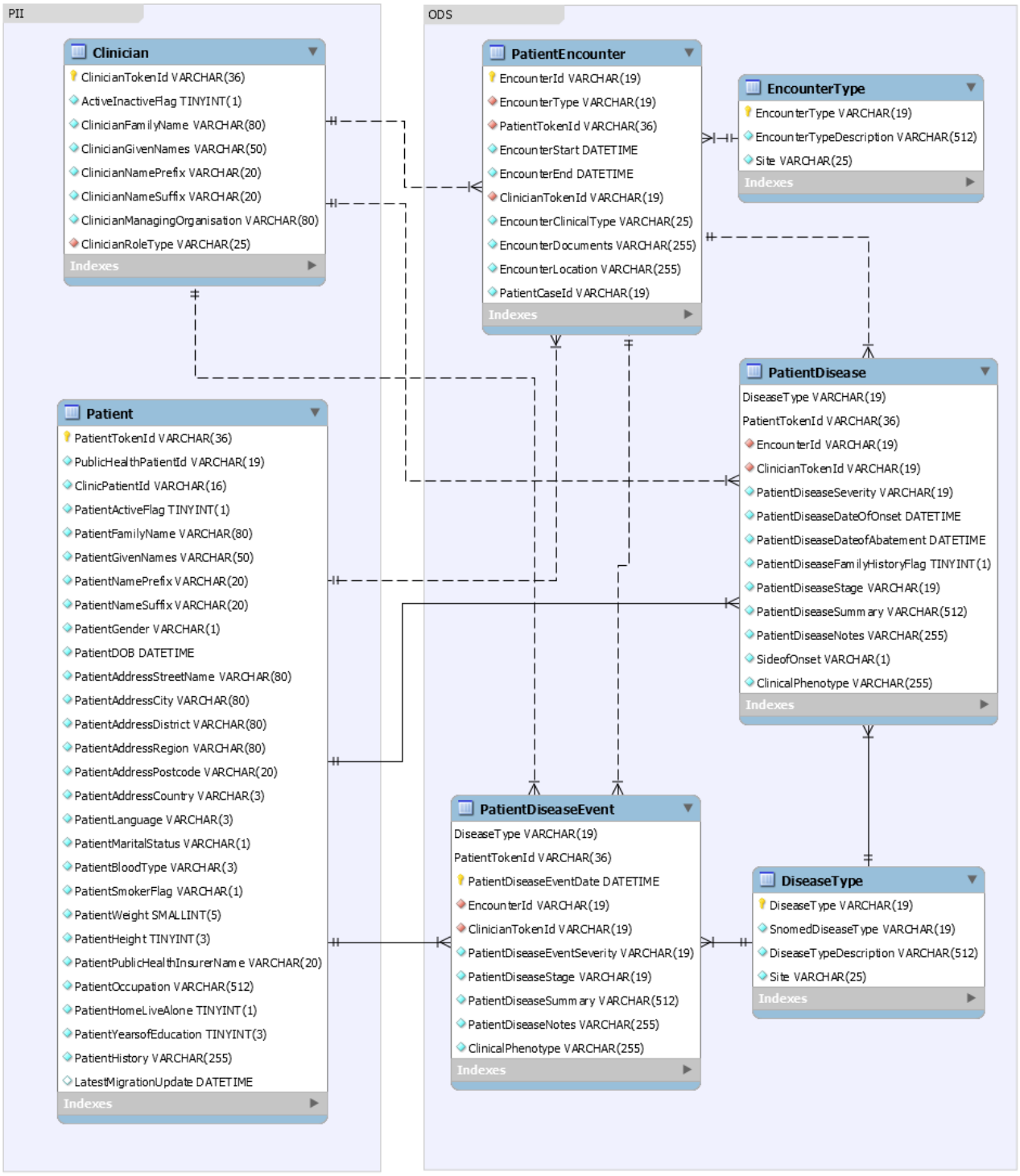


Figure 8: Database schema used for storing Encounters

4.4.5 Questionnaires

Data schema is depicted on Figure 9 defines data tables for storing questionnaires meaning filled values based on these questionnaires.

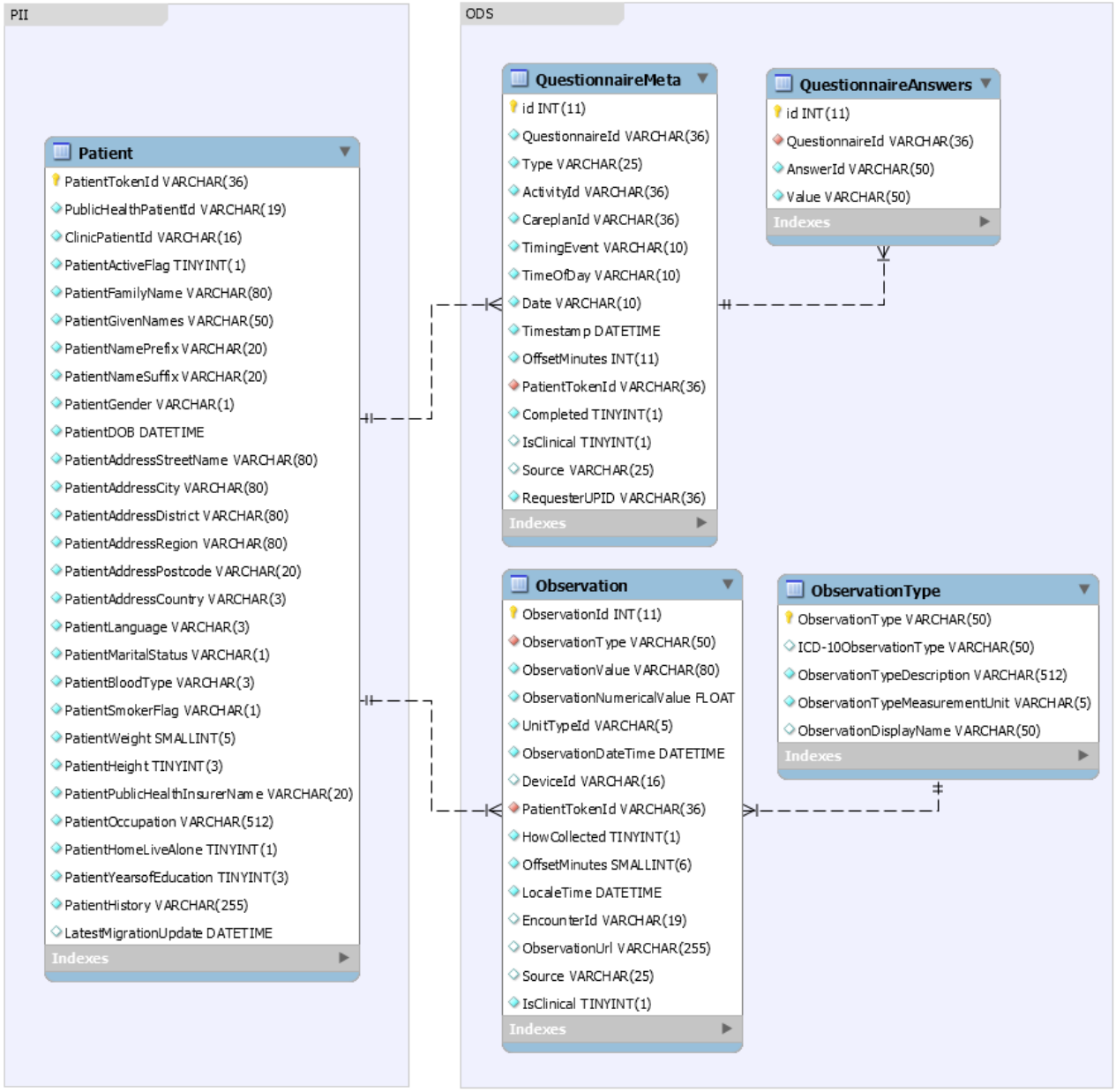


Figure 9: Database schema used for storing Questionnaires

4.4.6 Push notifications

Schema defining DB table for storing push notification is on Figure 10 below.

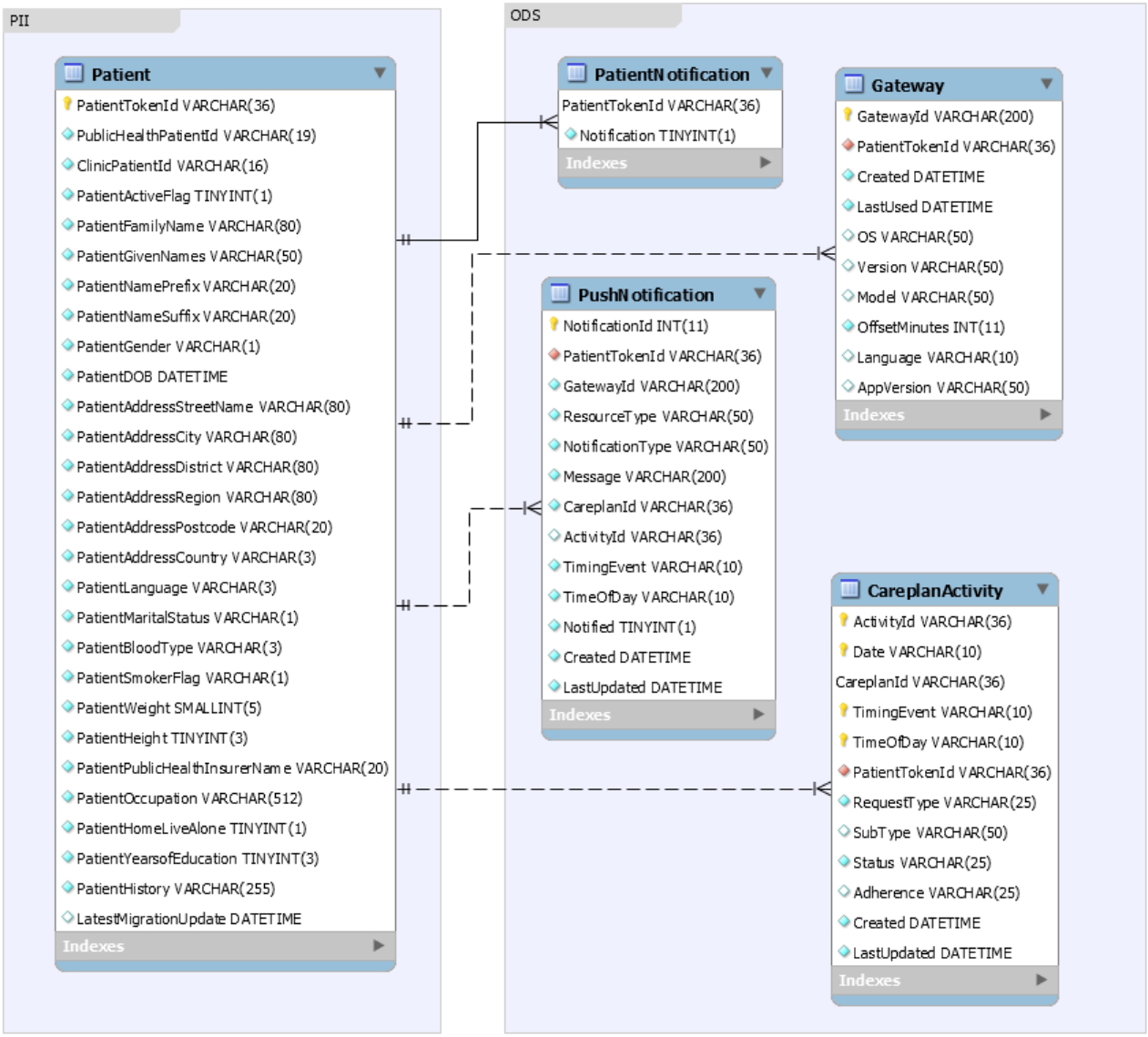


Figure 10: Database schema used for storing Push notifications

5 Security and Privacy Management

5.1 Security and Privacy Management - General Idea

The Security and Privacy Management subset is designed to provide: a comprehensive security by encrypting and filtering all external communications to PICASO services, protecting all communications between PICASO Public and Private Clouds as well as fine-grained privacy controls by enabling users to control the access to their personal, clinical and home monitoring data. The subset consists of four components:

- Public Access Manager (PAM) – component in the PICASO Public Cloud acting as a gateway between all communication between public cloud and external components
- Local Access Manager (LAM) – component in each of the remote PICASO Private Care Clouds providing gateway functionality between PICASO Public Cloud and internal local cloud components
- Identity Manager (IM) – component which stores user credentials and associated Unique PICASO Identifiers (UPIDs). Data is stored in a specialized data structure designed for constant time pattern marching regardless of number of datapoints. This structure allows to utilize IM in constant time regardless of number of users and will enable to scale in number of users with ease
- Policy Manager (PM) – component containing specialized data structure which enables to store complex data structures in a compressed manner

A thorough description of the component with dependency, activity, use case and sequence diagrams can be found in PICASO deliverable D7.4 First Private and Public Cloud Integration in sections 4.3 – 4.5. These components enable to create user accounts and manage data access as well as provide secure access channels to retrieve data.

5.2 Approach

The procedures of data access, privacy and identity management are designed to empower users by providing explicit and fine-grained control.

5.2.1 Provision of Unique PICASO Identifiers

All authentication and access control in PICASO is based on a Unique PICASO ID (UPID) that is assigned to each user. The UPID is a string of characters that – by itself - does not reveal any user related information. For each user, all data referring to that user are associated with the UPID of the user across all private PICASO clouds. The UPIDs are generated and made available by the Identity Manager in the Public PICASO Cloud and are assigned to specific users by the hospitals when user accounts are provisioned. Creating a patient account requires signing a written informed consent, a PICASO account is only created after the written informed consent has been obtained. The following minimum information is required by the Identity Manager:

1) For patients
   a) Credential data (username/hash (password + entropy))
   b) Email (for PW recovery/reset) to be obtained from PII database when required
   c) Valid client certificate for patient tablet
   d) Status: Active/Inactive
2) For Informal Carers
   a) UPID of patient who requested access for the Informal Carer
   b) Credential data (username/hash (password + entropy))
   c) Email (for PW recovery/reset) to be obtained from PII database when required
   d) Status: Active/Inactive
3) Formal Carers
   a) Role IDs (Specializations)
   b) Credential data (username/hash (password + entropy))
   c) Email (for PW recovery/reset) to be obtained from PII database when required
   d) Status: Active/Inactive

5.2.2 Management of User Status (active/inactive)

After patient signs the informed written consent, her/his status in PICASO is “active”. If patient decides to leave the trial, her/his status becomes “inactive” and access to her/his patient data will be revoked for all users

(patient itself, Informal Carers, Formal Carers). No further home-monitoring data for patient will be uploaded to the PICASO platform.

5.2.3 User Types and User Access to Data

Access rights to the PICASO platform are restricted according to the type and role of a user. The following types and roles are provisioned in trial 1:

- Patient
- Informal Carer
- Formal Carer:
    - Cardiologist
    - Rheumatologist
    - Psychiatrist
    - General Practitioner
    - Occupational Physician
    - Radiologist
    - Clinical Neurologist

The clinical roles have been obtained from the deliverable D8.1.

User Type: Patient

The access of patients is restricted to the Patient Dashboard and those data types that are displayed via the patient dashboard in particular home monitoring, medication plan and appointment plan. Clinical data, lab test results etc. are not be provided to patients via the patient dashboard.

Patient Access to Data

Patients can access all data provided in Patient Dashboard.

User Type: Informal Carer

The access of Informal Carer is limited to the data types provided to patients via the patient dashboard and further restricted by the patient choices detailing to which data types the Informal Carer should receive access (see above Informal Carer access).

Informal Carer access to patient data

Patients may grant Informal Carers access to one or more of the following sections of the patient's dashboard: treatment plan, appointment plan, home monitoring data.

To sign-up Informal Carers, patients must:

1) fill out and sign an enrolment form at the hospitals providing the name (first name, last name) of the Informal Carer as well as an email address of the Informal Carer
2) indicate which of the three datatypes they wish to share with the Informal Carer.
3) Provide the completed enrolment form to the hospital.
4) The Informal Carer must sign a document stating that he accepts the invitation and that he/she agrees that her/his personal data required to provide the service are stored/processed in the PICASO platform.
5) A PICASO account for the Informal Carer is only created after steps 1-5 have been completed

Informal Carers receive browser based access to the sections of the patient's dashboard to which access has been granted by the patient. Access is controlled via username/password and is possible from any internet connected device.

A classification of what data the three categories "treatment plan, appointment plan, and home monitoring data" shall comprise need to be defined by the clinical partners.

User Type: Formal Carer

Formal Carer can only access Clinician Dashboard, furthermore, access to patient data is restricted by the electronic consent provided by the patient. However, even with patient consent access to patient data by Formal Carers are further restricted by a Formal Carer's clinical role. The policy manager contains the policies regarding role based access by Formal Carers, i.e. what clinical roles have access to what data types.

By default, all data types are enabled for each role. The participating trial hospitals (UDUS and UTV) can at any time provide for each Formal Carer role a listing of which data types (if any) should NOT be accessible to a specific role.

Formal Carer access to patient data

The Formal Carer access to patient data granted via the signed consent letter depends on local policy:

1) It either grants access to all a patient's data for all Formal Carers participating in the trial (across participating institutions). Patients have the option to deactivate a Formal Carer's access to their patient

data via the patient dashboard. For this purpose, the patient can access a list of all participating Formal Carers in the trial and disable/re-enable Formal Carers individually.
   a) This access is further restricted by access limitations per the Formal Carers role.
   b) This access is *not* further restricted by access limitations per the Formal Carers role.
2) It grants no access for any patient data to all Formal Carers of the institutions who participate in the trial except if the patient grants explicit access to an individual carer via the patient dashboard. The patient has the option to revoke access for each carer the patient previously granted access via the patient dashboard.
   a) This access is further restricted by access limitations per the Formal Carers role.
   b) This access is *not* further restricted by access limitations per the Formal Carers role.
3) It grants access to Formal Carers to patient data based on the carer's role.

If access has been granted to a Formal Carer, the Formal Carer can access the clinician dashboard via a browser from any internet connected device.

Role based access for Formal Carers

For options 1a, 2a and 3, Formal Carer roles (like cardiologist, physical therapist, nuclear medicine physician) are defined by the hospital. The definition of each role consists of the accessible/non-accessible data categories. Such accessibility definition is done by the clinical partners. The categories in this definition are subset of the categorisation mentioned in case of Data Resource Browser.

5.2.4 Basic Principles of Access Control

All queries for data are sent by the requesting services to Patient Data Orchestrator. The Patient Data Orchestrator then consults the Policy Manager which screens the data queries and determines which queries or parts thereof can be allowed based on the access control rules. The Patient Data Orchestrator then responds only to those queries that were allowed.

For example, if a cardiologist tries to access data of the patient *x* via Clinician Dashboard using Data Resource Browser service a query for all relevant data types regarding that patient *x* is sent to the Patient Data Orchestrator. The Patient Data Orchestrator then queries the Metadata registry for the available data types. This query is screened by the Policy Manager which determines whether the Formal Carer access to data regarding patient *x* is enabled and – if that is the case - what data types are accessible to the cardiologist in consideration of his clinical role. The Patient Data Orchestrator will then only return information regarding the "allowed" data types. If some data types have been omitted, information stating that not all available data types could be provided due to access restrictions is part of response from Patient Data Orchestrator.

The granularity of data access is given by the granularity at which data types are categorized, the granularity of roles, and the granularity by which access restrictions are mapped from data types to roles. This information provided by the participating hospitals.

5.2.5 Personal Identifiable Information Storage

User data are processed in a non-identifying way wherever possible. The main component of such secure data processing is by linking data to a UPID for the user. Personal Identifiable Information (PII) (i.e.: first name, last name, address, contact information) are stored in a separate database in the Private PICASO Cloud, where the corresponding user account is administered. Only in that database the user's UPID is linked to its PII – thus such link is managed on private cloud only. All transactions that display PII must pull this information to the PICASO application layer for each request. One example of such application where PII are displayed to Formal Carers in Clinician Dashboard. Formal Carers can select patient and request acces for the information about the patient specified.

5.2.6 Sequence Diagrams

Sequence diagrams involving PICASO security and privacy components are presented in the following. Sequence diagrams depict data flow between components during the typical requests. Such flows are triggered when end PICASO components are serving end users (initiated by the user). Also, such sequences are triggered by the PICASO components, as (by above described) all communication among the cloud is being controlled.

For instance, in case the end component needs to present the data to the user (clinician or patient) the flow is triggered by the data request. In case of Care Plan Manager component, flow is triggered when data defining care plans are stored. Other examples are inter Cloud calls triggered by the components. Such Inter Cloud Communication is modelled on the sequence diagram on Figure 11.

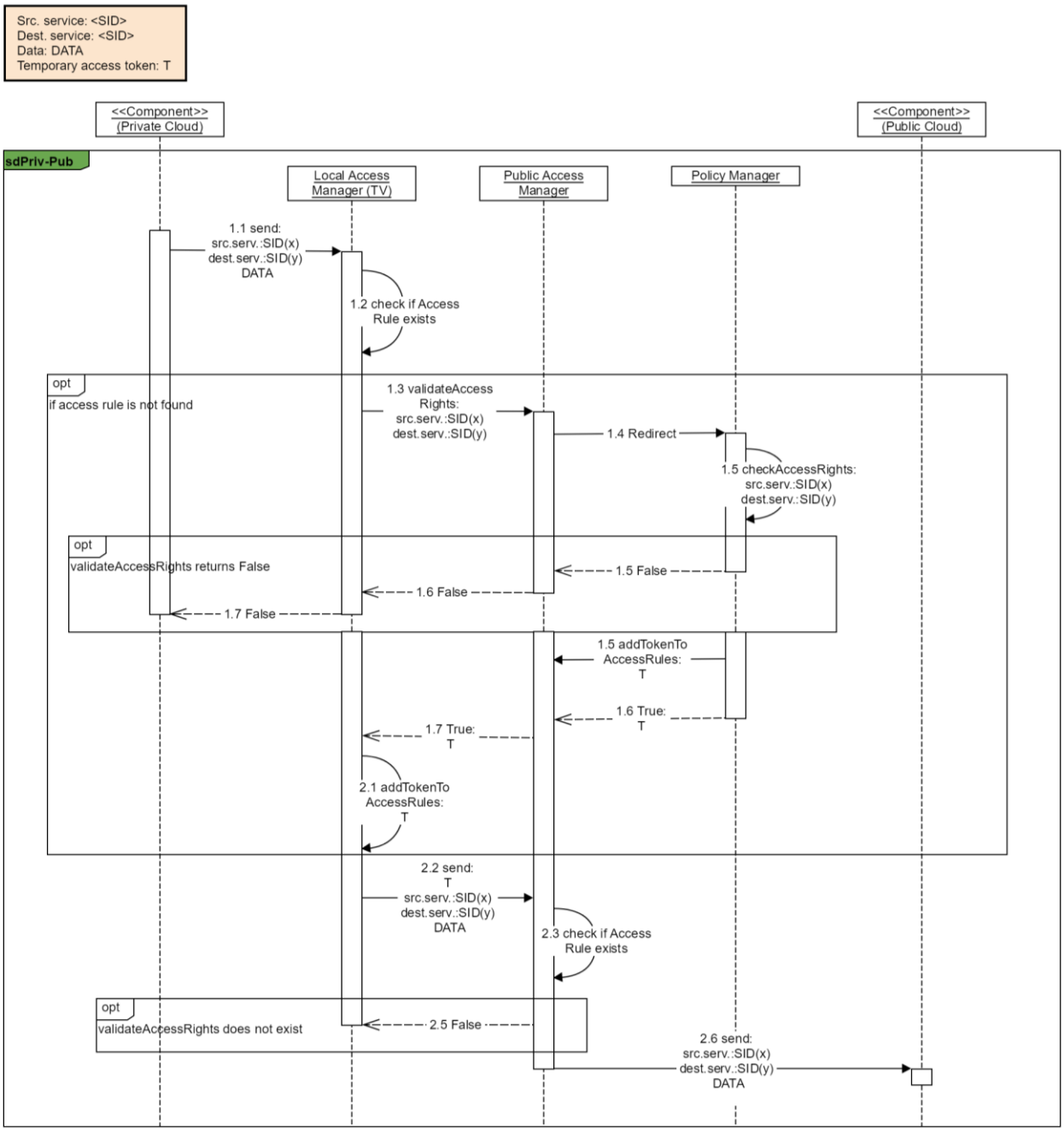


Figure 11: Sequence diagram of component calls between PICASO Cloud

The sequence demonstrates that there are many layers (represented by components) controlling the data access management triggered by when inter cloud communication occurs.

The Data Request Sequence is modelled on the diagram on Figure 12.

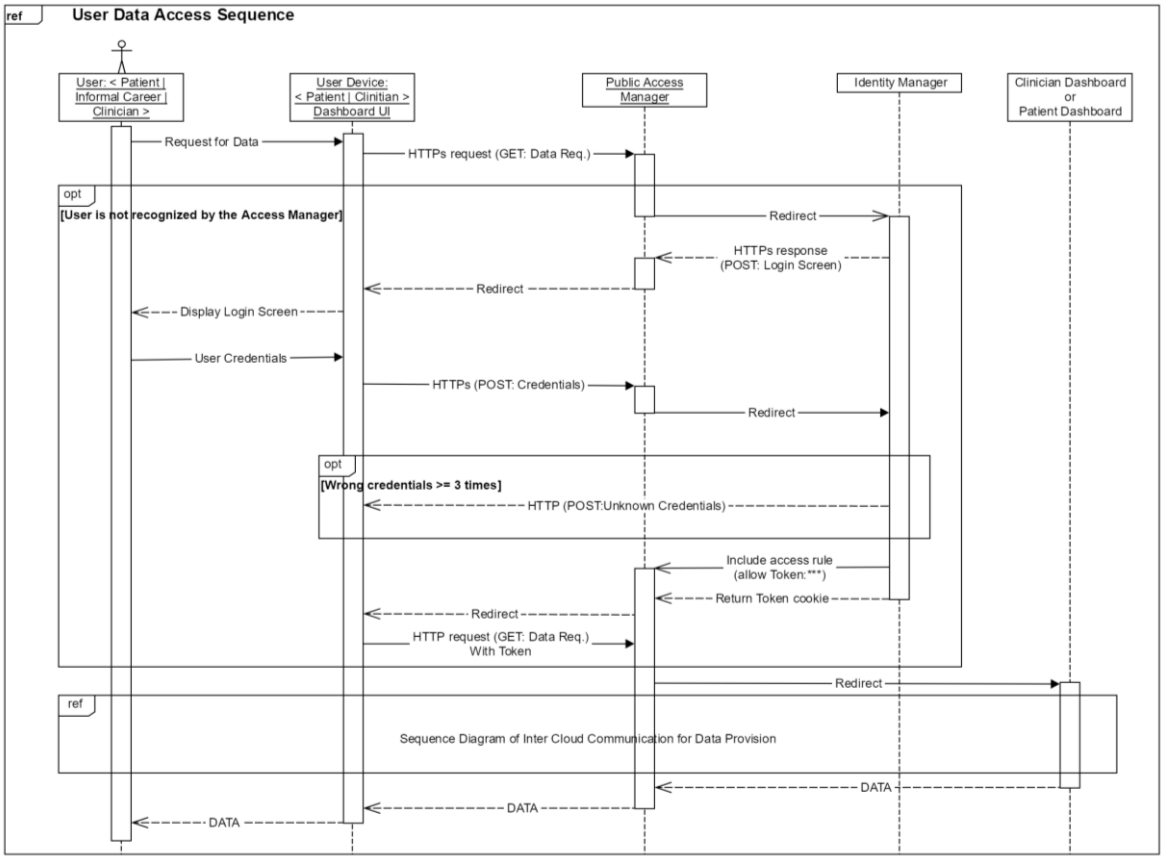


Figure 12: Data Request Sequence

As can be seen the data requests trigger flow that has to pass many layers of security management including verification of identity.

6 Shared Memory Manager

Shared Memory Manager runs on PICASO Public Cloud. It stores the metadata of messages passing from all ODSes. Metadata represent the only data required to retrieve the real content of information. Patient Data Orchestrator reads Metadata to retrieve all data available about patient and put the retrieved data into response to the Clinician Dashboard.

6.1 Patient Data Orchestrator

6.1.1 Description

The Patient Data Orchestrator (PDO) component serves as the data access layer for the PICASO application, interacting closely with Metadata Registry components and all other components, which require to consume data (Clinician Dashboard that wraps, Data Resource Browser, Patient Data Viewer, Care Plan Manager and Risk Manager).

PDO receives data requests from data consuming components, interrogates the Metadata Registry to determine whether the data exist and obtain the location of the actual data in the Clinical ODS Systems. Filtering of data according to policy rules is also part of the PDO functionality.

Metadata Registry provides the PDO with all relevant metadata including their locations in Clinical ODS systems. PDO then uses the retrieved metadata records to acquire the real data from relevant Clinical ODS Systems. The result from several Clinical ODS Systems are joined and returned to the requesting component; be it the Clinician Dashboard, Data Resource Browser, Care Plan Manager and Risk Manager component.

6.1.2 Dependencies

PDO is central component of data management, as it enables accessing integrated care data from Clinical ODS systems to the (GUI) components of Clinician Dashboard and has to filter the data according to the authorisation rules of Policy Management. The dependencies of PDO with components for data management are following:

- Metadata Registry - enables PDO to identify relevant ODSes for each query from Clinician Dashboard and thus to filter the querying of particular ODSes (omit irrelevant ODSes)
- Clinician Dashboard - each component embedded in Clinician Dashboard (such as Data Resource Browser) uses interface of PDO to query for data from ODSes, thus PDO provides appropriate interfaces for these components
- Clinician ODS - the source of integrated clinician data that are queried by PDO based on the data requests from components of Clinician Dashboard.
- Policy Manager - PDO consults authorisation rules from Policy Manager to filter data responses from ODSes. The orchestrated data response -orchestrated from particular responses from ODSes- satisfy the authorisation of logged in clinician.

6.2 Metadata Registry

6.2.1 Description

The purpose of the Metadata Registry (MDR) is to hold a reference to requester, requestee, data type and location information that is necessary to allow the Patient Data Orchestration component to retrieve the specific data requested by the PICASO application.

The metadata include:

- A unique identifier for each metadata registry entry – so that the PICASO application can collate whole “reports” which consist of multiple data items.
- Identifiers of requester (UPID of clinician), requestee (UPID of patient) and related data source (Clinical ODS) to be able to fetch the real data and also to filter metadata according to the policy rules by consulting the Policy Manager.
- Identifiers or real data in related Clinical ODS system.

- Type of data registered in the Metadata.
- Each time the new record in any of existing Clinical ODS systems is affected (created, updated and deleted), the metadata record is published and stored in Metadata Registry.

Each data consumption request to Patient Data Orchestrator is consulted with Metadata Registry to obtain all metadata records related to request. Metadata are filtered according to policy rules managed by Policy Manager.

6.2.2 Dependencies

MDR serves to Patient Data Orchestrator component and it is updated based on the updates of ODS Systems:

- PDO - MDR provides API for PDO that enable to identify relevant ODS Systems for particular request from Clinician Dashboard (request contains patient UPID which is basis for such identification)
- Clinician ODS System - the update of data related to particular patient UPID in each ODS system cause update of Metadata Registry for this UP.

7 Data Resource Browser

7.1 Description

The Resource Data Browser is a web-based, interactive interface where authentified clinicians can search for combination of all the information stored in the shared memory such us patients, other carers, data and care plans. The user retrieves data by querying the Data Orchestration (the call of DRB API is delegated to Clinician Dashboard, as it integrates the authentication service for clinician (data requester). The Data Orchestrator orchestrate data and it transforms them into predefined format suitable for DRB component. The query provides a visual image of which data are found and that the user can retrieve. The relationship between the data type available and the data owner is presented in the form of a mind map (i.e. a tree graph). DRB uses the same data types as Metadata Registry and Policy Manager and they are often referred as data categories in DRB context. The DRB graph is interactive and iterative meaning that it is dynamically updated when the user clicks on the different nodes up until the node is a leaf node. If, for example, a general practitioner searches for data related to her patient, the graph will show the actual patient as the centre node together with all relevant data categories including the carers in form of surrounding nodes. This also means that these carers has agreed to share this information with the doctor. By clicking on one of the carers, a new carer centric graph forms showing which data the carer has received from the patient (again provided that the doctor has been authorised to see this information). Finally, the doctor can click on a certain leaf node (leaf data category) and see all the measurements performed (including contextual data and again, provided the proper authorisation is established). The doctor can click around the different branches and see other carers' interventions, the care plans executed, and dig further into the relevant data according to her access rights. The Data Resource Browser is a read-only tool. It does not write any data within PICASO. However, logging of access to data (that are accessed by DRB) is done by the Activity Log. Note, such logging is triggered DRB but not directly performed by this component (it is performed within the sequence that provides data response to the DRB data request - see Patient Data Orchestrator and Activity Log components for details).

The DRB can be seen as GUI that directly visualise data types defined for management of care data and home measurements about patients according to authorisation of care professional (data requester).

7.2 Dependencies

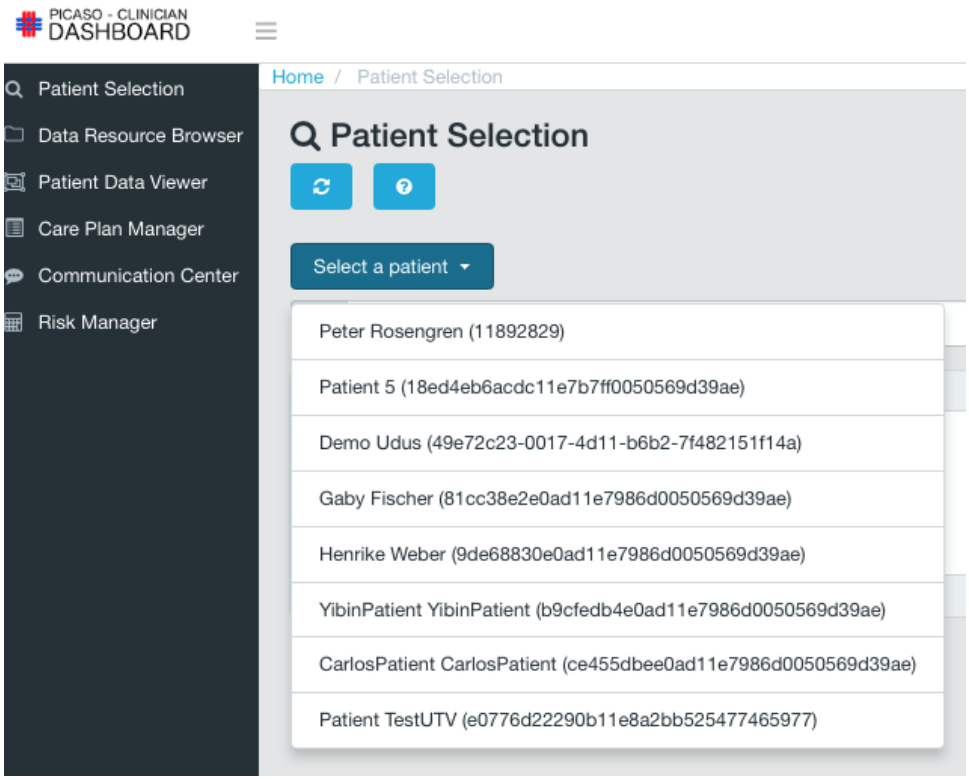
There are two dependencies of DRB with PICASO components from the data management perspective:

- Clinician Dashboard - it enables to obtain UPID of clinician who is logged in the Clinician Dashboard and UPID of patient that has been chosen by the logged clinician
- Patient Data Orchestrator - it enables DRB to access the integrated care data per selected Patient that are orchestrated from relevant PICASO ODSes. The data are also filtered based on the authorisation of clinician (stored in Policy Manager) on the requested patient's healthcare data. The orchestrator provides API dedicated for DRB that enables such access to the integrated healthcare data

8 Integrated Data Management in action

The following screenshots provide demonstration how are healthcare data (managed over PICASO Data Management Subset) visualised in the Clinician Dashboard and Data Resource Browser. Also, samples of these data, their source and meaning are explained in the comments addressing important features of the above described Data Management Components.

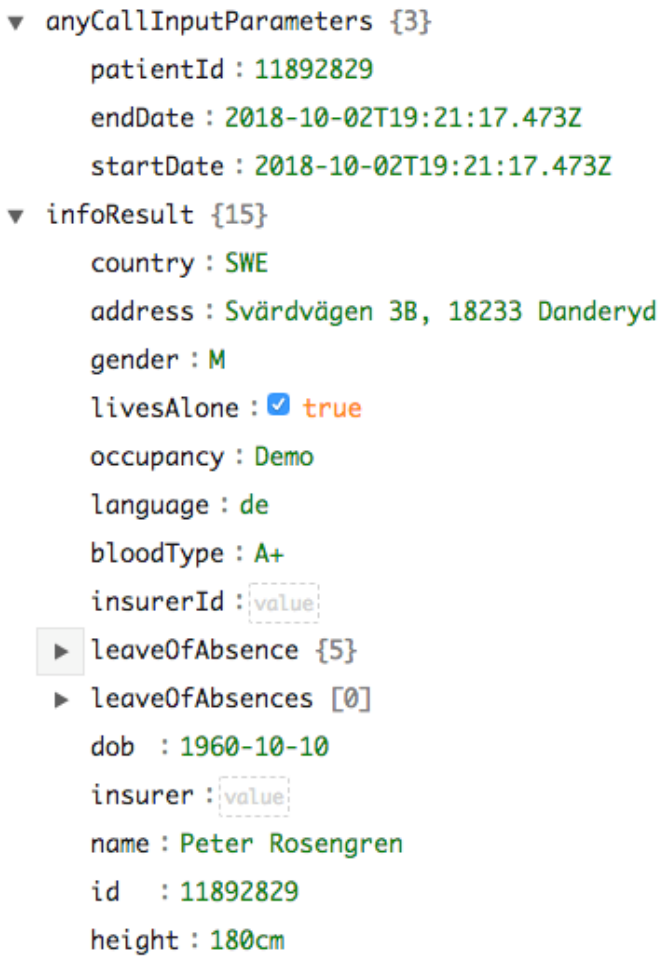
8.1 Selection of patient by Clinician



Comment: There are specific data services that gives list of Patient's UPID enabled for clinician UPID (I.e. logged in clinician). Then another service consults each patient's UPID against PII data in the Private cloud ODS (the only place where mapping between UPID and Patient's name can be obtained). Both of the service calls triggers sequence that includes privacy and security management (see also Figure 11 and Figure 14).

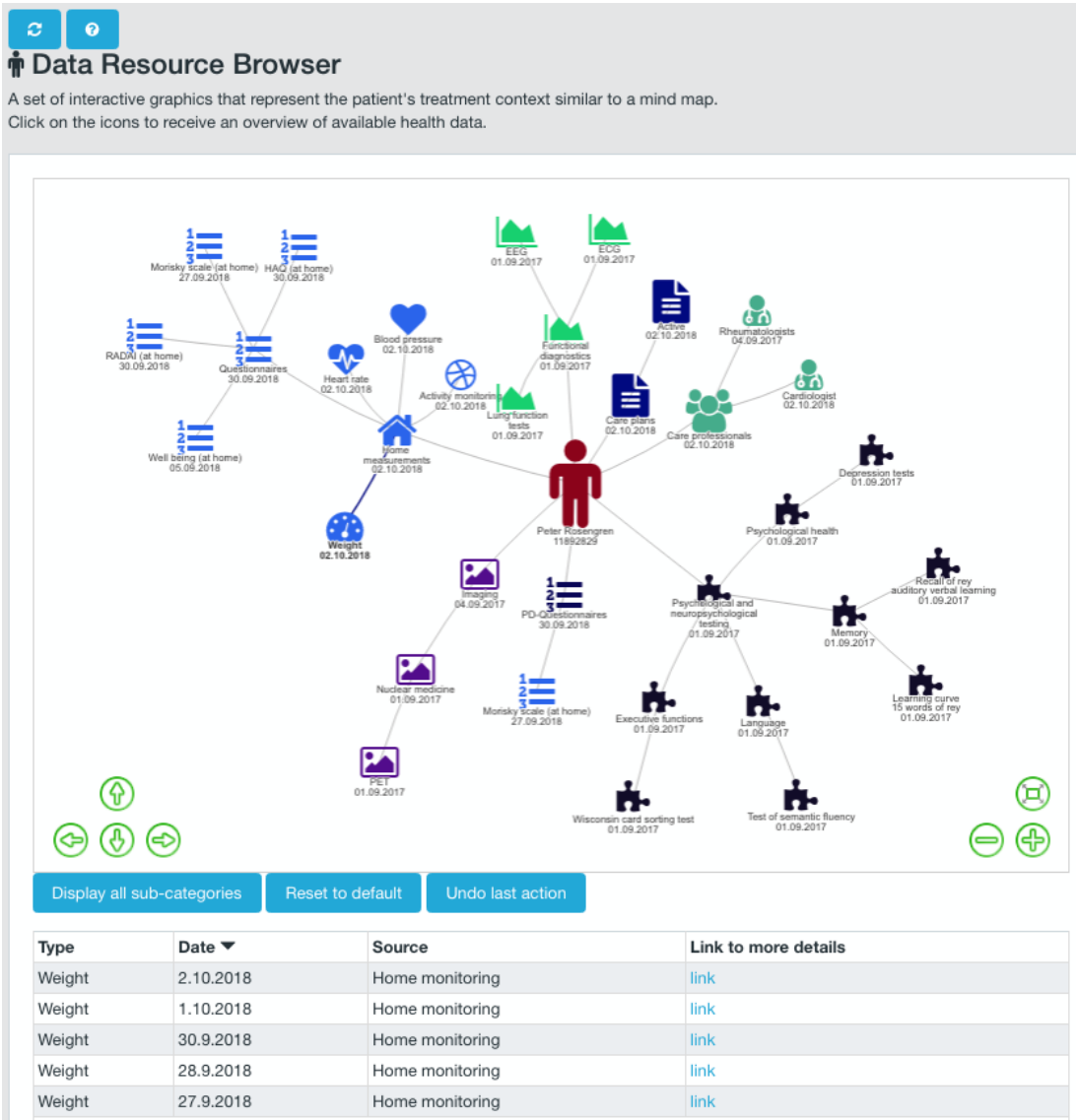
8.2 Personal data about patient

Comment: these personal data are displayed after the patient has been selected by logged in clinician. They are based on the response from Patient Data Orchestrator that by requests these personal data from relevant ODS. Such call on ODS is typical Public to Private cloud call. Thus, it triggers multilayer sequence that manages privacy and security aspects (see also Figure 11 and Figure 12).



Comment: The data response from Patient Data Orchestrator providing the displayed personal data.

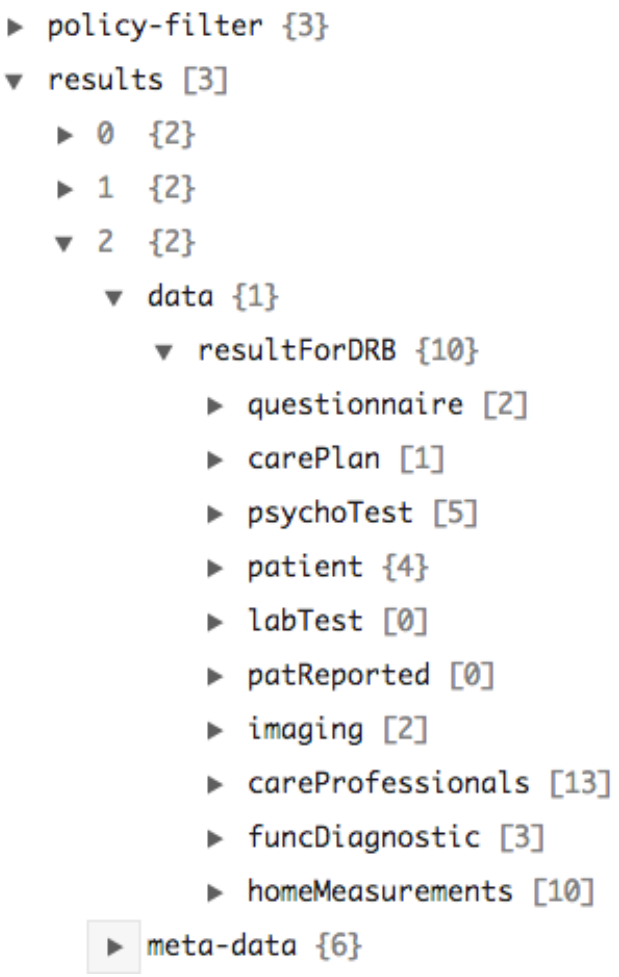
8.3 Data Resource Browser



Type	Date ▼	Source	Link to more details
Weight	2.10.2018	Home monitoring	link
Weight	1.10.2018	Home monitoring	link
Weight	30.9.2018	Home monitoring	link
Weight	28.9.2018	Home monitoring	link
Weight	27.9.2018	Home monitoring	link

Comment: All nodes displayed on the mind map corresponds to the data categories available for the patient. The selected leaf most specific category (weight) gives overview of entries available. Each entry has its source specified (here Home monitoring but in PICASO trials it can be UDUS RH or UTV). The data categories available are provided by the orchestrated responses from ODSes. The orchestration is done by Patient Data orchestrator. Note, there are more details about the data entries presented here. These details can be seen in the clinician tool called Patient Data Viewer (see deliverable D6.5 Second Decision Support and Interaction Tools).

8.4 Composed ODS responses for Data Resource Browser



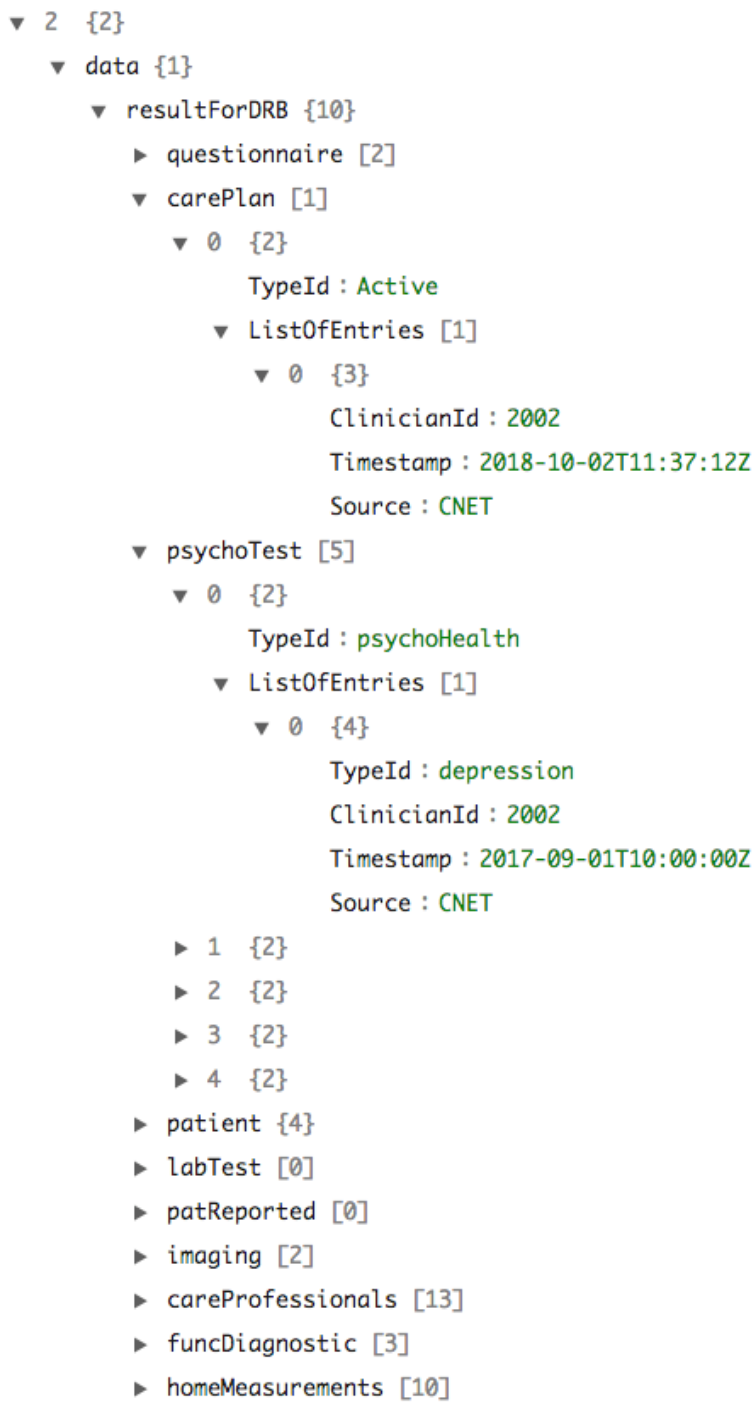
Comments: Data responses from ODS are composed by Patient Data Orchestrator. Here results from three ODSes (0, 1, 2) is presented. Note, the ODS Message Handler was incorporated in this call as it provides APIs over the ODS. Sample of results from one ODS can be seen below. Note, the results are filtered based on the policy-filter (below). The source of the data can be read in meta-data (also below).

8.5 Policy Manager


```
{
  "policy-filter": {
    "success": true,
    "message": "authorized",
    "data-types": [
      "RADAI",
      "sonography",
      "EQ5D",
      "attention",
      "HAQ",
      "name",
      "computer_tomography",
      "virology",
      "conventional_imaging",
      "walking_distance",
      "suspended",
      "blood",
      "steps",
      "night_sleep",
      "completed",
      "active",
      "weight",
      "heart_rate",
      "microbiology",
      "ECG",
      "EEG",
      "psychological_health",
      "morisky_well_being",
      "nuclear_medicine",
      "pain_ratings",
      "address_email",
      "hospital_patient_ID",
      "PD_severity",
      "executive_functions",
      "blood_pressure",
      "language",
      "global_cognitive_status",
      "lung_function",
      "insurer_patient_ID",
      "FFbH",
      "urine",
      "memory",
      "praxia"
    ]
  },
```


Comment: the filter from Policy Manager defines data categories which are enabled for the logged in clinician. In this sample all categories from the list are enabled, thus they are not filtered by the Patient Data Orchestrator.

8.6 Results from ODS



Comment: As can be seen the JSON nodes under the root “data” JSON node correspond to the core data categories from the DRB Mind Map (next to patient icon). Note, there are data entries in other than expanded nodes. However, only few nodes were expanded for the demonstration purposes on the screenshot above.

8.7 Metadata

Comment: here the source of the data is UDUS.

9 List of Figures