A Personalised Integrated Care Platform

(Grant Agreement No. 689209)

D5.7 Third Integrated Data Management Subset in Public Cloud

Date: 2019-06-25

Version 1.0

Published by the PICASO Consortium

Dissemination Level: Public

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: D5.7 Third 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: Demonstrator

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)	28-05-2019	Structure of deliverable
0.2	Marek Skokan (TUK)	03-06-2019	Update of Section 3 Architecture, Section 6 Shared Memory and Section 7 Data Resource Browser. Document for collection of partner's inputs
0.3	Matts Ahlsén (CNET)	11-06-2019	Update of Section 4 ODS system
0.4	Armanas Povilionis (INUIT/BOSARC)	13-06-2019	Update of Section 5 Security and Privacy Management
0.5	Marek Skokan	17-06-2019	Integration of inputs. Version for peer review created.
1.0	Marek Skokan	21-06-2019	Final version based on peer review comments

Internal review history:

Reviewed by	Date	Summary of comments
Carlos A Velasco	19-06-2019	Approved with minor comments

Index:

1 Executive Summary

This document presents an overview of the final 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 ICT solution is based on this approach provided a data management backbone for the PICASO Trial. The final version of integrated Data Management Subset components is described from a functional point of view and the dependencies between components are explained in this document. When no update of the related components occurred this document links to the description that covers the final state of the component's description (usually to D5.6 Second Integrated Data Management Subset in Public Cloud).

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 and components were (and are being) developed and integrated. This deliverable describes final state (or refer to it) of PICASO Data Management Subset components. The final status of the Data Management Subset is presented in this version of the deliverable. Note, there were not many significant changes in Data Management Subset when comparing it with the second version (previous) of deliverable (D5.6).

2.1 Purpose, context and scope of this deliverable

In this deliverable the final “after trials” status of PICASO Data Management Subset is described. It is a third and last version from the three deliverables. It provides a final “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 an 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 these deliverables (D5.7, D5.6 and D5.4).

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 – reflection of the final state
- Chapter 4 – ODS system - description of the final state
- Chapter 5 – Security and Privacy Management - description of the final state
- Chapter 6 – Shared Memory Manager - description of the final state
- Chapter 7 – Data Resource Browser - description of the final state

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 they enable management of healthcare data in PICASO system. All components and the dependencies that are presented in the previous version of this deliverable (D5.6) are valid and there were no updates that can be reflected in the architectural diagram and explained here. Thus, for the final architecture of the Data Management Subset, please, refer to D5.6 Second Integrated Data Management Subset in Public Cloud.

4 ODS system

4.1 Operational Data Store - ODS

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* 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*[1] *database* stores personal and demographic data related to the patients, their informal carers and clinicians.

In support for the clinical patient data processing, additional support databases are part of the data management subset,

The *ThirdParty database* subset stores activity data received from the FitBit third-party service, subsequently stored in the clinical database.

The *ServiceLog database* which records all incoming API requests from the ODS Message Handler (see below). In addition, an *ActivityLog* database, deployed in the Public Cloud, contains logs of all request going through the Public Cloud ODS Message Broker (see below).

The ODS data storage system is deployed in the Private Carer Cloud (Hospital DMZ) in isolation from the back-end clinical (and other hospital) systems, with no update dependencies between clinical systems and PICASO. However, clinical data extraction is performed periodically using specific ETL[2] 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.

[1] Personally Identifiable Information

[2] Extract Transform Load

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.

- **Careplan** // CRUD[3] 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.
- **LabTest** // POST of lab test, with a base 64 encoded string from a file (PDF, jpg, png, etc.) and stores it as a blob in the ODS with related meta data.
- **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.
- **Patient** // Retrieve information for a specific patient.
- **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 FHIR 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.

[3] Create Read Update Delete

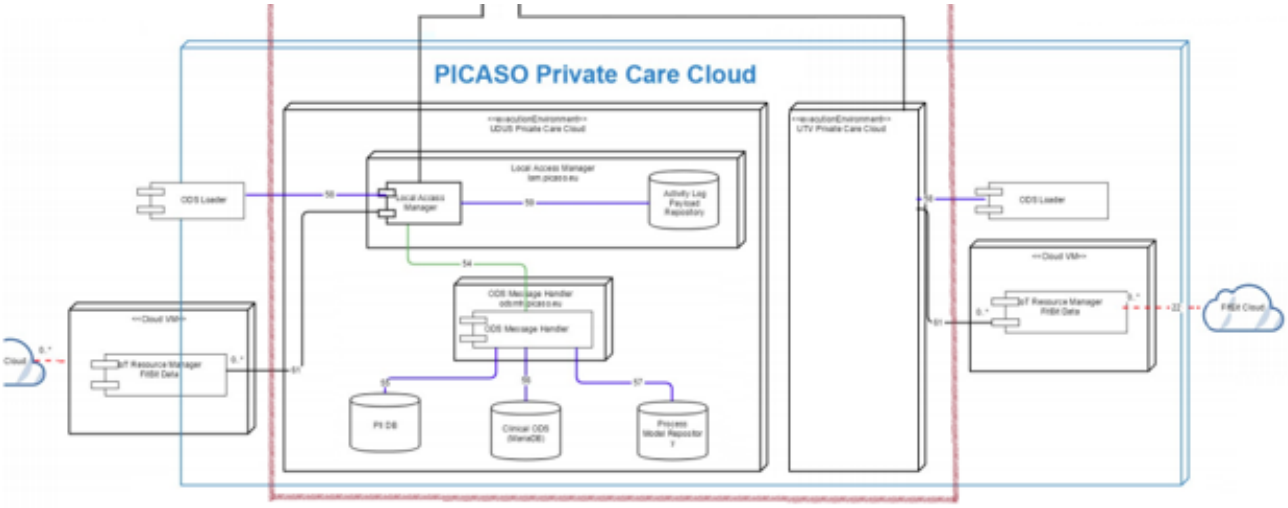

Figure 1: ODS Message Handler dependencies

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.

The message broker component is implemented using the open source software RabbitMQ[4]. This is a widely used open source message broker with an extensible architecture. It implements the AMQP 0-9-1 protocol[5] 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] https://www.rabbitmq.com/

[5] http://www.amqp.org/sites/amqp.org/files/amqp0-9-1.zip

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.

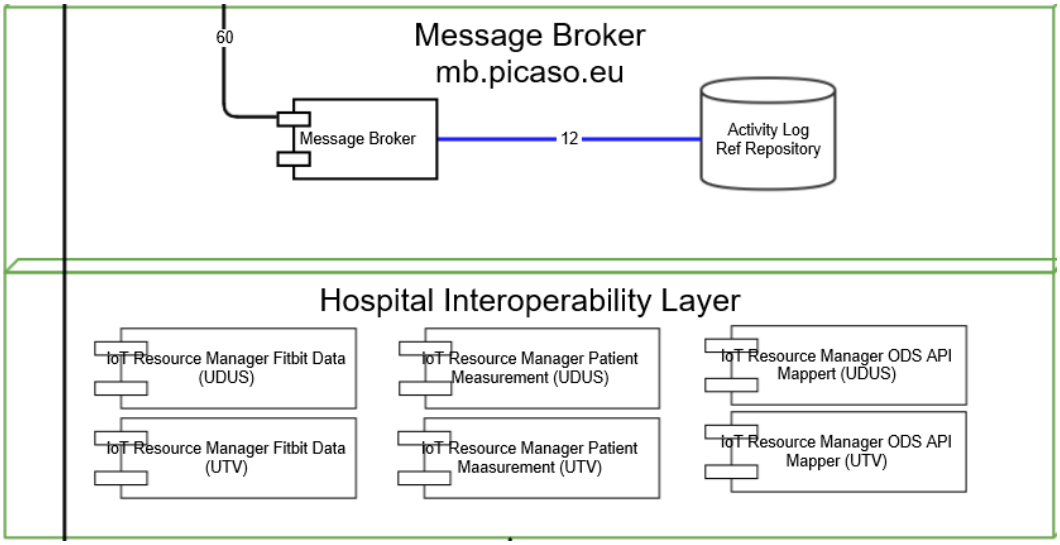

Figure 2: Message Broker dependencies

The Message Broker also maintains an Activity Log repository

4.4 ODS Schema

The main table subsets of the ODS clinical databases are depicted in the following figures for an overview how data are stored in the PICASO ODS. The ODS is the main storage component in the data management process.

The Clinical data subset contains all operational data for the users, such as care plans, reported home measurement, reported medication intakes, patient reported outcomes from questionnaires etc. The table below briefly explain the main clinical data tables.

Table	Description	In use (Y/N)
Careplan	Stores raw JSON careplan as blob together with some meta data	Y
CareplanActivity	Stores careplan activity information, converted from careplan resouce and used by the Patient Dashboard diary	Y
CareplanResource	Stores raw JSON careplan resource as blob together with some meta data	Y
CareplanResourceHistory	Stores older raw JSON careplan resource as blob together with some meta data	Y

Table	Description	In use (Y/N)
ClinicianRole	One or many roles assigned to a clinician	Y
ClinicianType	Type reference table for clinician roles	Y
Device	Device information used by the patients	Y
DeviceType	Type reference table for devices	Y
DeviceTypeCodeSystem	Type reference table for devices and different code systems	N
DiseaseType	Type reference table for diseases	Y
EncounterType	Type reference table for encounters	Y
FollowUpAppointment	Booking information for Appointment Requests (Careplan resource)	Y
Gateway	Gateway information used by the patients	Y
LabResult	File blob storage and meta data for images, blood test, lab test etc.	Y
LeaveOfAbsence	Leave of absence information for patients	Y
MedicationIntake	Intake information about the medication consumed by the patients	Y
Observation	Default storage for observations (e.g. daily aggregated steps, blood pressure, weight)	Y
ObservationCodeSystem	Type reference table for observations and different code systems	N
ObservationHourly	Hourly observation storage (e.g. hourly aggregated steps and heart rate)	Y
ObservationIntraDay	Higher sample rate of observation (e.g. minute data for steps and heart rate)	N

Table	**Description**	**In use (Y/N)**
ObservationType	Type reference table for observations	Y
PatientCarer	Relationship between patient and carer	Y
PatientClinician	Relationship between patient and clinician	Y
PatientDisease	Disease information for a patient	Y
PatientDiseaseEvent	Disease event information for a patient	N
PatientEncounter	Encounter made by the patient (e.g. visit clinician)	Y
PatientNotification	Notification flag enabled/disabled for a patient	Y
PatientProfile	Profile information for a patient	N
PatientReminders	Reminders flag för a patient	N
PatientSymptom	Symptom list for a patient	N
PatientTimes	Time information for a patient (e.g. time for breakfast)	N
PatientTreatment	Treatment information for a patient	N
PatientTreatmentEvent	Treatment event information for a patient	N
PushNotification	Created push notification used to notify the patient	Y
QuestionnaireAnswers	Answers to a fulfilled questionnaire	Y
QuestionnaireMeta	Meta data for a fulfilled questionnaire	Y
QuestionnaireStructure	Questionnaire type encoded as JSON	Y
SymptomType	Type reference table for symptoms	N

Table	Description	In use (Y/N)
TreatmentStopType	Type reference table for stop reasons	N
TreatmentType	Type reference table for treatments	N

Table 1: ODS tables

4.4.1 PII DB

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

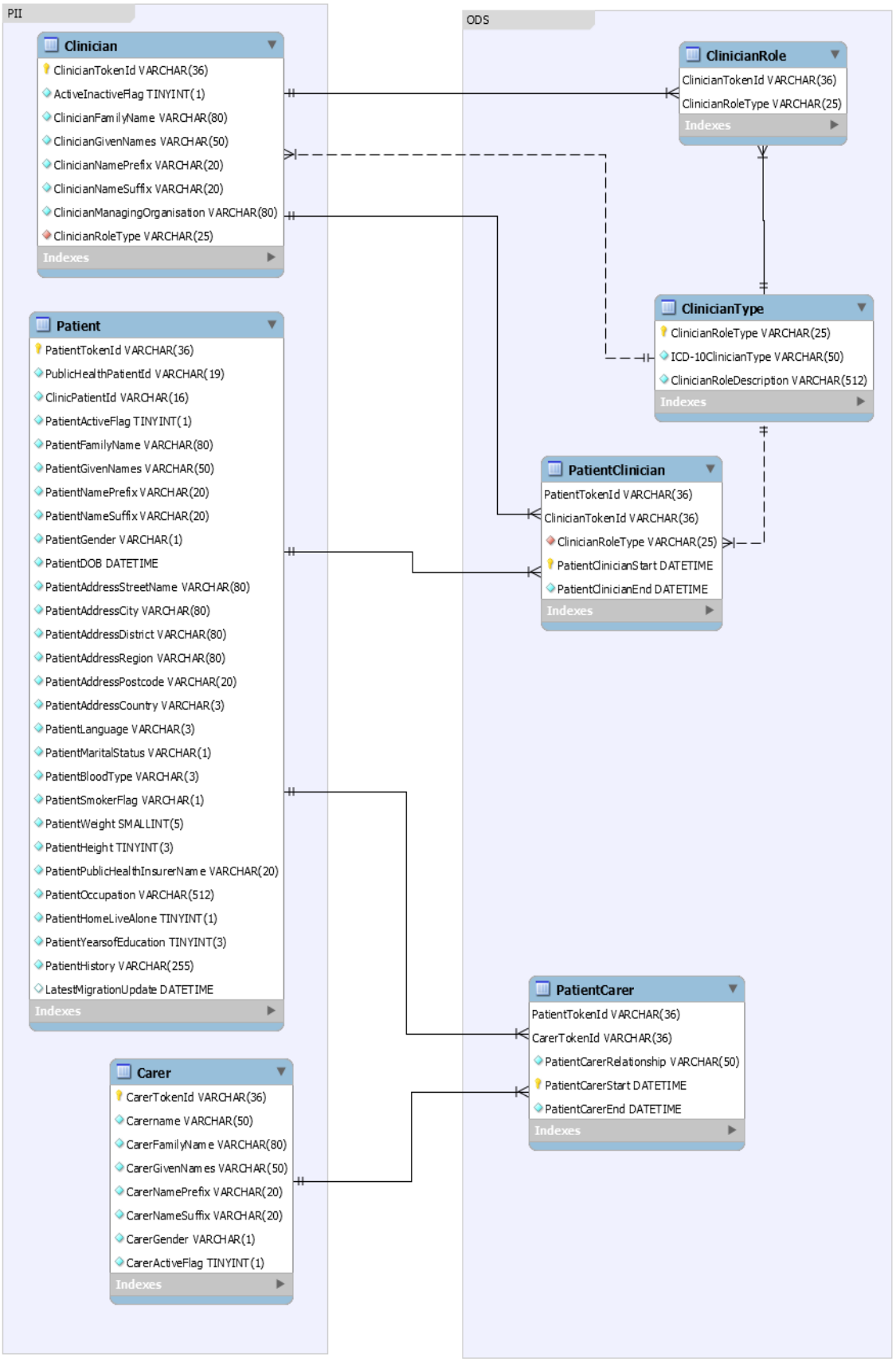

Figure 3: The PII database schema for storing data about patients, clinicians and informal carers

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

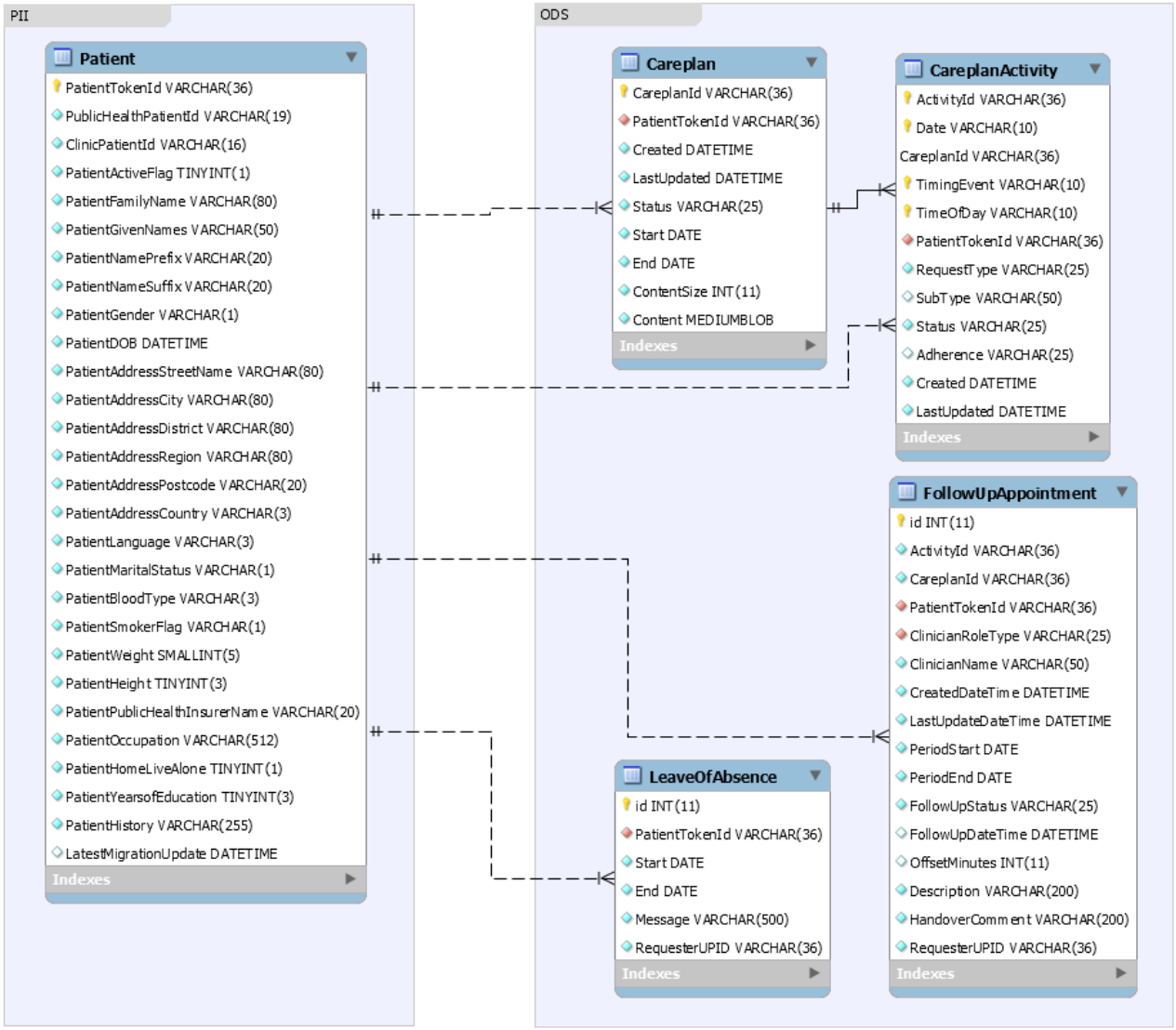

Figure 4: Database schema designed for storing data about Care Plans

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

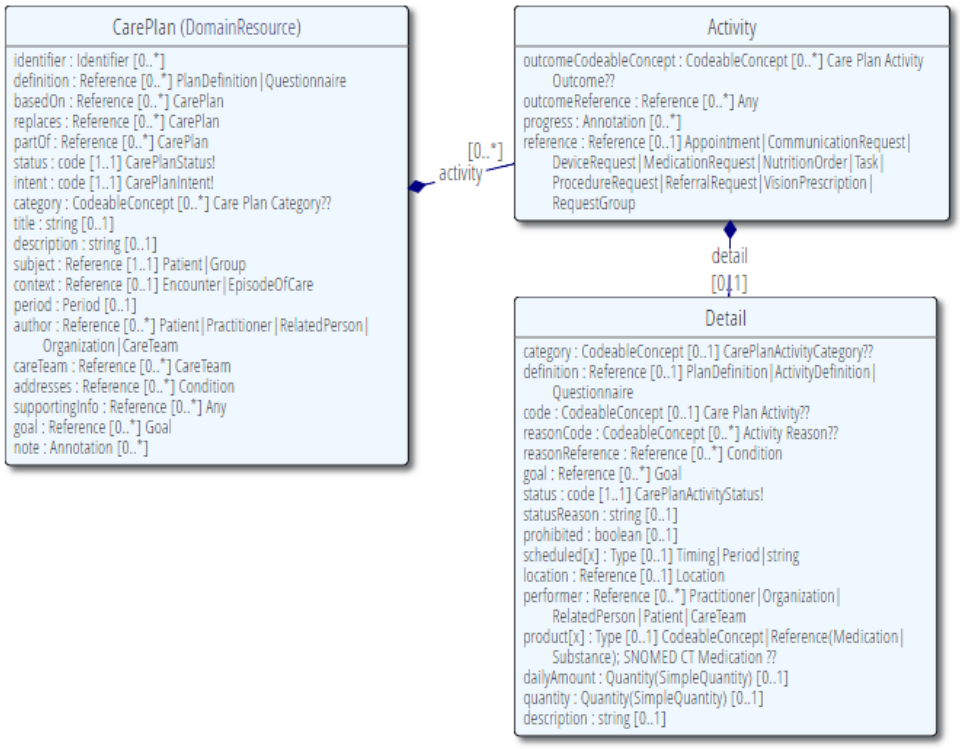

Figure 5: FHIR CarePlan resource

4.4.2 PICASO Observations

Figure 6 depicts the schema for PICASO Observations. The observations come from devices connected to the patients' tablet and from the FitBit cloud. The calculated results (scores) from questionnaires are also stored as observations.

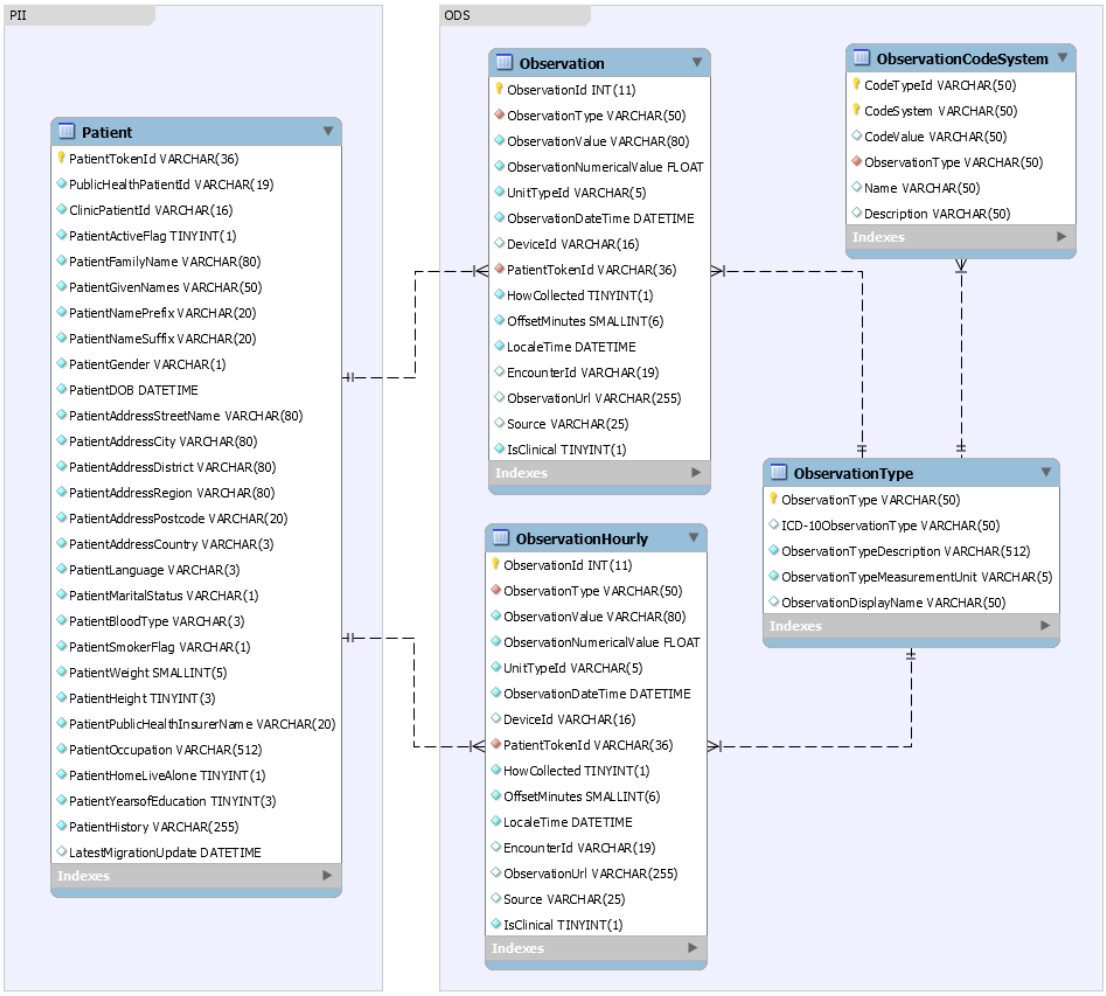

Figure 6: Database schema used for storing Observations

4.4.3 Encounters

Figure 7 depicts the data schema for PICASO Encounters, such as visiting a clinician.

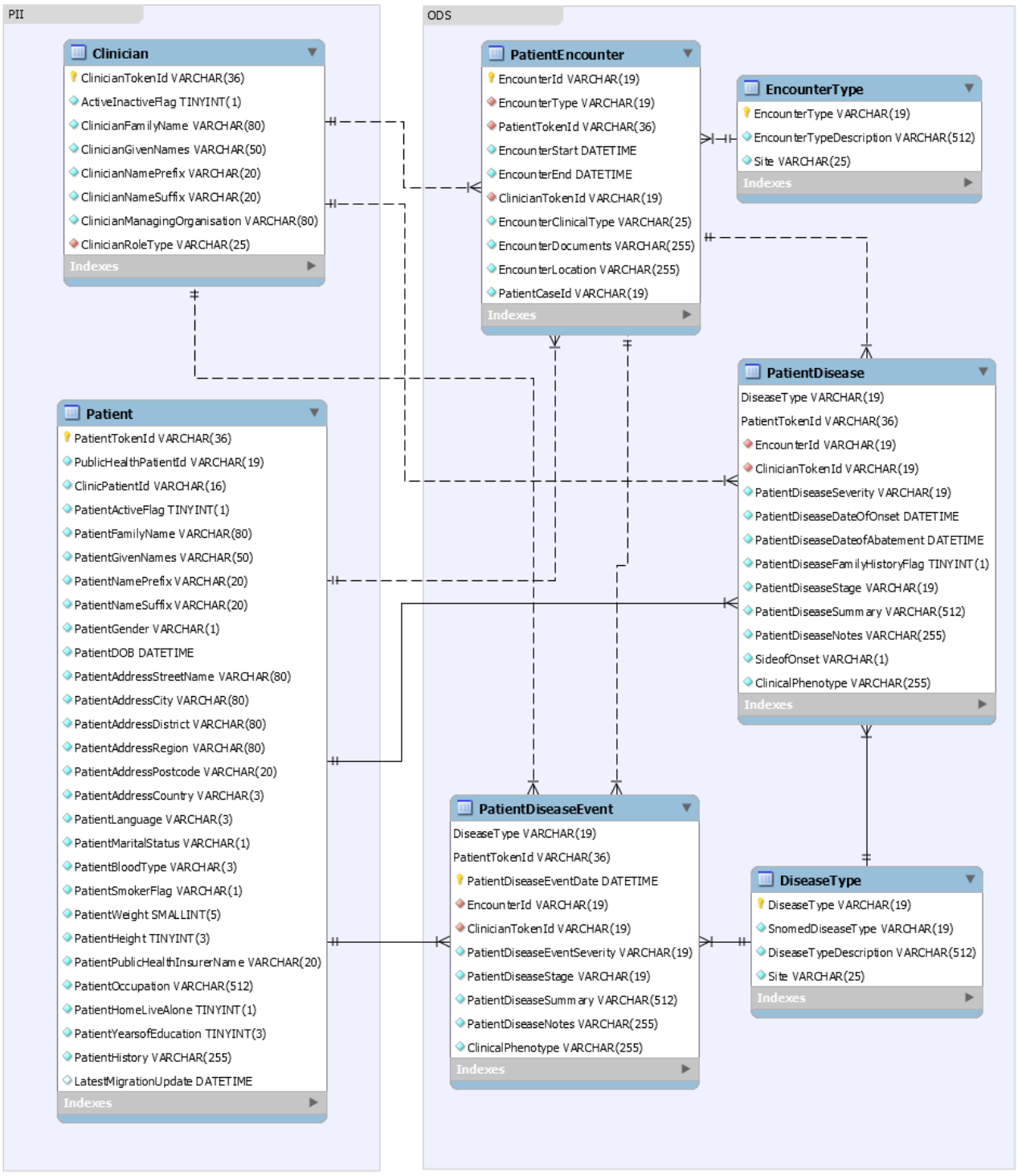

Figure 7: Database schema used for storing Encounters

4.4.4 Questionnaires

Figure 8 defines the tables for storing Questionnaires data including patient responses based on these questionnaires.

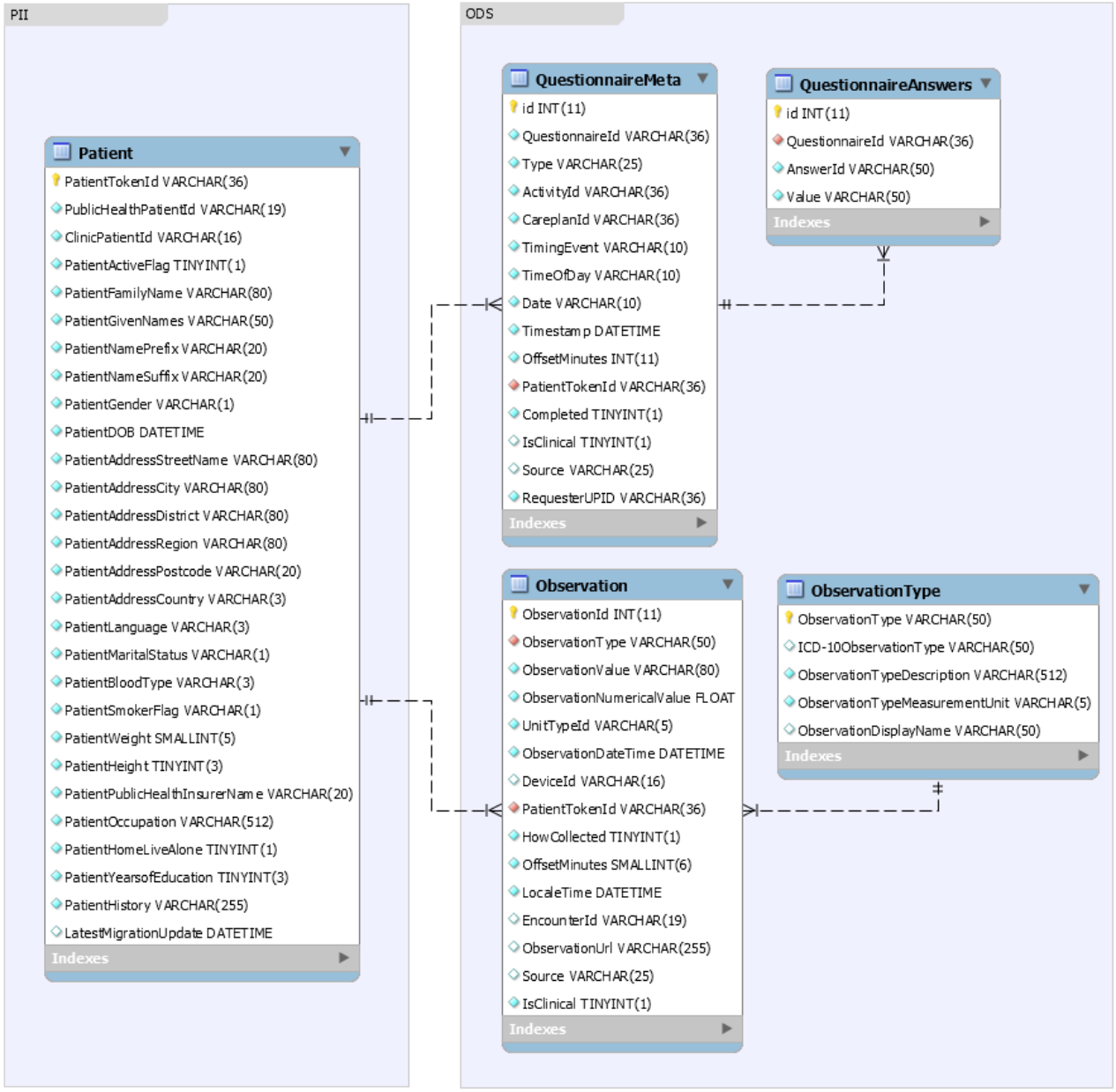

Figure 8: Database schema used for storing Questionnaires

The different Questionnaire types are structured following the FHIR Questionnaire standard, encoded in JSON format and stored as BLOBs in the database. These are subsequently retrieved by the Clinician Dashboard and matched with the answers from the individual patient.

4.4.5 Push notifications

Regular patient reminders are the result of care plan activities (CarePlanActivity table) that are overdue. *Push Notifications* are used as a complement to the regular reminders. Whereas the latter require the Patient Dashboard web browser to be open on the user tablet device for the user to be alerted, Push Notifications can be sent to alert a user device regardless of this. Schema defining DB table for storing push notification is in Figure 9 below.

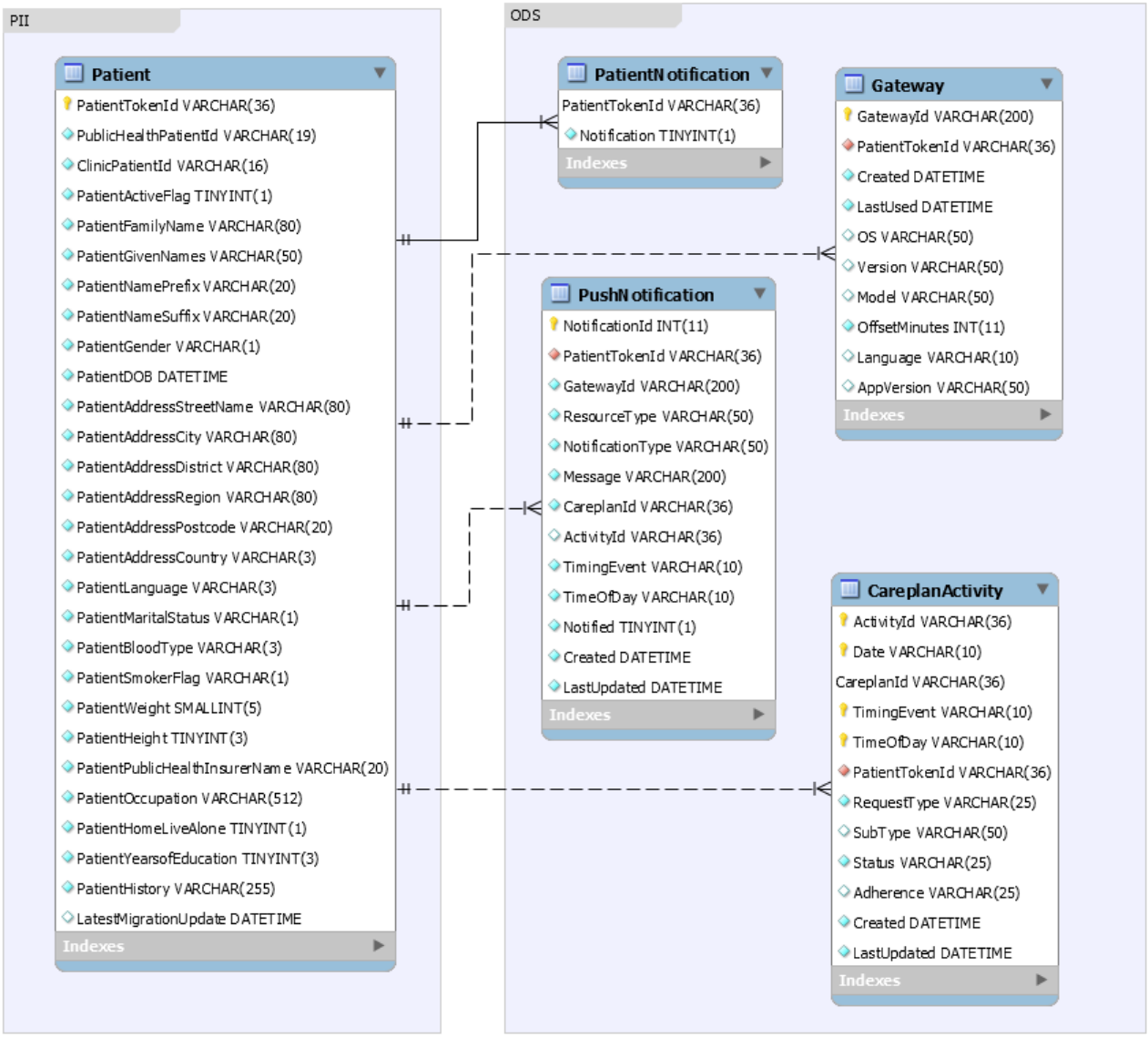

Figure 9: Database schema used for storing Push notifications

5 Security and Privacy Management

5.1 Security and Privacy Management - overview

The Design of Security and Privacy Management subset was refactored form the previous version described in deliverable *D5.6 Second Integrated Data Management Subset in Public Cloud* to implement operating-system-level virtualization also known as containerization. This enables to system to be more modular, flexible and scalable. It also, enables grated monitoring and system management capabilities, while still providing same functional capabilities: 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.

Refactoring of the Security and Privacy Management subset also provided a greater stability of the system and increased performance significantly (see section 5.3). Security and Privacy Management 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

were incorporate in to one product called DIVA (DIstributed Validation Authority). DIVA ensures that data is only shared if all policies and transaction specific privacy and security requirements are met. Technology of DIVA encapsulates the methods and solutions allowing the validation of correctness of access policies at multiple distributed locations as well as ensuring that policies are correctly synchronized between the different Access Managers.

A thorough description of the component with dependency, activity, use case and sequence diagrams can be found in PICASO deliverables D7.4, D7.7 and D7.9.

5.2 Monitoring and Administrative tools

With DIVA INUIT has created a suit of Command Line Interface (CLI) tools set for monitoring and managing the distributed components from one administrator environment. Tools enables administrators track the server up-times and loads, it also allows to monitor not only virtual machines performance, but separate processes and selected parameters running in virtual environments of DIVA components. Tools enable system administrators to react quickly to any issues and provide a comprehensive troubleshoot. Administrative toolset includes opensource components like CURL, openSSL and ab (ApacheBench) configured to continuously measure the performance virtual machines and HTTP web servers.

5.3 Security advancements

The reverse proxy node was configured to enforce whenever it is possible usage of the Transport Layer Security (TLS) protocol version 1.3 (TLS 1.3 was defined in August 2018) to secure all communications between their servers and web browsers.

In addition, security components are ready to utilize Datagram Transport Layer Security (DTLS) communication protocol. Because DTLS is based on User Datagram Protocol (UDP) it enables to provide TLS security without packet reordering problem. Thus, enabling faster and more stable communication over Virtual Private Network) VPN tunnel between PICASO Public Cloud and PICASO Private Cloud instances.

OS configuration.

DIVA can switch upon the need to use different libraries (GnuTLS, LibreTLS, OpenSSL) for implementing TLS and DTLS protocols. That said DIVA uses the latest SSL libraries and is configured to update regularly form trusted repositories.

5.4 Privacy approach

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

5.4.1 Provision of Unique PICASO Identifiers

All authentication and access control in PICASO are 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

5.4.2 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.

5.4.3 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.

5.4.4 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.

5.4.5 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 access for the information about the patient specified.

5.4.6 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 in Figure 10.

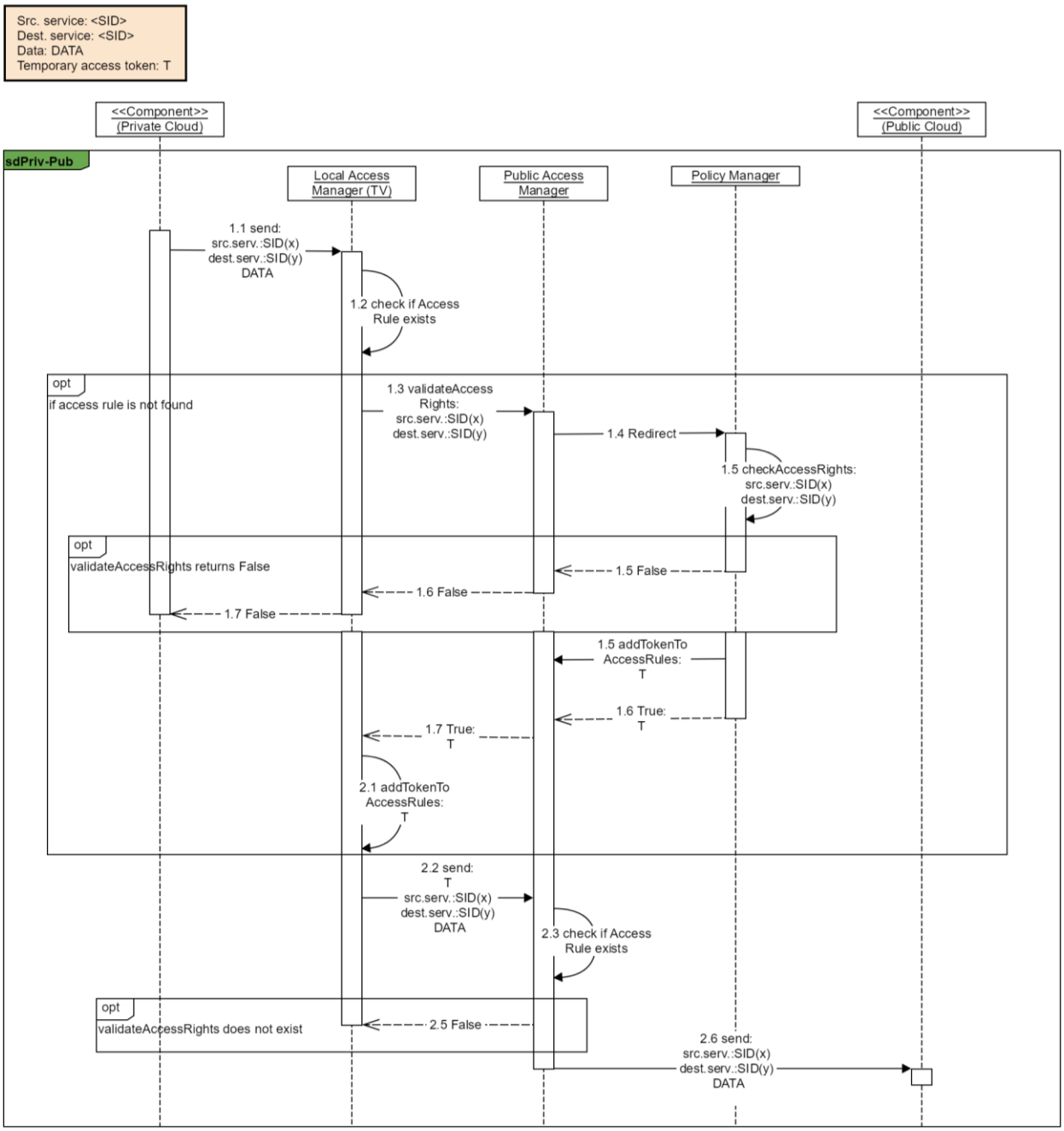

Figure 10: Sequence diagram of component calls between PICASO Cloud

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 in Figure 11.

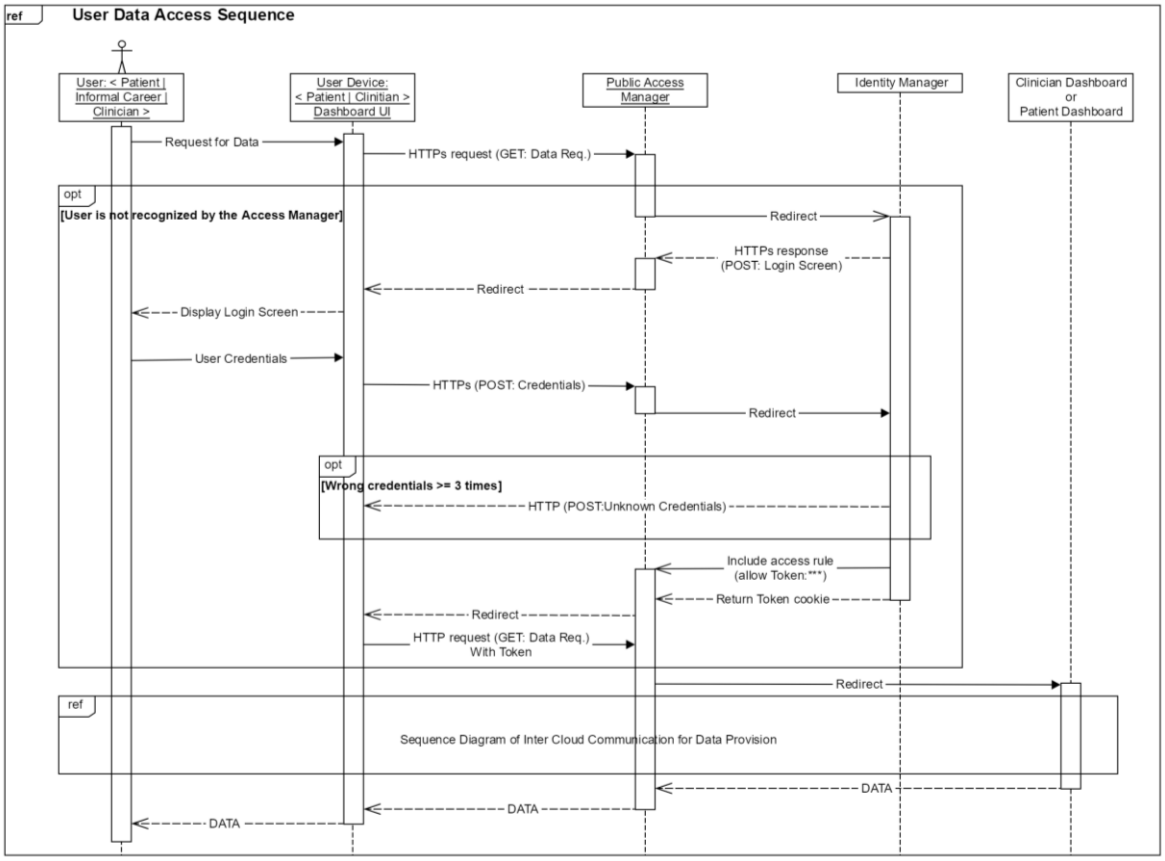

Figure 11: Data Request Sequence

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 consists of Metadata Registry and Patient Data Orchestrator components. The overall concept and functionalities of Shared memory manager was not updated comparing to previous deliverables (D5.6, D5.2). Though, there was one small update of the Patient Data Orchestrator that is described in the following.

6.1 Update of Patient Data Orchestrator

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.

7 Data Resource Browser

7.1 Description

The Data Resource Browser is a web-based, interactive interface where authenticated clinicians can search for combination of all information stored in the shared memory such us information about patients, other carers, health records and care plans. The user retrieves data by querying the Data Orchestration considering the authorisation policy. For more information about how Data Orchestration and Policy Management of data are involved in the data requests/response for DRB see D5.6 Second Integrated Data Management Subset in Public Cloud.

The updates in DRB consist of changes related to integration with Patient Data Viewer, new data categories and updates of some icons.

7.2 Update in Dependencies with other components

The dependency of DRB with PDV was updated, as DRB is part of one integrated visualisation tool serving clinicians in the PICASO Clinician Dashboard. The UPID of clinician who is logged in the Clinician Dashboard and UPID of patient that has been chosen by the clinician is a basic dependency, as they are used in data requests constructed by both of these integrated visualisation tools. Second level of the dependency are data categories that are reflected by icons in DRB and by names of views and charts, timelines and tables displayed by the PDV.

7.3 Update of data categories

The feedback from running trials as well as feedback obtained from outer world (e.g. IEEE Vis2018 conference) result in adding new data categories into DRB Mind Map. These two categories were added: Medication Reporting and Diseases. Both categories are represented as new icons in the Mind map and are associated with patient directly.

Figure 12: New icons for Medication Reporting and Diseases

Comment: Figure 12 depicts new icons connected to Patient representing Medication Reporting and Diseases categories in the DRB patient centric Mind Map

7.4 Update of functionalities

7.4.1 Integrated DRB and PDV

The following screenshots provide demonstration how are healthcare data (managed over PICASO Data Management Subset) visualised in the Clinician Dashboard by integrated DRB and PDV aiming at functionalities of the first visualisation tool. The screenshots are explained in the comments below them. They are addressing most important updates and new features.

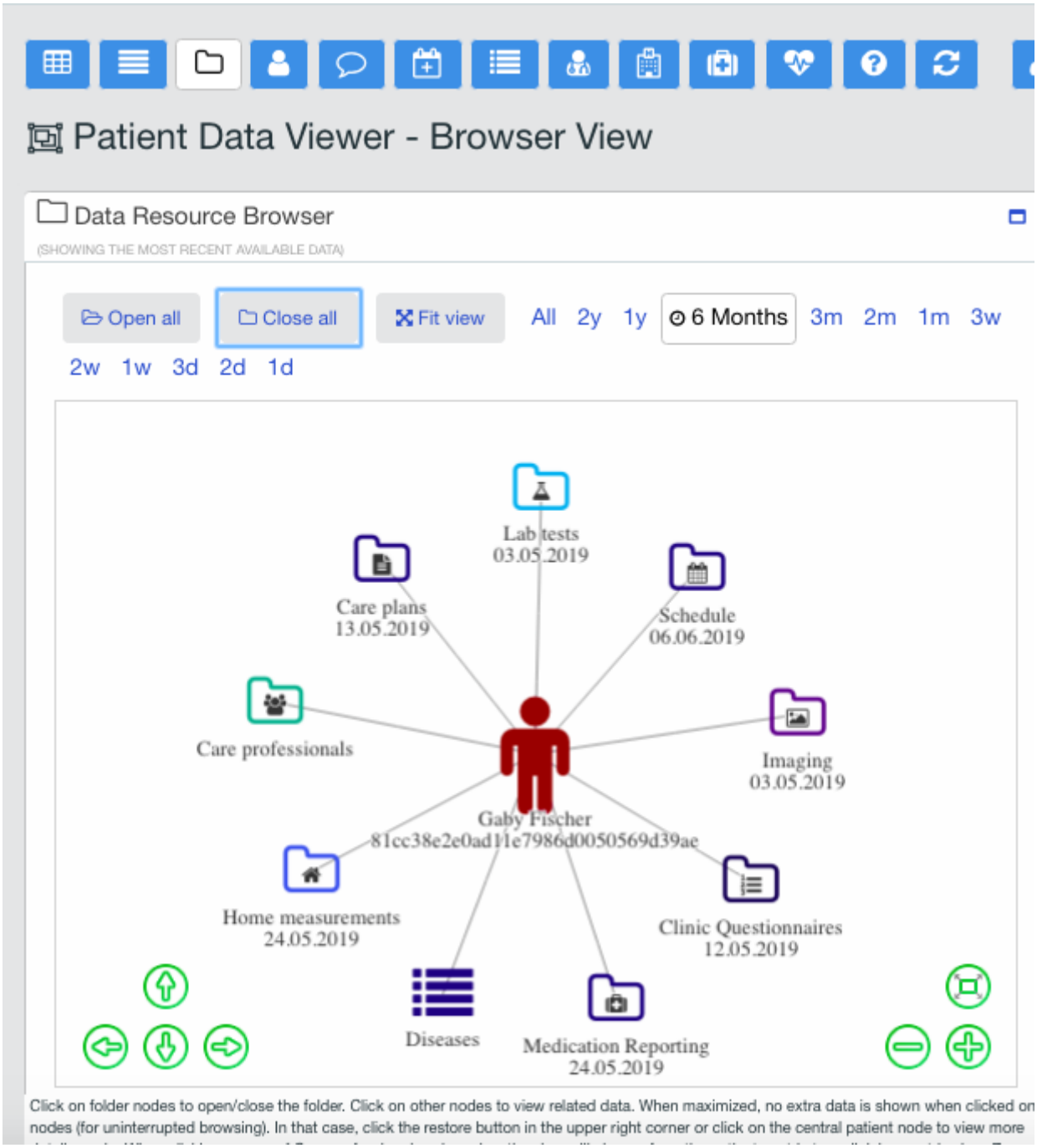

Figure 13: Browser view in PDV containing interactive mind map

Comment: The DRB is one view in the PDV now. It is called Browser view (see Figure 13). The buttons (Open all, Close all and Fit view) are now above the frame for mind map. Time period can be chosen by predefined buttons for time periods above the frame of mind map. By using such time periods the data out of them are filtered and this is reflected by the mind map. All nodes displayed on the mind map corresponds to the data

categories available for the patient. The icons that appears as folders can be expanded (see also other screenshots). This provides information to the user that Patient's data related to the more specific categories are available. This was the major icon update in DRB.

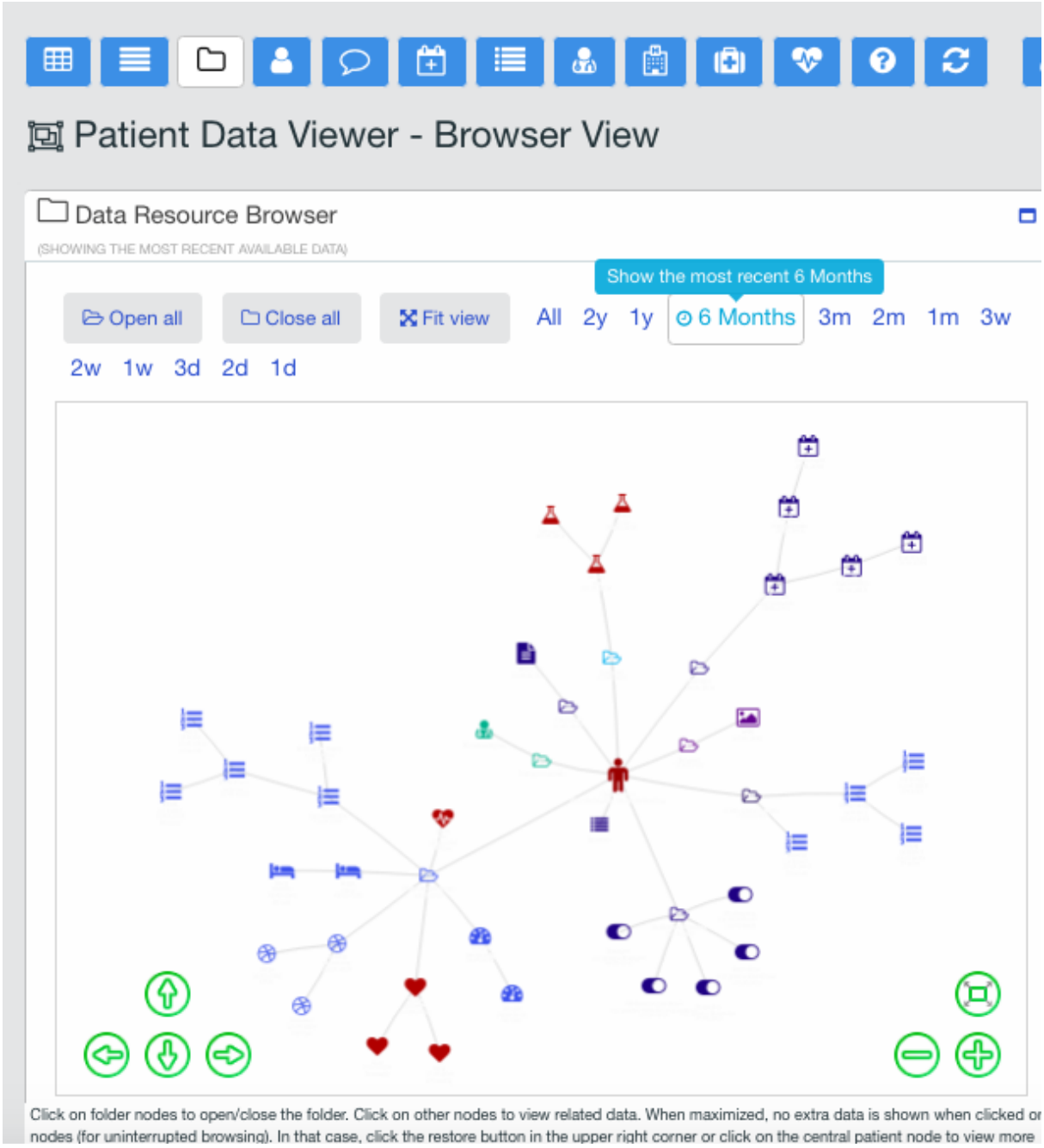

Figure 14: Expanded nodes for chosen demo patient

Comment: Screenshot of expanded nodes for chosen demo patient that are relevant to the patient's data not older than 6 months is in Figure 14.

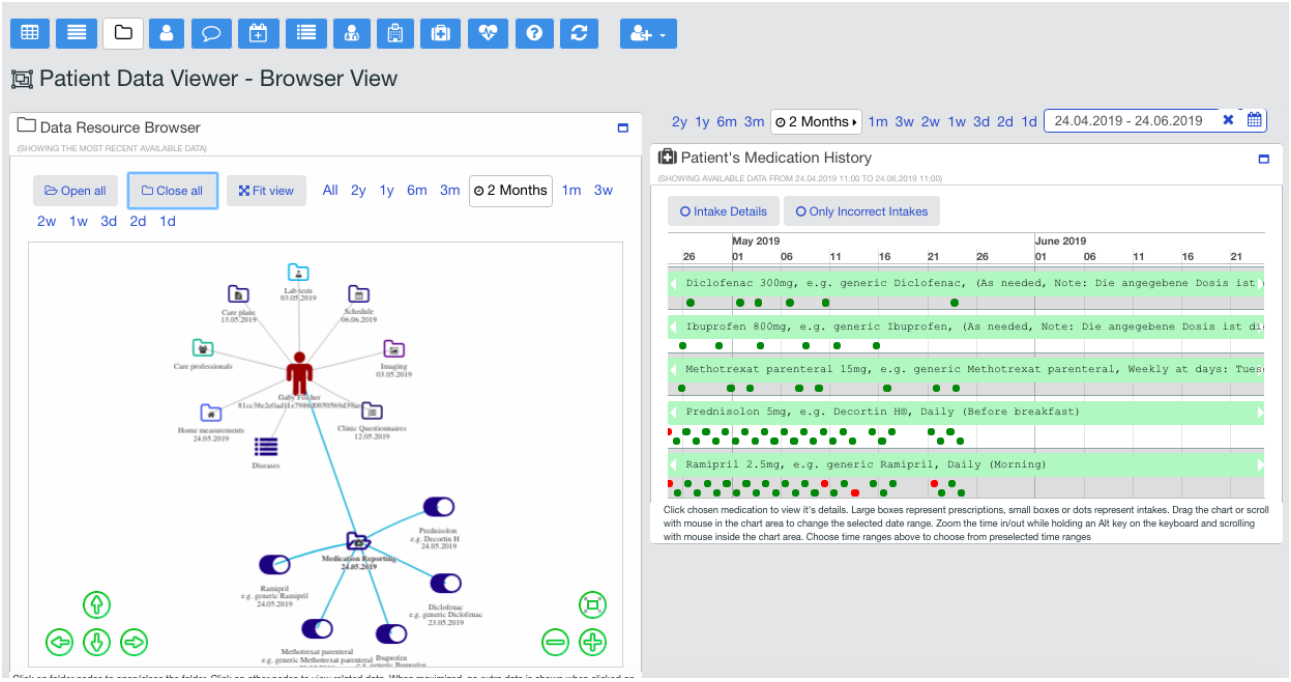

Figure 15: Timeline displayed on the right-hand side of the mind map

Comment: In this updated version, any selected category will cause relevant chart or timeline to be displayed on the right-hand side (see Figure 15). Here, Medication Reporting category is expanded and that cause timeline with Medication History to be displayed on the right-hand side.

Note, there are more details about the data entries presented on the timelines and charts. The presentation of such details is enabled by the specific functionalities of PDV which are described in deliverable D6.7 Third Decision Support and Interaction Tools.

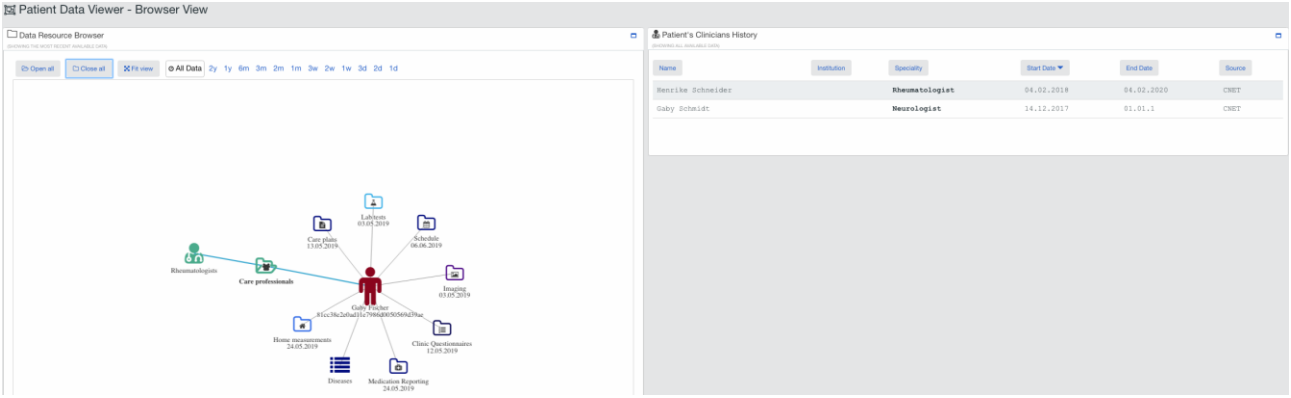

Figure 16: Care professionals on the Patient centric view

Comment: Care professionals that were taking care about the patient with details on the right-hand side (Figure 16). By clicking on care professional, the view is switched from Patient centric to Clinician centric.

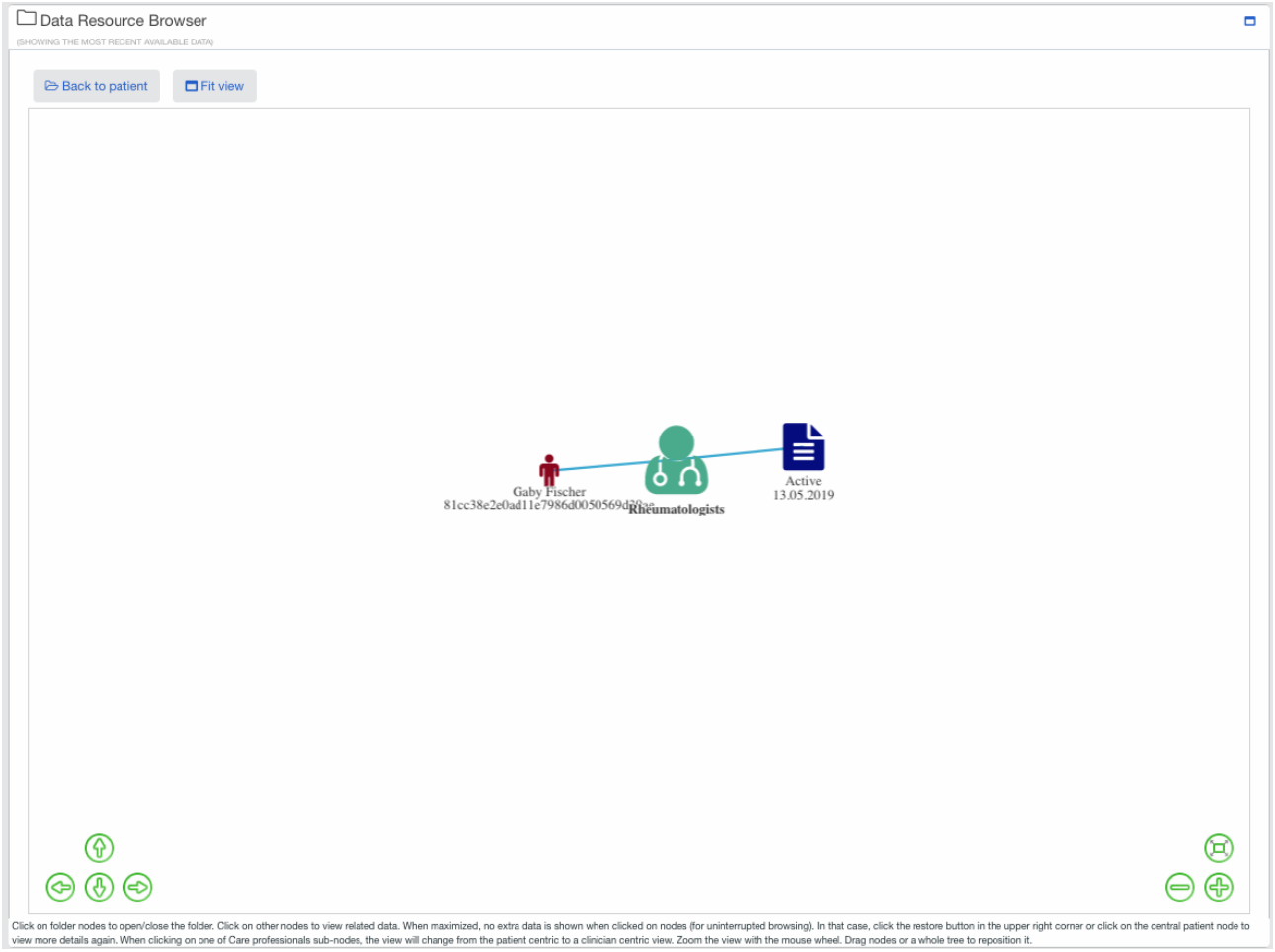

Figure 17: Clinician-centric view of Data Resource Browser

Comment: Updated Clinician centric view provides more intuitive ways to return to patient centric view - thru associated icon on the mind map or over dedicated button above the mind map called Back to patient (see Figure 17).

8 Summary and Conclusions

The third (final) version of Data Management Subset in Public Cloud is now deployed and it supports both clinical trials. There were considerable amounts of updates related to components when comparing this third version with the previous second version. These updates of components were rather their evolutions. They were based on the feedback from trials as well as from bug-fixing activities. There were no such updates that affected architecture of the Data Management Subset.

There were some proposal of updates that went beyond the reasonable scope of the project. The update of user profiles in terms of their preferences is main example. It means implementation of thorough concept for irrelevant data hiding based on certain clinician role as well as preferences defined by specific user. It would cost more effort than available in the project. Such update would affect all components in the Data Management Subset and it can be considered as a main candidate for future (beyond the project) extension of Data Management Subset in Public Cloud.

The overall conclusion is that Data Management Subset in Public Cloud has well met the requirements from other PICASO components and from the clinical trials.

List of Figures and Tables

Figures

Tables