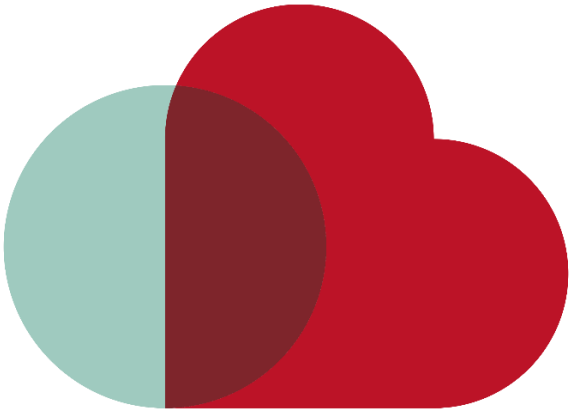


retention

SMART HEART FAILURE MANAGEMENT

Horizon 2020 Project RETENTION

"HEART FAILURE PATIENT MANAGEMENT AND INTERVENTIONS USING CONTINUOUS PATIENT MONITORING OUTSIDE HOSPITALS AND REAL WORLD DATA"

Research and Innovation Action
H2020-SC1-BHC-2018-2020
GA 965343

Duration: 48 months from 01/05/2021
Coordinator: Institute for Communication and Computer Systems

Deliverable ID.:	**D3.2**	
Deliverable title:	**RETENTION Architecture**	
Planned delivery date:	28/02/2022	
Actual delivery date:	30/06/2022	
Deliverable leader:	DATAMED SA	
Contributing partners:	ICCS, FORTH, STS, AEGIS, SIESLR	
Dissemination Level:	**X**	PU = Public
		CO = Confidential
		CL = Classified

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 965343.

Document information and history

Deliverable description

This report presents the architectural design of the RETENTION solution (solution). It includes an overview of the different main sub-components of the platform, that is: i) the RETENTION Global Insights Cloud infrastructure, where the participants' (previously anonymised) data are eventually analysed using Big Data algorithms according to workflows defined by the clinical researchers; ii) the RETENTION Clinical Site Backend infrastructure, where participants' data reside (per Clinical Site) and are being utilised for predictions and personalised interventions; and iii) the RETENTION Patient EDGE, a layer responsible for co-ordinating home devices'/sensors' usage data collection and publicly available data from external vendors. The main part of the deliverable deals with identifying the general components, their utility in the solution, the main dataflow interactions, and security/deployment design decisions. The appendices provide detailed specifications of each of these, following the general structure/order of the main document.

Version N.	Date	Author	Reviewer	Milestone*	Notes
V 0.1	*01/08/2021*	*N. Polyzos, G., Anagnostopoulos, G. Del Toro (DM)*		*Creation of ToC*	
V 0.2	*16/11/2021*	*N. Polyzos, G. Anagnostopoulos, G. Del Toro (DM), Y. Goletsis, M. Roumpi (FORTH), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*		*Updated ToC,*	*Update according to the 2nd PCC meeting.*
V 0.3	*03/12/2021*	*N. Polyzos, G. Anagnostopoulos, G. Del Toro, A. Prentakis (DM), Y. Goletsis, M. Roumpi (FORTH), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*			*Finalisation of responsibilities and timetable. Choice of architecture and architectural diagram.*
V 0.4 – V 0.6	*03/12/2021-28/02/2022*	*N. Polyzos, G. Anagnostopoulos, G. Del Toro, A. Prentakis (DM), Y. Goletsis, M. Roumpi (FORTH), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*		*1st round of contributions*	*Working versions*
V 0.7	*14/3/2022*	*N. Polyzos, G. Del Toro, A. Prentakis (DM), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*		*1st final draft version*	
V 0.8	*14/4/2022*	*N. Polyzos, G. Del Toro, A. Prentakis (DM), M. Vakalellis, L. Kallipolitis, (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*		*2nd round of contributions*	*Updated version to accommodate updated/enriched end-user requirements*
V 0.9	*30/4/2022*	*N. Polyzos, G. Del Toro, A. Prentakis (DM), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis*	*Y. Goletsis, M.Roumpi (FORTH), I.*	*1st review comments*	

Version N.	Date	Author	Reviewer	Milestone*	Notes
		(STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)	*Kouris (ICCS), I. Basdekis (STS)*		
V 0.91	*2/5/2022*	*N. Polyzos, G. Del Toro, A. Prentakis (DM), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*			*Updated version to accommodate review comments*
V 0.92	*28/5/2022*	*N. Polyzos, G. Del Toro, A. Prentakis (DM), M. Vakalellis, L. Kallipolitis (AEGIS), I. Basdekis (STS), I. Kouris (ICCS), I. Nicolae, G. Danciu (SIESRL)*			*Updated version to accommodate user requirements introduced during the 3rd PCC meeting*
V 0.93	*03/06/2022*		*Y. Goletsis, M. Roumpi (FORTH)*	*Proposed for 2nd Review*	
V 0.94	*13/06/2022*		*I. Basdekis (STS)*	*2nd Review Comments*	
V 0.95	*20/06/2022*	*G. Del Toro (DM)*			*2nd review comments addressed*
V0.96	*21/06/2022*	*G. Del Toro (DM)*		*Incorporate appendices*	
V 0.97	*27/06/2022*		*I. Basdekis (STS)*	*Final Review by TCr*	*Final TCr review comments provided*
V 0.98	*28/06/2022*	*G. Del Toro (DM)*			*Final TCr review comments incorporated*
V 0.99	*29/06/2022*		*Y. Goletsis, M. Roumpi (FORTH)*	*External Release Version*	
V 1.0	*30/06/2022*		*M. Haritou (ICCS)*	*Final PCr review & modifications*	*Submitted Version*

** The project uses a multi-stage internal review and release process, with defined milestones. Milestone names include abbreviations/terms as follows:*

TOC = "Table of Contents" (describes planned contents of different sections);

- *Intermediate: Document is approximately 50% complete – review checkpoint;*

ER = "External Release" (i.e. to commission and reviewers);

- *Proposed: document authors submit for internal review;*
- *Revised: document authors produce new version in response to internal reviewer comments approved: Internal project reviewers accept the document.*

Table of Contents

List of Abbreviations

Essential abbreviations used in the document:

HF	Heart Failure
Carer	Caregiver
GIC	Global Insights Cloud (part of the system)
CSB	Clinical Site Backend (part of the system)
PE	Patient EDGE (part of the system)
PD	Patient Devices
RWD	Real World Data
BDAE	Big Data Analytics Engine or BDA Engine
GICDB	GIC Dashboard
GICMST	GIC Model Specification Tool
GICDI	GIC Disease Insights
GICBDAE	GIC Big Data Analytics Engine
GICDPS	GIC Decision & Policy Support
GICDL	GIC Data Layer
CSBDB	CSB Dashboard
CSBDAEE	CSB BDA Engine Executor
CSBDSS	CSB Decision Support System
CSBDL	CSB Data Layer
PEMA	Patient EDGE Mobile Application
PELHG	PE Local Home Gateway
DoA	Grant Agreement or Document of Agreement
m2m	Machine to machine
IoT	Internet of Things
(m)IoT	Smart Mobile - Internet of Things

Table of Figures

List of Tables

1 Executive Summary

The primary goal of the RETENTION project is to develop an integrated platform that gathers and analyses health-related data flows, with further analysis of day-by-day Heart Failure study participants' activities. Such continuous data collection and processing will later provide the input for personalised interventions that support the healthy and independent living of the study participants. Within this context, the proposed RETENTION architecture aims to bring together state-of-the-art privacy-preserving technologies, big data analytics technologies and mechanisms for managing usage data relevant to the RETENTION study indicators, to create the foundation upon which all these components depend and enable the RETENTION solution to deliverer evidence-based personalised interventions for Heart Failure study participants (patients) by: (a) continuously monitoring and collecting medical, clinical, physiological, behavioural, psychosocial, and real-world data of the patients, (b) analysing these data using innovative model-driven big data analytics, statistical, artificial intelligence and machine learning techniques, (c) detecting patterns in the HF disease progression and the quality of life of the patients, (d) cross checking and validating them against the clinical literature, and (e) offering transparent, explainable and verifiable decision making capabilities that leverage the evidence produced by the underlying data analysis.

The RETENTION Architecture that adheres to the "Privacy by Design" principle (General Data Protection Regulation - GDPR) forms a solution that allows study participants' data (e.g., personal health records, usage devices'/sensors' data, notifications to be generated) to remain under the control of Pilots participating in the RETENTION study (i.e., 6 clinical centrees in Greece, Italy, Germany and Spain), while still allowing the further utilisation of the data in the context of big data analytics considering the privacy, and the limitation of (hardware) resources to perform complex machine learning analytics. Knowledge (ML models and their applicability) to be produced can be made available to the RETENTION Pilots, can be applied to subsets or specific patients, and assist clinicians in their activities.

This deliverable that presents all high-level components of the RETENTION solution, complies with actions of the DoA and the proceedings of Deliverable D3.1 (end user requirements), generating the architecture of the RETENTION solution to achieve project aims including the integration of the developed solution into clinical practice: i) managing usage data generated by devices and sensors, ii) administering patients' medical data, iii) introducing and executing ML models for continuous learning, iv) providing personalised suggestions previously approved (vetted) by clinicians, v) presenting such functionality and results to end-users in a meaningful and user-friendly manner. Considering that health data are recognised as a special category of personal data (GDPR) and, as such, safeguards must be put in place to support the effective protection of them, in addition to the techniques to be applied (e.g., pseudonymisation, limitation of access encryption) the whole functionality (data integrity and the solution integrity as a whole) is to be protected (continuously monitored) by state-of-the-art security/privacy assessment mechanisms. In this context, this document deals with identifying the components and their utility within the platform, the main dataflow interactions, and security/deployment design decisions along with them. It also includes an overview of the main blocks of the RETENTION platform, that is:

- Global Insights Cloud (GIC)
- Clinical Site Backend (CSB)
- Patient Edge (PE)
- Participant Devices (PD)

In particular, the Global Insight's Cloud (GIC) provides mechanisms to support the management of previously anonymised data, statistical and machine learning analysis and model training considering them, and the

utilisation of the results of analyses (e.g., training machine learning models for predictions, processing in a higher level to evaluate policy making decisions). The GIC pools anonymised patient data from all pilot sites and in turn leverages advanced forms of global data analytics that will result in models learned from the data which will underpin evidence-based interventions. The GIC consists of the Big Data Analytics Engine (GIC@BDAE) that parses data (i.e., FHIR and non-FHIR data, models) stored in the Repository (GIC@Repository) and feed it further to the Model Specification Tool (GIC@MST), a component that manages machine learning models. The Disease Insights is an extension of the GIC@MST that allow data scientists to better understand and evaluate via visual aids the previously created models. The Decision and Policy Support (GIC@DPS) is a tool that utilises the outcomes produced by data analysis to form and evaluate interventions at a public health policy level which are actions that address specific policy objectives. The Dashboard (GIC@Dashboard) is the component that supports all interactions between GIC end-users and services in the backend based on the role assigned to the end-user by the Role-Based Access Control (RBAC) capabilities defined within the Security Component (GIC@SC). GIC@SC administers the authentication of the different types of end-users supported via Role-Based Access Control (RBAC), allows secure and authorised machine-2-machine (m2m) transactions to be performed (between Global Insight's Cloud and Clinical Site Backend), and handles aspects of the pseudonymisation process.

The Clinical Site Backend (CSB) is the infrastructure (one per Clinical site) that supports all clinical side operations. In particular the management of the clinical site study participants' (HF patients) basic information (i.e., personal data, personal identifiers, authorised clinicians, informal or formal caregiver(s) or relatives), their initial administration and baseline assessment (i.e., personal health record, questionnaires' answers) along with medical data of each visit, the management of devices/sensors and the monitoring of their utilisation (devices'/sensors' usage measurements, transmissions' metadata). The supported functionality will provide a clinical overview of each patient, as well as statistical comparisons via descriptive analytics and personalised predictions by the application of trained ML models. All RETENTION parameters (i.e., FHIR data, non-FHIR data) are stored in the Repository (CSB@Repository) to constitute the best available evidence, based on which ML trained models (as suggestions/hints), and in the end clinicians, consider configuring the triggering of personalised interventions. Each CSB instance consists of the Big Data Engine Executor (CSB@BDEE), a component responsible for managing descriptive analytics and the latest variant of any trained ML model to support personalised predictions, the Decision Support System (CSB@DSS), a rule-based system that enhances the ability of clinicians to take decisions (i.e., generated personalised interventions) according to pre-set rules, and the Dashboard (CSB@Dashboard) that provides the visual tools to allow clinicians to have the full profiling and monitoring of the patients to provide them with personalised treatment, and other mechanisms for all user roles supported. As with GIC, the Security Component (CSB@SC) supports the end-user management via a Role-Based Access Control (RBAC) to comply to data minimisation, pseudonymisation for de-identifying data and then transmitting them to GIC for further analysis, transparency in processing of personal data, secure machine-2-machine transmissions so that all sub-components communicate through a secure environment, and other appropriate technical (and organisational) measures to ensure security (i.e., confidentiality, integrity and availability) of data at all states (i.e., at rest, in processing and in transit). In addition to the above, a continuous Security and Privacy Assurance solution will comprise an integrated framework of models, processes, and tools to enable the real-time, continuous security and privacy posture assessment of the RETENTION deployment.

Both the GIC and the CSB (one instance per clinical site) constitute the RETENTION cloud infrastructure where all study participants' data are eventually stored (anonymously and pseudonymously respectively) and analysed using Machine Learning algorithms according to endpoints (clinical questions) defined by the clinical researchers.

The Patient Edge (PE) constitutes the layer of the RETENTION solution that deals with all smart (m)IoT devices and sensors installed at the home of each HF patient who will participate in the RETENTION clinical study. Each PE instance is referring to the personalised smart ecosystem dedicated to each of the monitored patients that embeds a variety of devices and sensors to collect RWD from the individual patients and the environment. The software sub-components of the PE are the Mobile Application (MobileApp), installed in the smartphone and paired with devices to be provided to each of them, that supports the continuous monitoring of the patient via the collection of medical, behavioural, psychosocial, and real-world data for him/her, and the Local Home Gateway responsible for gathering data from home sensors and their transmission to the CBS that the patient is associated with.

Types of devices and sensors that will be handed to the patients are: i) a Smartphone, ii) a Weight Scale, iii) a Smartwatch, iv) a Blood Pressure Monitor, v) an Oximeter, and vi) a pair of Bluetooth Low Energy (BLE) supporting a home temperature sensor, a humidity sensor, and the Local gateway.

The infrastructure of the RETENTION solution (i.e., CIG, CSB, PE) establish a hybrid hosting model to support automated continuous integration and delivery all the way through an uninterrupted process, ensuring (Best-effort delivery) that RETENTION solution will be up and running. To support this goal, an infrastructure lifecycle management will be adopted to successfully handle the capacity of the available resources and their optimisation, based on the resource forecasting. As part of the infrastructure monitoring, most of the system modules will be executed in virtual assets (virtual machines).

2 About this Document

This document corresponds to "D3.2 RETENTION Architecture", the second deliverable of "WP3- RETENTION Clinical and System Requirements & Platform Design", describes the work and the outcomes of "Task 3.3- RETENTION Platform Architecture & Design", and forms the conceptual design and architecture for the RETENTION project, developing a conceptual architecture adhering to the identified end-user requirements (presented in D3.1). It presents the overall architecture of the RETENTION platform, including the general representation of the architecture, detailed component descriptions that constitute the architecture, along with functionality and access interfaces of the RETENTION Patient Edge (Edge), the RETENTION Clinical Site Backend (CSB) and the RETENTION Global Insights Cloud (GIC) instances, the main components that constitute the RETENTION platform.

2.1 Role of the deliverable

The scope of the deliverable is to introduce the detailed architecture of the RETENTION platform with the aim to coordinate the implementation of the various technical components that constitute it. All supported hardware and software components, the interactions between them, the interfaces to the users and any other needed elements, will be thoroughly described in this document. The document is based on the DoA of the RETENTION, and the user requirements' elicitation (presented in D3.1), that defined the functional and non-functional requirements of the platform and main use cases to be supported.

Dedicated meetings and two workshops (see Appendices 6 and 7) with the participation of both technical and clinical partners have been performed to gather directions and feedback towards the finalisation of this deliverable. The outcomes of those determined priorities and technical aspects to be supported by the Platform, were in particular:

- the functionality constraints and capabilities to drive the Platform development
- to identify the security layer of the architecture to ensure adherence to the Privacy by Design principle and in general GDPR compliance
- to specify the interfaces and structural relations between different components of CIG and CSB
- to define the dependencies between components based on their interfaces
- to identify data flows, access control, data storage

The resulted RETENTION architecture is based on these requirements identified. In this context, secure interactions and privacy of data were considered as of high importance during the design stage.

Although the architecture was thoroughly designed, and all aspects of the system are based on the most reasonable current industrial-strength solutions to support requirements defined (in D3.1), still there is a probability of new (currently not supported) requirements to emerge during the project to serve new needs. Depending on the differences in relation to the version of the architecture reflected in the following, if significant differences occur this deliverable will be resubmitted, or in case of minor component-related changes those will be reported within the relevant (to each component) deliverable. In any case, all changes/amendments will be documented and justified.

2.2 Relationship to other RETENTION deliverables

This document constitutes the basis of most of the deliverables of the RETENTION project. The presented architecture will drive the work of WP4, WP5, WP6, WP7, part of WP8 and part of WP9, and will be the basis of:

- the Platform itself
- the technical evaluation of the system (together with the Requirements' Document)
- the D4.1 RETENTION Data Model, which generates the design & specification of the RETENTION Data Model, enabling the exchange, storage and processing of the heterogeneous data aggregated and generated during the platform's operation
- the D4.2 RETENTION Data Management enabling mechanisms version 1, and D4.3 RETENTION Data Management enabling mechanisms version 2, which describe RETENTION data repositories and data transfer and handling mechanisms (initial and final)
- the D5.1 RETENTION Analytics & Decision-making enabling mechanisms version 1, and D5.2 RETENTION Analytics & Decision-making enabling mechanisms version 2, which describe the delivery of the models, processes and components enabling the analytics, decision-making, and data and model sharing capabilities of RETENTION platform (initial and final)
- the D6.1 RETENTION Interfacing, Device Federation and Visualisation components version 1, and D6.3 RETENTION Interfacing, Device Federation and Visualisation components version 2, which describe the RETENTION Mobile Application, Gateway, and smart devices' federation, as well as CSB and GIC dashboard and visualisation components (initial and final)
- the D6.2 RETENTION Security & Privacy by design enabling mechanisms version 1, and D6.4 RETENTION Security & Privacy by design enabling mechanisms version 2, which describe the Security & Privacy mechanisms, including the two Continuous Security and Privacy Assurance Platform variants (initial and final)
- the D7.1 Integrated RETENTION platform version 1, and D7.3 Integrated RETENTION platform version 2, which include the delivery of the first (and second) version of the integrated RETENTION platform involving the first (and second) release of all components of WP4, WP5 and WP6 (initial and final)
- the D7.2 Report on integrated RETENTION platform version 1, and D7.4 Report on integrated RETENTION platform version 2, which are reports documenting the integrated platform's (a) functionalities and any amendments made to the original architecture and design, (b) outcomes of platform testing and (c) installation, deployment, and usage guidelines for the platform (initial and final)
- the D8.4 RETENTION Clinical & Technical Assessment & Validation Report version 1, and D8.6 RETENTION Clinical & Technical Assessment & Validation Report version 2, which describe intra- and inter-Clinical Trial's assessment & validation, and the platform's technical validation reports (initial and final)
- the D9.3 Communication, Dissemination, Impact Creation, Exploitation & Standardisation Report (interim), and D.9.5 Communication, Dissemination, Impact Creation, Exploitation & Standardisation Report (final), which describe dissemination, communication, impact creation, exploitation, and standardisation activities for the first half and second part of the project.

2.3 Structure of the document

The structure of this deliverable is as follows:

- Chapter 1 provides the Executive Summary.
- Chapter 2 is about this document and presents its role and relation with other RETENTION deliverables, the structure, and an overview of the User Requirements' document.
- Chapter 3 describes the RETENTION conceptual and detailed architecture. It starts by presenting the overall architecture starting from an overview, continuing with the relevant diagrams and justifications, and then continues by providing a complete description of each of the platform components. It specifies sub-components, giving a purpose, an overview, and a description to all layers that constitute the Platform (i.e., the GIC, the CSB, the PE and the devices/sensors).
- Chapter 4 describes the purpose and the overview of the platform infrastructure deployment.
- Chapter 5 summarises the conclusions derived from the work presented in this document.
- Chapter 6 provides the relevant references.
- Chapter 7 provides the appropriate appendices to the document.

2.4 Brief Overview of User Requirements' Document

Design-wise, the Platform constitutes of 3 layers:

- The Global Insights Cloud (GIC) supporting the management of analytics,
- The Clinical Site Backend (CSB) providing mechanisms for (each) clinical site clinicians to manage and operate on patients' data, and,
- The Patient Edge (PE) gateway where all the patient-associated devices/sensors reside and are being operated.

RETENTION has as a technical aim to integrate heterogeneous medical devices and sensors, smartphones and "smart home" equipment (all constitute the Patient Edge layer), to enable the continuous data collection from the everyday life of the RETENTION study participants, which will be later transmitted to the CSB and in turn to the GIC, to be analysed and obtain the evidence needed for vetted (by clinicians) personalised interventions promoting their health status. RETENTION will leverage big data analytics and learning capabilities, allowing for large scale analysis of the collected data, to generate this type of evidence required. To address this scope, the deliverable D3.1 provided a basic understanding of the mechanisms that RETENTION Platform must support, as seen from the point of view of the end-users, focusing on the requirements of clinicians, patients (or carers), data scientists, and administrators.

Considering the primary target group of the RETENTION end-users to be supported (Heart failure -HF- patients), a patient-centric design methodology has been followed via surveys and interviews conducted during the 1st year of the project with clinical partners to make sure that all their needs, within the scope of the RETENTION project, would be supported. As a result, several clinical use cases and procedures identified provided the fundamentals upon which the RETENTION Platform architecture has been formulated. Parameters considered were the RETENTION clinical study characteristics and the related risk factors, including the detailed list of variables resulting from current clinical practices and state-of-art research that should be monitored. In particular, in accordance with the Clinical Protocol (presented in D8.2) and the user requirements' analysis (presented in D3.1), the main set of variables to be monitored includes:

- Vital signs (blood pressure, heart rate, oxygen saturation).
- Activity tracking (steps, meters walked, other type of activities, continuous HR monitoring at baseline and during activity, time to recover).
- Sleep (hours of sleep, sleep patterns and quality).
- Possible symptoms (fatigue, dyspnoea, oedema, orthopnoea, appetite, dizziness).
- Medication adherence.
- Nutrition information (body weight, body composition, nutrition score).
- Possible depression symptoms.
- Cognitive status.
- Environmental variables (temperature, humidity, pollution) via home sensors or other external services.
- Ventricular assist device related variables (flow, power, pulsatility Index, alarms, etc.) via external services, photos, or questionnaires.

D3.1 also focused on defining the platform's functional and non-functional requirements from technical perspective (e.g., interfacing capabilities, supported interactions, compute and networking capabilities), conducting an up-to-date analysis of the pertinent technological landscape and the identification, specification, and prioritisation of system requirements for it. In addition, and considering the serious security threats, potential security vulnerabilities, and the privacy of the collected data within the EU regulatory landscape, security requirements cover areas such as end-user management, authentication, authorisation, and role-based access control (RBAC) management, pseudonymisation, logging mechanisms for auditing purposes, GDPR requests' management and continuous monitoring via security and privacy assessments. As an end-result, D3.1 provided the set of non-functional and functional requirements which were identified, and categorised in terms of basic functionalities, usability, performance, availability, and reliability, legal and ethical, security and privacy, data and data exchange and scalability such as the following categories:

- Authentication/Authorisation: use cases defined on which flows user identification and m2m validation is required, as well as role-based access to the data collected/generated and services.
- Privacy: since RETENTION involves the management of personal data, data stored will be pseudonymised within the context of the CSB instances and anonymised within the context of the CIG instance.
- Data acquisition: 1st version of data sources, structures, and acquisition rate was defined.
- Data flows/services: workflows to support the clinical monitoring of patients (continuous monitoring and collecting medical, clinical, physiological, behavioural, psychosocial data), the analysis of this data (using model-driven big data analytics, statistical and machine learning techniques), the detection of patterns in the HF disease progression and the quality of life of patients, the analysis of all those results and the support of rule-based personalised interventions.

The resulted use-cases target the three primary groups of RETENTION end-users:

I. the patient (study participants) (PE),

II. the carer (or caregiver) (PE), and

III. the clinical team (clinician or clinical expert) (CSB – GIC)

Still, functional, and non-functional requirements cater the basic needs of all other end-user groups to be supported, in particular: iv) administrator (CSB- GIC), v) data scientist (GIC), vi) policy maker (GIC), vii) tech support (CSB), and viii) (GDPR) auditor (CSB- GIC).

Considering the patients and the interactivity to medical devices, personal wearables, and smart home sensors, based on the feedback provided by RETENTION clinical partners, the smartphone device was recommended as more appropriate for the purpose (in comparison to a tablet). Via a mobile application, the patient will be able to review his/her measurements and submit them to the CSB, receive reminders (e.g., about their medication) and personalised alerts because of individual data analysis. The smartphone with Wi-Fi connectivity in place (perquisite for study participation) will support fast communication to the responsible for monitoring clinical team (per Pilot), and enhanced data acquiring capabilities since the usage data measured and collected by devices/sensors, and the questionnaires' answers, will be structured, annotated and timestamped prior of their transmission in order to meet the specific technical specification for the 2 types of repositories to be used (a FHIR and non-FHIR one).

All patient indicators will be monitored and based on a predefined period, while rule-based interventions/alerts can be created and transmitted to those individuals. Specifically for critical use cases (e.g., adherence to treatment), in cases of metrics indicating critical deviation from expected values, notifications will be sent to both the associated (to the individual) clinicians (CSB end-users) and to those specified as persons to be notified in such events (e.g., informal, or formal caregiver(s), relatives, non CSB end-users).

Since interoperability to external Personal Health Record (PHR) system will not be considered during the pilot phase due to security restrictions imposed by hospitals, during the first phase of the RETENTION project all clinical Personal Health Record (PHR) parameters will be inputted by the clinicians. M2m interoperability can be implemented under specific terms and agreements between the pilot organisations and the RETENTION.

Based on the user requirements, a range of different use cases and scenarios are described. This approach provides the opportunity for the end-users to describe how they conceive the use of the platform. The outcome of this process is summarised in the following table (Table 1).

Table 1: Summary of use cases (as per D3.1 Requirements)

Category	Use case code (in D3.1)	Name	Importance (priority)
Clinician's use cases	RTCL01	Creation of patient and data visualisation	Mandatory
	RTCL02	Patient-doctor interactions	Mandatory
	RTCL03	Alarms	Mandatory
	RTCL04	Event record	Mandatory
Patient's use cases	RTP01	Daily data entry	Mandatory
	RTP02	Special variables	Mandatory

	RTP03	Special events	Mandatory
	RTP04	Automatic messages	Mandatory
Carer's use cases	RTCA01	Daily data entry	Mandatory only for LVAD patients
	RTCA02	Automatic messages	Mandatory
Risk assessment generated by AI	RTBD01	Risk assessment generated by AI	Mandatory
Technical staff use cases	RTS01	Dashboard End-user moderated registration	Mandatory
	RTS02	Dashboard End-user login	Mandatory
	RTS03	Manage end-user account information	Mandatory
	RTS04	Associating a device ID to a patient	Mandatory
	RTS05	Configuring a device and App	Mandatory
	RTS06	Managing Public health policy decision-making models	Mandatory
	RTS07	Performing GDPR compliance check	Mandatory

Based on these definitions, the following representative use case diagrams illustrate the expected behaviour of the to-be-developed services.

Clinician's use cases

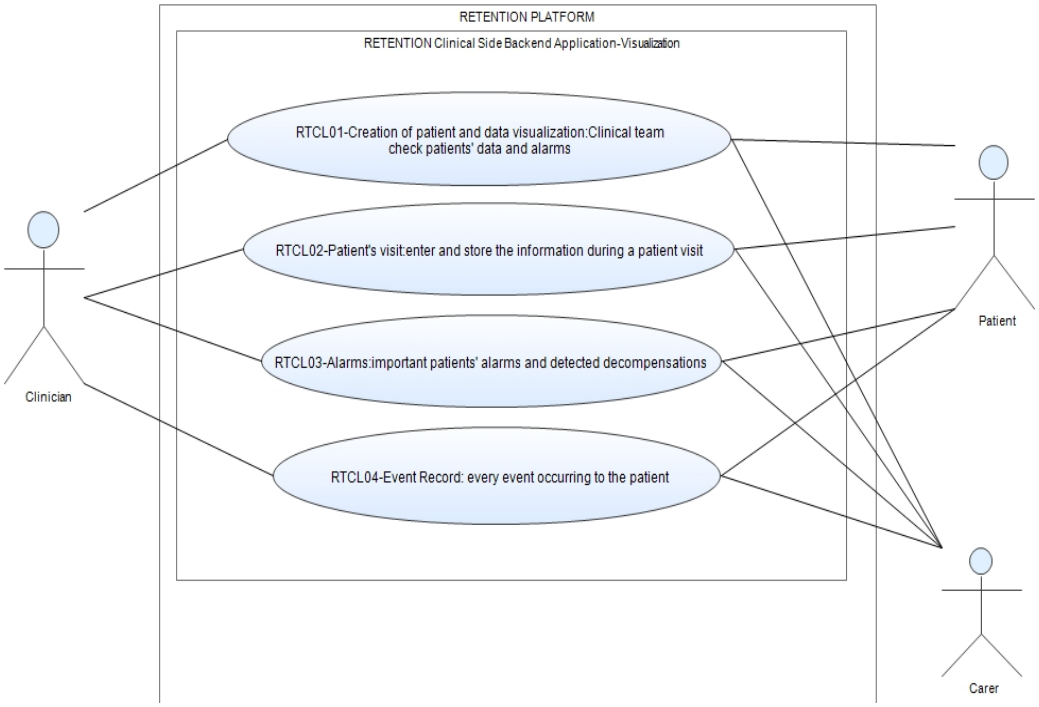


Figure 1: Clinician's use cases

Patient's use cases

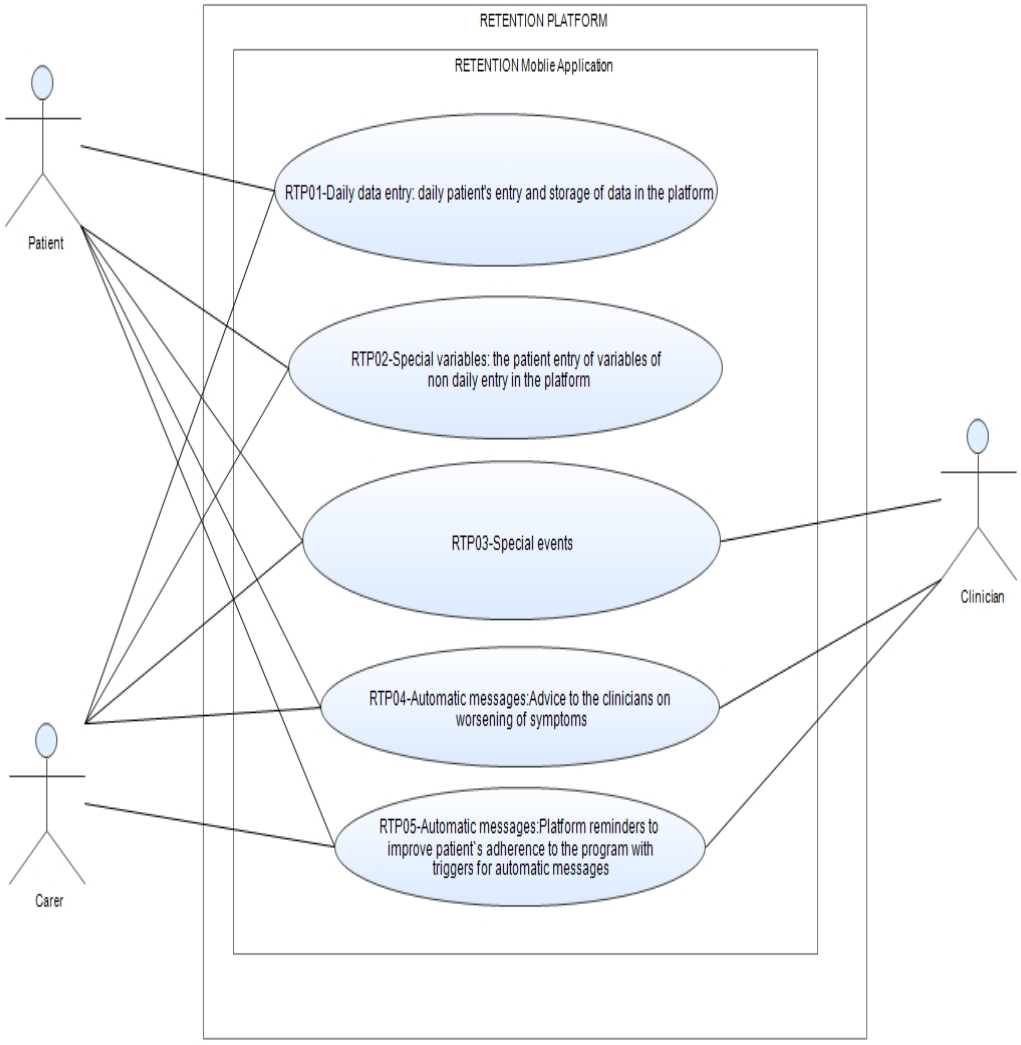


Figure 2: Patient's use cases

Carer's use cases

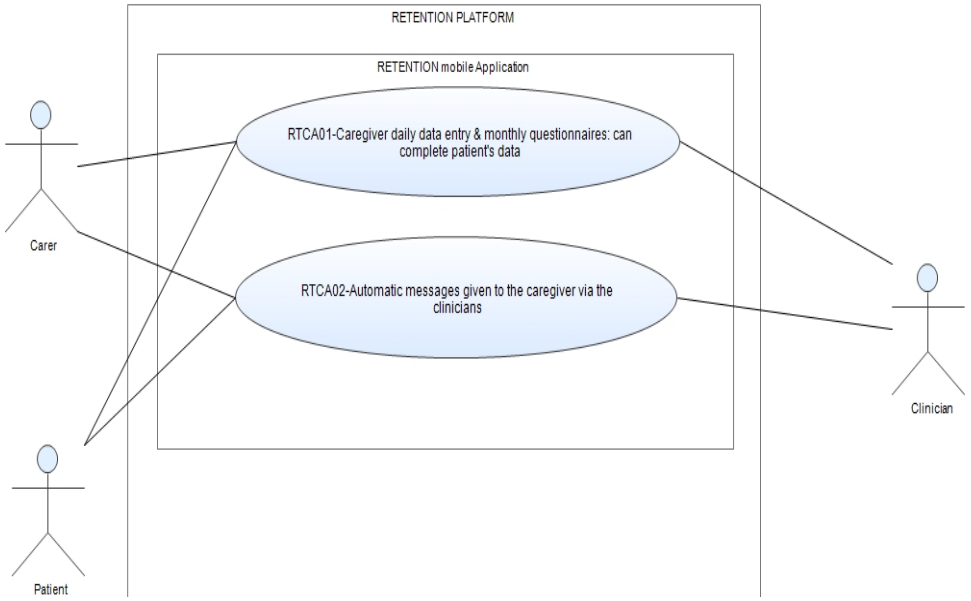


Figure 3: Carer's use cases

Example of an ML analytic: Risk assessment model

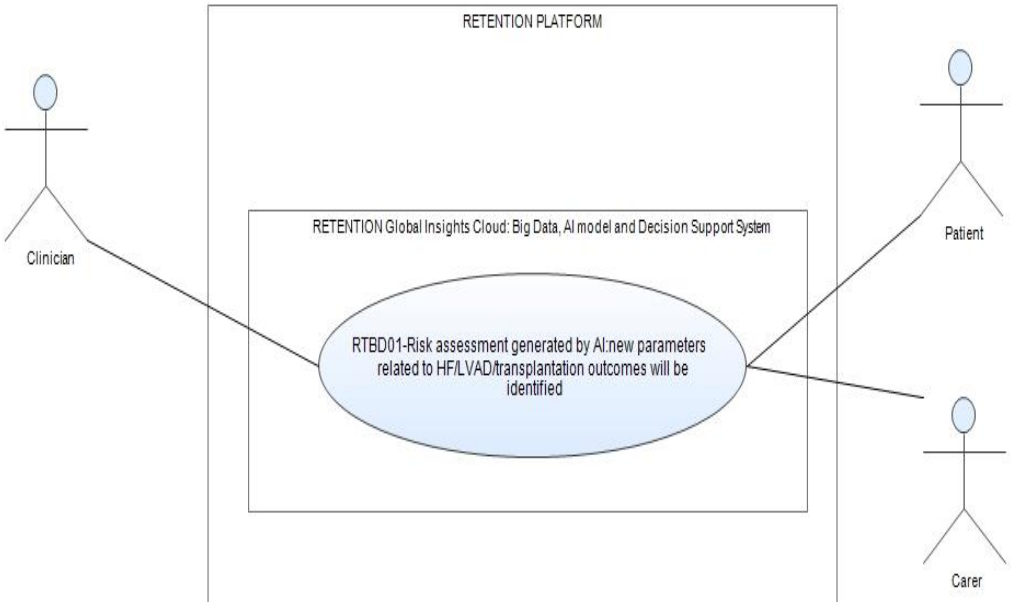


Figure 4: Actors interacting with an ML model

Technical staff's use cases:

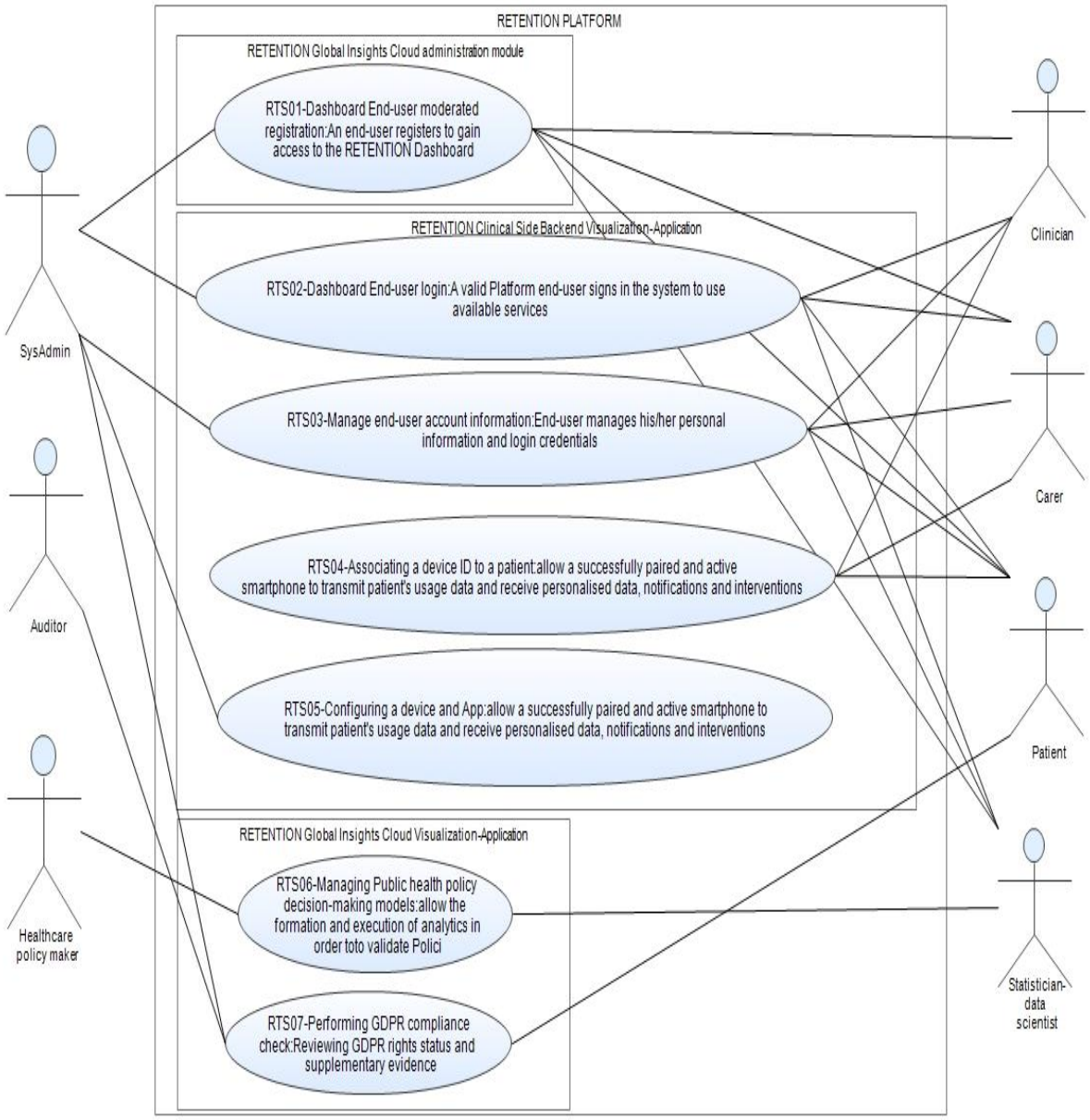


Figure 5: Technical stuff's use cases

3 RETENTION conceptual and detailed architecture

The purpose of the system architecture activities is to define a coherent, comprehensive solution to the RETENTION platform, based on principles, concepts and properties that are related and functional to each other in a logical way. In the following, a detailed description of the architecture of the RETENTION system is provided outlining the conceptual model, logical diagrams, and descriptions of each component that constitutes it.

3.1 RETENTION actors

The supported use cases (defined in D3.1, briefly presented in previous section) are associated with different end-user roles. We identified the following:

- System Administrator or IT/administrative staff: it refers to those responsible for the setup and reliable operation of the RETENTION Platform (GIC, CSB and MobileApp and Local Home Gateway). They should be able to ensure that the uptime, performance, resources, and security of the computers they manage meet the needs of the other users. The administrator may require access to the system components and to the registries accounting for the behaviour of the RETENTION Platform. Also, they manage the end-users' accounts of GIC and CSB.
- Clinician: it refers to a health care professional that works as a primary clinical case manager of a patient. A clinician diagnoses and treats patients (associated to a clinical site). The clinician uses the RETENTION platform (CSB) to increase the level of evidence-based practices and care plans and has access to all patients associated to his/her organisation.
- Patient: it refers to the patient who gave consent to participate to the RETENTION study (RETENTION study participant). He/she interacts via the Mobile application to provide usage data and feedback, and to acquire guidance or information about the treatment and the trajectory of personalised care plans.
- Carer (Caregiver): it refers to people providing formal or informal care (family caregiver, a respite caregiver, a home caregiver, or a primary caregiver) to the patient who needs extra help (acts on behalf of the patient).
- Data Scientist: it refers to a professional responsible for collecting, analysing, and interpreting the overall amount of data collected by the GIC.
- Healthcare policy maker: it refers to someone who exploits the statistical report and analytics resulting from the GIC to create policies and plans, especially for the good of a territory or community.
- (GDPR) Auditor: it refers to the role that is responsible for administering audits to the RETENTION platform (with the help of the admin, the DPO, and other project officials).
- Tech support: assisting the clinician only in the task of monitoring the usage data transmission monitoring (metadata).

3.2 Overview

The Architecture is based on a 3-Layer model (arises from a structured IoT architecture, modified for the RETENTION project):

Global Insights Cloud	The GIC functions as the main Big Data repository that hosts the Big Data analytics engine and services to support the policy making, offering to the Data scientist, clinical expert, or healthcare policy maker the tools to take the necessary decisions about Heart Failure disease management.
Clinical Site Backend	The CSB offers to the clinicians the tools to monitor their patients, gather their medical and usage data (evidence) and take "informed" decisions about them.
Patient EDGE	a) A mobile application and b) the home gateway, support the continuous monitoring of patients and the collection of real-world data associated to them.

Those layers interact with each other via secure channels, while data exchanges involve pseudonymised or anonymised data to ensure full data protection even in the case of a data breach. Briefly, the role of each layer is:

- Global Insight's Cloud (GIC): a cloud instance that is common for all RETENTION deployments and which is responsible for managing anonymised data & model ingestion and training, global analytics, and the generation of insights. Upon completion of best (performance-wise) trained models, those will be "pushed" to the Clinical Site Backend instances for application.
- Clinical Site Backend (CSB): per hospital backend instances of the platform, responsible for patient data management, local decision making, execution of analytics & interventions.
- The Edge (Gateway, Mobile Application, and home hub): a set of components deployed at the patients' environments, managing the devices'/sensors' usage data, questionnaires' answers and personalised notifications and alerts.

The following diagram (Figure 6) illustrates the Conceptual Architecture of the RETENTION Platform. Each component is self-reliant and has a specific function in the whole operation of the system. Architecture will be described in detail by the 4+1 model.

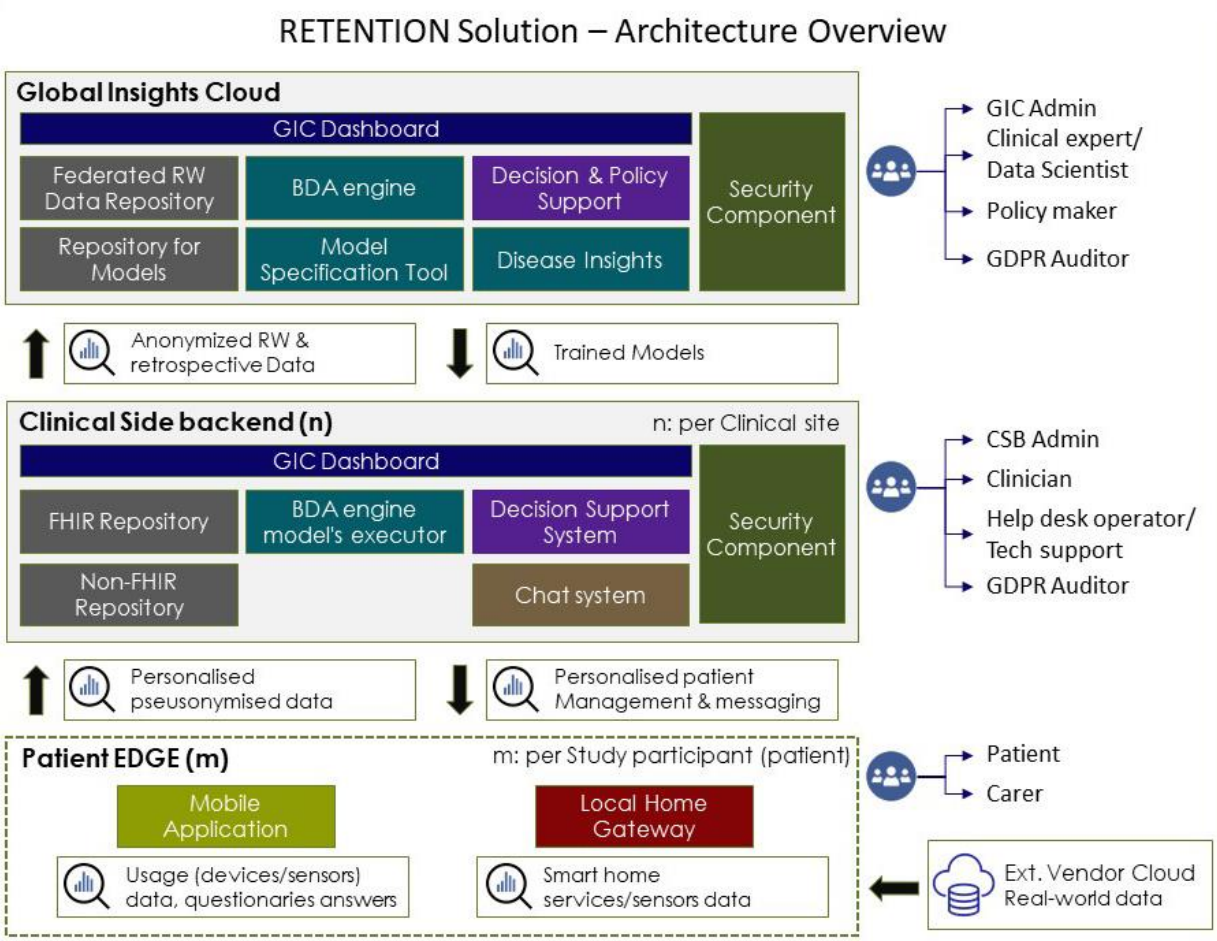


Figure 6: Overview of the RETENTION Architecture and actors operating within each layer

The RETENTION Platform will attain a level of man-machine interaction of the highest standards to enable user-friendly interactions for handling the complexity of workflows and their outputs, coping with the output of complex models, the verification of those via the visualisation of the knowledge encoded, and presentation of interventions.

To cope with this complexity, the design of the user interface will adhere to the following basic design principles:

- Provide simple and intuitive interfaces,
- Adhere to modern design principles (e.g., responsive web design, best practices for colour-coding, form design and data table design, mobile app usability best practices),
- Use of a modern framework for smartphone development with cross development on both well-established platforms,
- Follow all the provisions of the grant agreement (DoA).

3.3 RETENTION Architecture

The following figure (**Error! Reference source not found.**) illustrates all high-level components of the system, which will be introduced in the next sections in more detail. Components are mainly interconnected via REST

API interfaces, to facilitate integration. The following "Architecture diagram" subsection contains the general architecture description.

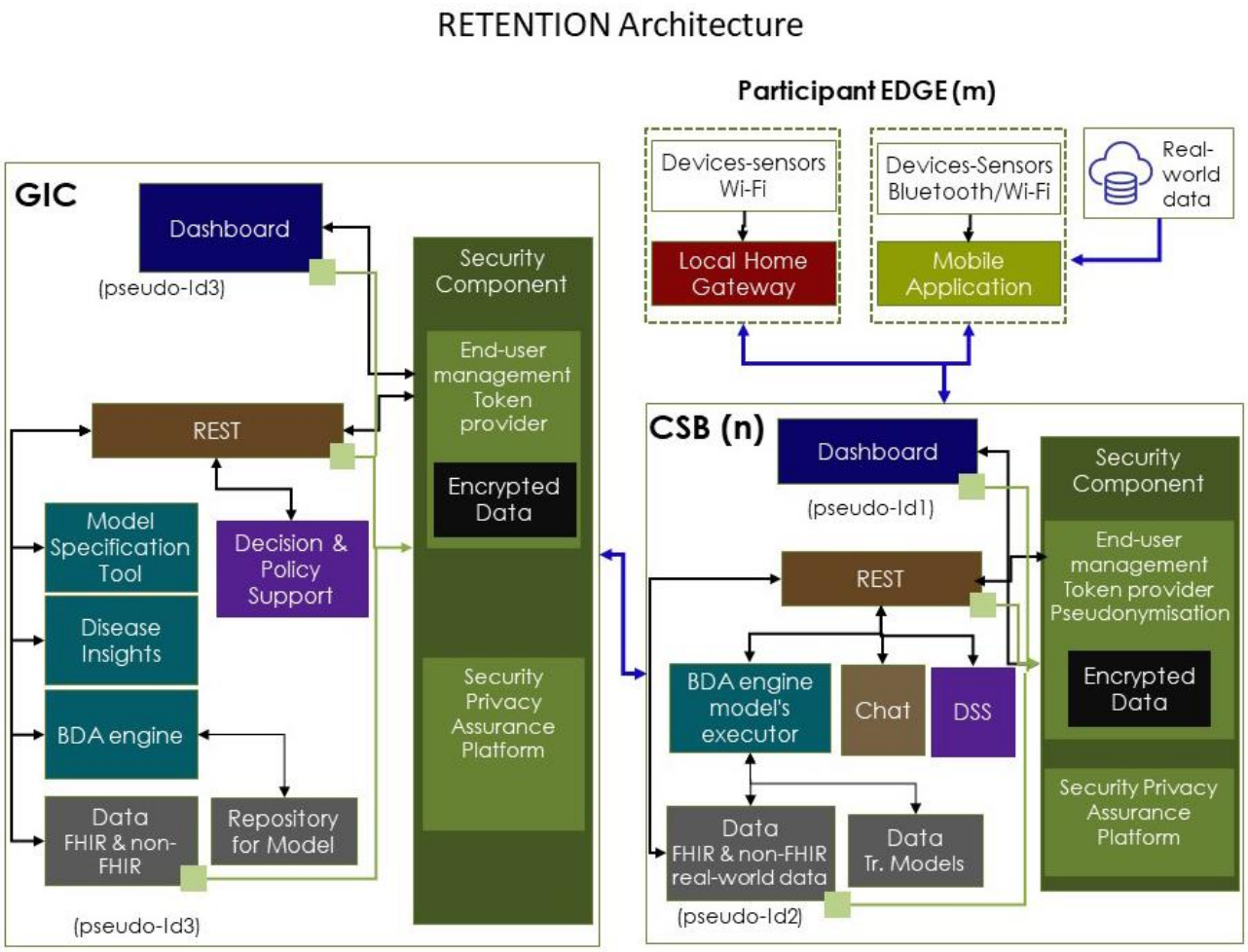


Figure 7: the RETENTION architecture

As defined in D2.2, the whole RETENTION solution (GIC and all 6 CSB instances) will be hosted at a computer room located in ICCS's premises (Athens, Greece). A CSB can be deployed within a clinical site infrastructure, provided that technical and operational requirements are met.

3.4 Architecture Diagram

The previous figure shows the overall RETENTION architecture. As can be seen, there are three main layers: i) the Global Insights Cloud, ii) the Clinical Site Backend, and iii) the Patient EDGE. The main purpose of these and their components is to accumulate, store and analyse the data gathered from different sources. Each Dashboard allows to input data and operate upon services provided. Both Dashboards are interacting with other components via REST interfaces. The REST layer provides the interfaces not only for the Dashboard but for m2m connections such as those triggered by the Mobile Application and the Local Home Gateway. Additionally, REST services provide interaction capabilities to the BDA engine and Data Repository with the different repositories reside in GIC or CSB. These repositories hold all information retrieved from devices,

sensors, mobile phones, and the BDA engine itself. Each instance of CSB interacts with the Local Home Gateway and the Mobile application (for those patients associated to the client site that operates the CSB) again through REST interfaces. The Local Home Gateway is the subsystem accumulating inputs from house-bound sensors, while the Mobile Application deals with the medical and non-medial (health and fitness) devices. This type of information is pre-processed (e.g., timestamped, aggregated, associated with a unique identifier for each participant) and sent to the CSB via REST services in compliance with GDPR rules. Interactions between those components, as well as authentication at the Dashboard(s) are secured by the Security Component, while end-user account information is held inside it.

Functionality per level and actor, according to the above two diagrams:

- Patient (PE):
  - Data collection level: Devices and sensors are connected (paired) via a) the mobile application and b) the edge gateway that collectively act as the patient EDGE.
  - Patient operates devices and sensors and transmits (effortless) usage data to the CSB.
  - Patients and carers (on behalf of those unable to operate themselves) have access to the Mobile application, can provide feedback (via questionnaires) or photos, chat (functionality will not be activated in the framework of the RETENTION trial study to avoid bias), and receive personalised notifications, depending on patient's condition.

  Carer: may act on behalf of a patient.

- Clinician (CSB):
  - Clinicians manage personal health record and questionnaires' data for those patients they are supervising, and view via the high level and detailed visualisations, the device/sensors' usage data being transmitted into the CSB.
  - Data stored in each CSB will be pseudonymised. Only designated clinicians have access to author medical and personal data of CSB patients.
  - Trained models can be applied to obtain a prognosis about several health indicators. In addition, the system will also generate suggestions to be considered by the clinicians relevant to the triggering of personalised interventions.

- Administrator (CSB and GIC):
  - Manages end-user accounts (e.g., accepts/rejects registration requests).
  - Is held accountable for answering to GDPR requests raised by study participants.

- Data analyst (GIC):
  - Manages ML models (the whole ML pipeline) and triggers the broadcasting to all CSB instances of those considered of best performance.

- GDPR Auditor (GIC):
  - Views GDPR request(s) issued by patients and whether they have been responded to.

- Healthcare policy maker (GIC):
  - Reuses outcomes of the ML analytics to create and evaluate health policies and plans.

- Tech support (CSB):

- Monitors the usage data transmission and triggers communications for technical assistance over the phone or email.

The following image (Figure 8) illustrates the physical view of the RETENTION Architecture. The virtual machines can run independently.

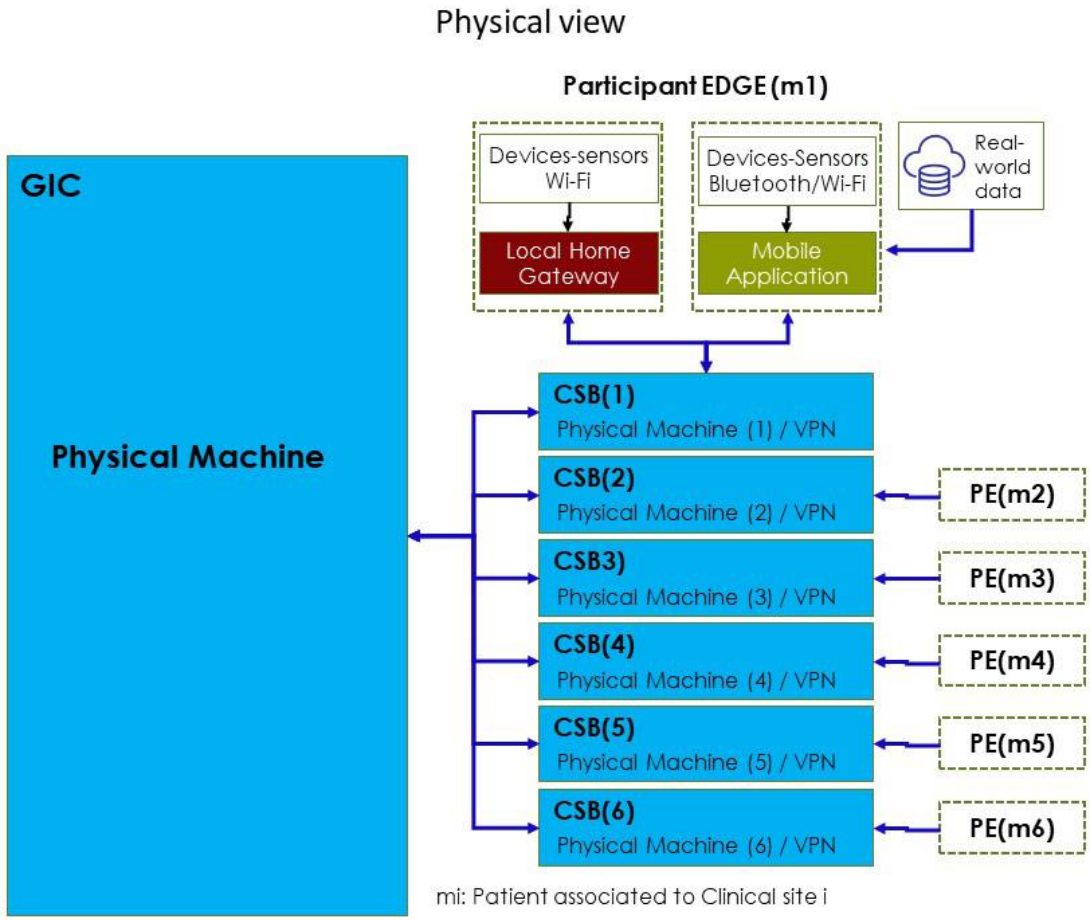


Figure 8: Physical view of the RETENTION system

The "physical machine" associated with each RETENTION clinical site is completely and logically independent module that can be used, moved, expanded, or contracted according to needs specified.

3.5 Components Description

The next sections introduce the different components identified above, and present to the readers an analytical description of their utility and how they fit the overall architecture. Their detailed interfaces are specified in the respective appendices. Cross-cutting, security-related components are described in section 3.5.5 Security Component) and Appendices.

Enriched technical descriptions of all components forming GIC, CSB and PE will be presented during the forthcoming deliverables of WP4, WP5 and WP6.

3.5.1 Global Insights Cloud (GIC)

The first module, named as the RETENTION Global Insights Cloud (GIC), will pool anonymised patient data from all sites (CSB instances) and will support the advanced forms of global data analytics that will result in trained ML models which will underpin evidence-based interventions. This module supports incremental forms of data analysis, necessary when new data sets become available to the GIC and the model verification capabilities envisaged for the platform, as well as the analysis of the findings for the purposes of public health decision making. Once models are trained, those can be transferred to the second (middle) module (RETENTION Clinical Site Backend) to be applied and generate suggestions/hints to be considered by the clinicians for triggering personalised interventions. The GIC is composed from the following modules that interact with each other:

- **Dashboard** that allows end-users to set up and execute ML workflows, and in turn validate the resulted models (through the Analysis Workflow Validation tool), and broadcast those of best performance. It also provides interaction elements for the Decision & Policy Support component's functionality. To provide these functionalities, the Dashboard behaves differently based on the role assigned to the end-user by the Role-Based Access Control (RBAC) capabilities of the Security Component.
- **Model Specification Tool** that manages machine learning models; **Disease Insights**, an extension of the Model Specification Tool which allows the data scientist to understand and evaluate better the previously created models.
- **Big Data Analytics Engine** (BDAE) that parses, filters data and feeds the Model Specification Tool.
- **Decision and policy support** is a service that capitalises on the results gained during the ML workflows to assist the evaluation of health policies that account those as (success or failure) criteria.
- **FHIR and non-FHIR repositories** where anonymised data are stored, and model data are registered.
- **REST API** support inner and outer (previously authorised by the Security Component) communications with GIC components and CSB.
- **Security Component** supports the authentication and authorisation processes, along with mechanisms to protect services and data flowing from/to the GIC (data in transit) as well as while data reside within repositories (data at rest).

3.5.1.1 GIC Dashboard (GIC@Dashboard)

The GIC Dashboard (or Dashboard & Visualisation component) offers user friendly visualisations and interfacing features tailored to the specific information and functions taking place at the global backend (features presented in the following Table 2).

Table 2: GIC Dashboard features and specification

Component Title	GIC Dashboard
Objectives / Brief description	The GIC dashboard and visualisation component will serve as the entry point for clinicians, researchers, policy and decisions makers, and auditors in the healthcare sector to the collected data sets and trained models. This data includes pseudonymised health related and monitor-related data from various sources as well as statistics that will be presented in a multipurpose interface addressing the needs of targeted stakeholders.

Technical pre-requisites and requirements	REST APIs are required to fetch/submit data. The visualisations will be offered via a unified web application based on AEGIS' Advanced Visualisation Toolkit (AVT). End-users will only need a browser to access the GIC@Dashboard.
Actors	The actors of the component are: - GIC Admin - Clinical expert/Data Scientist - Policy maker - GDPR Auditor
Interactions Inputs	Input of the component must be provided as an API or via some other method, e.g., direct access to the relevant data. The component will offer interaction with different types of users, therefore role-based access to different parts of the interface will be realised.
Interactions Outputs	Outputs of the component are the triggered events based on user actions that can include: - storing data in GIC repositories - trigger other GIC components (e.g., disease insights component) - export or visualise data in meaningful manner
Data format	inputs (preferably) in JSON format

3.5.1.2 GIC Model Specification Tool (GIC@MST)

The Model Specification tool serves as a prerequisite framework to allow the GIC Disease Insights and the GIC BDA engine to run. This framework provides processes for feeding the BDA engine with different types of data and supports the transmission of trained ML models to the CSB instances. To serve this purpose, it exposes services for managing and training ML models, while their outputs later are to be stored in the GIC repository (Data Models / Model Registry) and handled by the BDA engine processes. It also provides insights for models' prediction performance and model explanation (AI explainability) (features presented in the following Table 3).

Table 3: Model Specification tool features and specification

Component Title	Model specification tool
Objectives / Brief description	This module provides and ex pose the functionalities to train/test models using data from non-FHIR/FHIR database on GIC
Technical pre-requisites and requirements - hardware	Existing VM with minimum 16G RAM, 150 G Hard-drive, 8CPU-cores For large datasets and specific ML algorithms, the training process can take sometimes hours or even days and may consume the existing CPU/RAM resources
Technical pre-requisites and requirements - software	Linux based OS (ex. Ubuntu 20) Docker 20.10.7, Docker-compose 1.25.0 (minimum) The model specification tool will install from docker compose file, Jupyter notebook server The training part will be added as a separated service in the same docker compose file, using the kernel gateway feature provided by Jupiter

Actors	Jupyter notebook kernel gateway docker container Database
Interactions Inputs	Database -> Jupyter kernel gateway Notebook Notebook takes the training data from the Database
Interactions Outputs	Jupyter kernel gateway Notebook -> Database Notebook saves into Database the trained models The training models are serialised as pickle files
Data format.	Input: JSON Database Data Output: binary (pickle) files containing the trained model

Main role of the GIC@MST tool is to create and manage the ML models that will be stored in GIC registries. In following figures (Figure 9 and Figure 10), two sequence diagrams are provided: a) for model creation and b) for model structure understanding. By using GUI tools exposing these mechanisms, the data analyst can take optimal decisions in proposing one model versus another. A series of machine learning algorithms will be tested (test-and-error), and we shall select/keep the most successful (in terms of performance) ones. The evaluation process will be based on selected metrics utilising the GIC Disease Insights module.

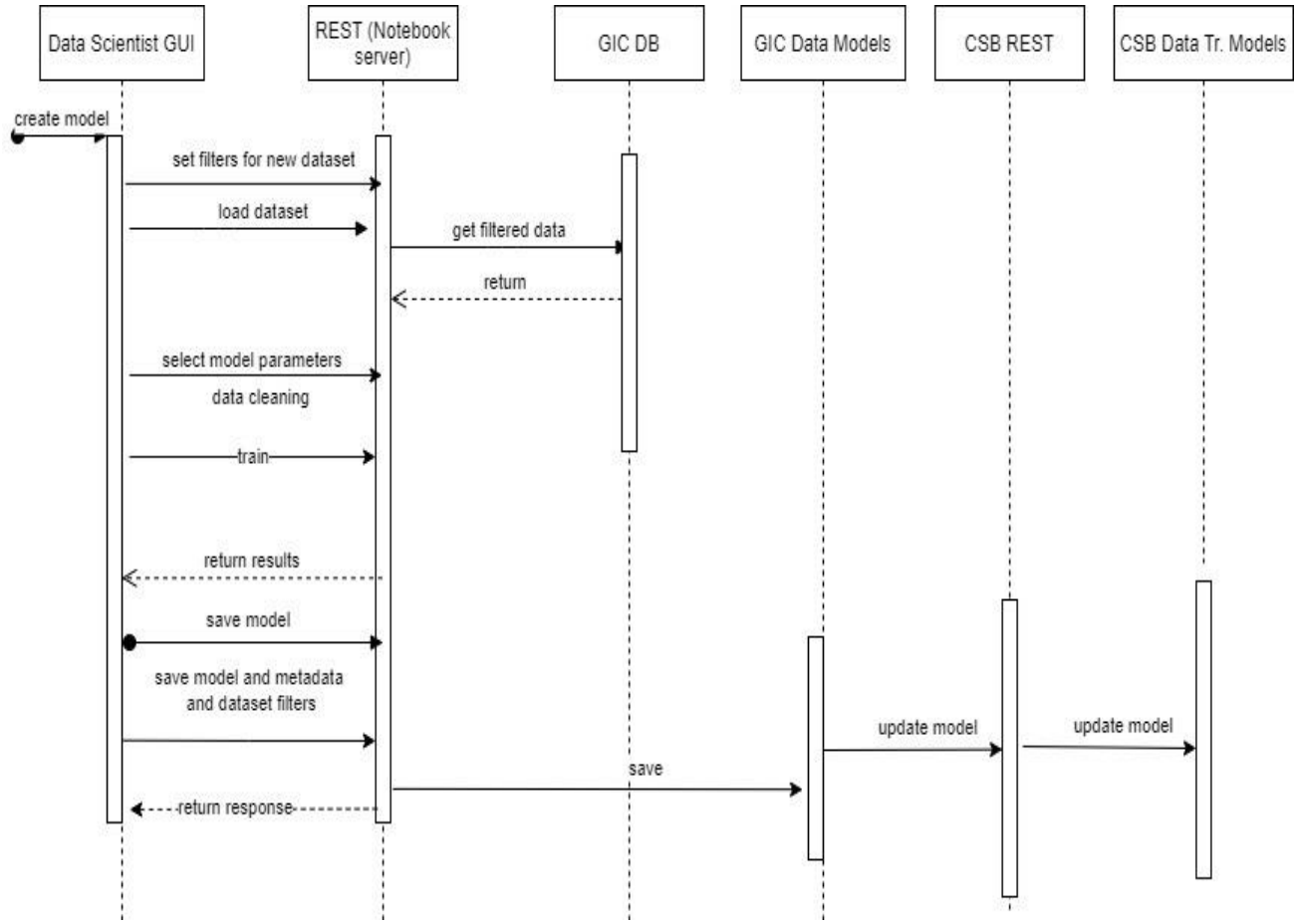


Figure 9: Sequence diagram for a) Model training

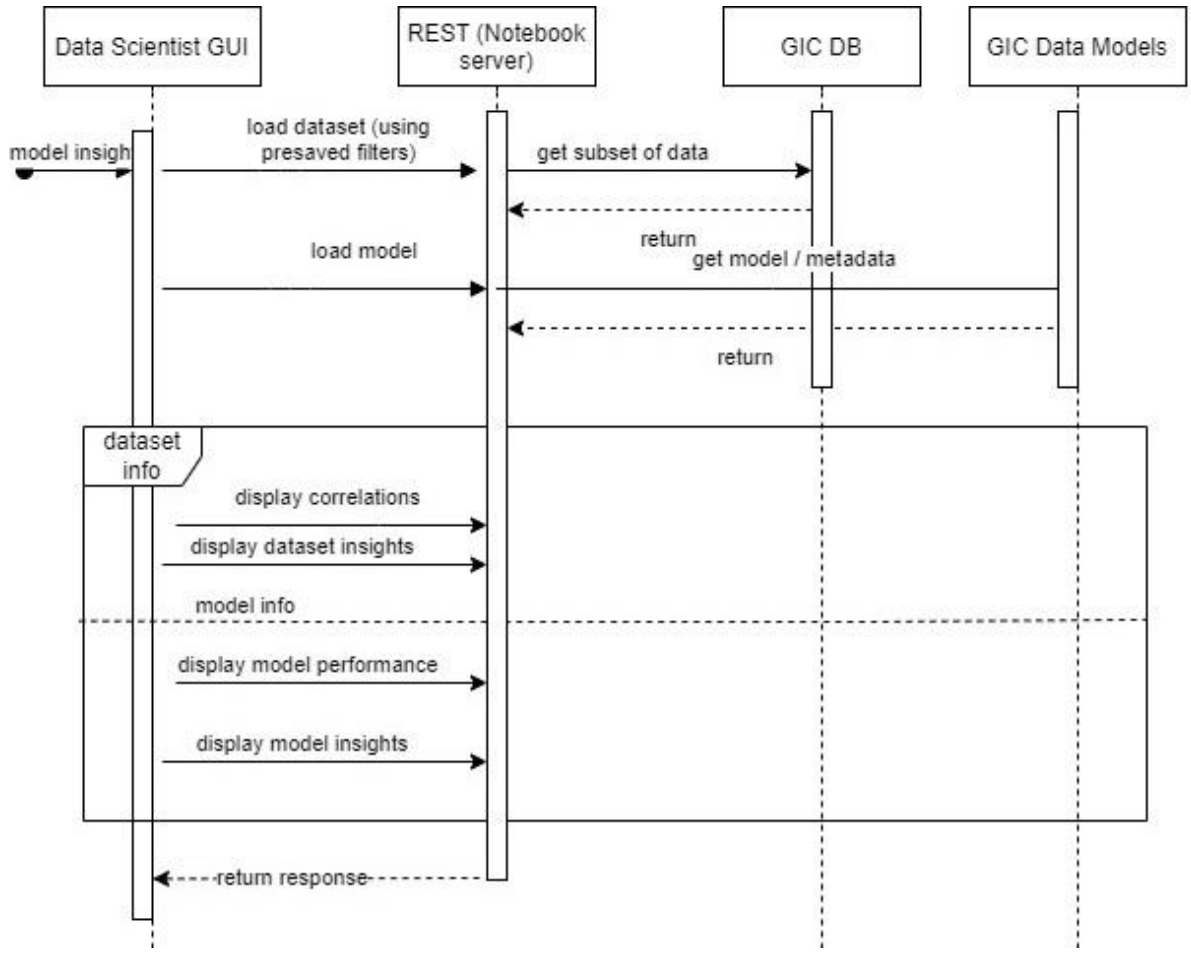


Figure 10: Sequence diagram for b) Model insights

3.5.1.3 GIC Disease Insights (GIC@DI)

The GIC Disease Insights is a module that resides in the GIC and supports the data analyst with the provision of various explanations regarding the models previously trained (mainly the performance of the trained model created with GIC@BDAE). Serving this aim, this module will provide means for model understanding and visualisation of its inner structure and behaviour, offering also explanation (AI explainability) and trustworthiness for the black box of the machine learning models (features presented in the following Table 2).

Table 4 : Disease insights features and specification

Component Title	Disease insights
Objectives / Brief description	This module will provide means for model understanding and visualisation of its inner structure & behaviour
Technical pre-requisites and requirements	Model specification tool Models that have been trained previously + metadata results from training process

Actors	Jupyter notebook containing ML algorithms Database with patient's data
Interactions Inputs	Notebook saves into Database along the models, the model's metadata that provides insights (Confusion Matrix, other model's performance KPIs)
Interactions Outputs	Notebook will provide the model's metadata for further visualisations (GIC@Dashboard)
data format	Input: Filters to restrict data request. Example: for specific use-cases only some models are relevant and thus should be considered. Output: metadata attached to the specific model in a JSON format

3.5.1.4 GIC BDA Engine (GIC@BDAE)

The Big Data Analytics Engine provides the means of communication and transfer of information between the GIC repositories and the Model specification tool. It handles data integration by distributing data and computation, and by efficiently supporting the model training process strongly interconnected with the Model Specification Tool. The GIC@BDAE utilises several strategies that will help succeeding at the training of the models by distributing the data to the ML algorithms within GIC@MST. This component also supports the pre-processing of input data, before serving the resulting dataset to the ML algorithm (features presented in the following

Table 5).

The GIC@BDAE has the technical capacity of handling large quantities of data (Big Data) through various mechanisms such as paging or using other algorithms found in libraries such as Spark (Matei Zaharia, 2016). Depending on the storage environment (best candidate: Spark data processing framework that can quickly perform processing tasks on very large data sets) it offers different modalities to connect to several Big Data sources.

RETENTION's technical team is currently experimenting with the Spark framework. This solution will be tested and validated in next phases of the project. Performance metrics will be compared with other potential alternatives, prior of deciding upon the final choice as for the open-source data processing framework to be utilised.

Table 5 : BDA Engine features and specification

Component Title	BDA engine
Objectives / Brief description	This module will provide with the capabilities of interacting with the three types of databases (CRUD operations) for two main purposes: - Populate input data for model training - Save/Retrieve models and model's metadata
Technical pre-requisites and requirements	Model specification tool Easy to scale -> work with SoA DB engine such as Elasticsearch/PostgreSQL etc Avoid bottlenecks or issues of type "out of memory" when querying data -> implement either data pre-processing mechanism or paging mechanism
Actors	Database – provide large quantities of data BDA engine – written functions that run on Jupyter notebook server from Model specification tool that ingest the provided data and deliver it to training algorithms

Interactions Inputs	Database -> BDA engine BDA engine -> ML Model specification tool
Interactions Outputs	Training models serialised as pickle files + models metadata in a custom format
data format	In – Data read from database Out – Reduced / Processed data to be delivered to ML model training

3.5.1.5 GIC Decision & Policy Support (GIC@DPS)

The Decision & Policy Support component will provide a user-friendly mechanism for supporting "what-if" analysis for the policy makers, subject to the results of the specification of the RETENTION data analytics models (primitive features presented in the following

Table 6). Based on the early user requirements for the GIC@DPS functionality to be supported that serve to guide the GIC system specification, a sequence diagram depicts (Figure 11) the basic function of creating a model that adheres to specific rules.

Table 6 : Decision & policy support

Component Title	Decision & Policy Support
Objectives / Brief description	This module provides the support for policy decision and support mechanism and will provide the user with means for policy rules definitions, modelling, testing and saving
Technical pre-requisites and requirements	Model Specification Tool
Actors	Database Model Specification Tool Decision & Policy Support Tool
Interactions Inputs	Database -> Model Specification Tool -> GIC Dashboard
Interactions Outputs	Policy model handling / Policy outcome analysis
data format	Input: Data read from database Output: Policy model analysis and handling

Presented features consider an estimate (early design) of the functionality to be supported by GIC@DPS considering outputs of ML models. The final version of the component will consider the specification of the RETENTION data analytics models (D5.1).

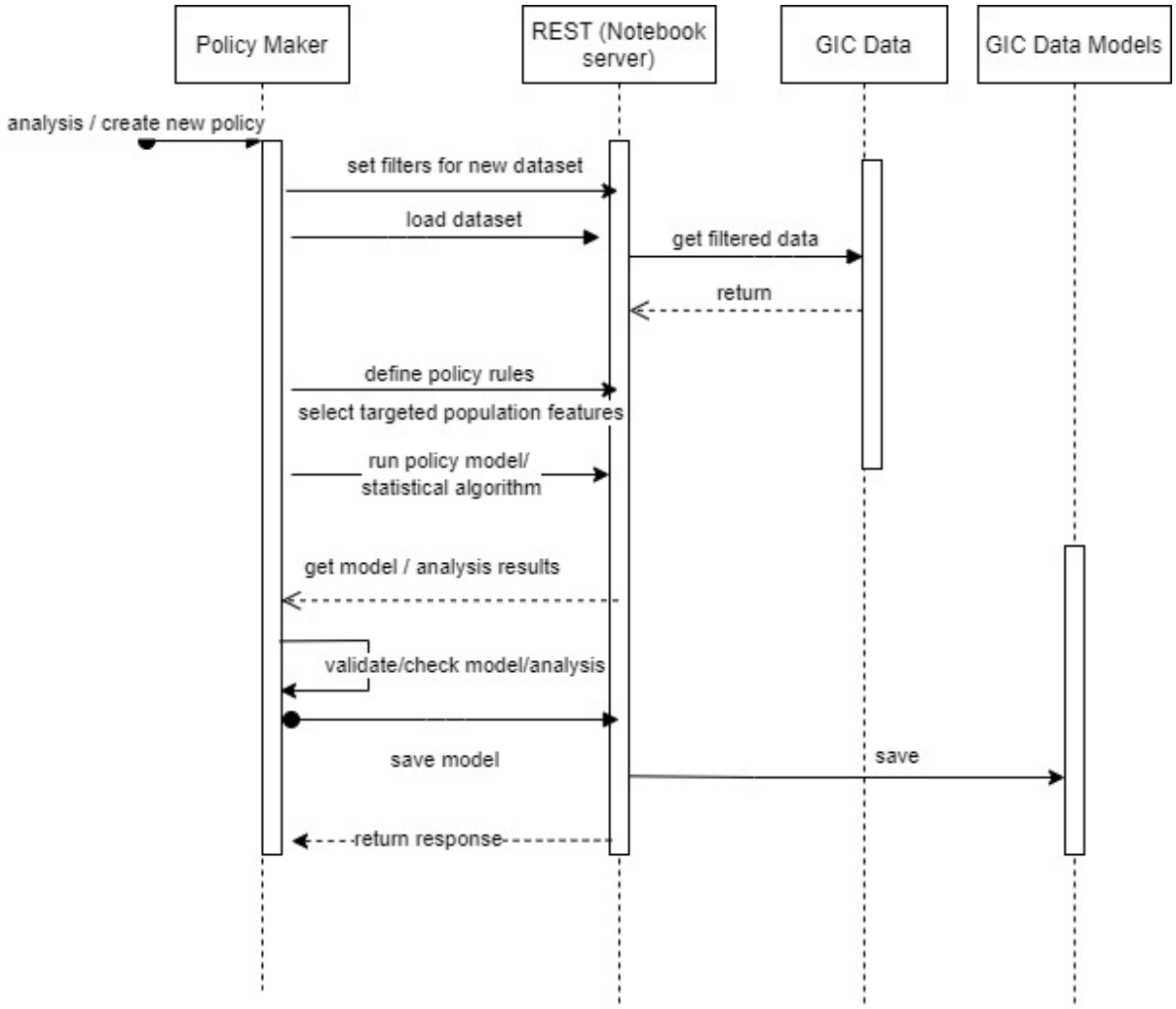


Figure 11 : Decision and policy support model/analysis via GIC Policy Maker Dashboard Actions

3.5.1.6 GIC FHIR and non-FHIR repositories (GIC@Data Layer)

The GIC@Data Layer is consisting of open-source repositories that will host all type of data in a fully anonymised fashion, later to serve the role of being input for training the ML models. As such, the GIC@Data Layer (both FHIR and non-FHIR repositories) refers to the data storage entities into which data will be partitioned for analytical or reporting purposes. The data will be available to the GIC@BDAE to process them with the analytics and decision models. Since the GIC@Data Layer will be supplied with data they have been previously structured and semantically enriched (within the context of CSB instances), these data repositories store structured anonymised data. As with CSB@Data Layer, the organisation of the data will conform to the RETENTION Reference Model. Three main categories of data will be stored:

- FHIR Repository: FHIR data (medical data) using LOINC and SNOMED-CT codes
- Non-FHIR Repository: sensors' data, structures accommodating DSS functionality
- Data Models: data representing input/output of model training process and models themselves

3.5.1.7 GIC REST API

The communication between the deployed components will be supported through REST APIs. The REST architectural style emphasizes the scalability of interactions between components, uniform interfaces, independent deployment of components, and the creation of a layered architecture to facilitate caching components to reduce user-perceived latency and enforce security. Each module/component provides REST APIs to facilitate the data interactions based on the specifications provided by each component.

The REST API will be under the auspices of the GIC Security Component. Thus, interactions between components via REST services, as well as authentication are secured by the Security Component (GIC@SC). Access to services (and data) is only provided once the end-user has been successfully authenticated, and has a role granted with this access. The GIC@SC guarantees the appropriate level of security, compliant with the GDPR rules.

3.5.2 Clinical Site Backend (CSB)

The second module, named as the RETENTION Clinical Site Backend (CSB), comprises a set of components deployed at the clinical sites responsible for managing and digesting the clinical and other data collected and transmitted from the recruited study participants. Each of these clinical sites will operate its own dedicated CSB instance, focusing on patient data ingestion as received from the RETENTION Edge instances of the monitored patients which, combined with clinical data, will enable the execution of local analytics based on ML trained models. Based on the results of these analytics, patient management (personalised) interventions can be triggered (subjected to clinicians' decisions), delivered via the corresponding RETENTION Edge instance (the Mobile Application) of each patient. Moreover, fully anonymised sets of data related to patients, the executed interventions, and their effectiveness, along with any new (non-verified) intervention model will be transmitted to the GIC, for further processing and model refinement. In this context, personalised interventions will be registered, stored, and further processed to facilitate backend analytics.

The CSB supports the clinical side operations. The daily patient check-up (through transmission of devices'/sensors' usage data and collected feedback), the initial patient administration and baseline, facilitates the visits to the hospital (as arranged by each clinical site), the pairing and monitoring of the usage of the devices and sensors handed to patients, and support the monitoring of their health via generated aggregated medical indicators. It also supports chat functionality for engaging communication with specific patient (functionality will not be activated in the framework of the Retention trial study to avoid bias). Clinicians can review descriptive analytics relevant to patients' medical condition, apply a ML model to acquire a prognosis on a specific indicator, and configure thresholds for triggering rule-based personalised interventions. The CSB is composed of the following components that interact with each other:

- **Dashboard** that provides interaction elements for administrating CSB end-users, patients and their medical and usage data, the application of ML models, the configuration of the thresholds triggering personalised interventions and GDPR requests' management. Functionality and data are subject to access limitations based on RBAC.
- **Big Data Engine Executor** manages variants of several ML models.
- **Decision Support System** supports the creation and transmission (to the Patient EDGE) of personalised interventions based on a rule-based logic that considers measurable facts from the patients.

- **Chat** is a module that enables CSB clinicians and patients (or carers) to communicate via text exchanges (functionality will not be activated in the framework of the Retention trial study to avoid bias).
- **FHIR and non-FHIR repositories,** where pseudonymised (personal health records, questionnaires, usage data, personalised real-world data), personalised interventions and trained ML models (**Repository for Models**) are stored.
- **REST API** supports inner and outer (previously authorised by the Security Component) communications with CSB components and GIC.
- **Security Component** supports the authentication and authorisation processes, along with mechanisms to protect services and data flowing from/to the CSB (data in transit) as well as while data reside within repositories (data at rest).

3.5.2.1 CSB Dashboard (CSB@Dashboard)

Like the GIC@Dashboard, the Dashboard of the Clinical Site Backend (CSB@Dashboard) is the component that is responsible for the interaction between the end-user types (roles) supported and the CSB services in the backend. The Dashboard behaves differently based on the role assigned to the end-user by the Role-Based Access Control (RBAC) capabilities of the CSB@SC. The following table (Table 7) presents its main features.

Table 7 : CSB Dashboard features and specification

Component Title	CSB Dashboard
Objectives / Brief description	The CSB@Dashboard component will serve as the entry point for clinicians for the monitoring and treatment of their patients Patients' monitoring and health related data from various sources be presented in a multipurpose interface addressing (primarily) the needs of clinicians CSB@Dashboard will also serve the system administration and technician needs
Technical pre-requisites and requirements	REST APIs are required to fetch/submit data The visualisations will be offered via a unified web application based on AEGIS' Advanced Visualisation Toolkit (AVT) End-users will only need a browser to access the Dashboard
Actors	The actors of the component include: - CSB Admin - Clinician - Tech support maker - GDPR Auditor
Interactions Inputs	Input of the component must be provided as a REST API The component will offer interaction with different types of users, therefore role-based access to different parts of the interface will be realised.
Interactions Outputs	Outputs of the component are the triggered events based on user actions that can include: - storing data in CSB repositories - trigger CSB components (e.g., chat)

	- export or visualise data in meaningful manner
data format	inputs preferably in JSON format

3.5.2.2 CSB BDA Engine Executor (CSB@BDAEx)

The BDA Engine Executor (or BDA engine model's executor) is a CSB component supporting the applicability of a previous trained ML model to predict the possible future outcomes of a patient's (health or wellbeing) indicator. The trained models are created within the GIC scope and upon end-user action (data analyst) then transmitted to all CSB instances. As such, this component provides means of receiving the latest variant of a ML model and applying it to predict patients' possible evolution of an indicator. The following table (Table 8) presents CSB@BDAEx main features.

Table 8 : Model executor tool features and specification

Component Title	BDA Engine Executor (or BDA engine model's executor)
Objectives / Brief description	Support predictability the possible future outcomes regarding patient's health based on training accomplished on GIC
Technical pre-requisites and requirements	Database to store/update model
Actors	Database – managing models trained on GIC Models' executor tool – interpret current models + custom metadata
Interactions Inputs	Database -> Model executor tool
Interactions Outputs	Update models serialised as pickle files + models metadata in a custom format
data format	Input: Data load model from database + Patient's data to be predicted Output: Predicted result regarding patients' health progress

The following sequence diagram (Figure 12) depicts basic functions of transferring trained ML models (from GIC to CSB) and its application to a specific case (Figure 13).

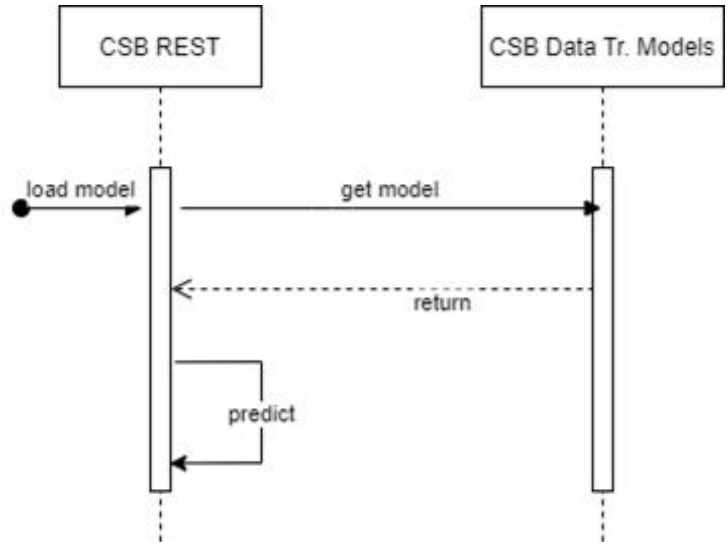


Figure 12: Transmitting a trained ML model: REST communication between GIC and CSB

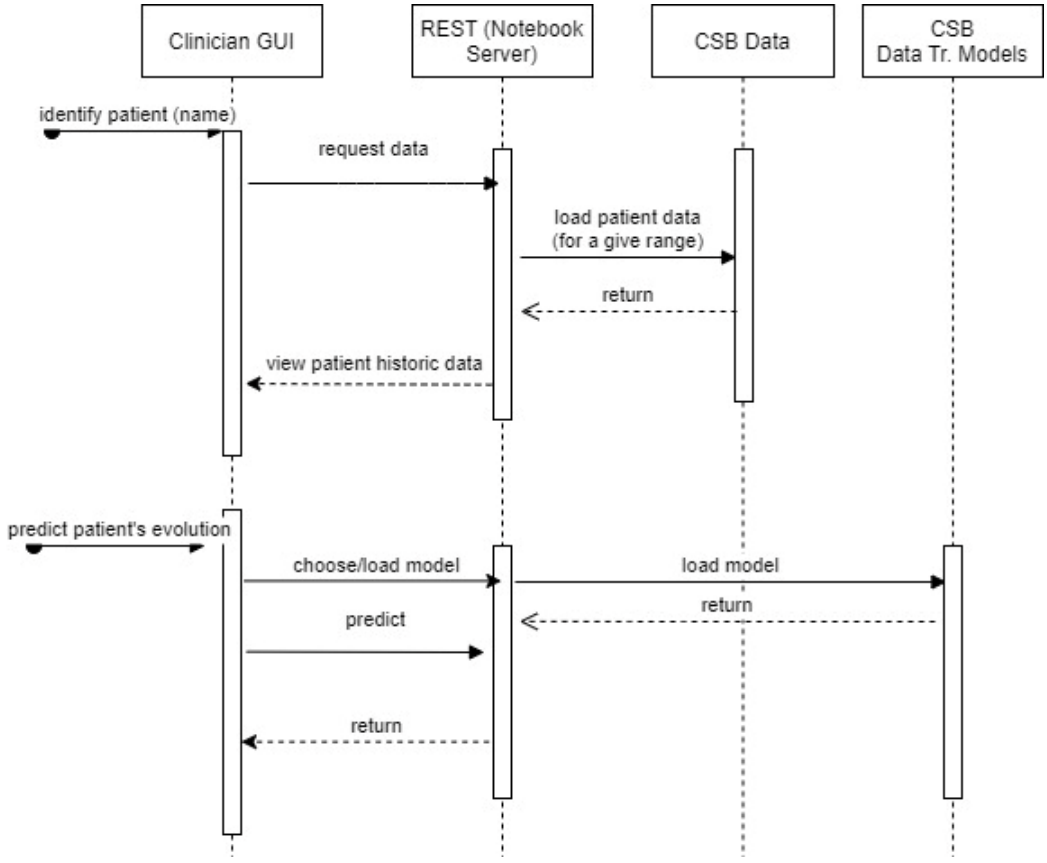


Figure 13: CSB BDA engine executor Sequence Diagram via CSB Dashboard Actions

3.5.2.3 CSB Decision Support System (CSB@DSS)

The CSB Decision Support System is an independent, rule-based system that enhances the ability of the clinical team to trigger decisions (in a form of personalised interventions) according to rules that will be

established by them. This component will model human reasoning and the decision-making process, so that measurable facts from the patients (e.g., repeated abnormal temperature and blood pressure measurements) will be processed and interventions will be suggested to clinicians for them to configure. The DSS may process both raw or aggregated data stored in the CSB repository and may also consider results of the CSB@BDAEx (stored in the non-FHIR repository). To trigger an action, DSS considers time parameter, patient's usage data values (e.g., pressure, pulse, temperature, VAD data, etc.) to bring to the attention of the clinical team. The following table (Table 9) presents CSB@DSS main features.

Table 9: Decision support system features and specification

Component Title	Decision support system
Objectives / Brief description	To create a rule-based system that will enhance the ability of the clinicals to take decisions, by checking data of patients against the pre-defined rules The rules are set by the clinical team
Technical pre-requisites and requirements	Rules (thresholds) are managed by the clinical team
Actors	Clinicians of CSB Patients (or cares) receiving the personalised interventions (via the Mobile App)
Interactions Inputs	Data from each CSB repositories via the REST API
Interactions outputs	Messages and suggestions to clinicians Personalised interventions
data format	Inputs/outputs in JSON format

3.5.2.4 CSB Chat (CSB@Chat)

CSB will support basic text chat functionality allowing real-time communications between patients and clinicians. This service is not for emergency use. The following table (**Error! Reference source not found.**) presents CSB@Chat main features, while sequence diagrams (Figure 14 : Chat CSB to Mobile Application) present the basic message exchanging.

Functionality will not be activated in the framework of the Retention trial study to avoid bias.

Table 10: CSB chat sub-system features and specification

Component Title	Chat support system
Objectives / Brief description	A text chat system will enhance the ability of the clinical team to communicate to patients (or vice versa) directly

Technical pre-requisites and requirements	Requires Mobile Application to support this exchange of text data
Actors	Clinician to a patient: sending/receiving text messages Patient (or carer) to CSB clinician: sending/receiving text messages
Interactions Inputs	Unregulated text
Interactions outputs	Unregulated text
data format	Inputs/outputs in JSON format

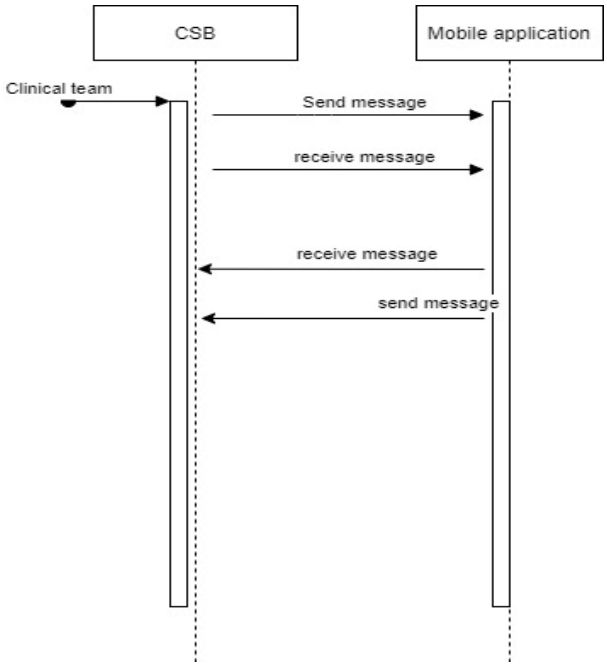


Figure 14 : Chat CSB to Mobile Application

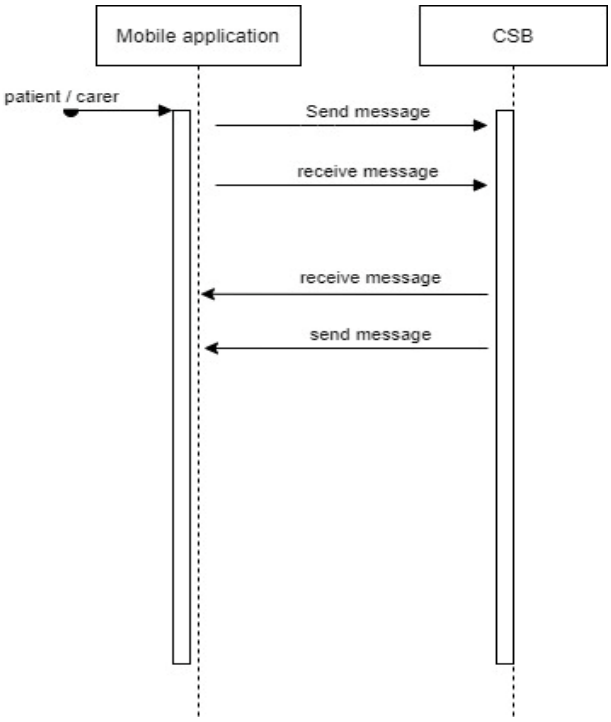


Figure 15 : Mobile App to CSB

3.5.2.5 CSB FHIR and non-FHIR repositories (CSB@Data Layer)

As with CIG repositories, those supporting operations of each CSB instance are open-source repositories that will host CSB patients' data (raw and aggregated), models and interventions. The CSB@Data Layer is responsible for collecting and organising all the prospective data that will be stored in the RETENTION platform. The Reference Model is the basis for organising all the data, including all the variables that describe the minimum requirements of a specific domain. The Reference Model is a hierarchical data presentation model like an ontology. The ontology represents the data in the form of entities (e.g. classes) and object properties. An Entity-Relationship approach is used for building the ontology.

The design of the RETENTION Reference Model is driven by the analysis of the files prepared by the clinicians regarding ranges (i.e. minimum and maximum values) of parameters of different types of patients (HF, Tx and LVAD). According to the Reference Model, each patient is linked with different types of data, each of which has one or more parameters. This data will follow the Reference Model specifications, and, hence, the CSB@Data Layer involved in the collection and organisation of data. The different types of data are organised in broader categories, as it is demonstrated in the following figure (Figure 16). For example, for a Medication it is considered by clinicians very important to know the specific pharmacological substance administered, the broader category that it belongs to, the dosage amount per day, and the frequency of administration (e.g. once or more per day). To support this notion, each variable in the Reference Model has its own value range, type, and parent class. The parent class is the category where the variable belongs to. For example, the variable "ethnicity" belongs to the class "Demographics" (type: integer, values: {1,8}).

The Reference Model is published in the form of an .OWL/.XML format ontology that contains the different types of data recorded along with the parameters of specific interest for each one of them. It should be noted that the design of the OWL ontology is driven by the analysis of the standards published by HL7 especially about the organisation of classes of data and the naming of their parameters. To this end, HL7 standards for

medical terminologies will be taken into consideration to enhance the semantic interoperability of the ontology based on SNOMED-CT, LOINC, ICD-10, ICD-11 and other terminologies. The terminology used (set of core terms or vocabularies) for each one of the specified parameters was also included in this ontology. Based on this. OWL document a Relational Database will be also designed for the storage of prospective data.

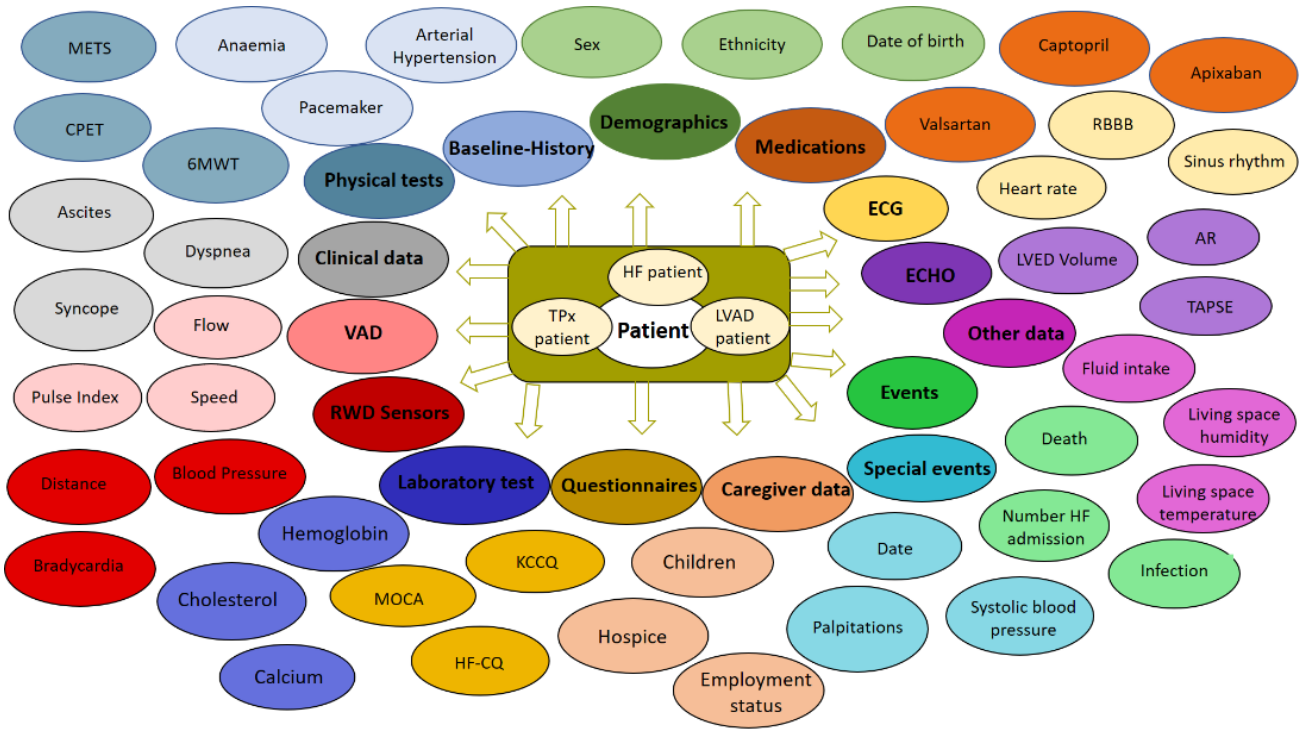


Figure 16 : Indicative Basic Data model

The 1st complete version of the RETENTION Reference Model presented in D4.1.

3.5.2.6 CSB REST API

As with CIG, the communication between the CSB deployed components will be done through REST APIs. Respectively, the CSB Security Component will authorise end-users and authenticate interactions between CSB components via REST services.

3.5.3 Patient EDGE (PE)

Each RETENTION Patient Edge (PE) instance, referring to the personalised smart ecosystem dedicated to each of the monitored patients, will embed a variety of smart home and wearable (m)IoT as well as wellbeing devices, to collect usage data from RETENTION study participants. Moreover, it features the necessary enablers for data aggregation, user interactions, and personalised interventions' delivery. The patient Edge has two sub-components defined collectively as "Patient EDGE":

- The Patient Edge Local Home Gateway (PE Local Home Gateway, or Home Gateway, or EDGE), and
- The Patient Edge Mobile Application (PE Mobile Application)

PE Home Gateway will be installed in the homes for local home sensors' data aggregation, pre-processing, and transmission to the CSB, as well as m2m communication to/from the CSB (for installing process or other basic technical configurations). Since all study participants will be provided with a smartphone which will run the PE Mobile Application, this application will be the instrument for gathering usage data and feedback in a unobtrusive and trouble-free fashion, and with minimal effort required to operate the devices and sensors to be handed as well. All in all, the PE will enable the continuous monitoring of patients and the collection of the medical, physiological, behavioural, psychosocial, and real-world data for such patients.

3.5.3.1 Patient Edge Local Home gateway (Local Home gateway - EDGE)

The handling of (non-medical) sensors' usage data relevant to environmental factors in the living environment of the study participants, and in particular data acquisition, storage, and upload to the CSB will be handled by the RETENTION Patient EDGE Local Home Gateway (PE Home Gateway, or Home Gateway, or EDGE), a component that supports the communication both with home sensors and with the external data provision services. For the interaction with the home sensors the EDGE will be configured to work as a local server that will be always running and "expecting" data to be consumed. Since the initial setup of the EDGE has been achieved, a Bluetooth connection and pairing will be established between the EDGE and the home sensors. Then the data exchange can take place. For the data acquisition the BLE protocol will be applied, and the data exchange will occur through the necessary services and characteristics (supported by sensors' SDKs). This will enable the EDGE to receive real time data from the sensors.

The EDGE will be configured for querying paired sensors for data every 1 hour, and subsequently the patient living space data (e.g. temperature, humidity) will be frequently transmitted through the day. Initially, data will be stored locally to the EDGE's local database to avoid data loss. At a specific time, each day, a predefined algorithm will run on the EDGE machine to calculate the aggregate values of the daily obtained values (of humidity and temperature, e.g., median values). Upon completion of the aggregation, the calculated values will be appropriately timestamped, formatted in a .json file in a predefined format, so a POST request to the CSB REST API can take place, and the home sensors' data can be stored successfully in the CSB non-FHIR repository.

For communication with external data services, the EDGE will be utilised to receive the outdoor analytics and post them to the CSB. This process will be achieved by utilising the Python Copernicus API, and in particular the Climate Data Store Application Program Interface (CDS API). CDS API is a service that provides programmatic access to the climate data store datasets (like ERA5 and others). Via this CDS API client, requests are possible by providing the necessary input variables such as year, month, day, time, longitude, latitude and receiving the requested output variables such as temperature in the specified region. This information will be parsed from the data that will be obtained through the API and then a second post request will be executed, obtaining all the necessary outdoor analytics (humidity, temperature and air pollution). This information will be also stored in the local EDGE's database to avoid data loss. The data acquisition from the CDS API will occur at least once per day, as per the protocol. In a similar way, other external services can be accessed.

EDGE will be self-contained and will automatically update the system data, without the intervention of the patient/carer. The following table (Table 10) presents EDGE main features.

Table 11 : Home gateway hub

Component Title	PE Local home gateway
Objectives / Brief description	Software & Hardware system that connects the home devices/sensors to the RETENTION system and cohorts and aggregates usage data
Technical pre-requisites and requirements	Connectivity to patient's Wi-Fi network (router) Usage data will be visible only via the application (not available for other installed applications) To collect World data (based on localisation) from external public services (local area weather, pollution information if available) Usage data timestamped, associated to patient identifier and aggregated
Actors	Patients and their carers
Interactions Inputs	Local devices/sensor data (as transmitted by the device/sensor) External device/sensor data (as given by the services)
Interactions outputs	Basic on/off and connecting to a Wi-Fi network Outputs on the Mobile application and device
data format	Inputs/outputs in JSON format

In the following figure (Figure 17), the basic communication concept between the EDGE and the functionalities can be observed.

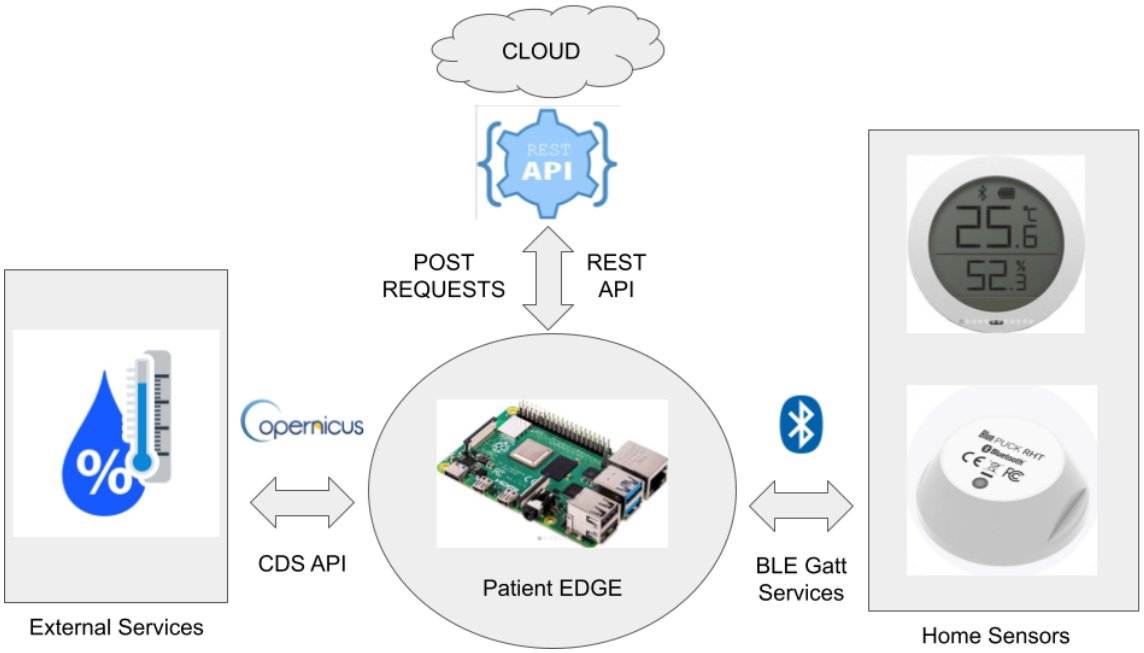


Figure 17 : A basic concept for the communication between Patient Edge and the rest of the functionalities

The EDGE's software will be developed in line with the requirements needed for end-users that are not familiar with technology. Taking this design requirement into consideration, the EDGE will be designed to allow for effortless use of its basic capabilities. The component will be plugged and only a few actions will be

required to be performed by the end-user for the initial setup. The EDGE will be connected via Ethernet cable directly to the router to minimise unnecessary configurations needed for Wi-Fi, and the home sensors will be placed next to the EDGE at a distance of less than one (1) meter.

The basic OS that will be running in the EDGE will be Raspberry Pi OS (Raspbian), which is based on Debian OS. Core components will be a range of processes and scripts all having a specific functionality to achieve to make the software more robust. Some examples of these functionalities will be (

Figure 18 and Figure 19): i) one for the communication with the home device and one for the external services, ii) one watch-dog process which will always check if the main processes are running and if not get them back on, iii) one process which will store all the acquired data to the local database, iv) one process that will be used for posting the data to the REST API, and v) one to check if data have been successfully posted or configure the software to try again the next time. Then, sensor-oriented scripts are going to be implemented to check the sensors' status such as battery level, to avoid data loss. The development process will also consider memory management techniques to avoid memory overflow. The software in general will be developed in such a way that if any technical problem occurs, the patient will be able to turn the EDGE off and on again by pressing only the power button, and the necessary scripts and processes will start working normally again, automatically.

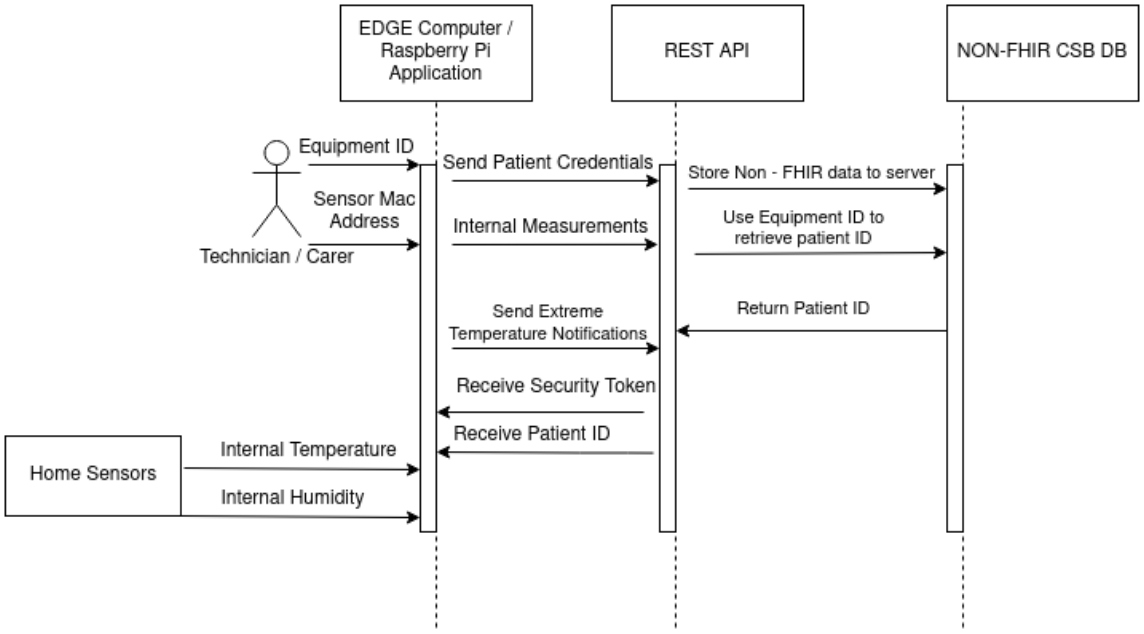


Figure 18 : Home sensors' sequence diagram

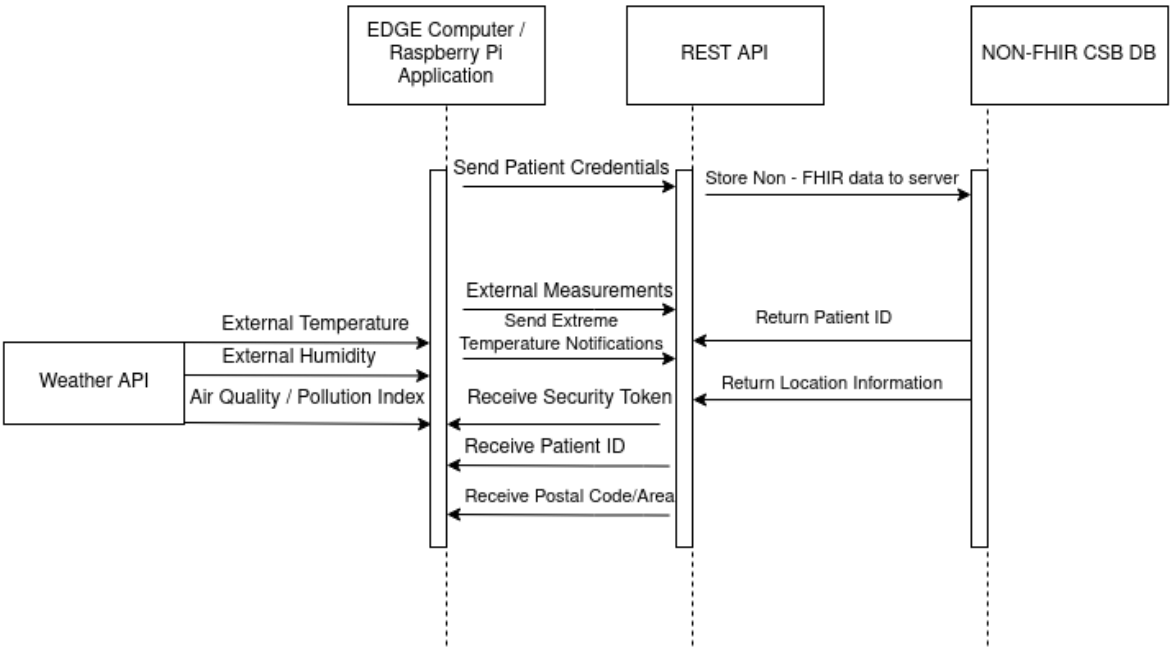


Figure 19 : weather information sequence diagram

The core programming language that will be used is Python. However, if needed for the different EDGE tasks and functionalities C, C++ and shell script will be used. Also, the program will be as interoperable as possible, and will enable a direct communication with the other EDGE machine (mobile phone) if information or data exchange is needed.

3.5.3.2 Patient Edge Mobile Application (Mobile Application)

From the patients' perspective, the main avenue of monitoring and interaction with the RETENTION solution will be the RETENTION Edge Mobile Application. This purpose-developed application will feature a user-friendly interface that gathers and transmits usage data to CSB, inform the end-users of the important parameters regarding their health and well-being and the management of their conditions, and deliver interventions. Examples of such features include highlighting the need to move more often or to avoid going out if the environmental conditions pose high risk (e.g., high particle count in the atmosphere), reminding pill intake, or facilitating communication with the monitoring clinical staff. These capabilities will augment the ones enabled by the Edge Gateway, as the latter will focus on monitoring and interventions related to the IoT ecosystem, while the Mobile Application will focus on wearable (bioelectronic) and medical devices, as well as on maintaining the RETENTION operation while the user is not at home. The application will maintain a high level of abstraction and focus on usability, and to be operated by elderly people or others without technical background.

The application will timestamp, associate to a patient identifier and (in cases of devices/sensors' data) aggregate data prior to their transmission to the CSB. The following table (Table 12) presents Mobile application main features. Screenshots of early prototype of the mobile application itself are provided in Appendix 3.

Table 12 : Mobile application features and specification

Component Title	Mobile Application
Objectives / Brief description (mandatory)	Supports the collection of usage data and feedback from patients or carers (on behalf of), as both will login to the system via the app The application will connect via secure channel with the CSB The patient or carer will be able to easily connect/pair devices with compatible BLE technology, to the smartphone and in extent to the mobile application The application will be able to register the connected device. Also, the application will be able to connect to CSB to send/receive data Whenever the application starts, it will check the condition of the patient (or via the carer) via a basic questionnaire and if the condition is worse, it will offer an advance health questionnaire for collection The patient or carer will be able easily visualise the data transmitted by the CSB (notifications, feedback). The application will offer visualisation of patient's usage data The patient or carer will be able to easily add, modify and submit information/feedback on questionnaires and/or surveys The patient or carer will be able to easily send text messages to CSB clinicians (this text chat service is not for emergency use) The patient or carer will be able to send photos, later to be viewed by CSB clinicians The patient (or via the carer) will be monitored for the patient's adherence to treatment (taking his medication timely and as prescribed) The application will receive personalised interventions from CSB and display them to the patient (or the carer)
Technical pre-requisites and requirements	When patient uses the Mobile application for the first time, he/she must agree to the collection and use of information in accordance with the RETENTION policy Minimum configuration settings: patient identifier (stored encrypted), IMEI, Gmail account (for enabling automatic updates) and Wi-Fi credentials. Those should not be erased whenever an update occurs The mobile application will be pre-installed on the android smartphone. Automatic updates must be supported by default (via Google store) Devices/sensors paired (preferably) by using Bluetooth Low Energy (BLE) Usage data is timestamped, associated to patient identifier and aggregated prior to transmission to the CSB
Actors	The patients and the carers The CSB The connected/paired devices/sensors
Interactions Inputs	The patient or career will interact with the system and will add local data as needed (ex from the VAD) Data will flow from the devices to the mobile application (EDGE)

	Data will flow for local conditions from external services
Interactions outputs	FHIR medical data to each CSB via protected API Non-medical data to each CSB via protected API
data format	Inputs/outputs in JSON format

In the following figure there is the sequence diagram for the mobile application. Using the mobile application, the patient or carer can update his/her data and status, receive information from the system and get useful information about his/her health.

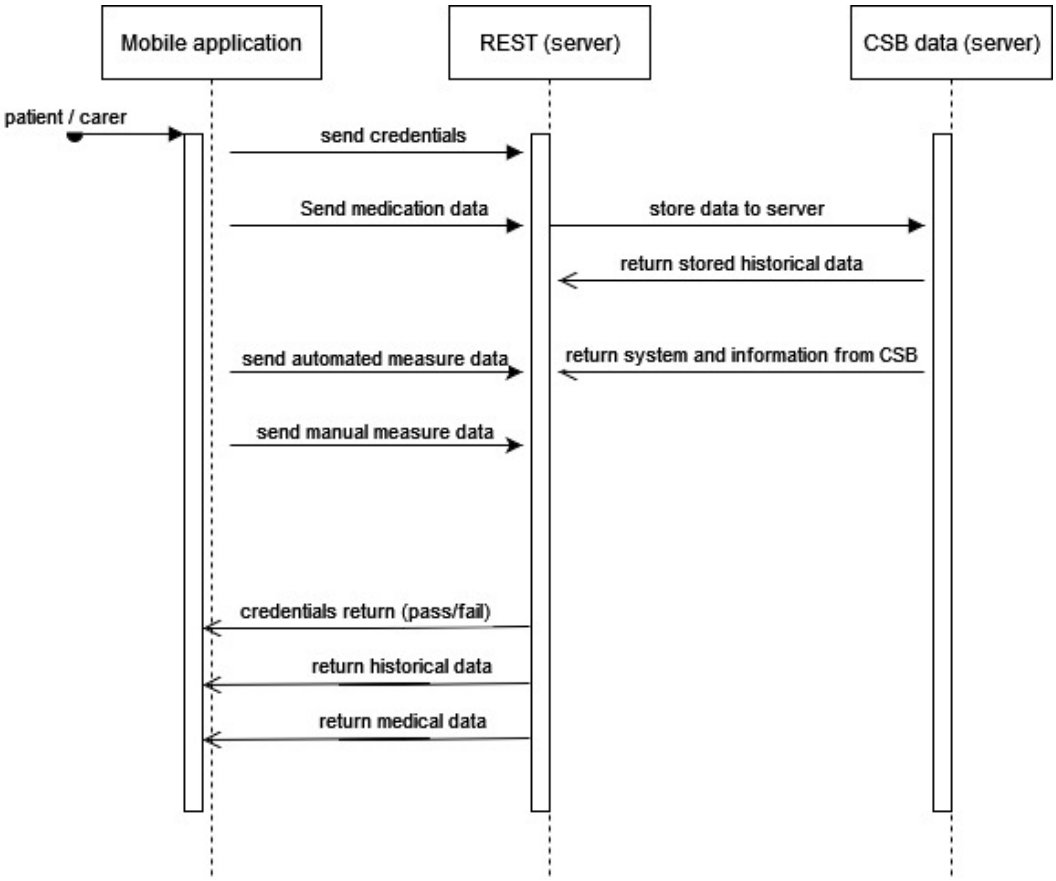


Figure 20 : Mobile Application sequence diagram

Heterogeneous patient-related data will be monitored, collected, and analysed in real time at the various CSB instances via the PE. More specifically, these will include:

- **Real-time Prospective Data**, covering data collected from the patients' PE deployments, including data from their smart watches, physiological/bioelectrical sensor data, mobile device data, smart home sensor and actuator data, and patient's environmental parameters. The data are related to the continuous monitoring of the patient and his/her compliance to treatment, as well as to the effects of the undertaken interventions.

- **Periodically Updated Data**, covering data collected and analysed through medical assessments and questionnaires via the PE (standardised and/or extended as required for the purposes of the project) conducted by medical experts. The data will be self-reported from questionnaires given to the patients, via typical medical data available to the healthcare providers managing the patients (e.g. patient medical history, aided by validated questionnaires), as well as pertinent closed clinical trial data, where available.

3.5.4 Participant Devices (PD)

To achieve the types of data analysis to serve the aims of RETENTION, (m)IoT devices and sensors will operate within patients' environments to enable the continuous monitoring of patients and the collection of the physiological, behavioural, psychosocial (raw/aggregated) data in an easy, unobtrusive, and non-invasive way.

The devices will be paired with the Mobile Application (that acts as a data collector) by using Bluetooth Low Energy (BLE) (or smart Bluetooth) technology that provides considerably lower power consumption operating for a longer period[1] while maintaining similar communication range as older Bluetooth devices. RETENTION provides and connects different types of devices measuring values such as blood pressure, body temperature, glucose, body composition, heart rate, weight. The types of devices supporting the requirements defined (in D3.1) are:

- Device #1 – Smartphone
  Since the Mobile Application is considered as a core technical component of the RETENTION solution, the smartphone that has this application installed will have the following technical characteristics: i) OS: Android O/S equal or greater than Android 10, ii) RAM: 3GB or more, iii) sufficient CPU power and multitasking capabilities (8-core phone), iv) Local storage more than 64GB.
- Device #2 - Weight Scale
  The smart weight scale that will measure study participants body weight, will have the following technical characteristics: i) equipped with digital electronic scale, ii) support Wireless connectivity, iii) enough battery life to last for long periods, iv) SDK or API to report data to the application.
- Device #3 – Smartwatch
  This device will provide data of activity (steps, distance, stairs), sleep (hours and quality) and heart rate monitoring. Technical requirements: i) SDK or API to report data to the application, ii) support Wireless connectivity, iii) synchronisation of collected data each time a new event is triggered
- Device #4 - Blood Pressure Monitor
  This medical device will support the blood pressure and heart rate monitoring. Technical requirements: i) SDK or API to report data to the application, ii) support Wireless connectivity, iii) synchronisation of collected data each time a new event is triggered.
- Device #5 – Oximeter
- The oximeter will provide oxygen saturation, heart rate, and changes in vital signs (pulse, blood pressure). Technical requirements: i) SDK or API to report data to the application, ii) support Wireless connectivity, iii) automatic data gathering iii) enough battery life to last for long periods.

[1] Bluetooth vs Bluetooth Low Energy, what's the difference? https://elainnovation.com/en/bluetooth-vs-bluetooth-low-energy-whats-the-difference/

- Device #6 - Bluetooth Low Energy (BLE) home temperature/humidity sensors
  The home sensors will be used to generate and transmit temperature and humidity measurements.
- Device #7 – Local gateway (hub)
  The local gateway is the device that will be connected to the home sensors and in turn transmit data to CSB and communicate/subscribe to external services to receive weather/ pollution data. Technical requirements: the EDGE PC will run on a Raspberry Pi 4 Model B 4GB, equipped with Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz, 4GB LPDDR4-3200 SDRAM, 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE, Gigabit Ethernet, 2 USB 3.0 ports; 2 USB 2.0 ports.

3.5.5 RETENTION Security Component

To support the aim of the RETENTION, the technical solution (involving both the CSB, the GIC and the EDGE) must support the integration of heterogeneous devices and sensor later to enable the continuous data collection from the study participants, and to analyse the collected data using novel data analytics' technologies. The security component supports a) monitoring the security of all operations, preserving the privacy, and providing the data subjects and b) full control of knowing by whom and how their data are being processed in a verifiable way. Adhering to this, in addition to administrative procedures in place (presented in D2.2) to ensure that personal data are processed fairly and transparently, this section provides a technical description of the Security Component and encompasses the security and privacy mechanisms to be implemented, through the prism of this component's use based on the security and privacy requirements (defined in D3.1).

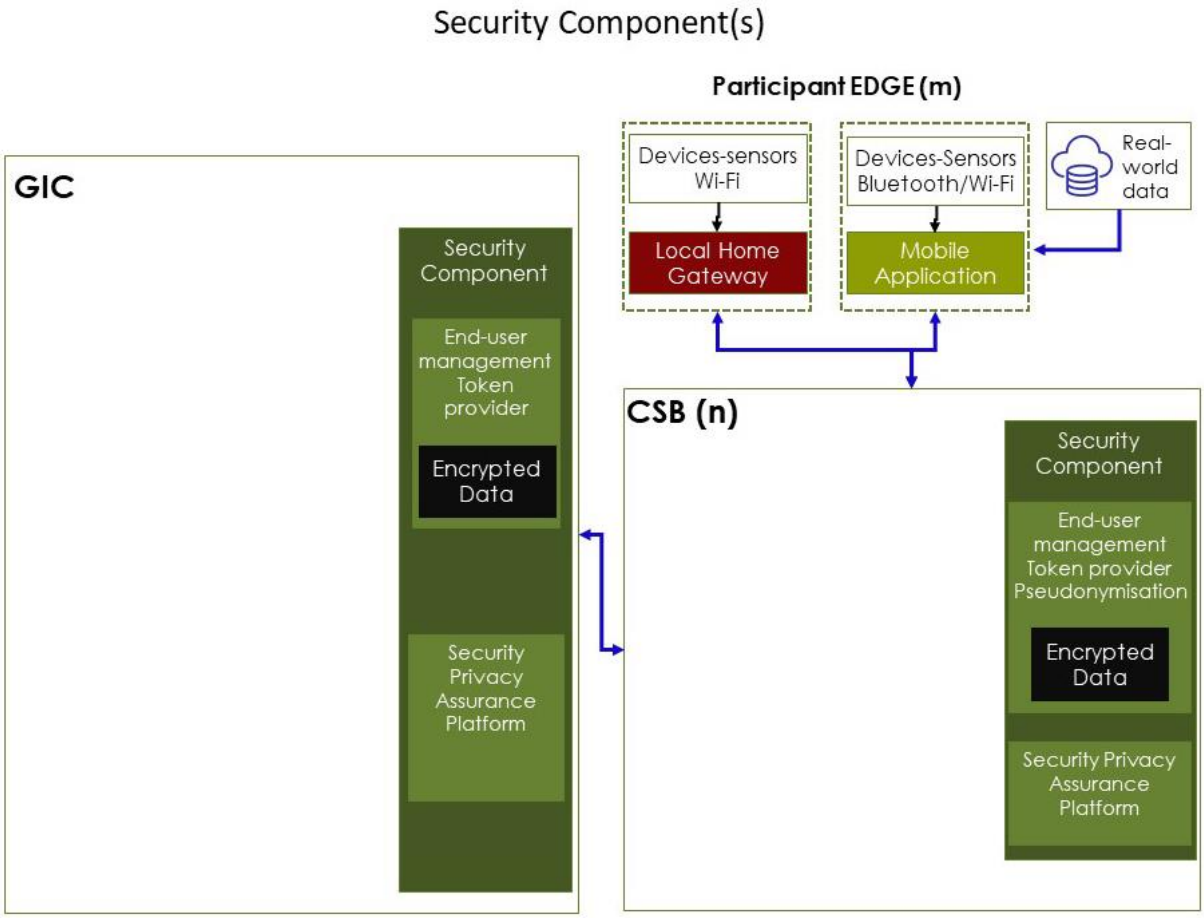


Figure 21 : RETENTION Security Components

Confidentiality, integrity, and availability are the three main cybersecurity principles of any security control (Neuman, 1977). Confidentiality is the property where, unless users' processes or devices are authorised to access, information is not disclosed (i.e., data and resources are protected from unauthorised access). Integrity entails guarding against improper information modification or destruction, including data authenticity (i.e., data is protected from unauthorised changes to ensure that it is reliable and correct). Availability means ensuring timely and reliable access to data (i.e., authorised end-users have access to the systems and the resources they need). Each of these three principles involves relevant protection mechanisms, which are described below, as they are derived from the various standards such as Common Criteria Evaluation Methodology (CEM) (ISO/SEC, 2009), and the Open-Source Security Testing Methodology Manual (ISECOM-OSSTMM, 2010), and related research efforts (Hatzivasilis, 2016).

The intended to be implemented mechanisms will comply with the Privacy and Security-by design principle, the notion by which security and privacy measures and enhancing technologies (PETs) are being embedded directly into the design of a system. On this axis, and given the legal obligations imposed by the General Data Protection Regulation (EU, 2016), data minimisation, pseudonymisation, transparency in the processing of personal data, and other appropriate technical (and organisational) measures are considered at an early stage of the platform design to ensure that GDPR requirements are met. This way it is possible to preserve the anonymity of big data (i.e., devices/sensors usage data, medical history, analytics, interventions stored in the Repository), the confidentiality of any personal data, and Personal Identifiable Information (PII) (i.e., IDs association records, and Dashboard end-users profile information stored in the Security Component), the

privacy and the integrity of data (KPI-3.1, KPI-3.2, KPI-3.3) according to state-of-the-art guidelines (e.g., encryption guidelines of NIST (NIST, 2020), role-based and application-level security access control, Secure Sockets Layer, Denial-of-Service Prevention).

A. Pseudonymisation via IDs management

Data protection is a critical issue for the RETENTION platform (CSB and CIG) and for this reason, data minimisation, authentication, and other security and privacy aspects are materialised with an in-between (REST API, Cloud components, RETENTION mobile application, and Home Gateway) component. The Security Component provides mechanisms that perform pseudonymisation and IDs associations, used for the authentication and authorisation of Cloud RESTful API to protect the transmission of any (sensitive or not) data, and it is also utilised for the management of privacy-related requests to demonstrate compliance with the GDPR. In this respect, the RETENTION Mobile application (Mobile app) that periodically ingests data from the everyday life of the study participants (i.e., heterogeneous sensors, assistive medical and mobile devices) to the CSB@Repository, has data protection mechanisms in place to provide security both while data are flowing from/to the Mobile app (data in transit) as well as while data stays temporarily in the smartphone's internal database (data at rest). IDs management, and personal data and PII removal techniques used were introduced in (Basdekis, 2019) and properly enhanced to meet RETENTION needs. IDs management involves the following basic processes:

- Each pseudonymised usage data record (i.e., sensors/devices usage data) transmitted by the Mobile app or Home Gateway to the CSB will be marked with a non-identifiable External pseudo-Id (Pseudo-Id1), utilised for associating and pairing all devices handed over to a study participant. The way this external pseudo-Id is stored in both Mobile app and Home Gateway local storage is such that it cannot be associated with the participant's identity in case of a loss, since no one may identify, directly or indirectly a subject. Upon reception, IDs will be replaced with another Cloud-generated Id (Pseudo-Id2), while PIIs will be stored in Security Component and then removed altogether from the record (the usage data part is allowed to be digested by the CSB Repository) (Figure 22).
- The Pseudo-Id1 that is provided by CSB, will be used to configure the responsible for transmitting usage data devices (i.e. smartphone or tablet, and Home Gateway) that will be given to a particular study participant, before handing them over to him/her. CSB@SC will maintain the association between the Pseudo-ID1 and Pseudo-ID2. Thus, the data in the CSB repository will be pseudonymised at rest. The Pseudo-ID2 will be used in the context of analytics being executed within this CSB scope. Vice versa, when a message is about to be transmitted by the CSB to a specific study participant, the generation considers at first the Pseudo-Id2, later, to be replaced by the Pseudo-ID1 prior to the transmission to the specific smartphone been given to the patient participant.
- The ID replacement process to be performed by the CSB@SC is carried out also during every REST trigger that transmits data from/to the CSB@Dashboard.

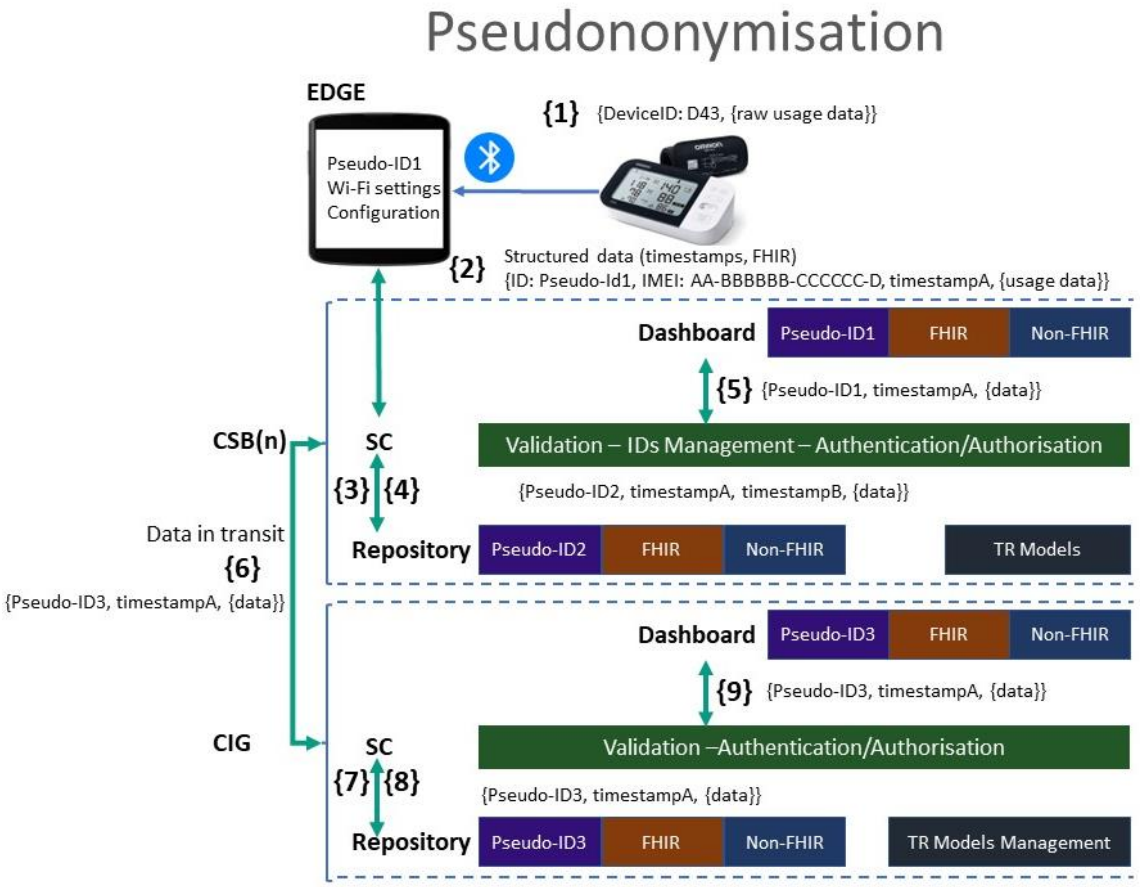


Figure 22: Pseudonymisation process supported by the Security Component in both CSB and GIC

B. Data transfer

Personal data transfers are not anticipated in the context of RETENTION project. However, any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or an international organisation shall take place only if, subject to the other provisions of the GDPR, the conditions laid down are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or another international organisation. All provisions shall be applied to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. Whenever RETENTION solution (CSB) processes personal data, this action will take place in the ICCS's server room (Greece). In no case resulted in the data leaving the EU (ICCS acts as Data controller).

C. Data integrity

Data integrity will be achieved by a variety of data protection methods including backup and replication, auditing (of access logs, GDPR requests status, etc.), data and input validation, duplication removal, and access controls.

D. Data minimisation

Authentication and authorisation, present the basic logic of how an end-user can log in into the system, as well as on how we can get the user info. Nevertheless, not only we should have that info but also, we should define an access control mechanism of how we apply this information.

Role-based access control (RBAC) refers to the idea of assigning permissions to end-users based on their role within an organisation. It is less prone to error because of its simplicity and manageability instead of assigning each user permissions. Based on user requirements, users are grouped and then each group is assigned a role. Afterward, each user is assigned one or more roles and each role is assigned with one or more permissions. The benefits are the following:

- create a systematic, repeatable assignment of permissions.
- easily audit user privileges and correct identified issues.
- quickly add and change roles, as well as implement them across APIs.
- cut down on the potential for error when assigning user permissions.
- integrate third-party users by giving them pre-defined roles.
- more effectively comply with regulatory and statutory requirements for confidentiality and privacy.

In the possibility that there are overlapping roles, the permissions that the user has is the union of the permissions of each role the user has, since RBAC is an additive model.

Access to the anonymised data in the GIC@Repository and those pseudonymised ones kept in CSB@Repository (in particular personal data and PII are stored encrypted within CSB@SC), will be granted through the realisation of RBAC to identified (In D3.1) end-user roles, limiting/preventing the access/process of Dashboard services (i.e., indirectly to data and information stored in the repository and to all other components) to what is directly relevant and necessary to accomplish a specified purpose.

In terms of services and how triggering them is controlled, all Restful APIs will need to first obtain a secure token from the Security Component. The authentication manager will utilise the WSO2 Identity Server and API manager (technical details presented in the following section WSO2 Identity server). The former builds agile, extensible CIAM solutions (by using the XACML rules) and the latter is a complete enterprise-class API management solution that combines easy, managed API access with full API governance and analysis. Each REST will check whether a specific end-user has access to a specific REST within a context (e.g., clinician: create a patient, clinician: associate a device, data analyst: create an analysis). The API Manager will be used by each REST service and will invoke an additional Header named "X-JWT-Assertion". This header contains an authentication and authorisation token that contains information about the identity of the end-user that has invoked the REST API. The developer of the API will use the token to verify that the user that invoked the REST call holds the relevant permissions. In addition, via the Security Component, limiting the access of each user on specific Organisation-based data will be accomplished (during the initial data gathering). In that sense, end-users of each pilot site (i.e., a different instance of CSB) will be able to have access to pseudonymised data (i.e., personal health records, usage data) only to study participants of their site/organisational unit. The system administrators will be able to manage end-users and perform actions such as system monitoring, services health checks, etc. In that sense, clinicians will have access only to relevant views of the Dashboard that relate to the pseudonymised medical history of study participants of the organisation they monitor, while technicians that will support the pilots, will have access to mechanisms for managing and monitoring the devices. Following this notion:

- CSB end-users (CSB internal roles such as Administrator, Clinician, Tech support, Data Scientist, Auditor) will be registered via the authentication manager.
- Mobile app and Home Gateway that trigger m2m REST API will be associated with a study participant.

Notably, even if in the unlikely event of malicious access to CSB@Repository is achieved, or data are leaked by administrator negligence, still will not be possible to reidentify study participants, since the association between participants Pseudo-Id1 and Pseudo-Id2 is stored in encrypted fashion in separate storage.

The procedures are accompanied by other security aspects covering the whole range of components, such as:

- Token-based access to RESTful API's.
- Protected logging system for monitoring data access to the Security Component data.

E. Storage limitation

Pseudonymous data (as a whole) will become anonymous when the separately stored IDs association records will be deleted. Thus, after the completion of the RETENTION project, data kept in CSB@SC will no longer be needed to conduct the research (e.g., analytics, interventions), and consequently will be erased and not further used for any data process.

F. Fair data process

Data collected are provided by the study participants voluntarily, in accordance with well-defined informed consent procedures, goals of data processes, and individual rights. In principle, usage data and resulting analytics and interventions do not consider any personal, discriminative references. As such, there is no risk of discrimination due to data processing conduct in the context of the RETENTION.

Table 13: GIC@Security Component features and specification

Component Title	GIC (or Cloud) Security Component: GIC@SC
Objectives / Brief description	Cloud Security Component is the component that enables authentication and authorisation at the RETENTION cloud (GIC) so that all components can communicate through a secure environment. The GIC@SC will use security standards to expose the cloud APIs securely for consumption.
Technical pre-requisites and requirements	Docker or Kubernetes for component deployment
Actors	M2m: CSB that invoke Cloud APIs GIC@Dashboard end-users: Administrator, Data Scientist/Clinician (or clinical expert), Healthcare policymaker, GDPR Auditor
Interactions Inputs	GIC@SC is the API Gateway that exposes the services to be consumed so the interaction inputs are those of the exposed components.
Interactions outputs	Same as Interaction inputs
Additional Information	The GIC@SC in order to expose the APIs it needs those APIS to be specified in OPENAPI format.

Table 14 : CSB@Security component features and specification

Component Title	CSB Security Component: CSB@SC
Objectives / Brief description (mandatory)	CSB@SC is the component that enables authentication and authorisation at the CSB so that all components can communicate through a secure environment. The CSB@SC will use security standards to expose the cloud APIs securely for consumption. In addition, CSB@SC will provide the pseudo anonymisation mechanism to be utilised upon patient data (Patient management). In this context, supports the management of patient objects (i.e., initial creation, update, read, delete), as well as the management of device association of them.

	Lastly, it handles GDPR requests issued by study participants.
Technical pre-requisites and requirements (mandatory)	Docker or Kubernetes for component deployment.
Actors	M2m: Devices (smartphone/tablet, and Home Gateway) that invoke CSB APIs CSB@Dashboard end-users: Administrator, Clinician (or clinical expert), Tech support (assists clinicians in device management), GDPR Auditor
Interactions Inputs (mandatory)	CSB@SC is the API Gateway that exposes the services to be consumed so the interaction inputs are those of the exposed components.
Interactions outputs(mandatory)	Same as Interaction outputs but the data will be pseudonymised
Additional Information (optional)	The CSB@SC to expose the APIs needs those APIS to be specified in OpenAPI format.

Security Component (the application architecture for both CSB and CIG of which is presented in the following Figure 23) consists of different off-the-shelf (OTS) components. For Identity Access Management (IAM), the WSO2™ identity server[2] (WSO2 IS) which is a leading open-source software identity server will be deployed. For authorisation and data pseudonymisation, the WSO2 API-Manager (APIM) is an OTS component responsible for handling those. In the following sections, a more detailed description of the Security Component components is provided.

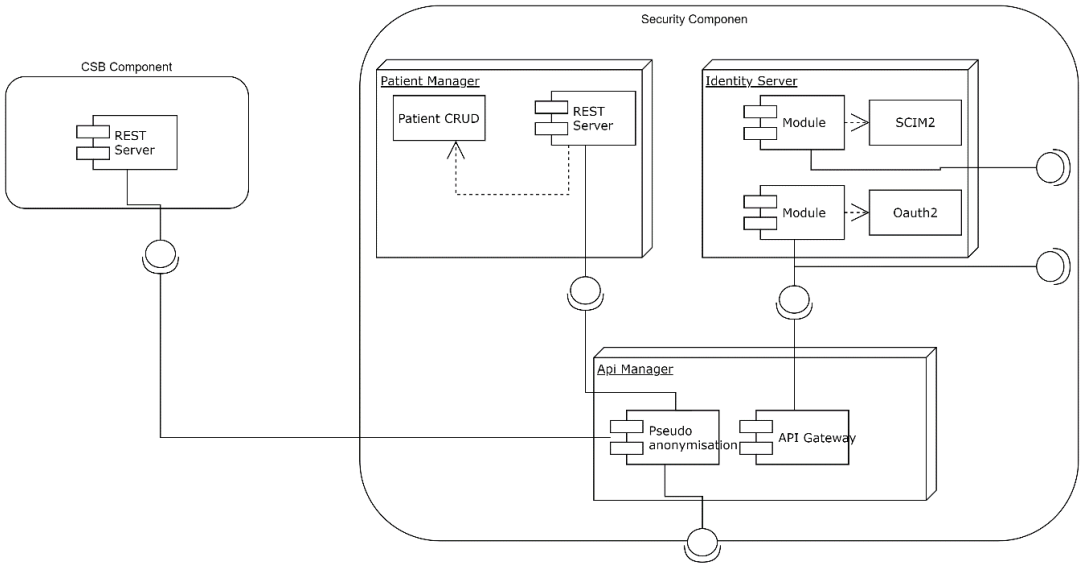


Figure 23: Application architecture of CSB@SecurityComponent

The WSO2 IS provides secure identity and access management by managing the identity of the end-users efficiently and by centralising their administration and monitoring. WSO2 IS enables extensible customisation to fit the needs of the RETENTION project, even though it is an OTS product. WSO2 will be used by both CSB and CIG administrators to manage the end-users through both its management console and its RESTful API. Apart from the registered end-users, WSO2 IS can be used as an identity provider for third-party systems that

[2] https://wso2.com/

have their own set of users. WSO2 Identity Server is an API-driven open source IAM based on SCIM[3]. OAuth2 and OpenID connect provide the notion of claims, which are extra information that we can add to the user's profile to suit the goals of the project. In this context, during the creation of a study participant a unique Pseudo-ID (Pseudo-ID1) is generated for each. This Pseudo-ID is then used for data pseudonymisation by WSO2 API manager.

The WSO2 API Manager's main features are the definition of RESTful APIs, the integration of governance policies, and access control with OAuth2. It supports OpenAPI (formerly Swagger) specifications and manages throttling, access level, and integration with various identity providers. It secures, protects, manages, and scales API calls by intercepting API requests and applying policies, such as throttling and security, using handlers, and managing API statistics. Upon validation of a policy, the Gateway passes Web service calls to the destination backend. If the API call is a token request, the Gateway passes it directly to the WSO2 Identity Server (Figure 24).

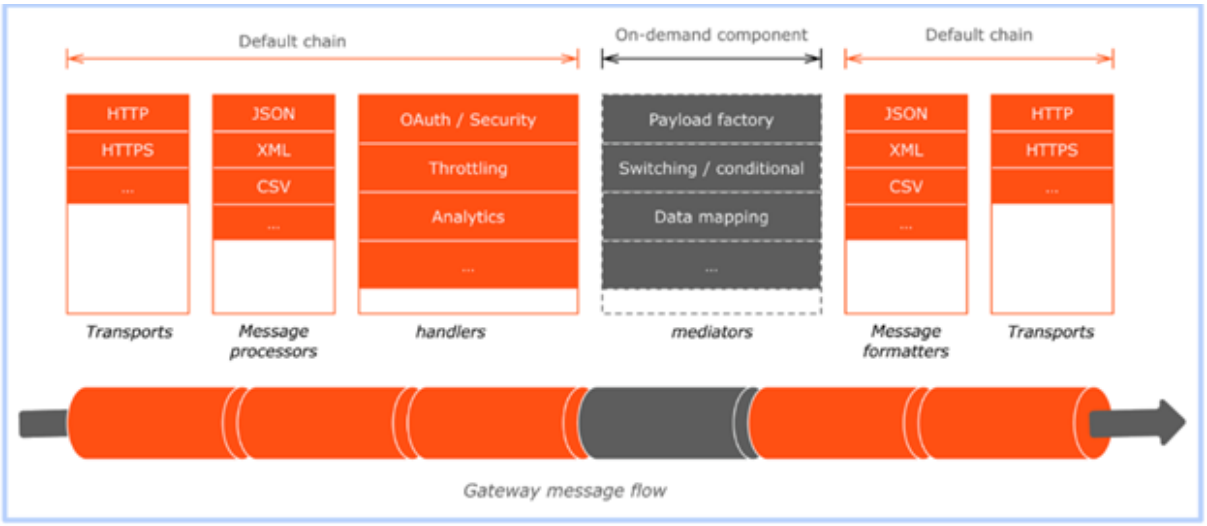


Figure 24: Message Flow

Messages that reach the Gateway are processed as follows:

- When a request hits the API Gateway, it is received by the Transports module, which is responsible for carrying messages in a specific format. The transport provides a receiver and a sender (for receiving and sending messages accordingly).
- The receiving transport selects a message builder, based on the message's content type, and uses the selected one to process the message's raw payload data and convert it into a common XML, which the Gateway mediation engine can then read and understand.
- The request is passed through a set of handlers that applies the quality of services on the request message, enforces security, limits request rate, and applies transformations on API requests if applicable
- After all the requests are routed to the backend endpoint, a message formatter (selected based on the initial message's content type) is used to build the outgoing stream back into its original format based on the message.

[3] http://www.simplecloud.info/

- The transport sends the message out of the Gateway.

In RETENTION, the WSO2 API-Manager Gateway will be the only exposed REST interface of cloud and CSB, all other components will expose their rest interfaces only on a private subnet. By utilising this approach, we guarantee that we provide authentication and authorisation to the RETENTION services. During the deployment of the CIG and CSB, each RESTful service of the components that will be exposed will be assigned with roles that the user needs to have to invoke the rest service. After the initialisation of the REST services a sequence of how the REST call can be invoked is depicted in the following image (Figure 25).

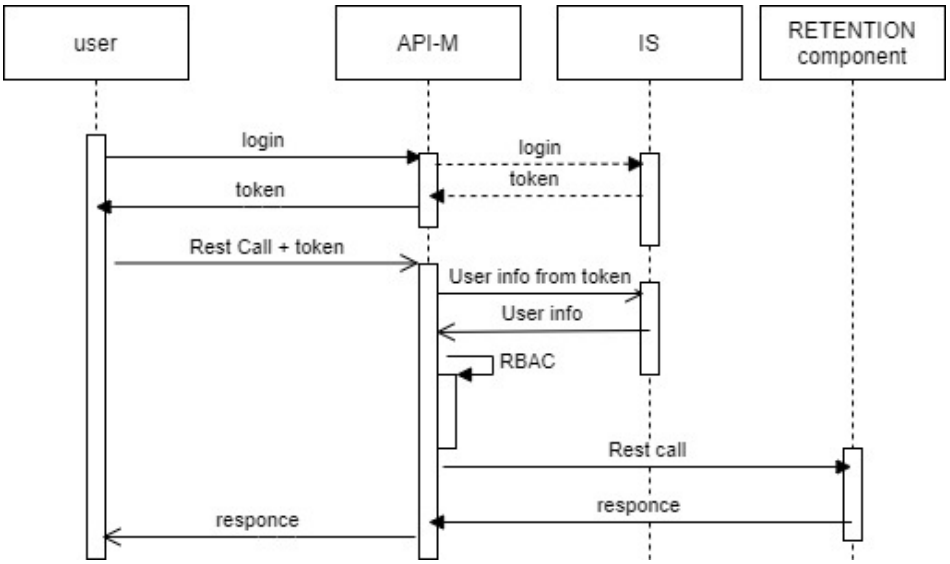


Figure 25: Authentication and Authorisation sequence

- During the login phase of the end-user, the user gets an authentication token. As already mentioned as soon as APIM receives a token-related call, it redirects it to the IS.
- Later, when the user makes a REST call to the RETENTION Component it also uses the authentication token.
- The APIM then will get the end-users info (i.e., claims, roles) from IS.

Then based on the defined roles specified APIM will decide if the user can invoke this service. If so, then APIM will proxy the request to the SB-Cloud component.

3.5.5.1 RETENTION Continuous Security and Privacy Assurance Platform

The RETENTION Continuous Security and Privacy Assurance Platform (RETENTION SPAP or SPAP), an instance of the Security & Privacy Assurance Platform developed by SPHYNX, is a subcomponent responsible for monitoring, testing, and assessing the runtime operations of GIC and CSB platforms. This subcomponent will, through an Event Captor Module developed for the purpose, audit critical components and processes of the infrastructure while leveraging monitoring mechanisms developed in the context of the project. Based on that input, the component will provide an evidence-based, certifiable view of the security posture of both platforms, with accountability provisions for changes that occur in said posture and the analysis of their cascading effects, supporting the runtime checking based on sets of associated claims and assessments. Also, the methodology and procedures for the automation of security certification are part of this component,

providing different certification models tailored to, e.g., specific security standards, service level agreements, or legal and regulatory obligations (e.g., GDPR).

The real-time, continuous assessment of the security posture of the organisation's platform will be enabled by a purpose-built Event Captor Module using Elasticsearch (ELK stack), which will be responsible for aggregating the required evidence from multiple sources related to the operation of individual components, as well as the overarching processes where these components are involved in. Several built-in security assessments addressing the Confidentiality – Integrity – Availability (CIA) principles among custom metrics that will be tailored with respect to the platform's components will be utilised, leveraging an evidence-based approach, to provide security assurance assessments with certifiable results. A high-level view of SPAP's architecture is presented in the following figure (Figure 26).

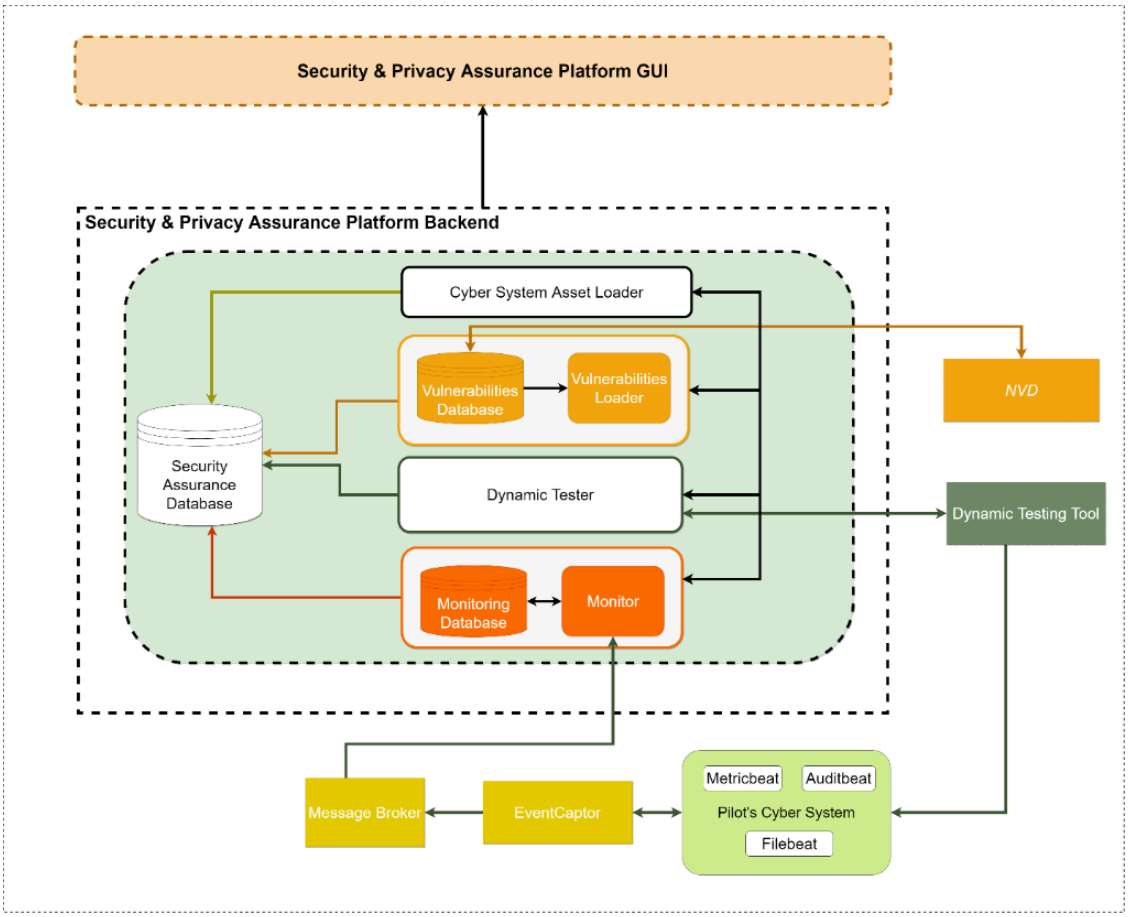


Figure 26: Security & Privacy Assurance Platform High-level architecture.

The SPAP is comprised of five primary modules:

- Cyber System Asset Loader: The component responsible for receiving the cyber system's asset model for the target organisation. This model includes the assets of the organisation, security properties for these assets, threats that may violate these properties, and the security controls that protect the assets and is based on an Assurance Model.
- Vulnerability Analyser: The Vulnerability Loader is responsible to identify known vulnerabilities of assets defined within an organisations' asset model. This component automatically constructs the Common Platform Enumeration (CPE) per asset and then retrieves its Common Vulnerabilities and

Exposures (CVE(s)) by searching in a local copy of the National Vulnerability Database (NVD). This copy is continuously updated by utilizing an in-house component that fetches the latest known CVEs from NVD's JSON files.

- EVEREST: A runtime monitoring engine, built-in Java, that offers an API for establishing the monitoring rules to be checked. This module is composed of two submodules: (a) the monitoring database and (b) the monitor. The role of the module is to forward the runtime events from the application's monitored properties and finally obtain the monitoring results.
- Event Captors: The Event Captor is a tool that, based on collected data and triggering events, formulates a rule or a set of rules and pushes the latter towards the monitoring module for evaluation. Data and events are mostly collected through Elastisearch based on lightweight shippers (namely Beats), such as Filebeat, MetricBeat, PacketBeat, etc., that forwards and centralises log data. Data can also be collected through Logstash, an open server-side data processing pipeline that ingests data from a multitude of sources transforms it, and then sends it to ElasticSearch. The Event Captor is initiated through the respective REST calls from the monitoring module.
- Dynamic Tester: The component responsible for initiating the testing assessment. The module consists of two components: (a) the dynamic tester or manager and (b) the dynamic testing tool.

This section provided the initial version of the privacy and security mechanisms supported by the Security Component, to encompass initial descriptions of assets developed, as well as their rationale and interoperability. This description paves the way to the forthcoming D6.2, in which more features will be added to provide further insights and strengthen the security and privacy mechanisms.

4 Platform Infrastructure Deployment

4.1 Purpose

The integrated platform of RETENTION supports a hybrid hosting model, to support project and future extensions of the platform. As described in the relevant sections of this document, the main components that will be deployed on the infrastructure will be CSB and GIC. GIC will be hosted on a private cloud infrastructure, located at ICCS's server room. CSB instances are planned to be hosted by the pilot sites. In case this is not feasible for any pilot site, they can be hosted at ICCS, in a separate environment, to comply with the architecture of the platform.

4.2 Overview

Provides the foundation to facilitate execution of applications and services. Such technologies range from bare metal to serverless and enable organisations to realise the benefits of cloud computing. In RETENTION, we will implement the following three technology options for cloud deployment: bare metal, VMs, and containers. The selection will be done case by case, evaluating the best solution for each component of the platform. For modules that are part of microservice-based modules and are stateless and immutable, containers orchestration will be implements (such as Docker containers).

For RETENTION project, the network infrastructure design is a critical component of the project success, as it will be the backbone service of the whole platform. The network infrastructure design must meet the specific configuration requirements and network management needs for the following devices:

- Structured Cabling
- Servers
- Firewalls
- Routers and Switches
- Rack and Stack
- Automation
- DNS

The infrastructure that will be built for the purposes of the project will provide a continuous monitoring of the network infrastructure to ensure it is always up and running. An infrastructure lifecycle management will be adopted, to successfully handle the capacity of the available resources and optimise them, based on the resource forecasting. As part of the infrastructure monitoring, most of the system modules will be executed in virtual assets (virtual machines), so tools to monitor the activity and performance of the VMs will be used. All the modules will require to pass a series of tests to verify that they fulfil their purpose before they are used in the production. Unit and integration tests will be part of the acceptance criteria to include a component in the final system. Extensive testing in a sandbox environment will be performed before the integration of each component to the hosting services.

Regarding the requirements for high availability (a feature which provides redundancy and fault tolerance) the goal is to ensure that the service is always available even in the event of a failure. To ensure this several servers will be set up in a cluster, so that if one server fails the others will continue processing and take on the processing load of the failed server. They will also provide several backup internet connections to ensure

the services are still accessible on the internet. An automatic failover mechanism will be installed, to assure the uninterrupted service provision in the cases of device malfunctions. Regarding other hardware fault tolerance requirements, RAID setup for the hard drives will be implemented in the servers. It will provide redundancy and fault tolerance, along with a positive impact on performance.

Hardware requirements

- Data storage and hosting will be in a single location, serving all the clinical sites. The RETENTION hosting setup will require a minimum of three hosts, all with access to the Internet and with an individual fixed public IP address. These can be either physical server computers or virtual machines running in a self-hosted data-centre infrastructure.
- Each computer host must have the following minimum specifications: i) 4 Core CPU, 4 vCPU or equivalent, ii) 64 GB of RAM for the backend hosts, iii) 1 TB SSD.
- Regarding the network, all hosts must be in the same subnet, each with a fixed public IP address, and must be connected to the Internet to get updated and to communicate with the Edge Mobile Application and the Edge Gateway. The minimum specifications for the network are: i) 1 GB Ethernet (internal network), ii) Latency max 50ms (internet), iii) 100 Mbits/second for bandwidth (internet), iv) Fixed public IPs (one for each host).

4.3 Integration & Testing

Upon completion of the applications development, the installation of the main systems components and their corresponding interconnections will follow (applications and systems software). Therefore, the readiness of the system, its adaptability, its flexibility in the integration of requirements, and the clinical team needs, will lead to the successful development and completion of the project through the critical success factors.

Software problems are much more difficult and much more costly to find and fix as the delivery-completion time of a product approaches. For this reason, it is necessary to constantly confirm the "quality" of a software product, in terms of its functionality and performance. Confirmation of the quality of a product includes procedures, such as the creation of "scenarios" to test the behaviour of the system, the entry of test data, the control of special procedures, and so on. The application software quality assurance methodology is briefly described below. The software quality control process is one of the most important activities of the project.

Software-hardware integration

For the integration, a staged approach is uses, as follows:

Stage 1: Installation

To organise the installation, the following steps will be followed:

- Virtual or On-site inspection of the infrastructure that will be used
- Study of installation requirements of the individual applications and scheduling of actions
- Creation and preparation of virtual machines
- Creation and generation of docker containers from each partner
- Gather the required docker containers for the installation

- Installation of the software stack in the available infrastructure
- Integration of the system
- Customisation of software for integration in the network environment

All modules will be implemented at this stage:

- GIC
- CSB
- EDGE

At the end of the phase, the initial environment of the above applications will be configured for every module (GIC, CSB and EDGE).

Stage 2: Configuration and Adjustments

At this stage, the necessary adjustments and configurations of the Applications will be made, in relation to the requirements of the individual services of the RETENTION System. The system and the application software customisation teams will deal with the configuration and adjustments that the system needs to function correctly as described in this document and the requirements. The Application Customisation and Design will consider the operational procedures of the project, the needs of the clinical team and needs of the system, and they will be mainly concern:

- the target user groups and the rights that will be assigned to them
- the roles they will play during the operation of the system
- the particularities of the clinical teams
- the particulars of the offered infrastructures
- the objectives of the project (as declared in the DoA)
- the organisation and Administration of the project, and
- any other elements that emerge during development, stage 1

At the end of stage 2, a configured and ready system is offered to the users for testing.

Integration technology

The technical team has chosen Docker (Docker, 2011-2022) as the underlining integration technology to be used for the system. The following Docker containers are required (Table 15):

Table 15: RETENTION docker containers

Logical subcomponents	Module	Total No. of containers
GIC Dashboard	GIC	6
Model specification tool	GIC	6
Disease insights	GIC	6
DBA Engine	GIC & CSB	7
DB-data (FHIR and non-FHIR)	GIC & CSB	7
Data models	GIC & CSB	7
DSS	CSB	6
CSB dashboard	CSB	6
Security component CSB	CSB	6
Security component GIC	GIC	1

REST API	GIC	1
REST API	CSB	6

Testing

The testing will be performed by conducting detailed tests and system performance tests and will be based on Scenarios and data prepared by the technical team and will be a complete guide for the process and testing of the systems. The following testing subtasks are scheduled to be performed (Figure 27):

- automated unit tests by each technical partner
- automated application and interfaces' tests by each technical partner
- integration tests by the technical team
- system test
- user acceptance tests, will be conducted with the clinical team and selected patients, as advised by the clinicians

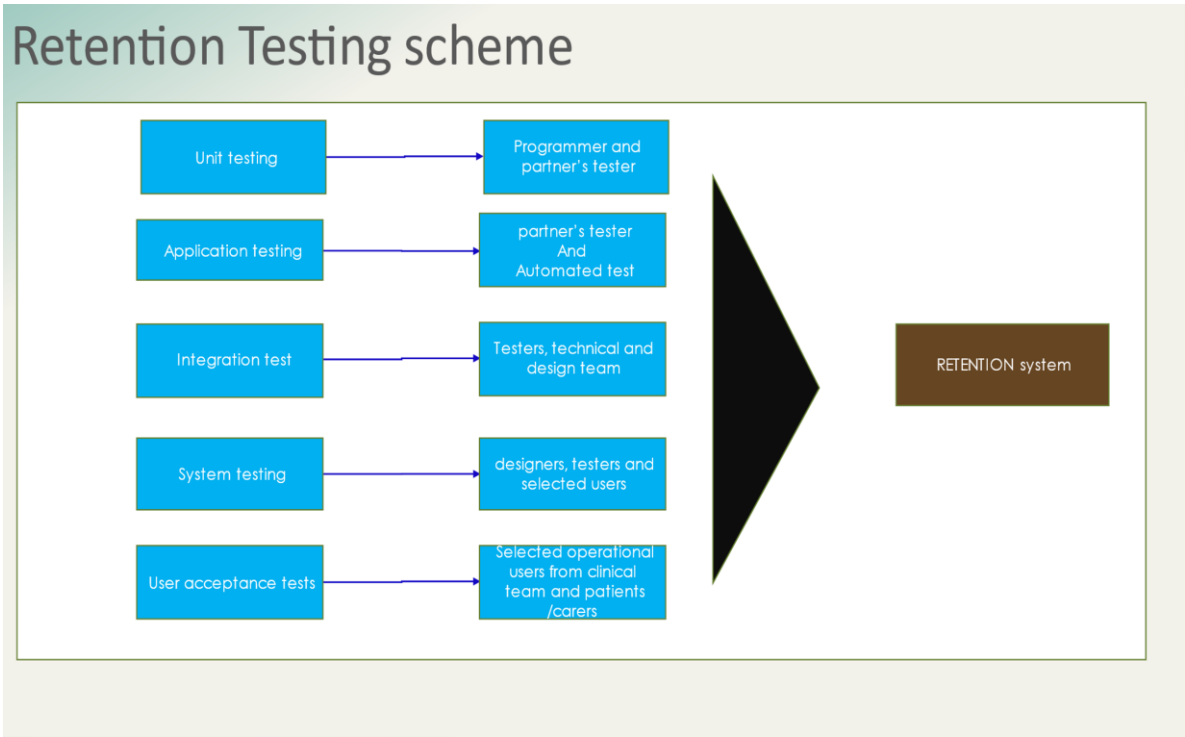


Figure 27 : Testing scheme

Unit testing

Developers that control the individual program units/sections and the corresponding testers, will have the first go for testing the individual subsystems of RETENTION. The programmer/tester checks that the program starts and executes its functions, validates the data entered on the screen or creates new entries in the database. The Unit Testing process certifies that the design and integration of all components of a subsystem or system, from the lowest level of analytical design to the highest level of Architecture, fully meets the requirements and their role in the development of the final system.

The testing process is scheduled to consider technical characteristics of the deployed RETENTION solution; thus the compatibility and interoperability of the different subsystems or components it consists of. The

anticipation is that the solution is 100% functional, efficient and covers the requirements of the RETENTION project.

Application testing

In this part of the tests, the individual applications will be tested against the testers and an automated test procedure that will ensure that the same results will be achieved with every revision of the system. The business logic is tested here, for coherence, consistency, and correct logic flow.

Integration testing

It is the next level of testing, aiming to confirm that individual program segments can communicate. Checks that the user can connect and navigate from one screen to another successfully. This level does not focus so much on the business logic of the operations but mainly on the robustness / reliability of the system. The Integration Testing process takes place in the physical space where the major subsystems of each (major deliverables) are installed. The key components are listed and derived from the basic system design. In integration testing, it is directly ascertained whether the subsystem operates in accordance with the design and requirements and the possibility of its cooperation with other subsystems of the project is certified.

Part of the Integration Test is the control and certification for the safe and accurate transfer of data between subsystems when they are interconnected and operational.

System testing

The System Test proves to the technical team that the system operates according to their understanding of business requirements. This is a complete test of all functions / subsystems by the Project team. The result of control at this level is to ensure that the system meets operational requirements. The system testing process refers to the whole system now when it is installed and operates in a pre-pilot phase and is distinguished in two levels. The first without data and the second with test data which are not going to be used in normal operation. The System Test will include the following:

- Examine the system with data, carefully processing the data and extracting correct and expected results.
- Confirmation and certification that user requirements are fully met, and the system has the expected supply and operation.
- Stress Test at the level of simulating an exceptional load of the system with virtual users. In this case, the strength and tolerance of the system to multiple processing requirements and its response times are also monitored.
- Reliability checks, including tests and checks for system availability.

User Acceptance test

It proves to the end users that the system works according to their own vision for their business requirements. In this phase, users use the program to process business processes and check for the correctness of the result. The entry of data on a screen and their processing by the system must be consistent with the DoA and the requirements document. The focus of the tests at this level is the efficient and correct execution of the business processes and they are not interested in possible system failures because it is the job of the tech team to correct all the problems that will arise during this phase.

In addition, the performance of the system is important and not only its proper operation, with the typical example of completing the actions in the desired time. It is noted that this phase is the last opportunity for end users to verify the correctness and functionality of the system before its final adoption.

Deployment

In the deployment phase, the system will be given to the clinical teams and the patients/carers to start filling with the real data. The system will be deployed in two phases: a) in phase one the system will collect data from all the groups, without passing any info to the patients, feeding in the meantime the AI models, and b) in the second phase, it will be able to fully support the clinical teams and their respective patients.

The main components of deployment are shown below:

- Availability. The system will be available to clinicians and their patients as specified in the functional specifications. The critical components of the system shall be available the users 24x7x365. During this time, the system shall provide 99.5% or greater availability for all critical functions. Automatic failover of critical components (as required to support the given availability) shall be provided.
- Security. The system will be fully secured, as outline above. The security of the system and the protection of sensitive personal data, in full compliance with the GDPR, is a basic requirement of the project, and an important factor in user management and other requirements. For the whole duration of the project, data will be managed as per the requirements of GDPR (The General Data Protection Regulation 2016/679) and/or any other applicable legislation. Some elements of this data, such as details of Patient Records, will be categorized as *Personally Identifiable Data*, i.e., information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual, will be only available to the clinicians and strictly restricted to anybody else. The data shall be used only for the purpose for which it is requested to be utilized, including and applicable to system admins and operators.
- Operations and Support (Operations). Operations and support will be conducted by each clinical site with full support from the technical team. The technical team will support the sites, that the sites will support the patients. Operational support will include two kinds: a) support from each site's personnel to its patients, and b) from the technical team to the site personnel (clinical or technical) and/or patients as second level support.

5 Conclusions

The current deliverable presents the initial reference architecture for the RETENTION Platform, by offering a detailed description of all components (modules) of:

1. the Global Insights Cloud,
2. the Clinical Site Backend,
3. The Patient EDGE components and devices.

The Global insight's Cloud (CIG) supports the data analysis, the ML model training, and the production of high-performance models. The GIC consumes anonymised data from CSB sites later on to transmit back the output of ML analysis (trained models) to advance the formations of evidence-based personalised interventions.

The Clinical Site Backend supports the daily patient check-up, the data gathering (i.e., initial patient administration and baseline, devices'/sensors' data), applies ML models and triggers previously vetted (by clinicians) interventions.

The Patient Edge enables the continuous monitoring of patients via the collection of usage data they produce (medical, physiological, behavioural, psychosocial, and real-world data), and provides means for collecting feedback and presenting suggestions.

The infrastructure to support this solution is based on VMs and Docker containers and the system will be cloud based. A description of integration of the system and the testing procedures was provided.

Representative mockups of the intended to be developed interaction elements are presented in the appendices. They focus on providing easy to use intuitive user interfaces, considering the diverse backgrounds and needs of the different users (patients, caregivers, and clinicians).

The results of the two co-design workshops that were held to optimise design views and workflows are also presented in the appendices, in the form of workshop reports.

In conclusion, this deliverable provided an understanding of the RETENTION system, as seen from the technical point of view, focusing on the modules and sub-modules it consists of. This work will drive the activities of WP4, WP5, WP6 and WP7.

6 References

Basdekis, I. (2019). Evidence based public health policy makin: tool support. *IEE world con*.

Docker. (2011-2022). *www.docker.com*. Retrieved from docker.com: www.docker.com

EU. (2016, April 27). *Official Journal of the EU*. Retrieved from EU GDPR RULE: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Hatzivasilis, G. (2016). Software security, privacy Adn dependability: metrics and measurement. *IEE software*, vol. 33, issue 4, 46-54.

ISECOM-OSSTMM, V. (2010). *OPEN-SOURCE security testing methodology manual.* Retrieved from www.isecom.org: https://www.isecom.org/OSSTMM.3.pdf

ISO/SEC, 1. (2009). geneva, switzerland: iso.

Kruchten, P. (1995). Architectural Blueprints-The 4+1 view model of software architecture. *IEE software*, 42-50.

Matei Zaharia, R. S. (2016). Apache Spark: a unified engine for big data processing. *Communications of ACM*, 56-65.

Neuman, A. J. (1977). Post-processing audit tools and techniques. *US Department of Commerce - national Bureau of standards*, 11-14.

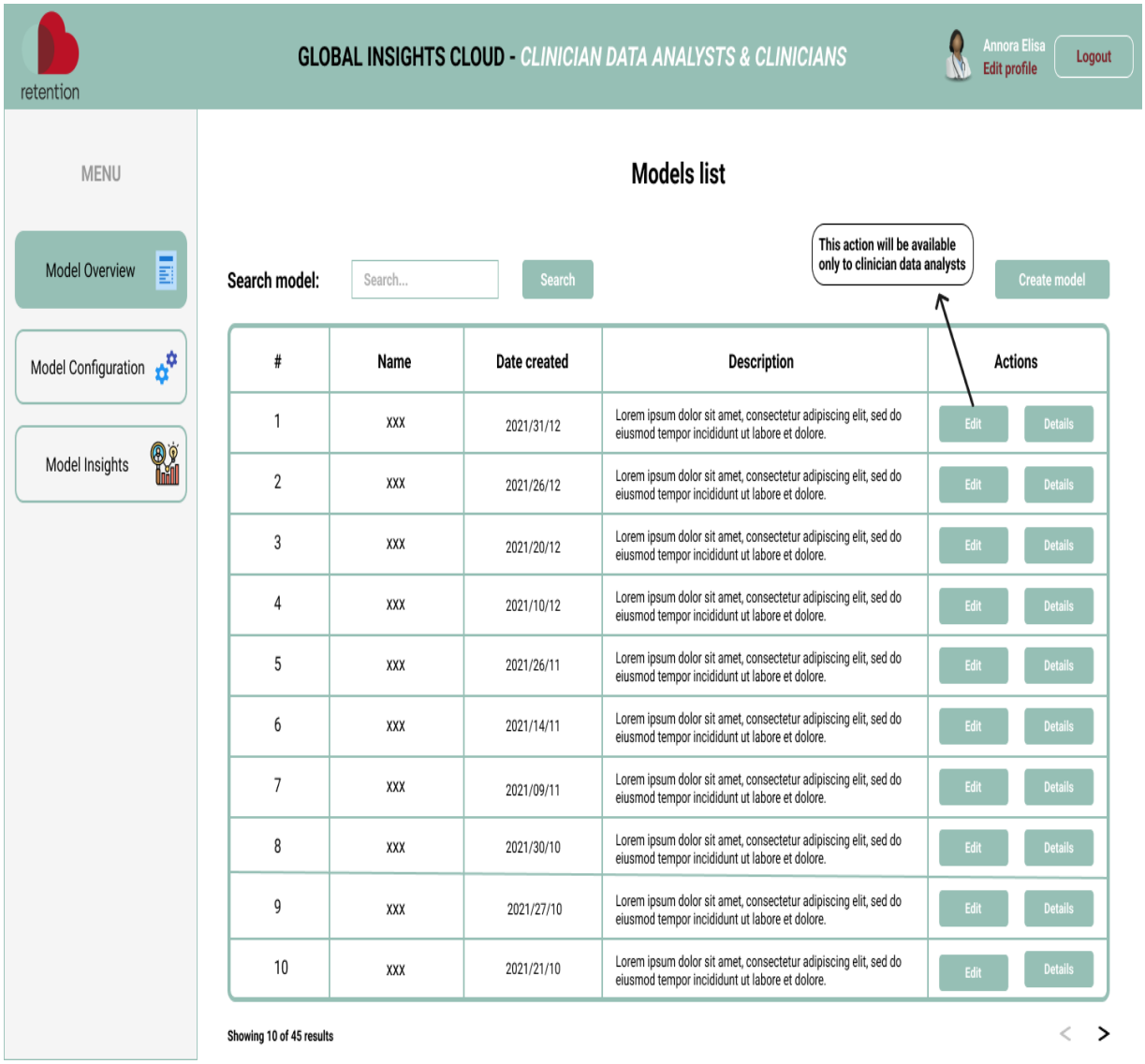
NIST. (2020). *Guideline for using Cryptographic standards in the federal government.* Retrieved from www.nist.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf

7 Appendices

Appendix 1: Global Insights Cloud Dashboard Mock-Ups (GICDBA) (AEGIS)

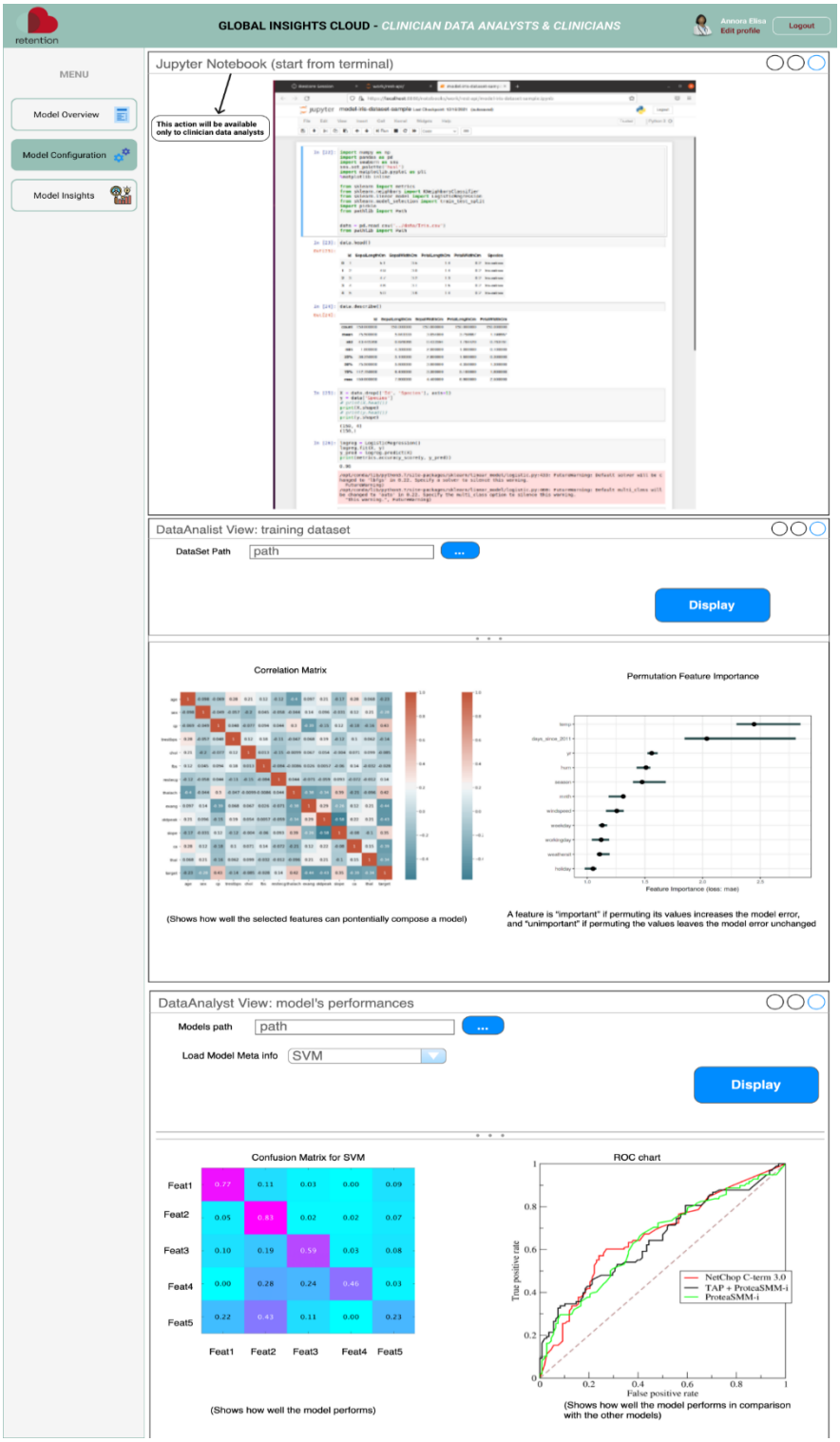
Model Overview: List of available models. The user can preview or edit an existing model.

Use Case: RTBD01, RTS06



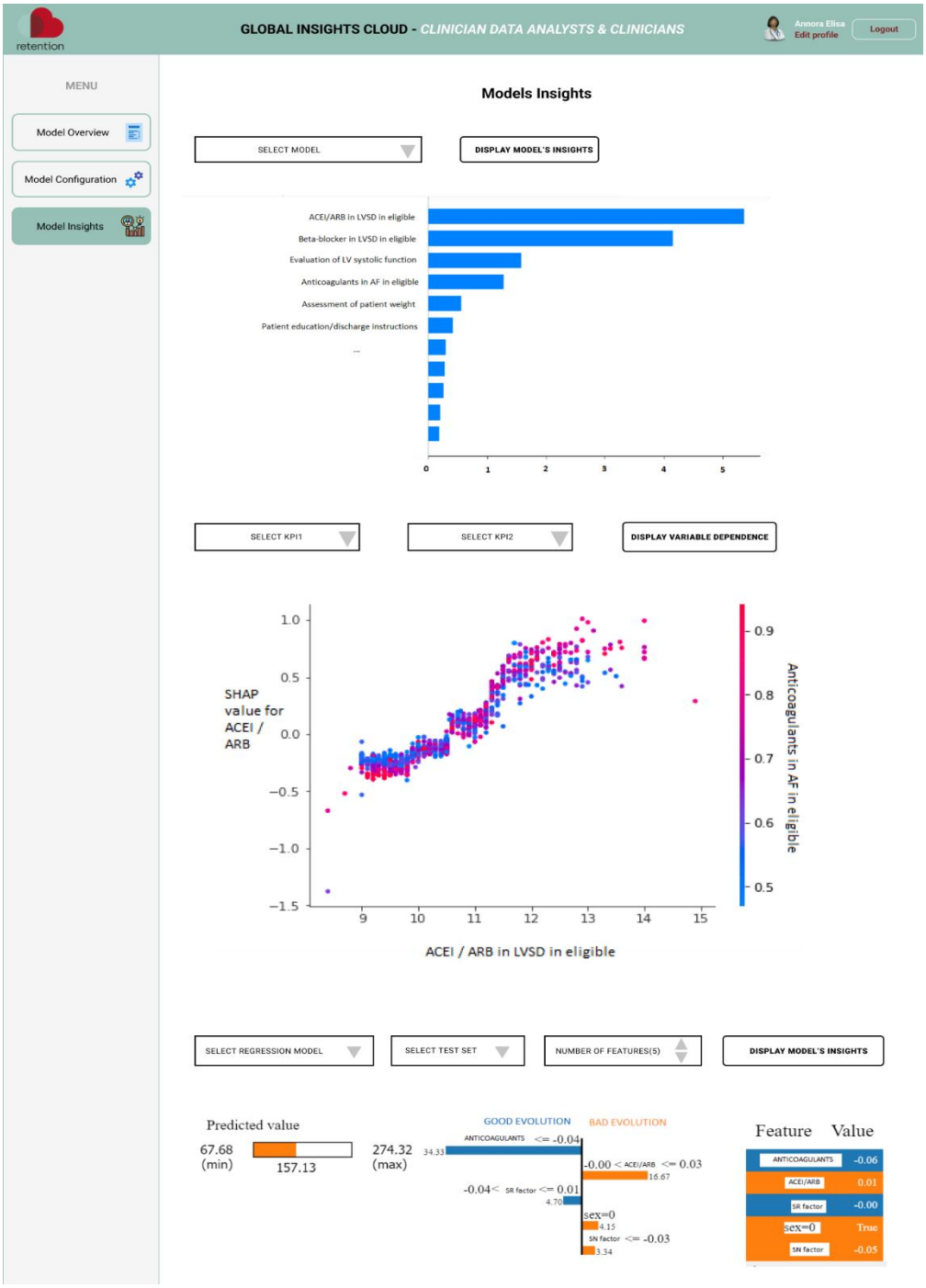
Model Configuration: The model creation and configuration environment. It also supports the training of the models.

Use Case: RTBD01, RTS06



Model Insights: Elaboration on model insights, the variables, the KPIs and the overall performance of the elected model.

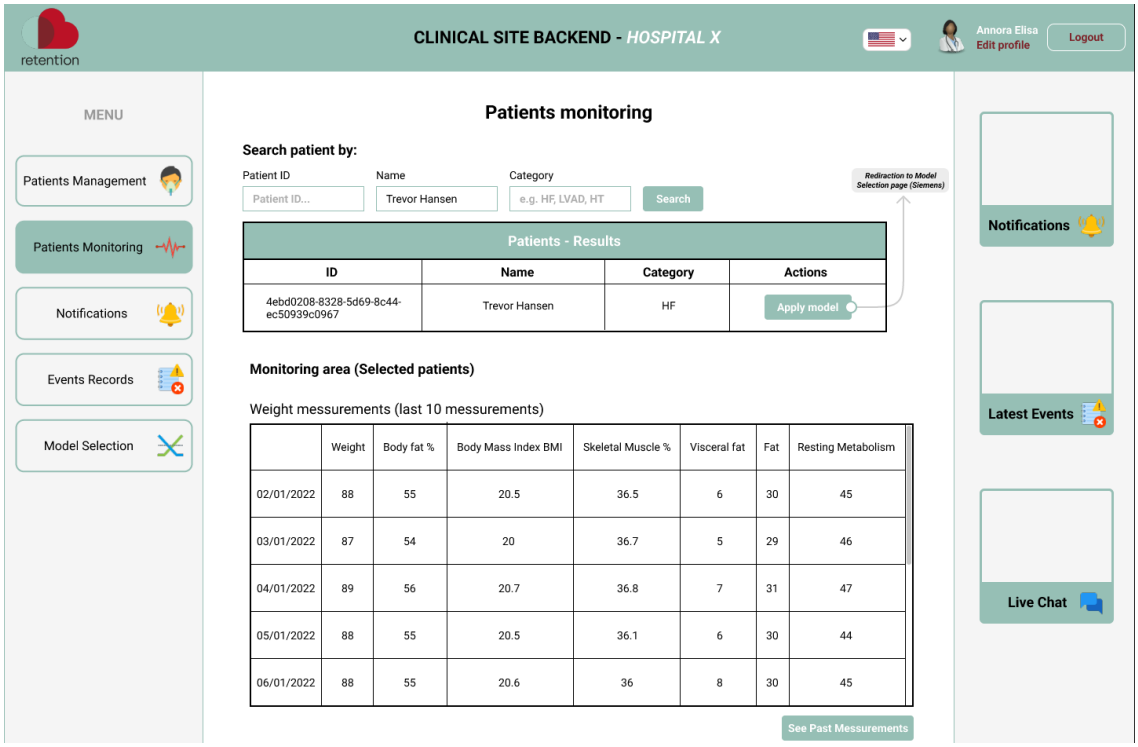
Use Case: RTBD01, RTS06



Appendix 2: Clinical Site Backend Dashboard Mock-Ups (CSBDBA) (AEGIS)

Pateints Monitoring: The frontend screen of the CSB includes the patient searching area and the monitoring details of the patient.

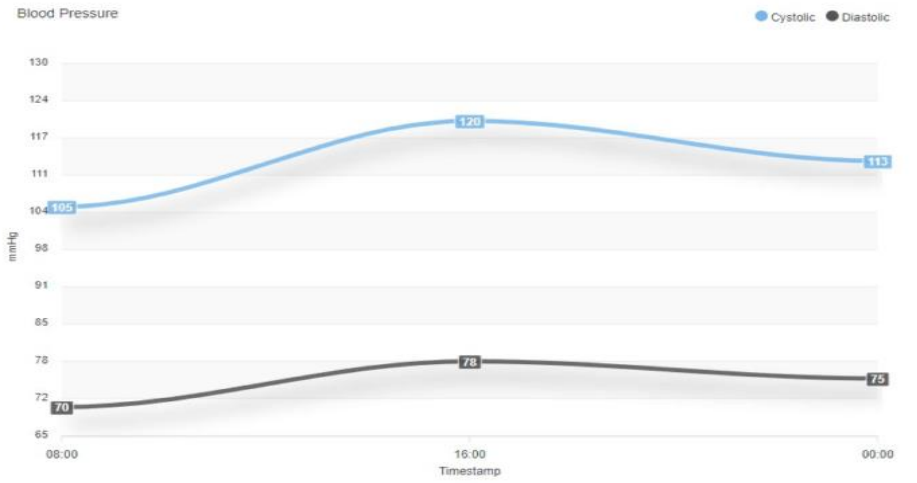
Use Case: RTCL01, RTCL02

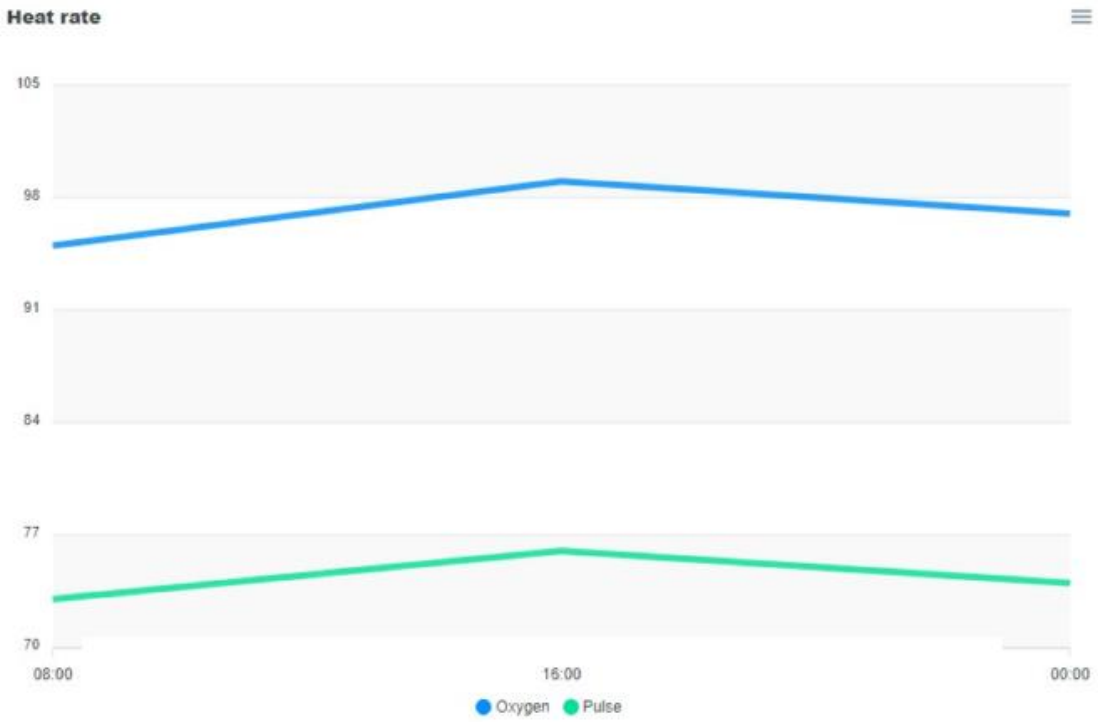


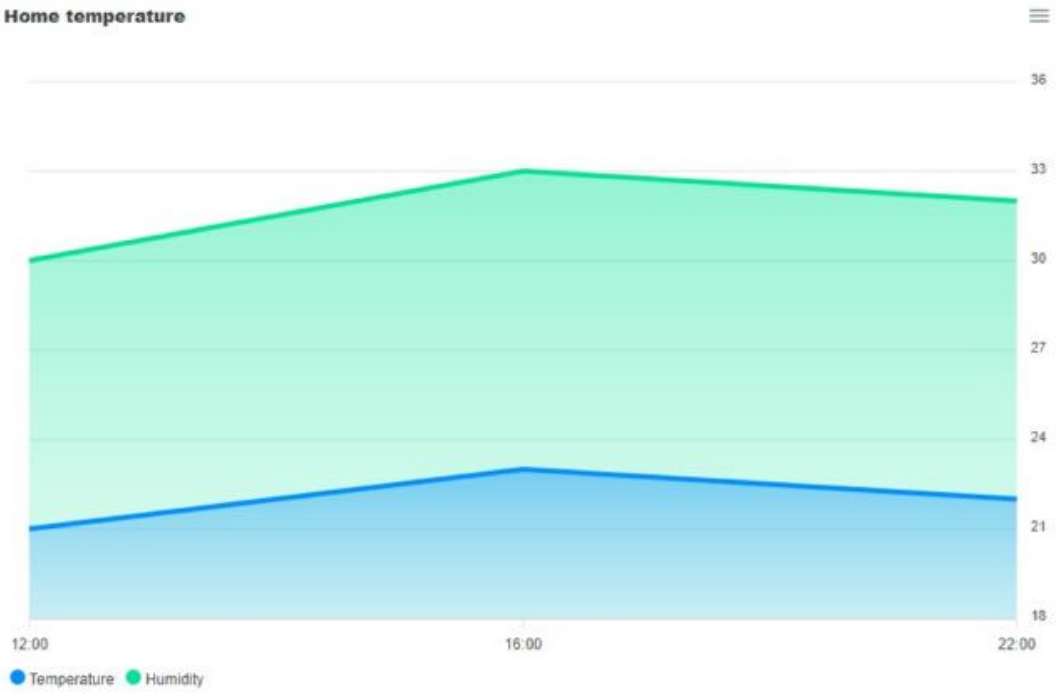
Temperature / Water / Calories (last 10 messurements)

	Body Temperature	Calories / Day	Water in	Water out
02/01/2022	??	??	??	??
03/01/2022	??	??	??	??
04/01/2022	??	??	??	??
05/01/2022	??	??	??	??
06/01/2022	??	??	??	??

See Past Messurements




Heat rate
105
98
91
84
77
70
08:00
16:00
00:00
Oxygen
Pulse


Home temperature
36
33
30
27
24
21
18
12:00
16:00
22:00
Temperature
Humidity

Weather / Polution

	Body Temperature	Calories / Day	Water in	Water out
02/01/2022	??	??	??	??
03/01/2022	??	??	??	??
04/01/2022	??	??	??	??
05/01/2022	??	??	??	??
06/01/2022	??	??	??	??

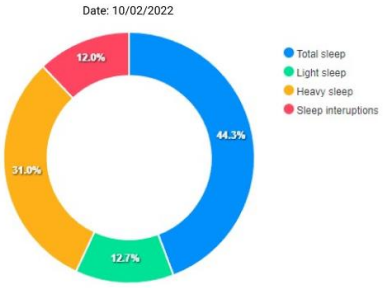
See Past Messurements

Activity monitoring

	Total steps	Distance (m)	Calories	Elevation (m)
02/01/2022	750	743	455	20
03/01/2022	700	690	400	15
04/01/2022	800	780	500	25
05/01/2022	780	760	475	23
06/01/2022	770	750	460	22

See Past Messurements

Sleep Metrics



Week average

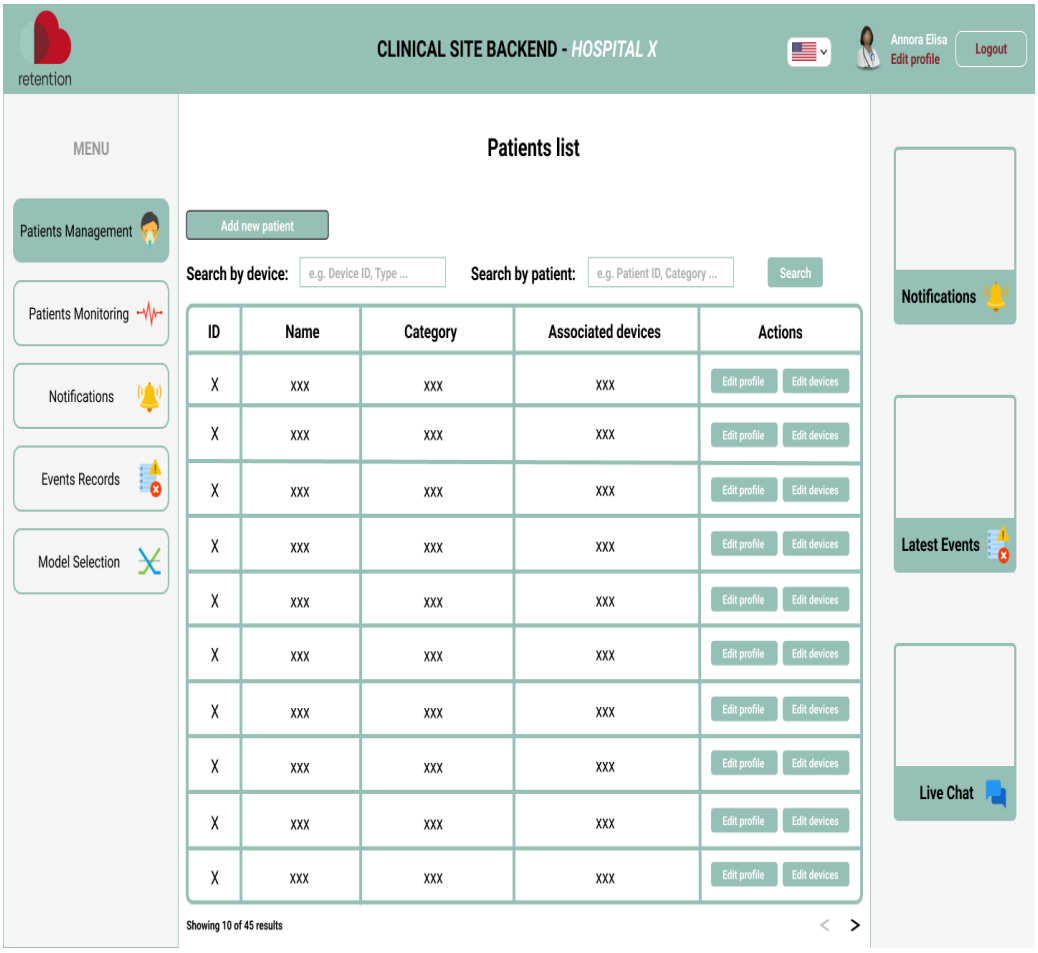
Total sleep: **7.35**
Light sleep: **2.11**
Heavy sleep: **5.15**
Sleep interuptions: **2**

In case selected patient is in VAD category, additional charts and tables will be displayed for the below categories

- Controller parameters
- Alarms
- RPMs
- Power consumption
- Flow
- Pulsatility index
- Coagulation values (INR)
- Driveline exit site evaluation

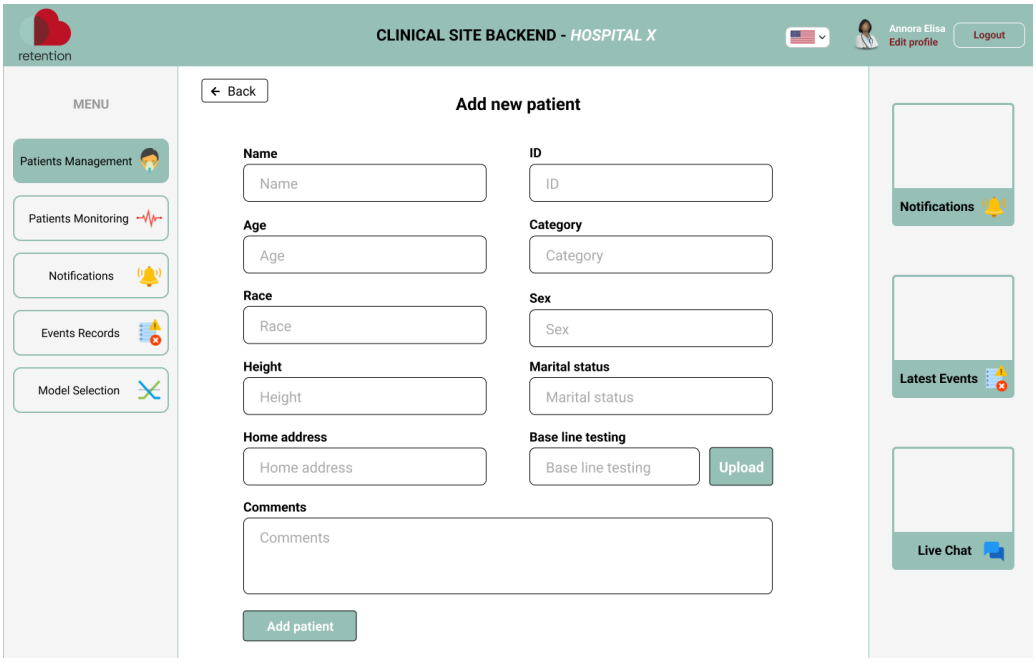
Display Patients: List of all patients, facilitating the edit of each profile and the association with specific device.

Use Case: RTCL01



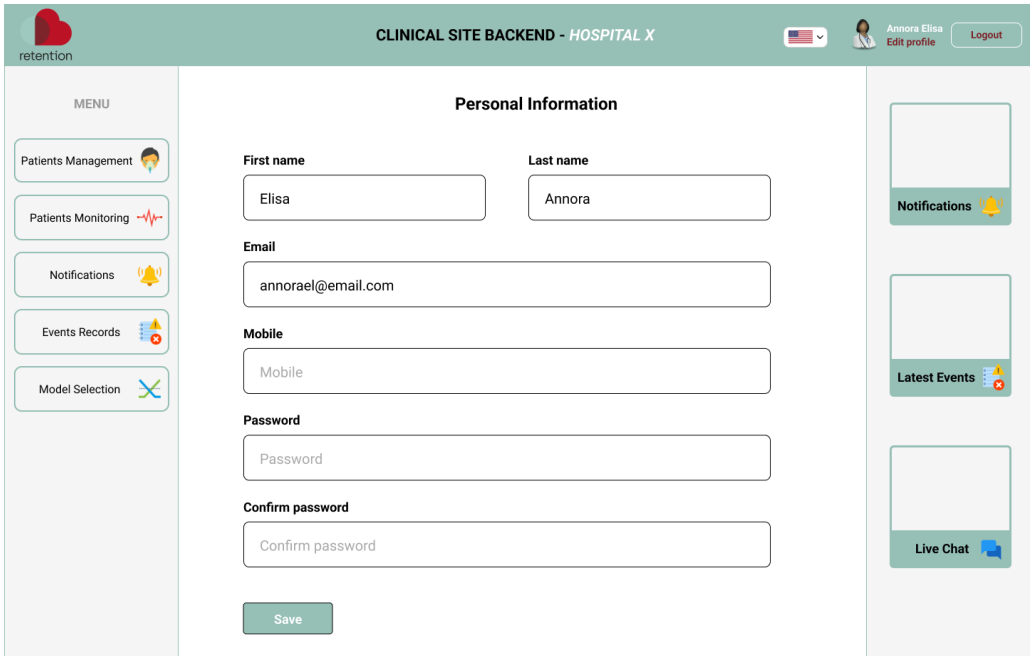
Add new patient: The creation of a new patient's profile/account

Use Case: RTCL01



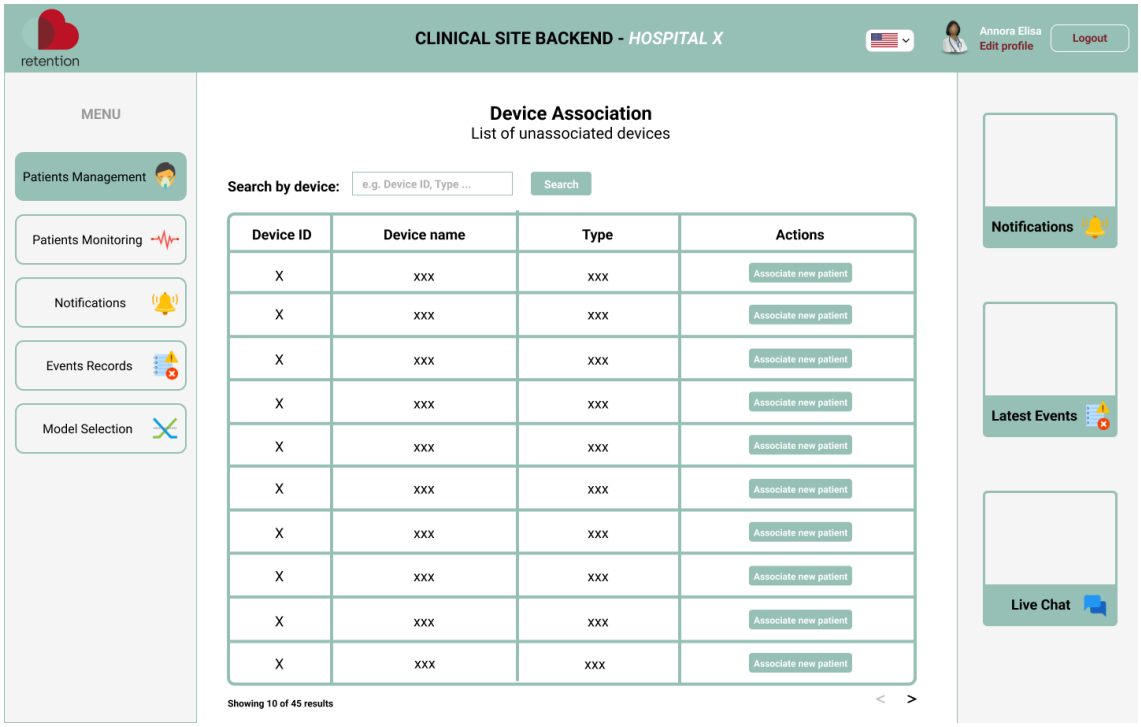
Edit Pateint's profile: The configuration page of a patient's profile

Use Case: RTCL01



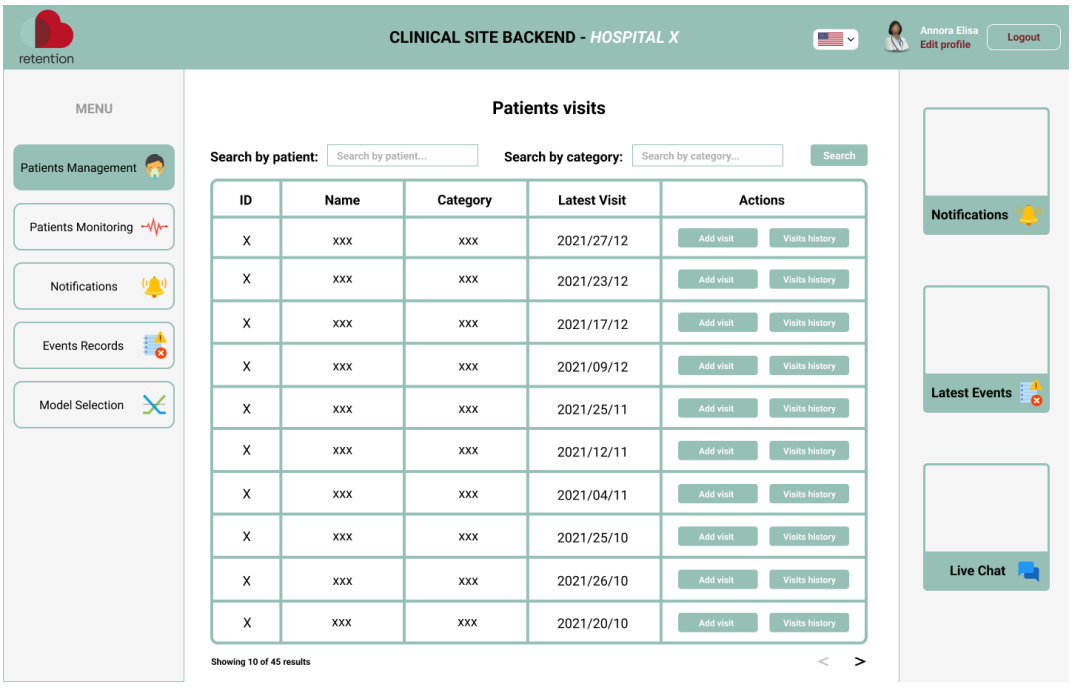
Device Association: Assignment of a spare device to existing patient.

Use Case: RTCL01



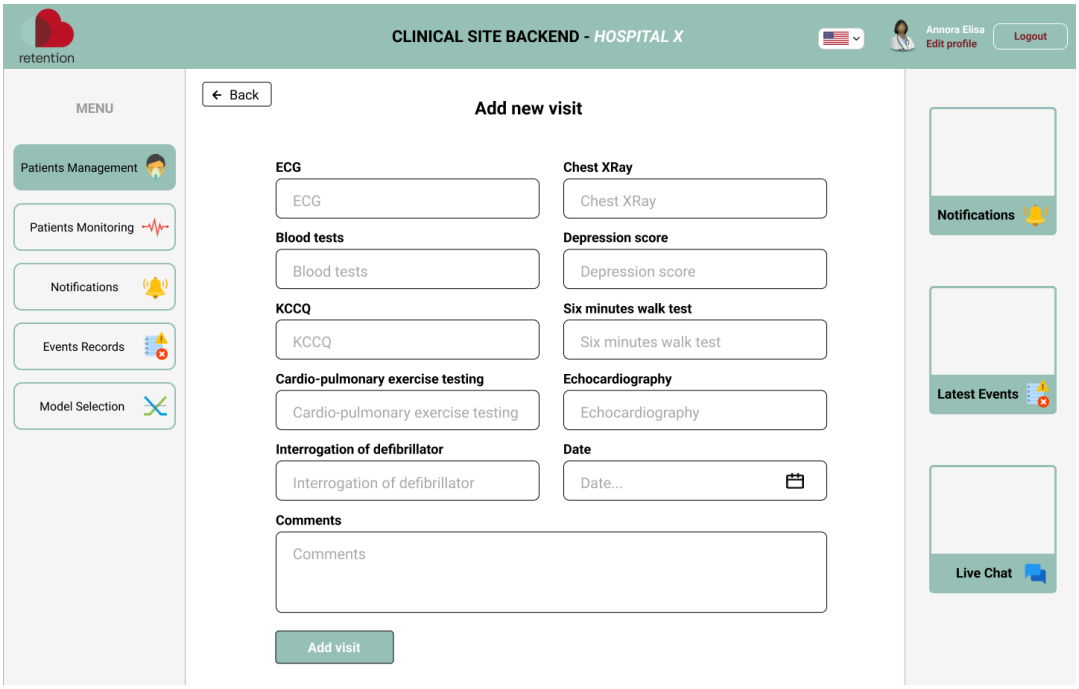
Pateints Vistis: List of all patient's visits for further editing.

Use Case: RTCL01, RTCL02



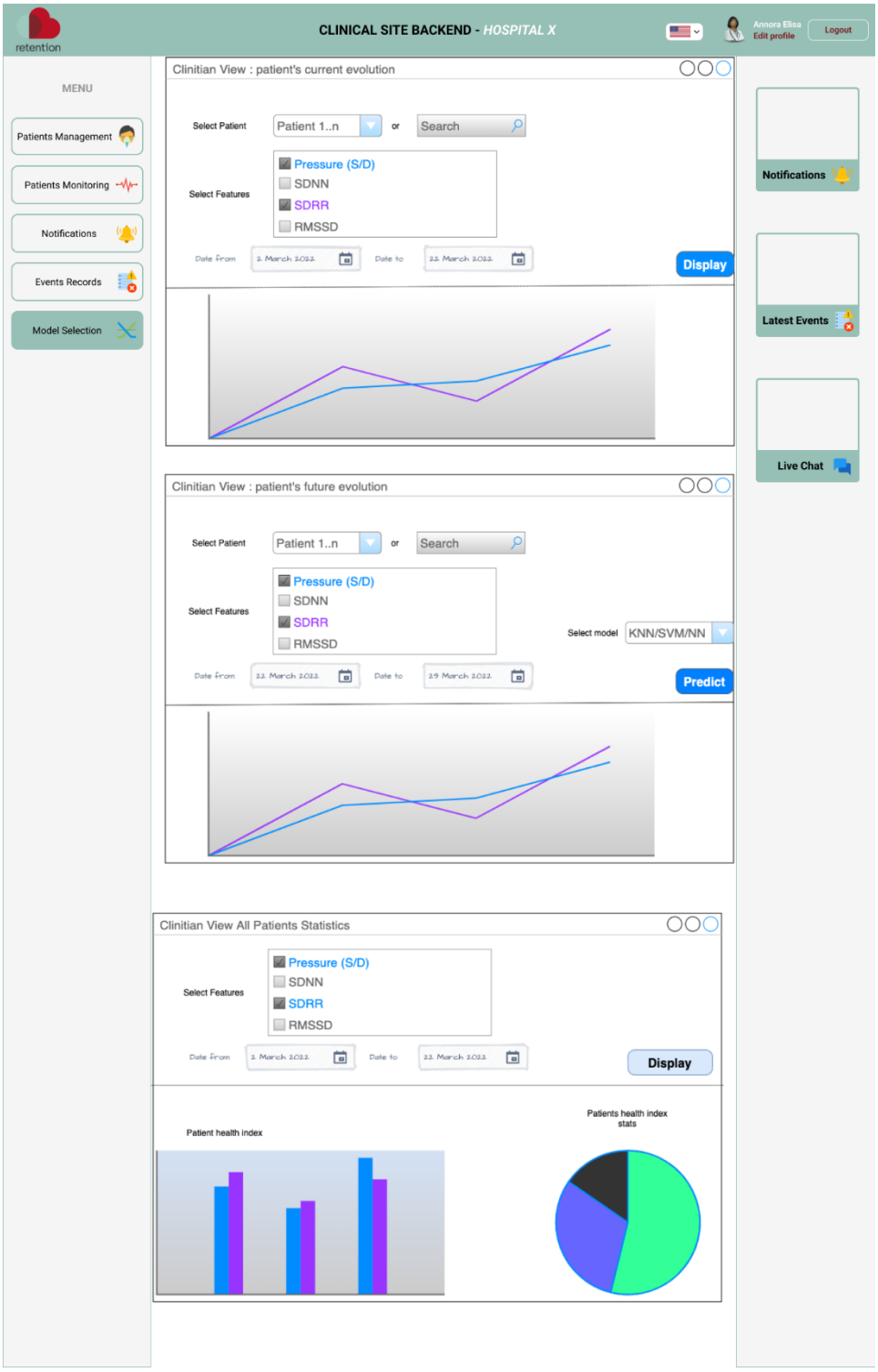
Add Pateint Visit: Data entry form for storing patient's visits and all related data.

Use Case: RTCL01, RTCL02



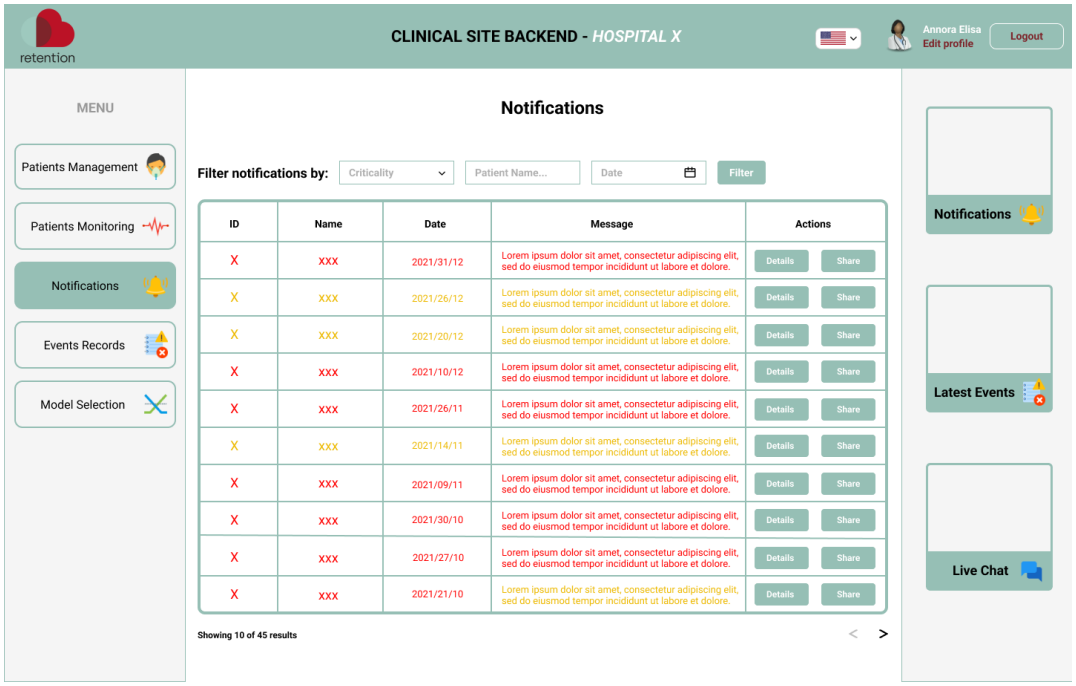
Model Selection: Insights of patient's disease evolution.

Use Case: RTCL01, RTCL02, RTBD01



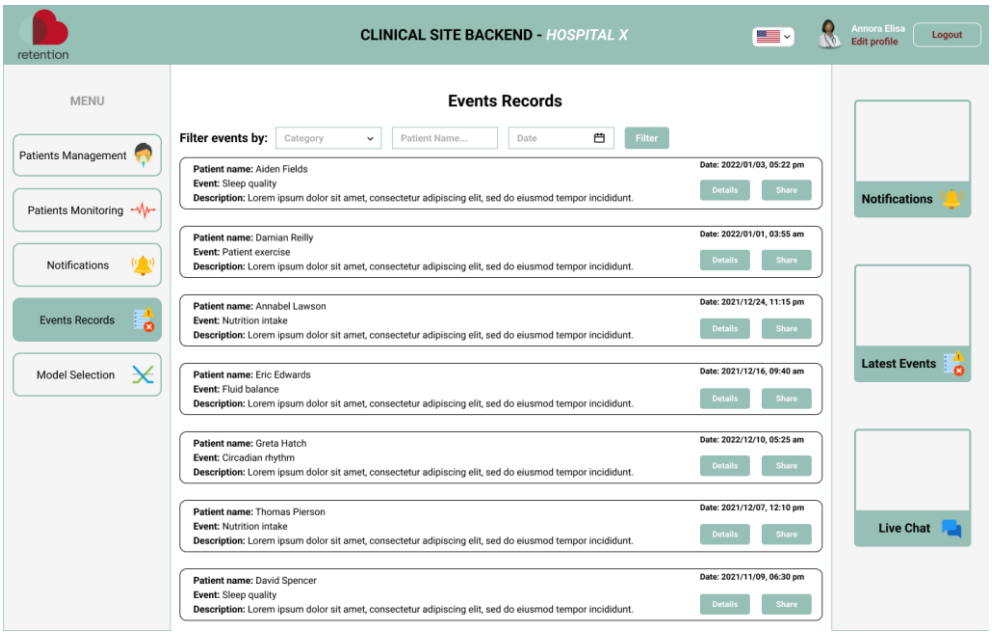
Notifications: List of all recent notifications.

Use Case: RTCL01, RTCL02, RTCL03



Events Records: List of all recent events.

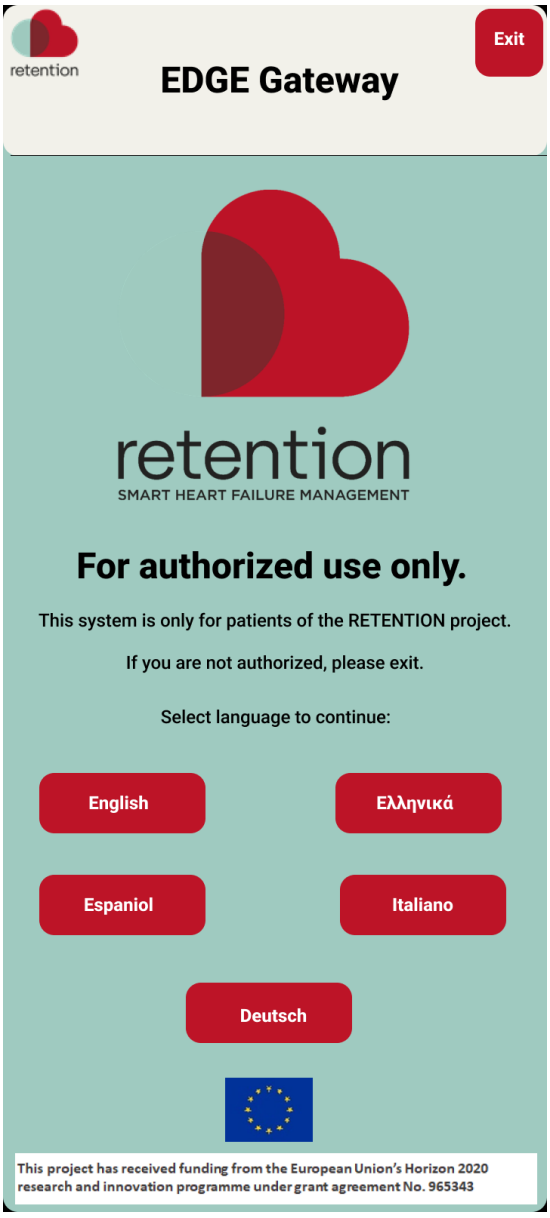
Use Case: RTCL01, RTCL02, RTCL03



Appendix 3: Patient Edge Mobile Application Mock-Ups (PEMA) (DM)

Introduction Screens

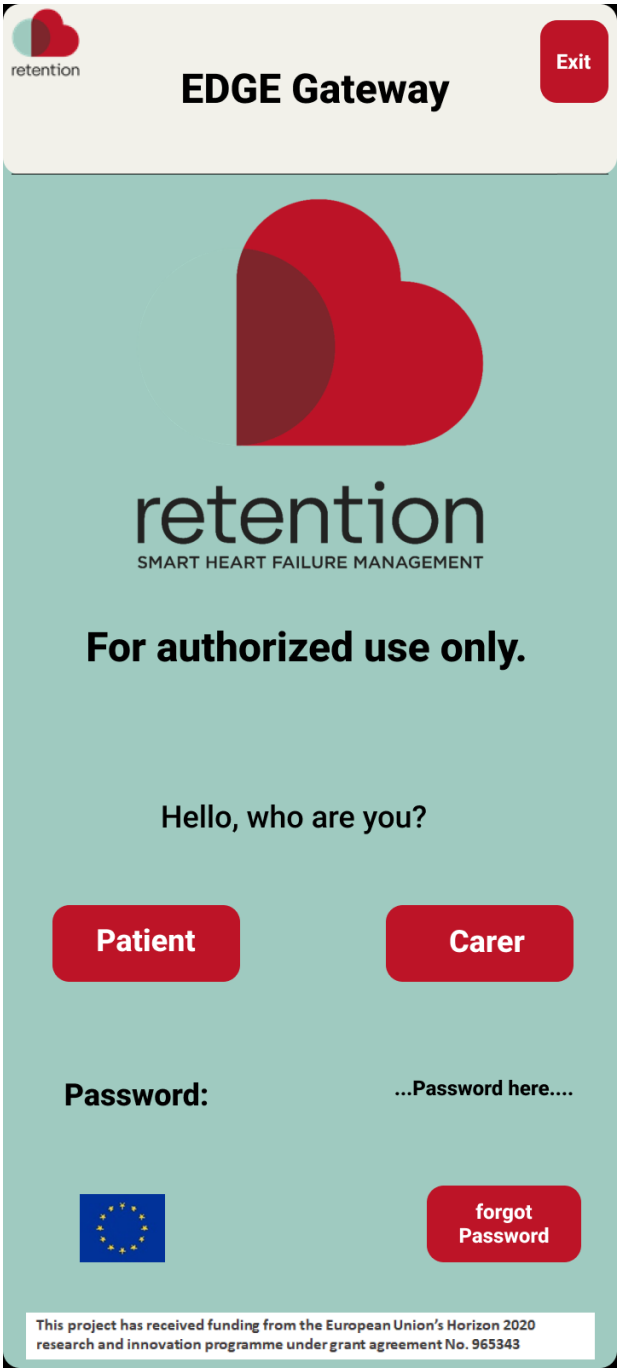
Welcome and Language:



Use Case:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry

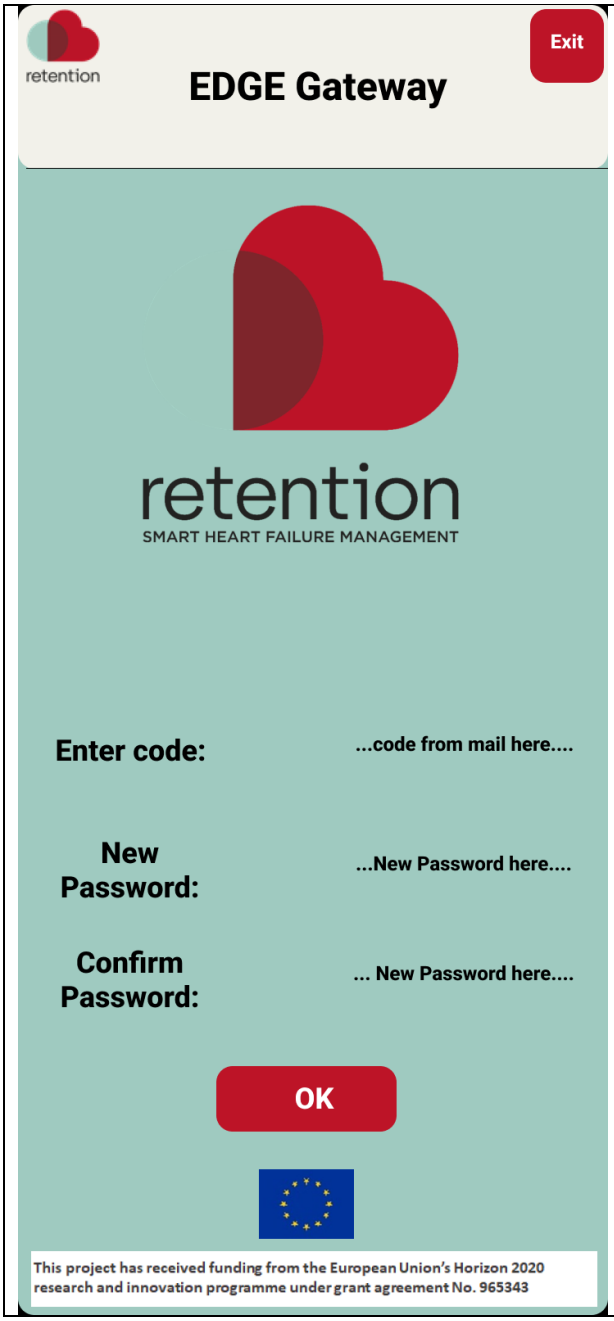
User name and password:



Use Case:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry

Change password:

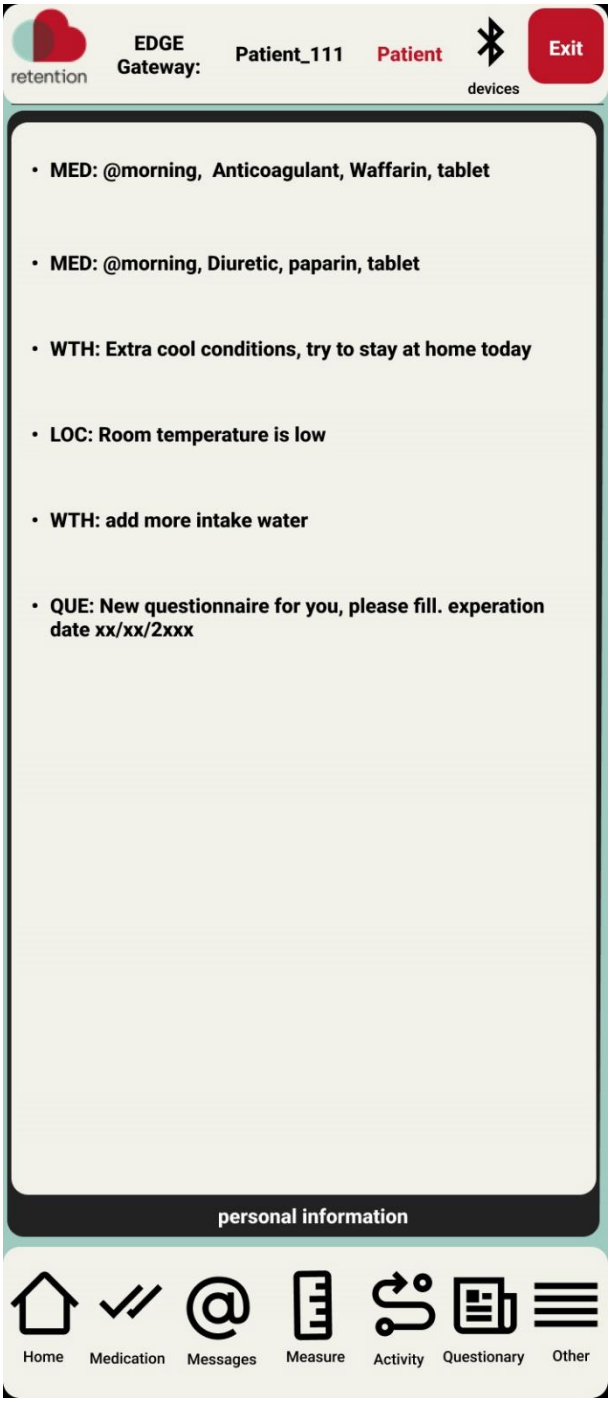


Use Case:

- RTS05: Configuring a device and App

Main screens: one-line – Large buttons and pop-up menus

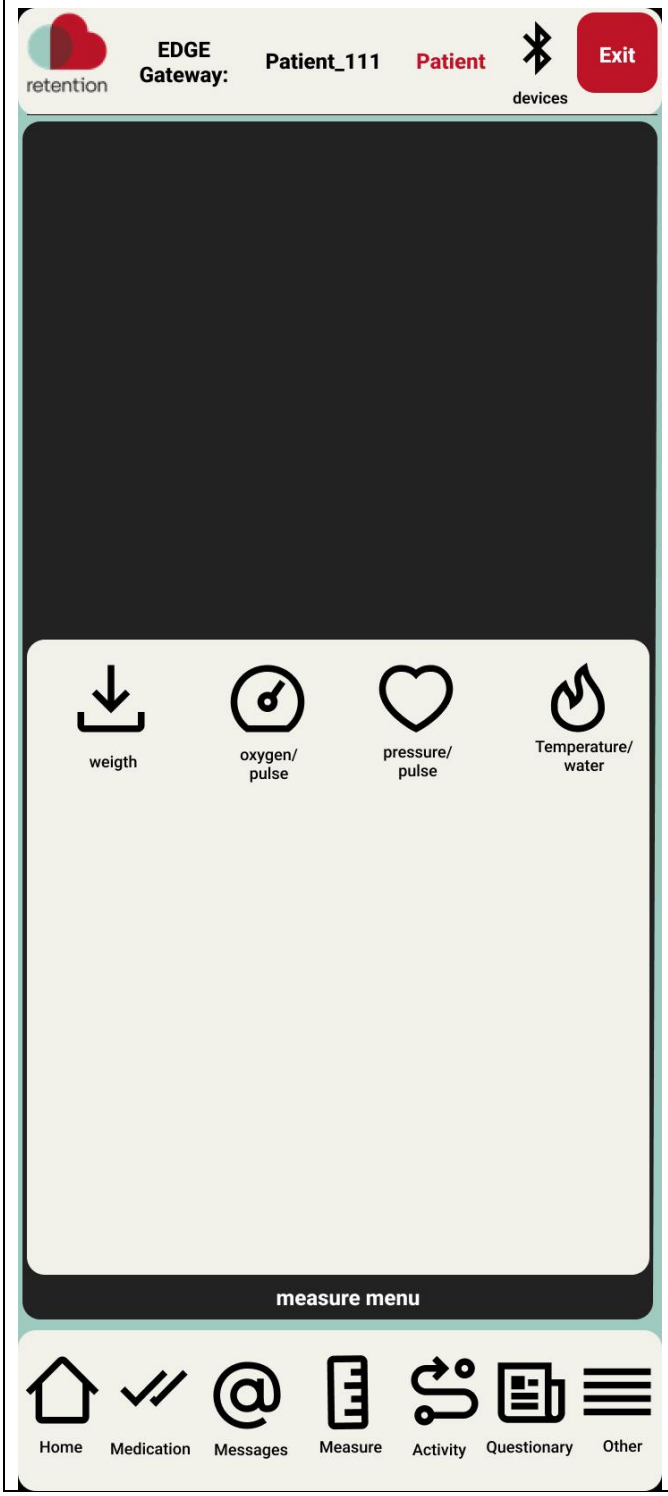
Landing page (message screen that contains important messages from all subsystems):



Use Case:

RTP01 – Daily Data Entry patient
RTCA01 Daily data Entry carer
RTP04 Automate messages patient
RTCA02 Automated messages carer

Measurements menu:



Use Case:

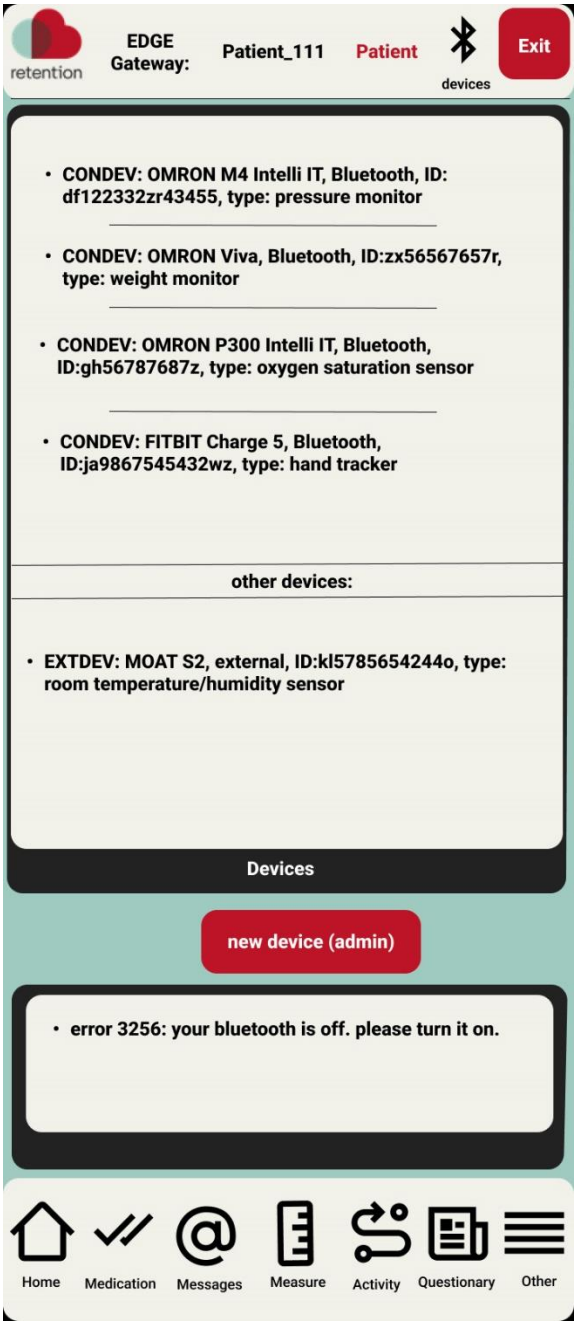
RTP01 – Daily Data Entry patient
RTCA01 Daily data Entry carer

Other (functions) menu

Use Case:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer

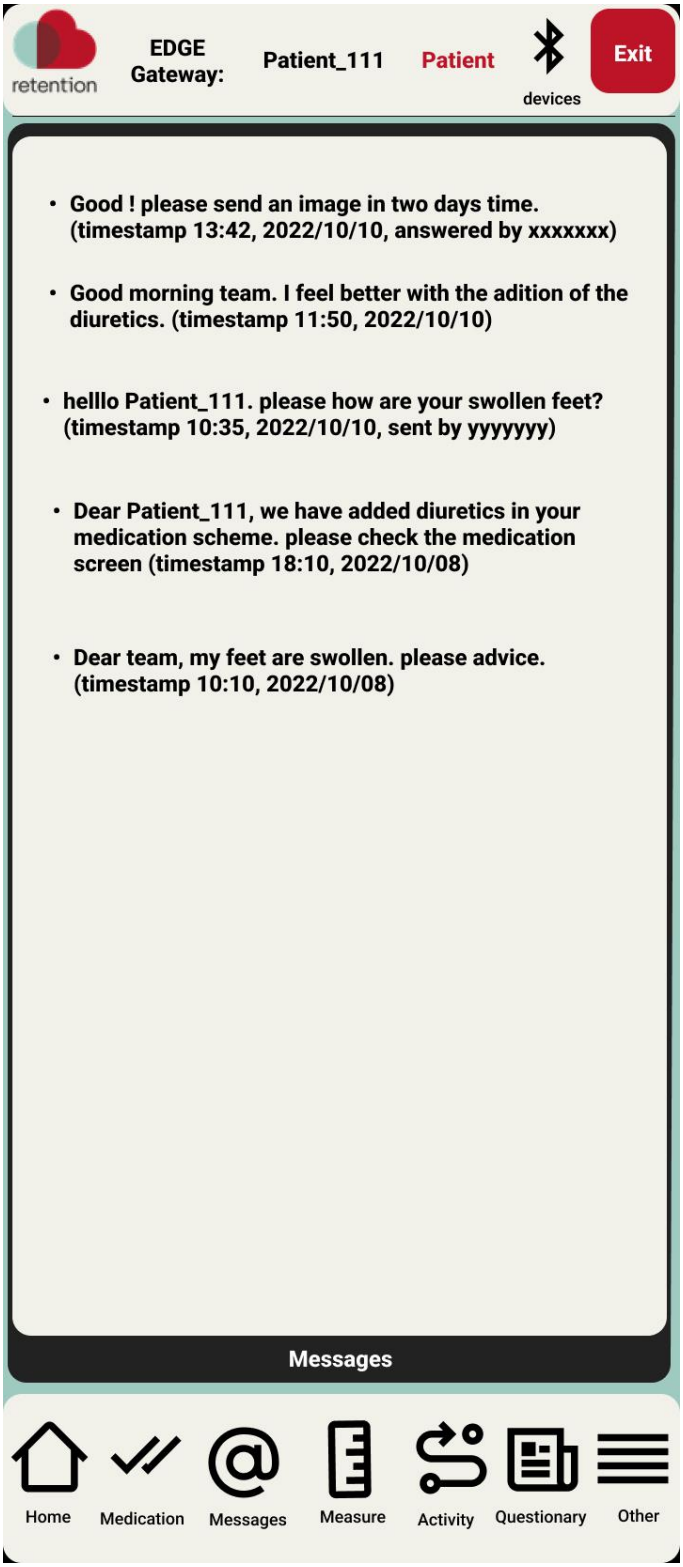
Connected devices screen – the patient/carer will not be a able to add or remove devices. (Only the admin will have the password or how to access the add/delete devices).



Use Case:

RTP04 – Automatic messaging patient
RTCA02 Atomatic messaging carer
RTS04 Associating device it to patient
RTS05 Configuring device and App

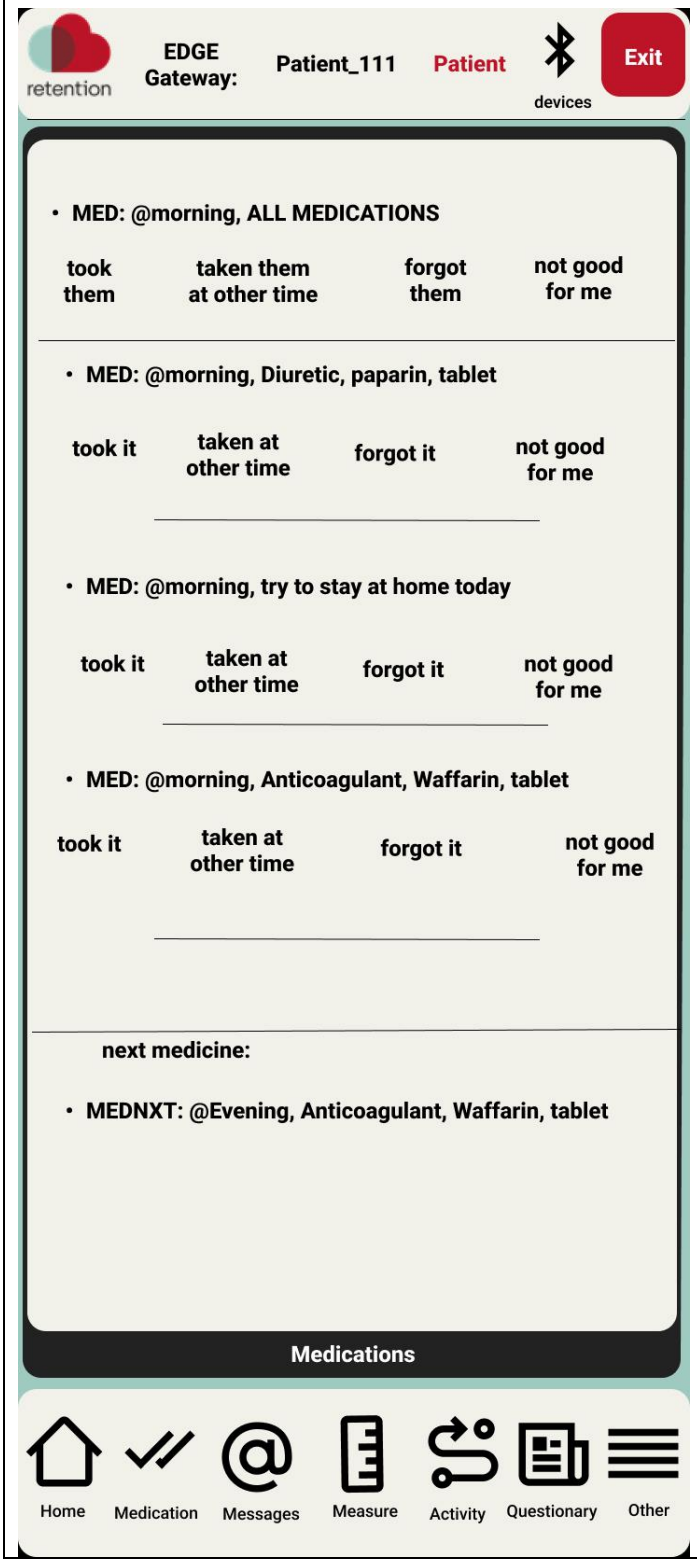
(offline) message screen to the clinical team



Use Case:

RTP01 – Daily Data Entry patient
RTCA01 Daily data Entry carer
RTP04 Automate messages patient
RTCA02 Automated messages carer
RTP03 Special Events

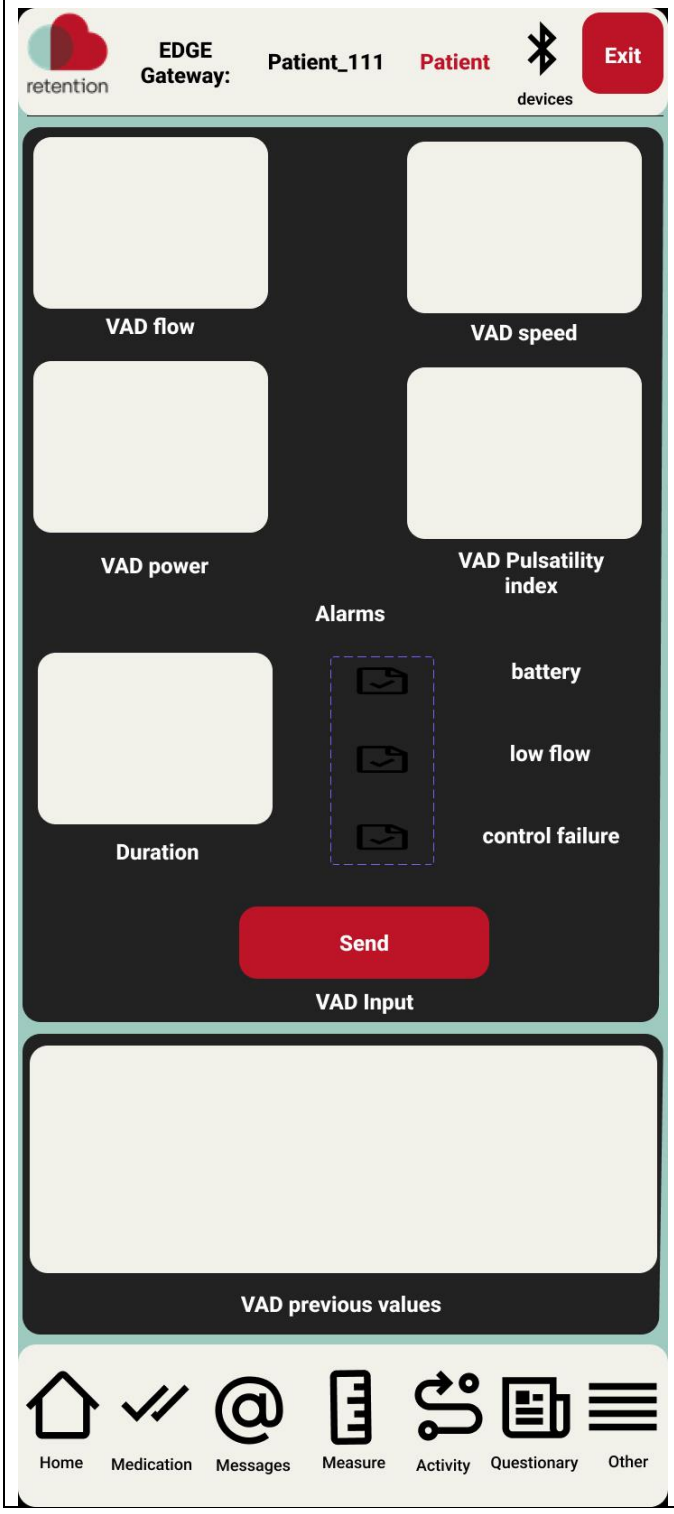
medication screen (will follow the allocated day slots: ex. morning, noon time, night):



Use Case:

RTP01 – Daily Data Entry patient
RTCA01 Daily data Entry carer
RTP04 Automate messages patient
RTCA02 Automated messages carer

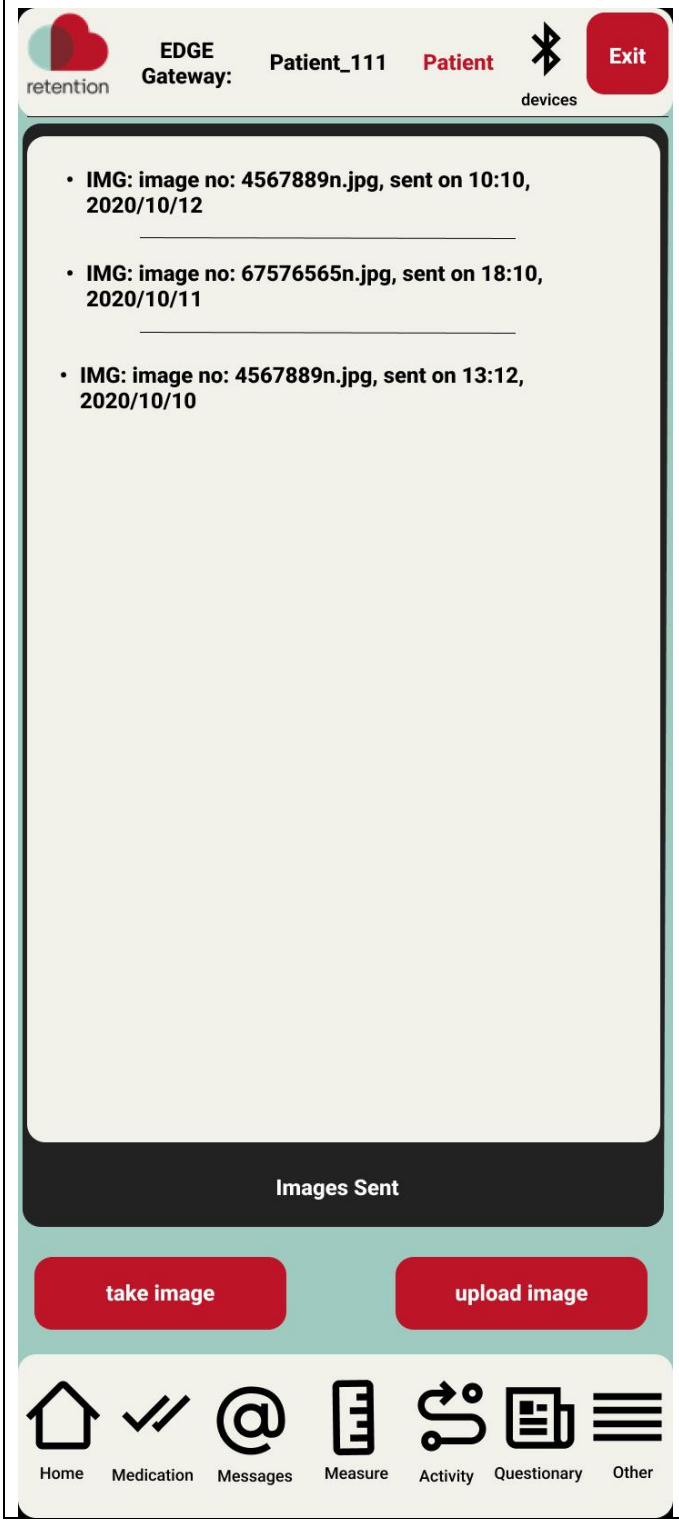
VAD input screen (activated for VAD patients only – manual input):



Use Case:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer
- RTP02 Special variables
- RTP03 Special Events

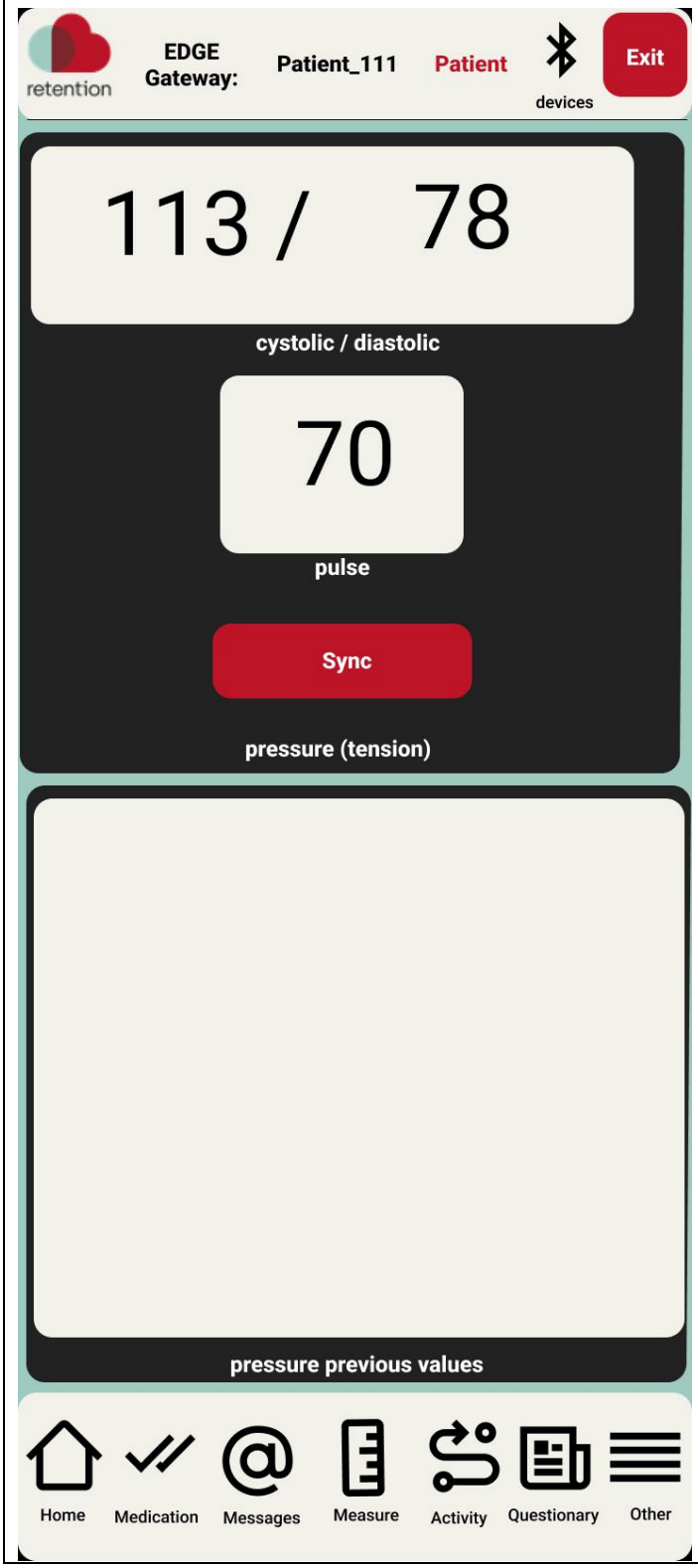
Image screen (a patient or carer can take a picture and upload it to the system, for viewing from the clinical team)



Use Cases:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer
- RTP02 Special variables
- RTP03 special events

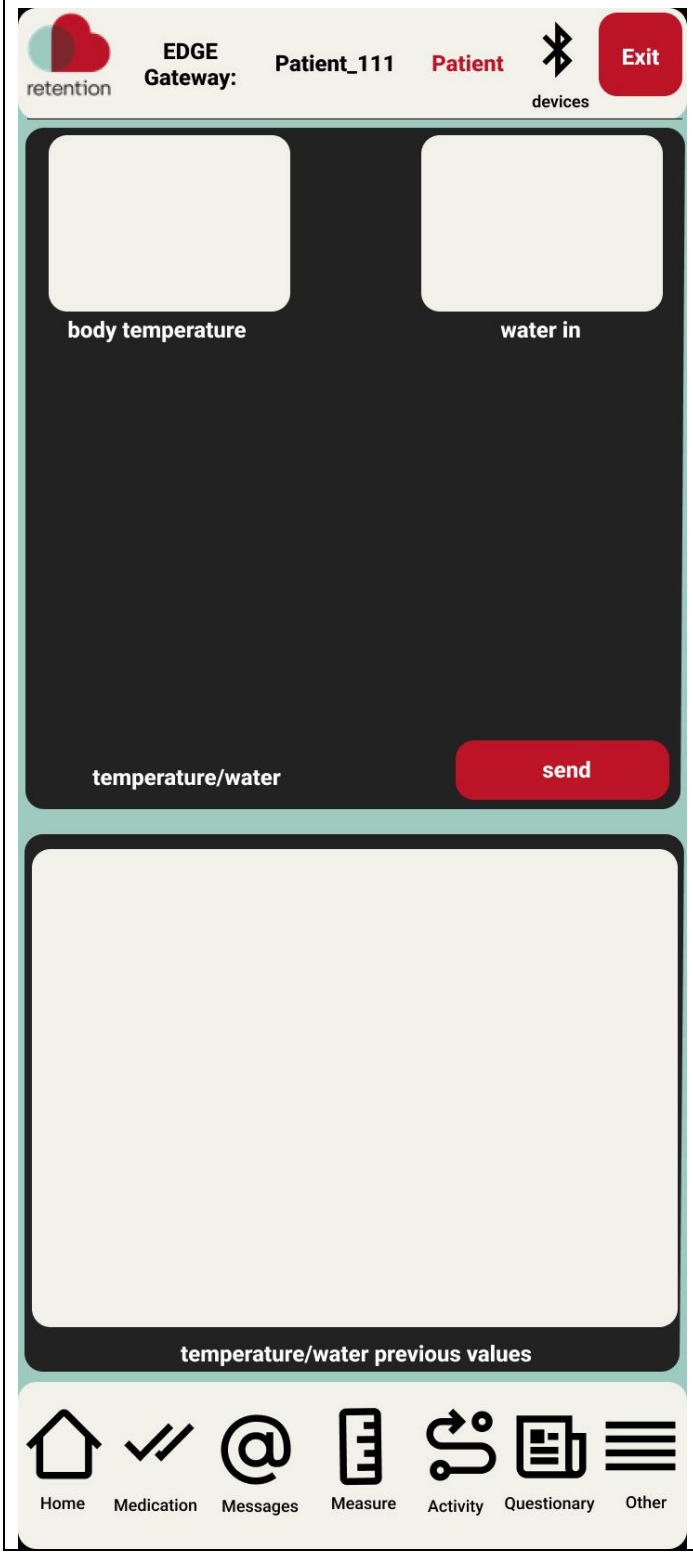
Automated pressure/pulse screen (used in conjunction with the medical tension meter):



Use case:

RTP01 – Daily Data Entry patient
RTCA01 Daily data Entry carer

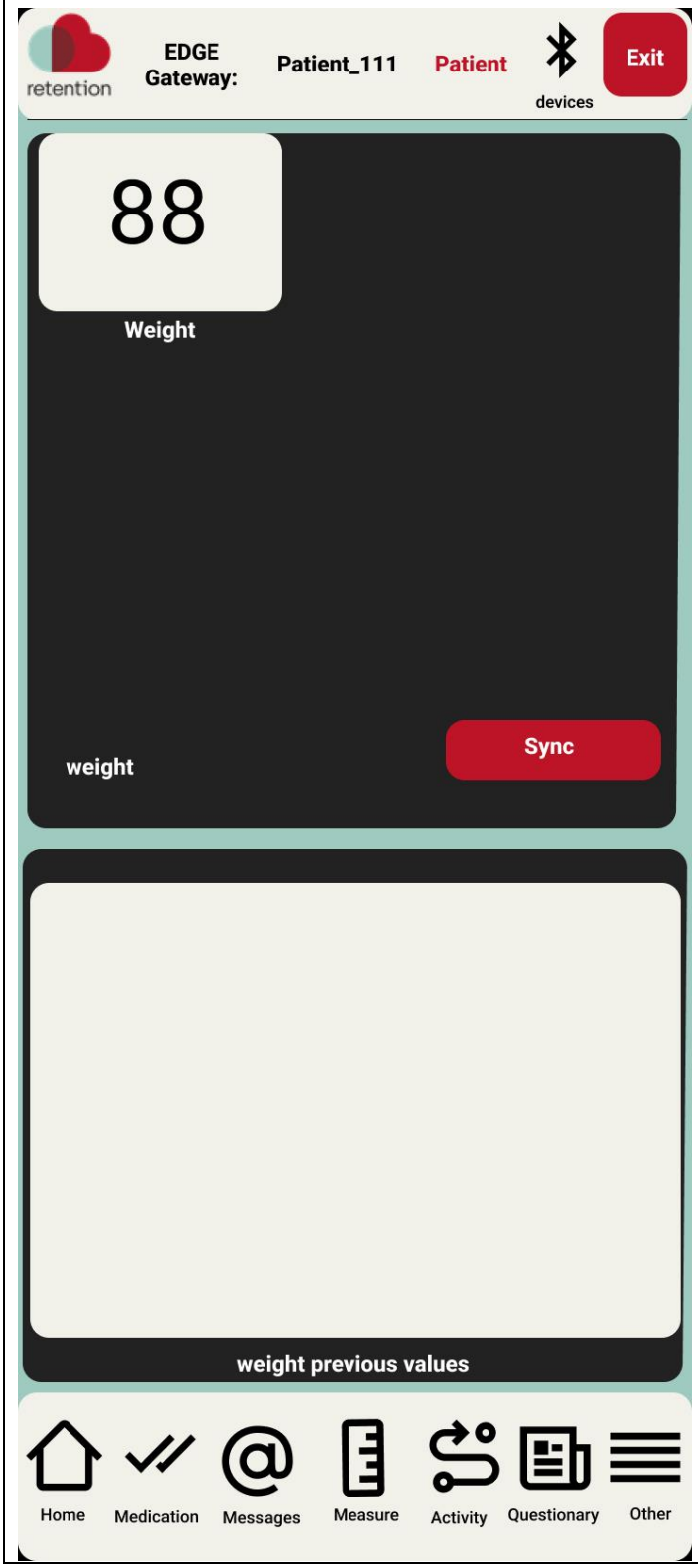
Body temperature and water-calories input screen (a very useful screen for transplanted patients for temperature input):



Use Cases:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer
- RTP02 Special variables
- RTP03 special events

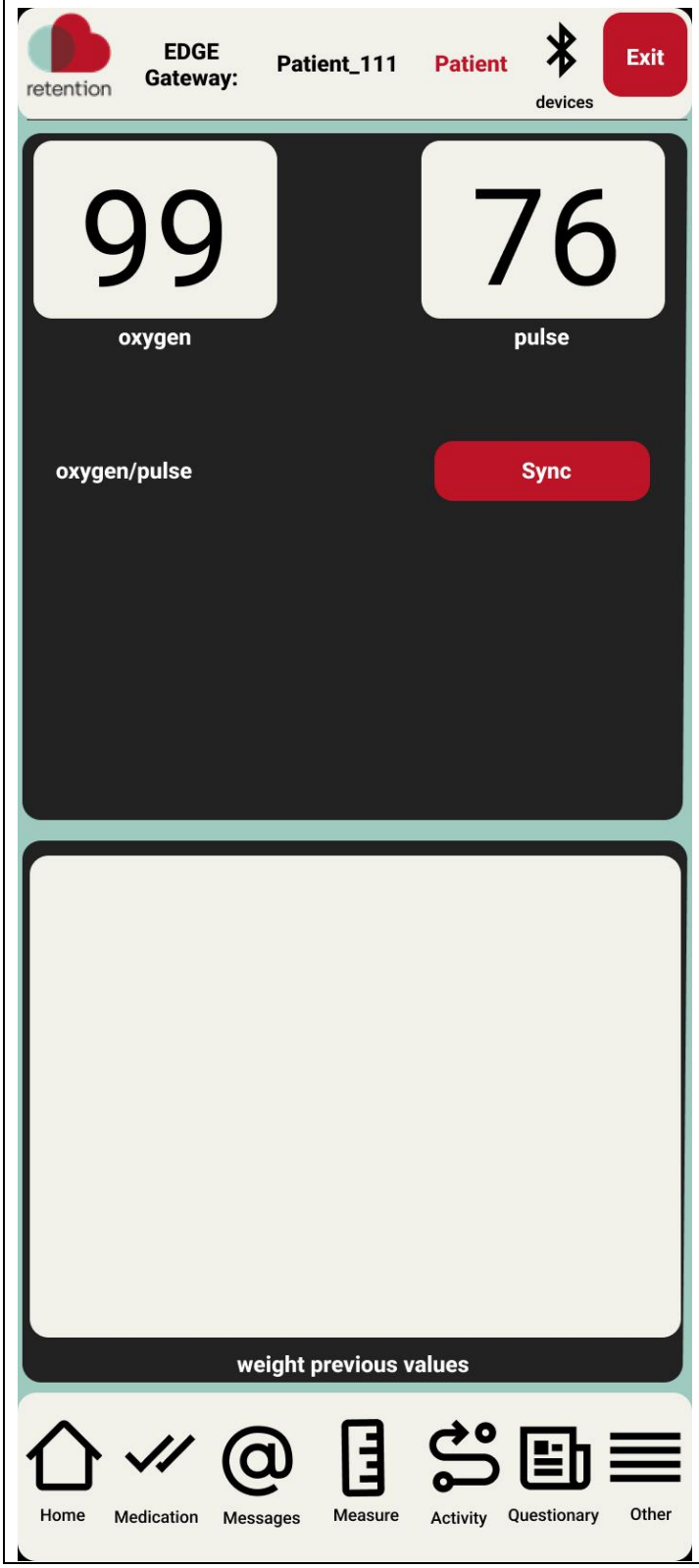
Automated weight screen (used in conjunction with the weight scale device):



Use Cases:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer

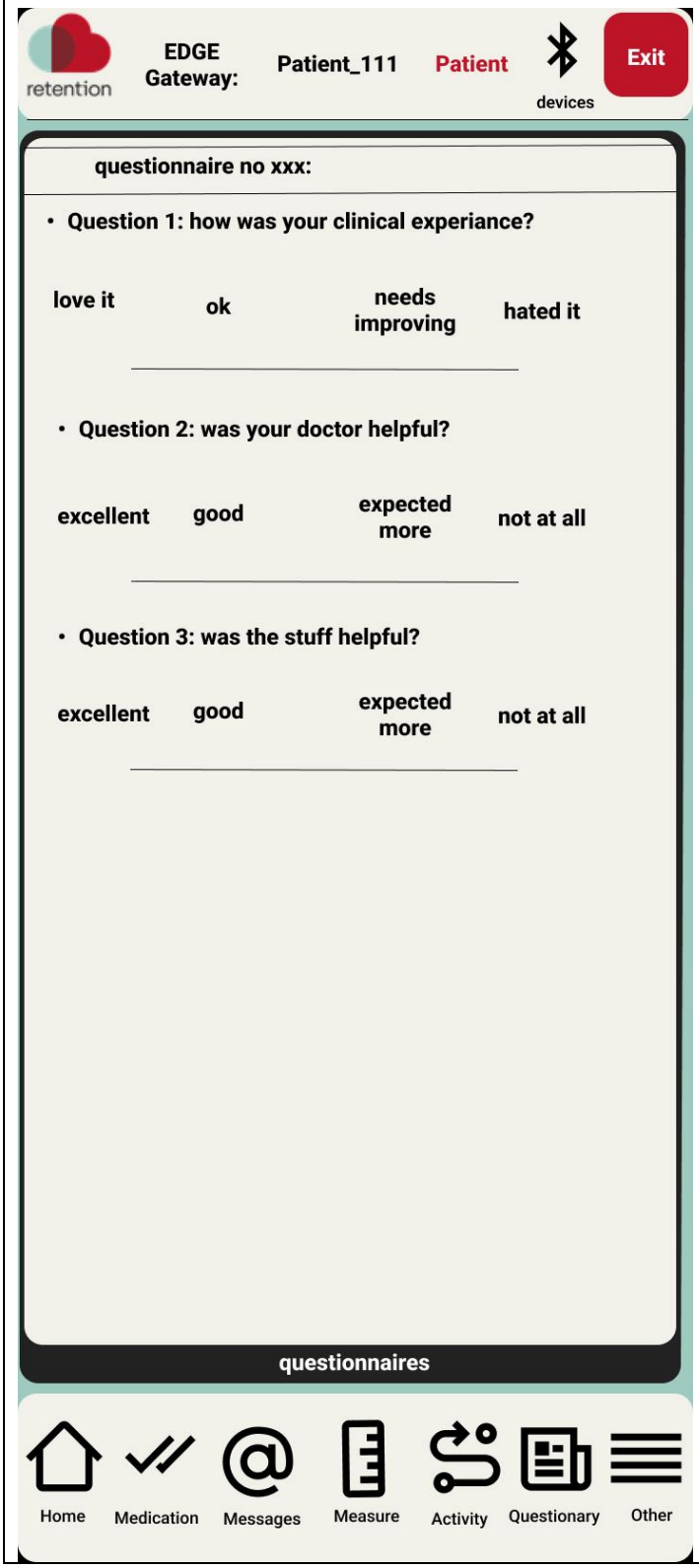
Automated oxygen-pulse screen (used in conjunction with the oxygen saturation meter):



Use Cases:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer

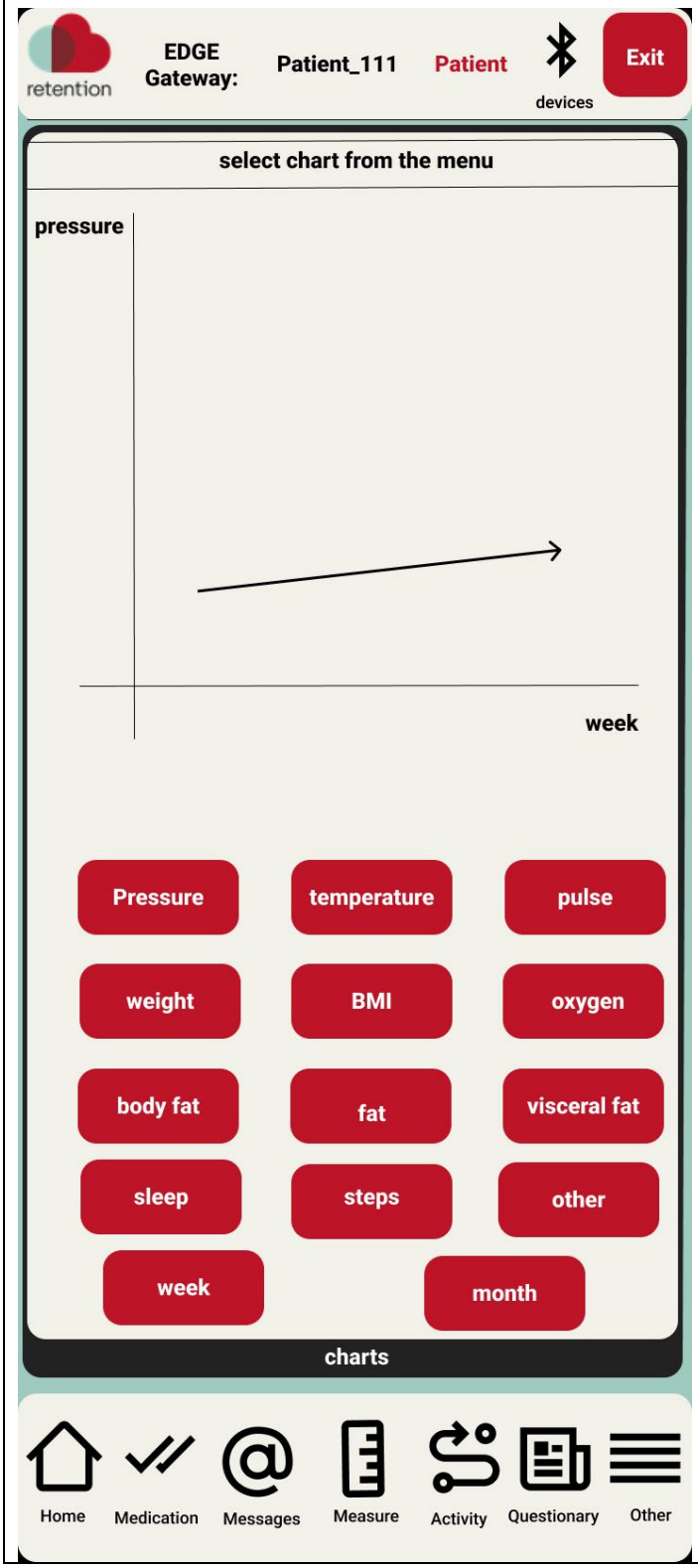
Questionnaires (only the ones that the patient-carer can and should do by himself):



Use Cases:

RTP01 – Daily Data Entry patient
RTCA01 Daily data Entry carer
RTP02 Special Variables
RTP03 Special events

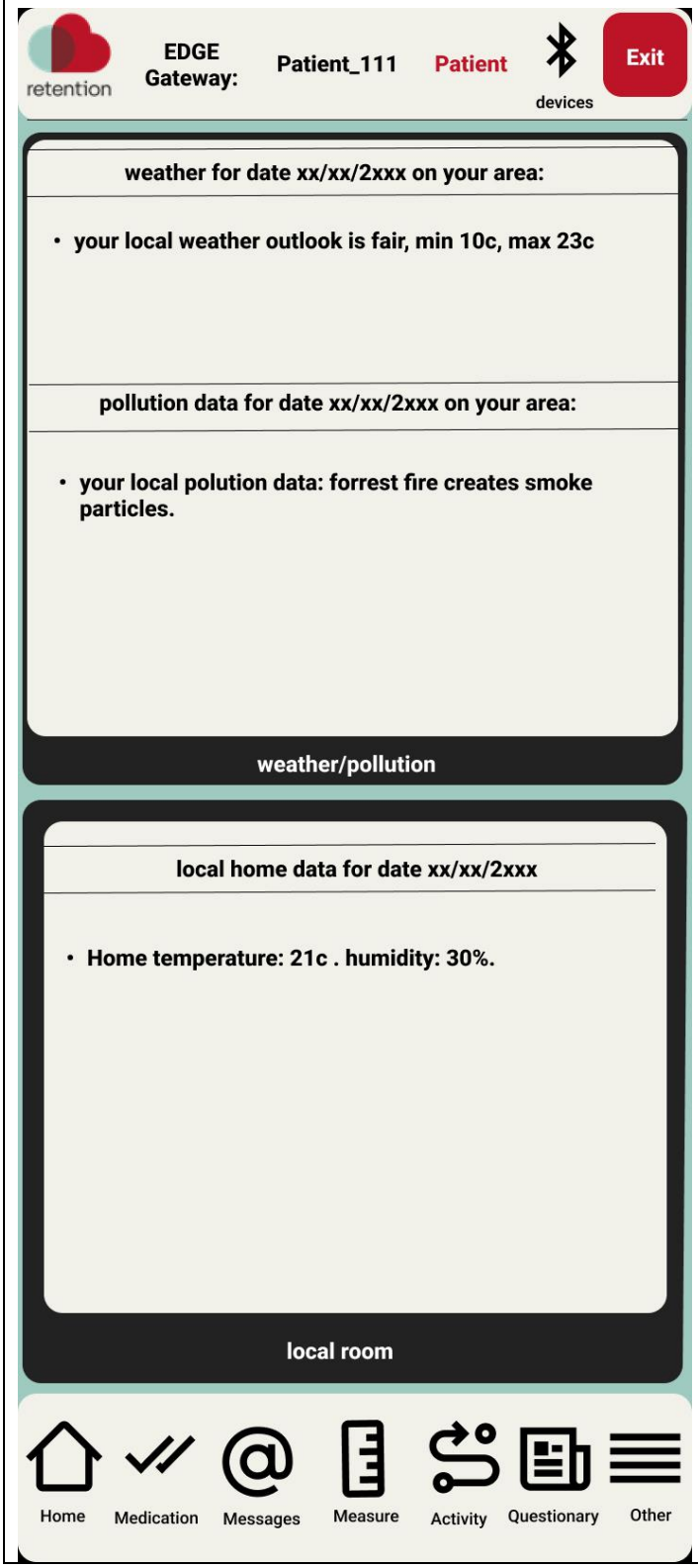
Charts screens (charts for the patient data, on a week, month or other basis, so the patient can check his progress):



Use case:

- RTP04 Automated messages patient
- RTCA02 Automated messages carer

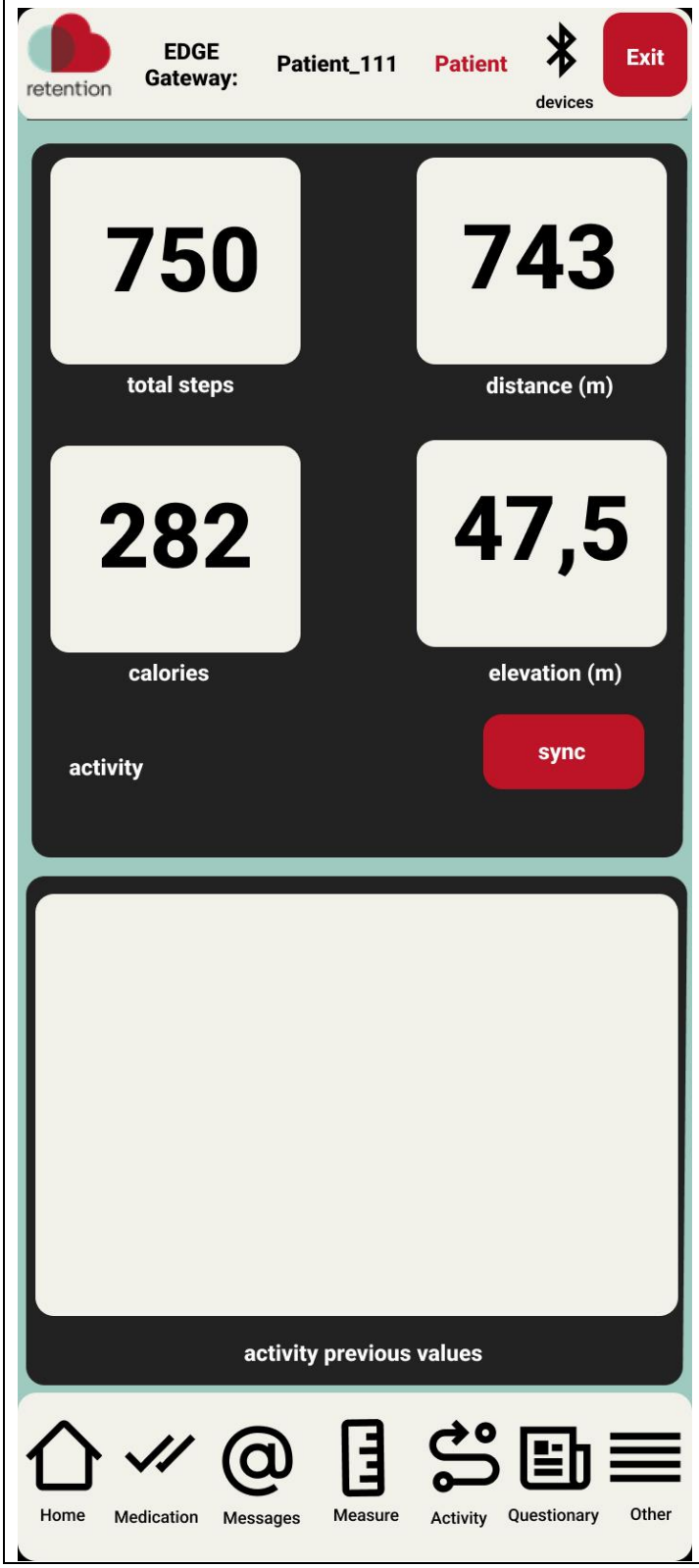
Automated weather and local house-room temperature (data from local weather local service, local pollution service – city wide, and local temperature- humidity from the sensors on the gateway):



Use case:

1. RTP04 Automated messages patient
2. RTCA02 Automated messages carer

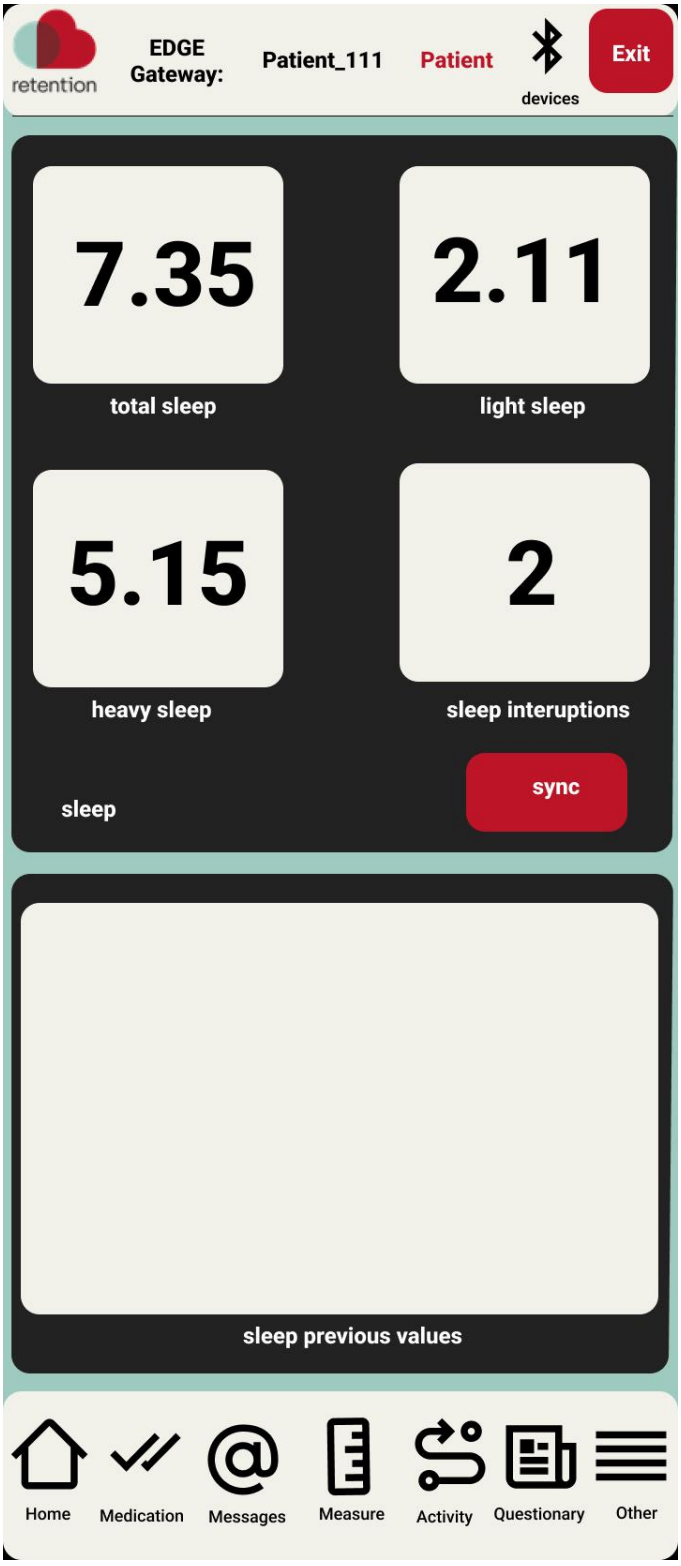
Automated activity from the tracker device (used in conjunction with the tracking device):



Use Cases:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer

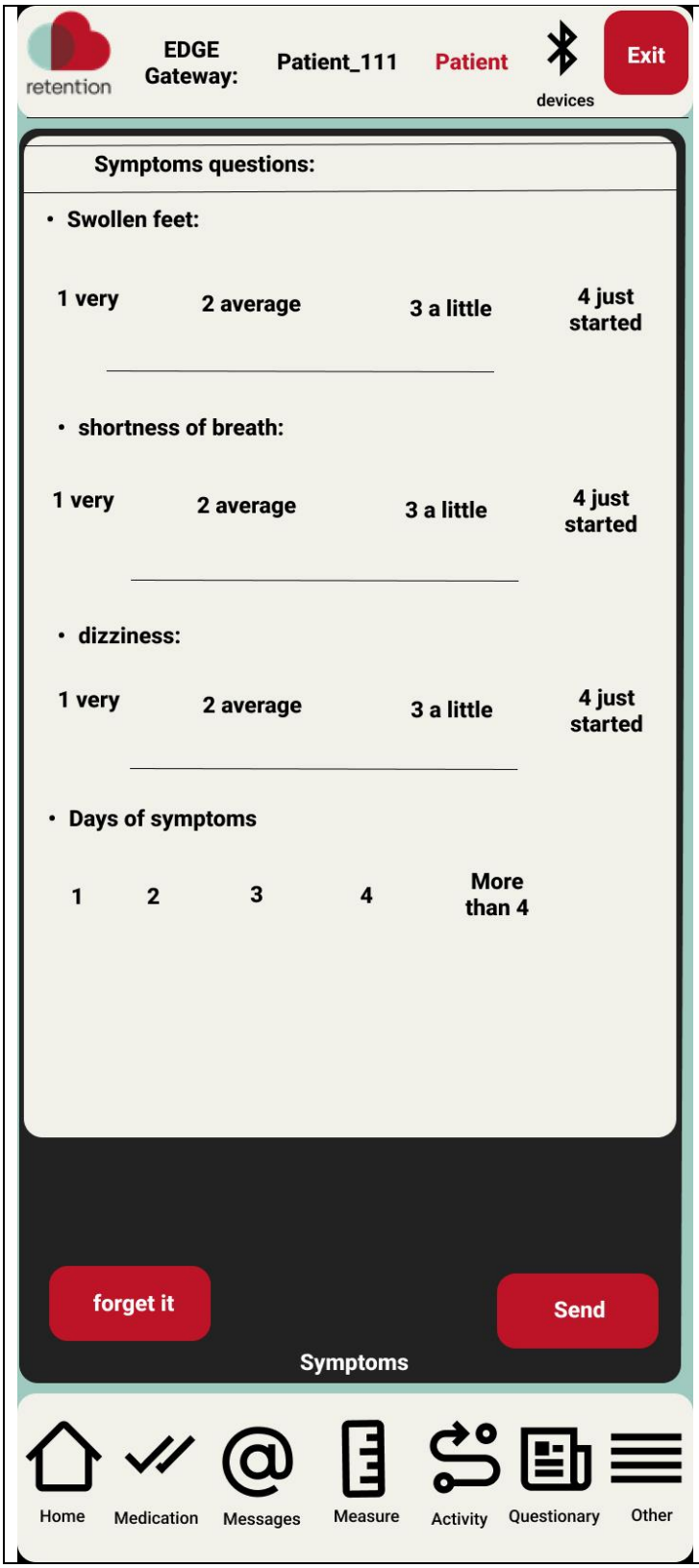
Automated sleep screen from the tracker device (used in conjunction with the tracking device):



Use Cases:

- RTP01 – Daily Data Entry patient
- RTCA01 Daily data Entry carer

Symptoms screen:



Use case:

- RTP02 Special variables

Appendix 4: User Requirements: Use Cases mapping

Category	Use case code	Name	Importance (priority)	Addressed by
Clinician's use cases	RTCL01	**Creation of patient and data visualisation**	Mandatory	CSB (Dashboard - creation of patient, baseline), patient edge (automatic creation)
	RTCL02	**Patient-doctor interactions**	Mandatory	CSB (Dashboard -patient monitoring, visits)
	RTCL03	**Alarms**	Mandatory	CSB (Dashboard - monitoring, DSS, AI prediction via the executor)
	RTCL04	**Event record**	Mandatory	CSB (Dashboard - patient monitoring)
Patient's use cases	RTP01	**Daily data entry**	Mandatory	Patient EDGE (mobile application)
	RTP02	**Special variables**	High	Patient EDGE (mobile application), CSB (Dashboard for specific patient-doctor interactions)
	RTP03	**Special events**	Mandatory	Patient EDGE (mobile application)
	RTP04	**Automatic messages**	Mandatory	Patient EDGE (mobile application), CSB (Patient monitoring)
Carer's use cases	RTCA01	**Daily data entry**	Mandatory only for LVAD patients	Patient EDGE (mobile application)
	RTCA02	**Automatic messages**	Mandatory	Patient EDGE (mobile application), CSB (Patient monitoring)
Risk assessment generated by AI	RTBD01	**Risk assessment generated by AI**	Mandatory	GIC (train the model), CSB (execute the model), after authorisation Patient EDGE (mobile application)
Technical staff use cases	RTS01	**Dashboard End-user moderated registration**	Mandatory	GIC (administration), CSB (Local Administration for each CSB)

	RTS02	**Dashboard End-user login**	mandatory	GIC (administration), CSB (Local Administration for each CSB)
	RTS03	**Manage end-user account information**	Mandatory	GIC (administration), CSB (Local Administration for each CSB)
	RTS04	**Associating a device ID to a patient**	Mandatory	CSB (Local Administration for each CSB), Patient EDGE (mobile Application)
	RTS05	**Configuring a device and App**	Mandatory	CSB (Local Administration for each CSB), Patient EDGE (mobile Application)
	RTS06	**Managing Public health policy decision-making models**	Mandatory	GIC (policy module, Statistics)
	RTS07	**Performing GDPR compliance check**	Mandatory	GIC (administration), CSB (Local Administration)

Appendix 5: Functional and non-functional User Requirements mapping

Non-Functional Requirements

Usability requirements

A system can have adequate functionality, but inadequate usability because it is too difficult to use. The usability requirements specify how easy the system must be to use.

Requirement ID:	**NF_US_01**	Priority:	Mandatory
Requirement title:		Ease of learning	
Description:		The functionalities and interfaces offered by the RETENTION platform should be easy to learn by all types of users. New users should be able to learn all the functionalities offered with minimum supervision.	
Rationale/Goal:		To ensure the quick adoption of new platform's users, without need for extensive trainings.	
Means of verification:		Usability Testing	
Dependencies:		NF_US_05	
Addressed by:		All modules: • GIC, • CSB, • EDGE More relevant to: • GIC Dashboard (GICDB) • GIC Decision & Policy Support (GICDPS) • GIC Disease Insights (GICDI) • CSB Dashboard (CSBDB) • CSB Chat system (CSBCHT) • Patient Edge Mobile Application	

Requirement ID:	**NF_US_02**	Priority:	Mandatory
Requirement title:		Responsive Interface	
Description:		User friendliness and responsiveness of the interface will be accomplished.	
Rationale/Goal:		User friendly, use in different machines (display)	
Means of verification:		Screen available in pc screen and phone/tablet display. Unit testing.	
Dependencies:		NF_US_03, NF_US_04	

Addressed by:	All modules: • GIC, • CSB, • EDGE More relevant to: • GIC Dashboard (GICDB) • GIC Decision & Policy Support (GICDPS) • GIC Disease Insights (GICDI) • CSB Dashboard (CSBDB) • CSB Chat system (CSBCHT) • Patient Edge Mobile Application

Requirement ID:	**NF_US_03**	Priority:	Mandatory
Requirement title:		Personalised interface	
Description:		The interface will be able to morph into the user requirements.	
Rationale/Goal:		Personalised treatment and information.	
Means of verification:		Dynamic way of defining the interface items. Unit testing.	
Dependencies:		NF_US_02	
Addressed by:		modules: • CSB, • EDGE More relevant to: • CSB Dashboard (CSBDB) • CSB Chat system (CSBCHT) • Patient Edge Mobile Application	

Requirement ID:	**NF_US_04**	Priority:	Mandatory
Requirement title:		Usability by design	
Description:		RETENTION and its components should be designed to meet high usability.	
Rationale/Goal:		High usability.	
Means of verification:		User Satisfaction.	
Dependencies:		NF_US_02, NF_US_03	

Addressed by:	All modules: • GIC, • CSB, • EDGE More relevant to: • GIC Dashboard (GICDB) • GIC Decision & Policy Support (GICDPS) • GIC Disease Insights (GICDI) • CSB Dashboard (CSBDB) • CSB Chat system (CSBCHT) • Patient Edge Mobile Application

Requirement ID:	**NF_US_05**	Priority:	Mandatory
Requirement title:		User guidance.	
Description:		RETENTION shall guide the user to the correct choices (wizards, list of possible values, non-modal windows, etc.).	
Rationale/Goal:		Task efficiency.	
Means of verification:		Task performance. Unit test.	
Dependencies:		NF_US_01	
Addressed by:		All modules: • GIC, • CSB, • EDGE	

Requirement ID:	**NF_US_06**	**Priority:**	**Optional**
Requirement title:		System Ergonomics: Multiple end-users devices support	
Description:		The UI of any part of the RETENTION system should adapt to the screen resolution that the users are executing.	
Rationale/Goal:		Ability to view and execute tasks on the RETENTION system, in different devices and screen resolution requirements on the available device.	
Means of verification:		Usability test with multiple devices. Unit testing.	
Dependencies:		NF_US_02, NF_US_03	
Addressed by:		All modules: • GIC, • CSB, • EDGE More relevant to: • GIC Dashboard (GICDB) • GIC Decision & Policy Support (GICDPS) • GIC Disease Insights (GICDI) • CSB Dashboard (CSBDB) • CSB Chat system (CSBCHT) • Patient Edge Mobile Application	

Requirement ID:	NF_US_07	Priority:	Mandatory
Requirement title:		Visualisation of the user's data.	
Description:		RETENTION shall use visualisation techniques for users' data, to be easier to read by the user.	
Rationale/Goal:		User satisfaction.	
Means of verification:		User Satisfaction.	
Dependencies:		NF_US_01, NF_US_02, NF_US_03, NF_US_04	
Addressed by:		All modules: • GIC, • CSB, • EDGE More relevant to: • GIC Dashboard (GICDB) • CSB Dashboard (CSBDB) • Patient Edge Mobile Application	

Requirement ID:	NF_US_08	Priority:	Optional
Requirement title:		W3C compliant	
Description:		User friendliness of the interface for disability will be accomplished.	
Rationale/Goal:		User friendly for users with disabilities.	
Means of verification:		W3C certification process.	
Dependencies:		NF_US_01, NF_US_02, NF_US_03, NF_US_04	
Addressed by:		modules: • CSB More relevant to: • CSB Dashboard (CSBDB)	

Performance requirements

Requirement ID:	NF_PR_01	Priority:	Mandatory
Requirement title:		System time response	
Description:		The time response of the RETENTION system and its components should not degrade with an increase in available datasets and models execution.	
Rationale/Goal:		Ensure system performance and stability under all conditions of the system and full data availability to the users.	
Means of verification:		Performance testing. System test.	
Dependencies:		NF_PR_02	

Addressed by:	All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure

Requirement ID:	**NF_PR_02**	**Priority:**	**Mandatory**
Requirement title:		Performance: System Capacity	
Description:		The capacity should be more than adequate for the system, without degradation in performance of the RETENTION system and its components. It should not degrade with an increase in new and available datasets.	
Rationale/Goal:		Ensure system capacity under all conditions of the system and full data availability to the users.	
Means of verification:		Performance testing. System test.	
Dependencies:		NF_PR_01	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_PR_03**	**Priority:**	**Mandatory**
Requirement title:		Performance: Concurrent users	
Description:		The system must support multiple users at the same time.	
Rationale/Goal:		Ensure responsiveness and stability under a full workload	
Means of verification:		Performance testing for server request processing times and acceptable concurrent user volumes. Acceptance tests – stress test.	
Dependencies:		NF_PR_01, NF_PR_02	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_PR_04**	**Priority:**	Mandatory
Requirement title:		Operational: smooth and seamless RETENTION system components interactions	
Description:		The RETENTION system should expose integration layers, capable for exchanging data and models between its components (e.g., through API interfaces, stream-processing bus etc).	

Rationale/Goal:	Smooth and Seamless data flow between the RETENTION system components
Means of verification:	By design and Performance and usability testing
Dependencies:	NF_PR_01, NF_PR_02, NF_PR_03, NF_PR_04
Addressed by:	All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure

Requirement ID:	**NF_PR_05**	**Priority:**	Mandatory
Requirement title:		Performance: Loading time	
Description:		The system needs to perform each function of the end user in under **15** seconds	
Rationale/Goal:		Ensure user experience	
Means of verification:		Calculation of the time taken to completely display the content of a specific page. User tests. units testing.	
Dependencies:		NF_PR_01	
Addressed by:		All modules: • GIC, • CSB, • EDGE More relevant to: • GIC Dashboard (GICDB) • GIC Decision & Policy Support (GICDPS) • GIC Disease Insights (GICDI) • CSB Dashboard (CSBDB) • CSB Chat system (CSBCHT) • Patient Edge Mobile Application	

Requirement ID:	**NF_PR_06**	Priority:	Mandatory
Requirement title:		Performance: System Uptime	
Description:		The system needs to have at least a 99.5% uptime and should be available, up and running 24x7, no matter the time zone.	
Rationale/Goal:		Ensure system reliability	
Means of verification:		By design. Server report. Stress tests.	
Dependencies:		NF_PR_01, NF_PR_02, NF_PR_03, NF_PR_05	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	NF_PR_07	Priority:	Mandatory
Requirement title:		Dashboard performance	
Description:		Speed and data accuracy for data entry.	
Rationale/Goal:		Not annoying to users	
Means of verification:		Meet the specs of the project. modules tests. System test. Applications tests.	
Dependencies:		NF_PR_01, NF_PR_02, NF_PR_03, NF_PR_04, NF_PR_05	
Addressed by:		modules: • GIC, • CSB More relevant to: • GIC Dashboard (GICDB) • CSB Dashboard (CSBDB)	

Requirement ID:	NF_PR_08	Priority:	Mandatory
Requirement title:		AI model performance	
Description:		Speed of the AI model, when running on dataset.	
Rationale/Goal:		To give fast and accurate responses to the doctor/decision maker	
Means of verification:		Meet the specs of the project. by design. Unit testing. System testing.	
Dependencies:		NF_PR_01, NF_PR_03, NF_PR_05, NF_PR_07	
Addressed by:		modules: • GIC, • CSB More relevant to: • GIC Model Specification Tool (GICMST) • GIC Disease Insights (GICDI) • GIC BDA Engine (GICBDAE) • CSB BDA Engine Executor (CSBDAEE)	

Availability and reliability requirements

Requirement ID:	NF_AR_01	Priority:	Mandatory
Requirement title:		Dashboard (top level)	
Description:		Availability of the system to take information at any time and give information at any time.	
Rationale/Goal:		To be always available for getting and processing data with 99.5% availability	
Means of verification:		Availability by design. System testing. Unit testing.	
Dependencies:		NF_PR_06	

Addressed by:	modules: • GIC, • CSB More relevant to: • GIC Dashboard (GICDB) • CSB Dashboard (CSBDB)

Requirement ID:	**NF_AR_02**	Priority:	Mandatory
Requirement title:		back end	
Description:		Availability of the system to take information at any time and give information at any time.	
Rationale/Goal:		To be always available for getting and processing data with 99.5% availability	
Means of verification:		Availability by design. System testing. Unit testing.	
Dependencies:		NF_PR_06, NF_AR_01	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_AR_03**	Priority:	Mandatory
Requirement title:		Edge gateway	
Description:		Availability of the edge computing software and system with 99.5% availability on the server side. The results that are provided to the users by the Edge gateway component should be accurate and reliable (sensitivity, specificity, precision etc.).	
Rationale/Goal:		To be always available for recording measures	
Means of verification:		Availability by design. System testing. Unit testing.	
Dependencies:		NF_PR_06, NF_AR_01, NF_AR_02	
Addressed by:		modules: • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_AR_04**	Priority:	Mandatory
Requirement title:		Web application	
Description:		Availability of the web application software and system with 99.5% availability	
Rationale/Goal:		To be always available for recording measures	
Means of verification:		Availability by design. System testing. Unit testing.	
Dependencies:		NF_AR_01, NF_AR_02, NF_AR_03	

Addressed by:	modules: • GIC, • CSB, • Platform security • Platform infrastructure

Requirement ID:	**NF_AR_05**	Priority:	Mandatory
Requirement title:		Phone/tablet application	
Description:		Availability of Phone/tablet software and system	
Rationale/Goal:		To be always available for recording measures	
Means of verification:		Availability by design. System testing. Unit testing.	
Dependencies:		NF_AR_04	
Addressed by:		modules: • EDGE	

Legal and Ethical requirements

Requirement ID:	**NF_LE_01**	**Priority:**	**Optional**
Requirement title:		Privacy of cloud data	
Description:		Data stored in the Backend platform are pseudonymised (IDs, end-user registration information) and anonymised (usage data, medical records, analytics, interventions)	
Rationale/Goal:		Data privacy	
Means of verification:		legal requirements tests, by design and continuous monitoring	
Dependencies:		NF_LE_02, NF_LE_05	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_LE_02**	Priority:	Mandatory
Requirement title:		Consent for Personal Data	
Description:		Even though a consent will be signed before to start using the system, the consent will be also acknowledged and “signed” (check boxed date and name) on the first time the application is executed.	
Rationale/Goal:		Data privacy.	
Means of verification:		legal requirements tests, unti tests, by design and continuous monitoring	
Dependencies:		NF_LE_01, NF_LE_05	

Addressed by:	All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure

Requirement ID:	**NF_LE_03**		Mandatory
Requirement title:		Implement “Privacy by Design”	
Description:		The RETENTION Project (i.e., platform, app, management procedures been supported by digital means) shall implement appropriate technical and organisational measures which are designed to implement the data protection principles (lawfulness, fairness & transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity & confidentiality; accountability).	
Rationale/Goal:		Data privacy.	
Means of verification:		By design and continuous monitoring. legal requirements test	
Dependencies:		NF_LE_01, NF_LE_02, NF_LE_04	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_LE_04**		Mandatory
Requirement title:		Implement “Privacy by default”	
Description:		The RETENTION Project (i.e., platform, app, management procedures been supported by digital means) shall implement, per processing activity, appropriate technical and organisational measures which are designed to implement data-protection principles and that ensure that by default only personal data which are necessary for each specific purpose of the processing are processed.	
Rationale/Goal:		Data privacy.	
Means of verification:		By design and continuous monitoring. legal requirements test	
Dependencies:		NF_LE_01, NF_LE_02, NF_LE_03	

Addressed by:	All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure

Requirement ID:	**NF_LE_05**	Priority:	Mandatory
Requirement title:		GDPR compliance	
Description:		The RETENTION Project (i.e., platform, app, management procedures been supported by digital means) shall implement appropriate measures to ensure and to be able to demonstrate compliance with the data protection and security legal framework.	
Rationale/Goal:		Data privacy	
Means of verification:		By design and continuous monitoring. legal requirements test	
Dependencies:		NF_LE_01, NF_LE_02	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_LE_06**	Priority:	Mandatory
Requirement title:		Respect data subject rights	
Description:		The RETENTION Project (i.e., platform, app, management procedures been supported by digital means) shall, among others by means of appropriate technical and organisational measures, allow for data subjects to exercise their rights in relation to the processing of their personal data.	
Rationale/Goal:		Data privacy	
Means of verification:		By design and continuous monitoring. legal requirements test	
Dependencies:		NF_LE_05	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_LE_07**	Priority:	Mandatory

Requirement title:	Maintain records of processing activities
Description:	The RETENTION platform shall maintain records of processing activities.
Rationale/Goal:	Data privacy
Means of verification:	By design and continuous monitoring. legal requirements test, unit test, system test, intergration tests
Dependencies:	NF_LE_04, NF_LE_05
Addressed by:	All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure More relevant to: • GIC Data Layer and REST API (GICDL) • CSB Data Layer and REST API (CSBDL)

Requirement ID:	**NF_LE_08**	Priority:	Mandatory
Requirement title:		Notify and communicate personal data breaches	
Description:		The RETENTION Project (i.e., platform, app, management procedures been supported by digital means) shall take all necessary measures to detect security and data incidents, and to allow for the notification of personal data breaches to the supervisory authority and, if necessary, to the data subjects.	
Rationale/Goal:		Data privacy	
Means of verification:		By design and continuous monitoring. legal requirements test	
Dependencies:		NF_LE_05, NF_LE_06	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_LE_09**	Priority:	Mandatory
Requirement title:		Implement pseudonymisation, anonymisation or deletion	
Description:		The RETENTION Platform shall pseudonymise, anonymise or delete personal data, where deemed appropriate, in order to comply with the core data protection principles	

Rationale/Goal:	Data privacy
Means of verification:	By design and continuous monitoring. legal requirements test. Unit testing. System test.
Dependencies:	NF_LE_05
Addressed by:	modules: • Platform security

Security and Privacy requirements

Requirement ID:	**NF_SP_01**	Priority:	Mandatory
Requirement title:		Role-based access control (RBAC)	
Description:		Accessibility – Platform shall provide the data access according to security and privacy policies. Limit access to information and information processing facilities, using role-based access control.	
Rationale/Goal:		Privacy and security.	
Means of verification:		Legal requirements testing. Units testing. Systems testing.	
Dependencies:		NF_LE_03	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform infrastructure More relevant to: • Platform security	

Requirement ID:	**NF_SP_02**	Priority:	Mandatory
Requirement title:		Role-based access control (RBAC)	
)Description:		Platform shall provide mechanisms to configure security and privacy policies	
Rationale/Goal:		Privacy and security.	
Means of verification:		Legal requirements testing. Units testing. Systems testing.	
Dependencies:		NF_LE_03	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform infrastructure More relevant to: • Platform security • Administration	

Requirement ID:	**NF_SP_03**	Priority:	Mandatory
Requirement title:		Data backup	

Description:	Platform will facilitate mechanism for storage facilities of all usage data and log files
Rationale/Goal:	Privacy and security.
Means of verification:	Units testing. Systems testing.
Dependencies:	NF_LE_07
Addressed by:	All modules: • GIC, • CSB, • EDGE • Platform infrastructure More relevant to: • Administration

Requirement ID:	**NF_SP_04**	Priority:	Mandatory
Requirement title:		Effectiveness	
Description:		Platform will support secure, private and trust exchanging of data among different entities (i.e., smartphones, services).	
Rationale/Goal:		Privacy and security.	
Means of verification:		By design. Units testing. Systems testing. Acceptance tests	
Dependencies:		NF_LE_06	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform security • Platform infrastructure • Integration & testing	

Requirement ID:	**NF_SP_05**	Priority:	Mandatory
Requirement title:		REST API	
Description:		Platform will implement REST API to facilitate the data exchange with entities (i.e., smartphones, services).	
Rationale/Goal:		Privacy and security.	
Means of verification:		By design. Units testing. Systems testing. Acceptance tests.	
Dependencies:		NF_SP-01	
Addressed by:		modules: • GIC, • CSB More relevant to: • GIC Data Layer and REST API (GICDL) • CSB Data Layer and REST API (CSBDL)	

Requirement ID:	NF_SP_06		Mandatory
Requirement title:		Communication channel security	
Description:		Platform must guarantee the secure communication with a total of 450 end-users simultaneously.	
Rationale/Goal:		Privacy and security.	
Means of verification:		By design. Units testing. Systems testing. Acceptance tests	
Dependencies:		NF_PR_03, NF_SP-02	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform Security • Platform Infrastructure	

Requirement ID:	NF_SP_07	Priority:	Mandatory
Requirement title:		GDPR Audit	
Description:		Platform will maintain a log of all operations performed upon personal data	
Rationale/Goal:		Security and privacy	
Means of verification:		Legal requirements testing	
Dependencies:		NF_LE_07	
Addressed by:		modules: • GIC, • CSB, • Platform Security • Platform Infrastructure relevant to: • Administration • user roles	

Requirement ID:	NF_SP_08	Priority:	Mandatory
Requirement title:		Secure Authentication	
Description:		Registered end-user connecting to the platform must be authenticated via secure channels (HTTPS)	
Rationale/Goal:		Security and privacy	
Means of verification:		Units testing. Systems testing. Acceptance tests	
Dependencies:		NF_LE_03, NF_SP-09	

Addressed by:	modules: • GIC, • CSB, • Platform Security • Platform infrastructure (system software) • Integration & testing Relevant: • to user role

Requirement ID:	**NF_SP_09**	Priority:	**Optional**
Requirement title:		Physical Security (Data centres)	
Description:		Prevent unauthorised physical access and protect against theft, damage, and minimise loss of operations.	
Rationale/Goal:		Privacy and security	
Means of verification:		By design. System test. Security test.	
Dependencies:		NF_SP_02, NF_SP-08, NF_SP_10	
Addressed by:		modules: • Platform Security • Platform infrastructure • Integration & testing Relevant: • Administration	

Requirement ID:	**NF_SP_10**	Priority:	Mandatory
Requirement title:		Operational Security	
Description:		Ensure proper and regular operation, including appropriate measures for continuous Security & Privacy Assurance tool monitoring of all RETENTION layers and components, to ensure best possible protection against malware, and security/privacy vulnerabilities and threats	
Rationale/Goal:		Security and privacy	
Means of verification:		By design. Systems tests. Acceptance tests.	
Dependencies:		NF_SP-02, NF_SP-09	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform Security • Platform infrastructure • Integration & testing Also relevant: Administration	

Requirement ID:	**NF_SP_11**	Priority:	Mandatory
Requirement title:		Securing personal data	
Description:		Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of personal data been stored	
Rationale/Goal:		Security and privacy	
Means of verification:		By design. Unit testing. System testing. Regulatory and compliance.	
Dependencies:		NF_SP-07	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform Security • Platform infrastructure • Integration & testing	

Requirement ID:	**NF_SP_12**	Priority:	Mandatory
Requirement title:		Incident management	
Description:		Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security/privacy incidents, and appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data	
Rationale/Goal:		Security and privacy	
Means of verification:		By design. Unit testing. System testing. Continuous monitoring.	
Dependencies:		NF_SP_06, NF_SP_10	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Platform Security • Platform infrastructure • Integration & testing	

Data and data exchange requirements

Requirement ID:	**NF_DE_01**	Priority:	**Mandatory**
Requirement title:		Data storage or exchange format	
Description:		Data storage/exchange format should respect the existing standards like HL7, or other predefined ones like JSON/CSV/XML/SQL Data Types or other common health data format	
Rationale/Goal:		Unify the structure of data to facilitate the data modelling step	
Means of verification:		By design.	
Dependencies:		NF_SP_04, NF_DE_02	

Addressed by:	All modules: • GIC, • CSB, • EDGE

Requirement ID:	**NF_DE_02**	Priority:	**Mandatory**
Requirement title:		Data Exchange Protocol: transport	
Description:		Enhanced transport requirements should be Secure HTTP (HTTPS) for complex messages	
Rationale/Goal:		HTTPS consists of the standard HTTP layered on top of a secure Transport Level Security (TLS1.2 minimum required) session which ensures a secured communication	
Means of verification:		Unit testing. Integration tests. System test. Acceptance test	
Dependencies:		NF_DE_01, NF_SP_04	
Addressed by:		All modules: • GIC, • CSB, • EDGE • Integration & testing • Platform security • Platform infrastructure	

Requirement ID:	**NF_DE_03**	Priority:	**Optional**
Requirement title:		Data Exchange Protocol	
Description:		For lightweight messages we should use MQTT, or more secured similar protocols (like MQT-TZ)	
Rationale/Goal:		MQTT makes it easy to encrypt messages using TLS and authenticate clients using modern authentication protocols, such as OAuth.	
Means of verification:		Unit testing. Integration tests. System test.	
Dependencies:		NF_DE_01, NF_DE_02	
Addressed by:		Modules: • Platform security	

Requirement ID:	**NF_DE_04**	Priority:	Mandatory
Requirement title:		Data storage	
Description:		Data should be stored in a SQL/NoSQL timeseries database	
Rationale/Goal:		Easy to scale and access the required data	
Means of verification:		By design. Unit testing. Integration tests. System test.	
Dependencies:		NF_DE_01, NF_DE_05	

Addressed by:	Module: • GIC, • CSB • Integration & testing More relevant to: • CSB Data Layer and REST API (CSBDL) • GIC Data Layer and REST API (GICDL)

Requirement ID:	**NF_DE_05**	Priority**:**	Mandatory
Requirement title:		Encrypted data transmission	
Description:		Mobile App to transmit data via a secure HTTPS channel, while the Dashboard to provide authentication subject to Authorisation policy. Symmetric key encryption based on the Advanced Encryption Standard (AES-256) algorithm, or other based on the Secure Hash Algorithms family to be utilised.	
Rationale/Goal:		Even in case that connection is hacked, transmitted data is protected from reading	
Means of verification:		By design.	
Dependencies:		NF_DE_04	
Addressed by:		Module: • GIC, • CSB, • EDGE • Platform security	

RETENTION Global Insights Cloud

Requirement ID:	**NF_GIC_01**	Priority**:**	Mandatory
Requirement title:		Security: Passwords management	
Description:		A System Administrator role will manage user roles and authorisations for the restricted access based on use roles	
Rationale/Goal:		Every user has access to data and views based on his role	
Means of verification:		Audit to user roles and assignments – Usability testing	
Dependencies:		NF_SP_01, NF_SP_02	
Addressed by:		Module: • GIC, • Platform security Relevant to: • Administration • User Roles	

Requirement ID:	NF_GIC_02	Priority:	Mandatory
Requirement title:		Security: Secure data flow	
Description:		Data and intervention models flowing between GIC and CSB should be secured from attacks (e.g. 'man in the middle' type of attacks)	
Rationale/Goal:		Ensure that the system adequately satisfies the security requirements	
Means of verification:		Security testing	
Dependencies:		NF_GIC_01, NF_SP_01	
Addressed by:		Module: • GIC, • Platform security • Integration & testing	

Requirement ID:	NF_GIC_03	Priority:	Mandatory
Requirement title:		Operational: GIC components interactions	
Description:		The GIC should expose an integration layer capable for exposing data and models between its components (e.g., through API interfaces, stream-processing bus etc).	
Rationale/Goal:		Seamless data flow between GIC components	
Means of verification:		Performance and usability testing	
Dependencies:		NF_GIC_01, NF_SP_10	
Addressed by:		Module: • GIC, • CSB, • Platform security Relevant to: • GIC Data Layer and REST API (GICDL)	

RETENTION Clinical Site Backend

Requirement ID:	NF_CSB_01	Priority:	Mandatory
Requirement title:		Security: Passwords management	
Description:		A System Administrator role will manage user roles and authorisations for the restricted access based on use roles	
Rationale/Goal:		Every user has access to data and views based on his role	
Means of verification:		Audit to user roles and assignments – Usability testing	
Dependencies:		NF_SP_01, NF_SP_02	

Addressed by:	Module: • CSB Relevant to: • Administration • User Roles

Requirement ID:	**NF_CSB_02**	Priority:	Mandatory
Requirement title:		Security: Secure data flow	
Description:		Data and intervention models flowing between CSB and GIC and between CSB and RETENTION Patient End should be secured from attacks (e.g. 'man in the middle' type of attacks)	
Rationale/Goal:		Ensure that the system adequately satisfies the security requirements	
Means of verification:		Security testing	
Dependencies:		NF_CSB_01, NF_SP_01	
Addressed by:		Module: • GIC • CSB • EDGE • Integration & testing	

RETENTION Patient Edge & Gateway and analytics

Requirement ID:	**NF_PE_01**	Priority:	Mandatory
Requirement title:		Patient edge always on	
Description:		The patient edge will be 99.5% ON, for the use of the patient and the carer	
Rationale/Goal:		For the patient to send measurements, the gateway must be always on	
Means of verification:		By design	
Dependencies:		NF_PE_03	
Addressed by:		Module: • EDGE • Platform security • Platform infrastructure	

Requirement ID:	**NF_ PE _02**	Priority:	Mandatory
Requirement title:		Patient edge connectivity and protocols	
Description:		The edge gateway must provide all available protocols and connections for the devices in project	
Rationale/Goal:		To get all data form the patient or carer	
Means of verification:		By design	

Dependencies:	NF_PE_03
Addressed by:	Module: • EDGE • Platform security

Requirement ID:	**NF_ PE _03**	Priority:	Mandatory
Requirement title:		Patient edge API	
Description:		Simple and adequate API to communicate with external devices	
Rationale/Goal:		to be simple for a new device to get onboard	
Means of verification:		By design	
Dependencies:		NF_PE_02	
Addressed by:		Module: • EDGE • Patient devices	

Requirement ID:	**NF_PE_04**	Priority:	optional
Requirement title:		Adequate streaming engine	
Description:		Adequate streaming capabilities for real time data, in volumes and speeds	
Rationale/Goal:		To be able to stream data in high volumes and speeds	
Means of verification:		By design	
Dependencies:		NF_PE_01	
Addressed by:		Module: • EDGE • Patient devices	

Requirement ID:	**NF_PE_05**	Priority:	Mandatory
Requirement title:		Easy to integrate with AI, BI, DSS, other applications	
Description:		Easy to integrate with other applications, by following industry standards, like HL7.	
Rationale/Goal:		To be able to integrate with other applications	
Means of verification:		By design	
Dependencies:		NF_PE_01, NF_PE_02, NF_PE_03	
Addressed by:		Module: • EDGE	

Requirement ID:	**NF_PE_06**	Priority:	Mandatory
Requirement title:		Full secure edge software	
Description:		Security for patient and carer data is of outmost importance, so the gateway must be able to operate under a security scheme (end to end encryption)	
Rationale/Goal:		To be able to work under a high security scheme	

Means of verification:	By design
Dependencies:	NF_SP_01
Addressed by:	Module: • EDGE • security

Scalability

Requirement ID:	**NF_SM_1**	**Priority:**	Mandatory
Requirement title:		Scalability	
Description:		Refers to the capability of the platform to scale-up or down the hardware resources in a dynamic manner in order to adjust the abovementioned to the requested workload changes, maximizing the use of resources.	
Rationale/Goal:		A cloud platform must be expandable in terms of hardware and software components.	
Means of verification:		By design	
Dependencies:		NF_SP_10	
Addressed by:		Module: • Platform infrastructure	

Functional Requirements

Authentication & Authorisation

Requirement ID:	**FN_AA_01**	Priority:	Mandatory
Requirement title:		Security – End-user registration	
Description:		1. An end-user of the platform might gain access to the RETENTION platform if he/she provides a valid email, full name, organisation, role and a hard-to-guess password; CAPTCHA to determine whether the user fills mandatory fields is real or a spam robot; 2. An email notification containing a link is generated to validate the email sent upon registration completion. In order to proceed, the end-user should verify his/her email address using the specific link. 3. Upon successful validation, registration request will be subject to administrator approval. Administrator will contact a responsible for the specific organisation (each RETENTION organisation must nominate at least one “responsible person”) to confirm the end-user’s identity, role and email. Upon receiving and confirming the relevant information, enters the admin area to approve or deny the registration request. • Alternatively, already has a list of all the accepted end-users/roles per organisation 4. An email notification is sent informing about the outcome (acceptance/rejection).	

Rationale/Goal:	End user registration
Means of verification:	• Email with a unique link to validate the registered email; • Registration data is stored in the end-user account (encrypted); • Confirmation email is sent to the validated email address. System logs this transmission. ○ If end-user entered invalid data or chose to cancel the account creation request, no account record will be created.
Dependencies:	NF_GIC_01, NF_CSB_01
Addressed by:	modules: • CSB, • EDGE • Security Relevant to: • Administration • User roles

Requirement ID:	**FN_AA_02**	Priority	**Mandatory**
Requirement title:		Security – End-user login	
Description:		1. In order to login, the valid end-user should provide his/her email address and the password. 2. System checks credentials against the stored ones (e.g., compare the encrypted entered password with the stored hash) and • upon successful match (login), logs the end-user in the Dashboard (home page); • displays an error message to the user and redirects to the login form. On the third failed attempt, CAPTCHA mechanism is activated.	
Rationale/Goal:		User login	
Means of verification:		• CAPTCHA to determine whether the user is real or a spam robot; • System logs all login attempts (email, IP, timestamp).	
Dependencies:		FN_AA_01	
Addressed by:		modules: • CSB, • EDGE • Security Relevant to: • Administration User roles	

Requirement ID:	**FN_AA_03**	Priority**:**	**Mandatory**
Requirement title:		Security - End-user logout	

Description:	1. The end-user logouts from his/her RETENTION platform account; 2. Upon successful log out, the system displays a success message to the end-user.
Rationale/Goal:	logout
Means of verification:	• System logs all logout attempts (email, IP, timestamp).
Dependencies:	FN_AA_02
Addressed by:	modules: • CSB, • EDGE • Security Relevant to: • Administration User roles

Requirement ID:	**FN_AA_04**	Priority**:**	**Mandatory**
Requirement title:		Security: Modifying end-user's registration info	
Description:		1. Admin/end-user selects end-user registration record; • Admin is able to alter account status, and role; • End-user is able to alter his/her email, full name and role (to be approved); He/she can also change the account password. 2. Upon successful alternation, the system displays a message to the admin/end-user. 3. End-users are sent an email notification if they change or reset their email or/and password on their account. Password changed notifications are not sent if the end-user is in an inactive state.	
Rationale/Goal:		FN_AA_01, FN_AA_02	
Means of verification:		• System logs email or password attempts (email, IP, timestamp). • System logs informative email timestamp.	
Dependencies:		FN_AA_01 ,FN_AA_02	
Addressed by:		modules: • CSB, • EDGE • Security Relevant to: • Administration • User roles	

Requirement ID:	**FN_AA_05**	Priority**:**	**Mandatory**
Requirement title:		Security/Privacy: Create a study participant (minimum personal) record	

Description:	Recruitment: patient (or study participant) is recruited for RETENTION, he/she goes to the local pilot partner and signs the consent form) 1. The patient is registered at the local clinical system of the pilot partner (outside RETENTION scope). An ID is associated with his/her medical record; 2. RETENTION patient record is created by a authorised end-user (e.g., CCM). During this process, system will create automatically a pseudo identifier (Pseudo-Id1) for the patient, while the external ID is also stored; • Alternatively, Pseudo-Id1 is stored withing the scope of the local clinical system. 3. When it creates Pseudo-Id1, the system will also create a second (internal) pseudo identifier (i.e., Pseudo-Id2) and associate it with Pseudo-Id1 simultaneously; 4. IDs association (i.e., between Pseudo-Id1 and Pseudo-Id2) is stored in encrypted fashion. This Pseudo-Id2 will be used by the RETENTION system onwards as the id for any data that will ever be received for the particular patient (e.g., via the app). The association will be used in data ingestion and extraction. Pseudo-Id2 will NOT be communicated outside from RETENTION system. 5. RETENTION patient record will contain the Pseudo-Id1, a randomly associated email (for enabling the smartphone's automated update mechanism), the clinical organisation has been associated with, the consent timestamp along with up to 3 clinical case manager(s) (valid RETENTION end-users) and up to 3 caregivers/close relatives (emails) that can be informed in case of an emergency (patient provides consent to do so). 6. Caregivers/close relatives are sent an email notification indicating that where they are informed in case of an emergency for a particular RETENTION study participant.
Rationale/Goal:	Security, privacy authorisation, GDPR,
Means of verification:	• System logs viewing/editing attempts of personal information records been made (email, IP, timestamp). • System logs informative email timestamp.
Dependencies:	FN_AA_02
Addressed by:	modules: • CSB, • EDGE • Security Relevant to: • Administration • User roles

Requirement ID:	**FN_AA_06**	Priority:	**Mandatory**
Requirement title:		Security/Privacy: Alter study participant record	

Description:	1. An authorised end-user (e.g., CCM) alters, the randomly associated email, or the clinical organisation, or any of the associated clinical case manager(s)/ caregivers/close relatives. 2. Caregivers/close relatives are sent an email notification indicating that where they are informed in case of an emergency for a particular RETENTION study participant
Rationale/Goal:	Security/Privacy: Create a study participant (minimum personal) record
Means of verification:	• System logs viewing/editing attempts of personal information records been made (email, IP, timestamp). • System logs informative email timestamp.
Dependencies:	FN_AA_02, FN_AA_05
Addressed by:	modules: • CSB, • EDGE • Security Relevant to: • Administration • User roles

Requirement ID:	**FN_AA_07**	Priority:	Optional
Requirement title:		Privacy: GDPR requests management	
Description:		1. Patient through his/her smartphone or an authorised end-user(s) (e.g., pilot partner CCM who recruited him/her) through the Dashboard may initiate a GDPR request, stating the category and accompanying text if is deemed appropriate; 2. Upon the receipt of such a request, system administrator (and other if necessary) will proceed copying with the particular request; 3. Response (and relevant data in machine-readable format if applicable) will be delivered to patient's smartphone or the relevant clinical partner respectively.	
Rationale/Goal:		Security, privacy authorisation, GDPR	
Means of verification:		• System logs GDPR request initiation and changes in its status.	
Dependencies:		NF_LE_05	
Addressed by:		modules: • GIC • CSB, • EDGE • Security Relevant to: • Administration • User roles	

Requirement ID:	FN_AA_08	Priority:	Optional
Requirement title:		Privacy: Maintain records of processing activities	
Description:		Logging mechanism of GDPR requests tracks the progress of individual cases (i.e., participant's Id, requested-on behalf, status, request timestamp, time-limits, assigned-to, justification, completion timestamp (if any)) and demonstrates compliance with the GDPR (compliance with timescales, maintained logs for audit, evidence to be requested by the supervisory authority).	
Rationale/Goal:		Security, privacy authorisation, GDPR	
Means of verification:		• System logs GDPR request initiation and changes in its status.	
Dependencies:		NF_LE_07	
Addressed by:		modules: • GIC • CSB, • EDGE • Security Relevant to: • Administration • User roles	

Requirement ID:	FN_AA_09	Priority:	Mandatory
Requirement title:		Privacy: authorisation levels	
Description:		The system will have full security with compartmentalised levels, with at least security for each level, security for the role and security for .	
Rationale/Goal:		Security, privacy and authorisation	
Means of verification:		Unit test, system test, vulnerability test.	
Dependencies:		FN_AA_10, NF_SP_02	
Addressed by:		modules: • GIC • CSB, • EDGE • Security Relevant to: • Administration • User roles	

Requirement ID:	FN_AA_10	Priority:	Mandatory
Requirement title:		Privacy: authorisation system	
Description:		The system will have full security with compartmentalised levels, with at least security for each level, security for the role and security for all roles. At least with the following Roles:	

	• Patients and carers • Clinicians • Statisticians/policy makers • Administrators. The administrators will accept the doctors, The clinicians will accept the patients and the carer
Rationale/Goal:	Security, privacy and authorisation
Means of verification:	Unit test, system test, vulnerability test.
Dependencies:	FN_AA_09, NF_SP_02
Addressed by:	modules: • GIC • CSB, • EDGE • Security Relevant to: • Administration • User roles

Audit Tracking and Administrative

Requirement ID:	**FN_TA_01**	Priority:	**Optional**
Requirement title:		Audit tracking	
Description:		The system will have full audit tracking in all levels.	
Rationale/Goal:		Security, privacy authorisation, GDPR	
Means of verification:		• System logs GDPR request initiation and changes in its status.	
Dependencies:		NF_SP_07	
Addressed by:		modules: • Security Relevant to: • Administration • User roles	

Business rules: corrections, cancellations, and adjustments of transactions

Requirement ID:	**FN_BT_01**	Priority:	**Mandatory**
Requirement title:		corrections, cancellations, and adjustments of transactions	
Description:		All system corrections, cancellations, and adjustments of transactions will be monitored and can audited at any time	
Rationale/Goal:		Business rules	
Means of verification:		Unit test, system test, acceptance tests.	
Dependencies:		FN_TA_01	

Addressed by:	modules: • GIC • CSB, • EDGE, • Security Relevant to: • Administration • User roles

Certification and Devices

Requirement ID:	**FN_CD_01**	Priority:	**Optional**
Requirement title:		Certifications	
Description:		Certifications as needed.	
Rationale/Goal:		System certifications	
Means of verification:		Legal requirements.	
Dependencies:		NF_LE_06	
Addressed by:		modules: • EDGE Relevant to: • Administration	

Data and Reporting

Requirement ID:	**FN_DR_01**	Priority:	**Mandatory**
Requirement title:		Historical data	
Description:		Historical data will be maintained according to the GDPR rules	
Rationale/Goal:		History of the data in the system	
Means of verification:		By design and continuous monitoring.	
Dependencies:		NF_LE_05, NF_LE_07	
Addressed by:		Modules: • CSB	

Requirement ID:	**FN_DR_02**	Priority:	**Mandatory**
Requirement title:		Reporting	
Description:		Historical data will be maintained according to the GDPR rules	
Rationale/Goal:		Reporting and GDPR compliance	
Means of verification:		Unit test. System test. Acceptance test.	
Dependencies:		FN_HR_01, NF_LE_05	
Addressed by:		Modules: • GIC • CSB	

Requirement ID:	FN_DR_03	Priority:	Mandatory
Requirement title:		Data input frequency	
Description:		Data shall be provided at a regular interval and constantly fed into the Big Data analytics and models update platform.	
Rationale/Goal:		Constant data input frequency.	
Means of verification:		Add module that counts number of reports daily	
Dependencies:		NF_DR_02	
Addressed by:		Modules: • GIC • CSB	

Requirement ID:	FN_DR_04	Priority:	Mandatory
Requirement title:		Data mechanisms and processes.	
Description:		All processes and mechanisms for data cleaning, linking and merging various individual data, must be defined and implemented in an automated manner. Data cleaning process ensuring that invalid data are not considered.	
Rationale/Goal:		Interoperability layer: Prep data as input for AI models.	
Means of verification:		By design. Systems testing. Acceptance tests.	
Dependencies:		NF_DE_01	
Addressed by:		Modules: • GIC • CSB • EDGE • Security components	

External Interfaces

Requirement ID:	FN_EI_01	Priority:	Optional
Requirement title:		External interfaces	
Description:		The system will be able to connect to external systems if that will be required according to interoperability standards	
Rationale/Goal:		Connect to external systems	
Means of verification:		system testing	
Dependencies:		NF_DE_01, NF_DE_02	
Addressed by:		Modules: • GIC • CSB • Security component	

Mobile Application

Requirement ID:	FN_MA_01	Priority:	Mandatory
Requirement title:		Secure Connect to the RETENTION system.	

Description:	when it starts up, the application connects automatically to the system, via secure channels. The mobile phone/tablet is registered to the systems to be accepted.
Rationale/Goal:	AUTO-Connect to the RETENTION system.
Means of verification:	Unit testing. System testing. Integration testing.
Dependencies:	NF_SP_02
Addressed by:	Modules: • EDGE • Integration & testing

Requirement ID:	**FN_MA_02**	Priority:	**Mandatory**
Requirement title:		User login	
Description:		The patient or carer can login to the RETENTION system via the mobile application	
Rationale/Goal:		Connect to the RETENTION system.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_01	
Addressed by:		Modules: • EDGE • Integration & testing	

Requirement ID:	**FN_MA_03**	Priority:	**Mandatory**
Requirement title:		Wellness advanced report	
Description:		The patient or carer will be able to insert with ease the advanced report of the patient at the moment of use. The application will do this if the patient IS NOT feeling well (typical medical questions).	
Rationale/Goal:		Get the advanced wellness report from the patient or carer, when the patient is not feeling well.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • CSB • EDGE • Integration & testing	

Requirement ID:	**FN_MA_04**	Priority:	**Mandatory**
Requirement title:		CONNECT local (on the mobile device) or external devices (direct to the cloud).	
Description:		The patient or carer will be able to easily connect devices with compatible technology, to the phone/tablet and in extent to the mobile application and the RETENTION system. The application	

	will be able to recognise the device and send/receive data. All new devices will be reported to RETENTION.
Rationale/Goal:	Connect devices to the phone/tablet and in extension to the RETENTION system.
Means of verification:	Unit testing. System testing. Integration testing.
Dependencies:	FN_BT_01, FN_MA_02
Addressed by:	Modules: • CSB • EDGE • Integration & testing

Requirement ID:	**FN_MA_05**	Priority:	**Mandatory**
Requirement title:		Basic data capture from local (on the mobile device) connected devices.	
Description:		The patient or carer will be able to easily capture data from locally connected devices to the phone/tablet via protocols like Bluetooth or others. (Devices must already be connected to the phone/tablet and registered in the mobile application and in extension to the RETENTION system).	
Rationale/Goal:		Capture onboard data form devices.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02, FN_MA_03	
Addressed by:		Modules: • CSB • EDGE • Platform security	

Requirement ID:	**FN_MA_06**	Priority:	**Optional**
Requirement title:		Extended data capture from external devices, NOT directly connected to the mobile device	
Description:		The patient or carer will be able easily connect devices to the mobile application that are external to thephone/tablet and mobile application. (Devices must already be connected to mobile application and registered in it and in extension to the RETENTION system.	
Rationale/Goal:		Capture data from external devices.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02, FN_MA_03	
Addressed by:		Modules: • CSB • EDGE • Platform security	

Requirement ID:	FN_MA_07	Priority:	Mandatory
Requirement title:		Data visualisation from devices.	
Description:		The patient or carer will be able easily visualise the data from the platform. Ex. for the oximeter, the mobile app will display the % of oxygen at the given time.	
Rationale/Goal:		Data visualisation.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02, FN_MA_03	
Addressed by:		Modules: • EDGE • Integration & testing	

Requirement ID:	FN_MA_08	Priority:	Optional
Requirement title:		Visualise the Electronic Health Record on system.	
Description:		The patient or carer will be able to easily visualise parts of Electronic Health Record kept by the RETENTION system.	
Rationale/Goal:		EHR Data visualisation.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • EDGE • Integration & testing	

Requirement ID:	FN_MA_09	Priority:	Mandatory
Requirement title:		Add or modify and submit questionnaires or surveys.	
Description:		The patient or carer will be able to easily add, modify and submit questionnaires and/or surveys given by the clinical teams.	
Rationale/Goal:		Add, edit and submit questionnaires ans surveys.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • EDGE • Integration & testing	

Requirement ID:	FN_MA_10	Priority:	Optional
Requirement title:		Panic or problem alert.	
Description:		The patient or carer will be able to easily alert the medical team for a PANIC or DANGEROUS condition.	
Rationale/Goal:		Panic and/or dangerous condition alert to the medical team.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	

Addressed by:	Modules: • EDGE • Integration & testing

Requirement ID:	**FN_MA_11**	Priority:	**Mandatory**
Requirement title:		TEXT Messaging system that connects to the medical team.	
Description:		The patient or carer will be able to easily send a TEXT message to the medical team (NOT emergency).	
Rationale/Goal:		Messaging the clinical team for advice and information. On NON-dangerous conditions.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • EDGE • Integration & testing	

Requirement ID:	**FN_MA_12**	Priority:	**Mandatory**
Requirement title:		chat system that connects to the medical team.	
Description:		The patient or carer will be able to easily live chat with the medical team.	
Rationale/Goal:		Chat with the clinical team for advice and information.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • CSB • EDGE • Integration & testing	

Requirement ID:	**FN_MA_13**	Priority:	M**andatory**
Requirement title:		chat system with photograph send support	
Description:		The patient or carer will be able to send photos to the medical team.	
Rationale/Goal:		Inform medical team with photos	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • CSB • EDGE • Integration & testing	

Requirement ID:	**FN_MA_14**	Priority:	**Mandatory**
Requirement title:		Adherence to therapy.	

Description:	The patient (or via the carer) will be monitored for the patient's adherence to treatment (taking his medication timely and correctly) .
Rationale/Goal:	Patient adherence to treatment.
Means of verification:	Unit testing. System testing. Integration testing.
Dependencies:	FN_MA_02
Addressed by:	Modules: • CSB • EDGE • Integration & testing

Requirement ID:	**FN_MA_15**	Priority:	**Mandatory**
Requirement title:		Integration and visualisation of external services data	
Description:		the system will integrate and visualise external data, such as pollution, temperature and others.	
Rationale/Goal:		Integration of External services data.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • CSB • EDGE • Integration & testing	

Requirement ID:	**FN_MA_16**	Priority:	**Mandatory**
Requirement title:		Automated system messages	
Description:		the mobile application will receive automate system messages from the RETENTION AI or DSS and pass them to the patient or carer.	
Rationale/Goal:		To receive automated system messages.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02	
Addressed by:		Modules: • CSB • EDGE • Integration & testing	

Requirement ID:	**FN_MA_17**	Priority:	**Mandatory**
Requirement title:		Manual system messages (via the clinical team)	
Description:		the mobile application will receive manual system messages (via the clinical team), generated by the clinical team, down to the patient or carer.	
Rationale/Goal:		To receive messages from the clinical team.	
Means of verification:		Unit testing. System testing. Integration testing.	

Dependencies:	FN_MA_02
Addressed by:	Modules: • CSB • EDGE • Integration & testing

Requirement ID:	**FN_MA_18**	Priority:	**Mandatory**
Requirement title:		Personalisation of data and interface	
Description:		the mobile application will adapt the behaviour and visualisation	
Rationale/Goal:		Personalised interface.	
Means of verification:		Unit testing. System testing. Integration testing.	
Dependencies:		FN_MA_02, NF_US_03	
Addressed by:		Modules: • CSB • EDGE • Integration & testing	

Dashboard Interactions

Requirement ID:	**FN_DI_01**	Priority:	**Mandatory**
Requirement title:		CSB: Access to specific patient variables	
Description:		Clinicians need to have access to full insights and variable knowledge of each patient and all types of variables should be presented in a clear and understandable way	
Rationale/Goal:		Clear clinical view of patient	
Means of verification:		System testing	
Dependencies:		NF_CSB_01	
Addressed by:		Modules: • CSB • Integration & testing	

Requirement ID:	**FN_DI_02**	Priority:	**Mandatory**
Requirement title:		CSB: Store patient's visit data	
Description:		Clinicians have to be able to enter and store information during a patients visit from a predefined list of actions	
Rationale/Goal:		Update system data after patient's visit	
Means of verification:		System testing	
Dependencies:		FN_DI_01	
Addressed by:		Modules: • CSB • Integration & testing	

Requirement ID:	**FN_DI_03**	Priority:	**Mandatory**

Requirement title:	CSB: Chat functionality
Description:	Clinicians have to be able to be informed about chat interaction or patients message request in a convenient way
Rationale/Goal:	Not miss chat message between clinician and patient/care giver
Means of verification:	System testing
Dependencies:	FN_MA_12
Addressed by:	Modules: • CSB • Integration & testing

Requirement ID:	**FN_DI_04**	Priority:	**Mandatory**
Requirement title:		CSB: Validation of proposed intervention	
Description:		Retention dashboard will display the proposed intervention to clinician for specific patient that it should be accepted by the clinician	
Rationale/Goal:		Approved and validated interventions	
Means of verification:		System testing	
Dependencies:		FN_DI_01	
Addressed by:			
Addressed by:		Modules: • CSB • Integration & testing	

Requirement ID:	**FN_DI_05**	Priority:	**Mandatory**
Requirement title:		CSB: Alarm/Notification creation	
Description:		The clinician approves an intervention and the system creates the relative notification on patient's device	
Rationale/Goal:		Approved and validated notifications	
Means of verification:		System testing	
Dependencies:		FN_DI_04	
Addressed by:		Modules: • CSB • Integration & testing	

Requirement ID:	**FN_DI_06**	Priority:	**Mandatory**
Requirement title:		CSB: Special events notification	
Description:		The visualisation provides a notification area in order the clinician to be informed about special events triggered by patient/care giver	
Rationale/Goal:		Communication of special events	
Means of verification:		System testing	
Dependencies:		FN_MA_10	

Addressed by:	Modules: • CSB • Integration & testing

Requirement ID:	**FN_DI_07**	Priority:	**Mandatory**
Requirement title:		CSB: Device management for activation/deactivation	
Description:		The clinician can assign a specific monitoring device to a patient after her enrollment. Also, she can deactivate this device if needed	
Rationale/Goal:		Association of a device to specific patient	
Means of verification:		System testing	
Dependencies:		FN_MA_04	
Addressed by:		Modules: • CSB • Integration & testing	

Requirement ID:	**FN_DI_08**	Priority:	**Mandatory**
Requirement title:		GIC: Models transfer from GIC to CSB	
Description:		The data analyst should be able to validate an intervention model to be used in CSB interventions	
Rationale/Goal:		Model trained in GIC to be executed in CBS intervention models execution environment	
Means of verification:		System testing	
Dependencies:		FN_GIC_02	
Addressed by:		Modules: • GIC • CSB • Integration & testing	

Requirement ID:	**FN_DI_09**	Priority:	**Mandatory**
Requirement title:		GIC: Identification of new parameters	
Description:		The data analyst should be informed about new parameters identified as a result of data analysis	
Rationale/Goal:		New/updated models	
Means of verification:		System testing	
Dependencies:		FN_DI_10	
Addressed by:		Modules: • GIC • Integration & testing	

Requirement ID:	**FN_DI_10**	Priority:	**Mandatory**
Requirement title:		GIC: Data analysis for research purposes	

Description:	A data analyst / researcher can perform statistical analysis of the available data and the system provides a set of predefined functions and visualization widgets
Rationale/Goal:	Statistical analysis of available data for research purposes
Means of verification:	System testing
Dependencies:	FN_DI_09
Addressed by:	Modules: • GIC • Integration & testing

Requirement ID:	**FN_DI_11**	Priority:	**Optional**
Requirement title:		GIC: GDPR and audit check	
Description:		An auditor should have access to all GDPR and audit check requests with detailed info regarding the status of the completion process and the persons involved	
Rationale/Goal:		Facilitation of audit check	
Means of verification:		System testing	
Dependencies:		NF_LE_05, NF_SP_07	
Addressed by:		Modules: • GIC • Integration & testing	

Requirement ID:	**FN_DI_12**	Priority:	**Mandatory**
Requirement title:		GIC: Patients' devices configuration	
Description:		The system administrator has to be able to apply pseudo-anonymised IDs of patients' devices, facilitating their configuration	
Rationale/Goal:		Patient's devices configuration	
Means of verification:		System testing	
Dependencies:		NF_LE_05	
Addressed by:		Modules: • GIC • Integration & testing	

The top-level BI-AI, Big Data, applications

AI (Artificial Intelligence) / ML (Machine Learning):

Requirement ID:	**FN_BIAI_01**	Priority:	**Mandatory**
Requirement title:		AI Models Build and Deploy	
Description:		The top-level layer will support the creation and editing of AI models and the components needed to execute the analytics, the DSSs and support the clinical interventions.	
Rationale/Goal:		AI design and development for risk/status prediction	
Means of verification:		Perform technical tests, model performance	

Dependencies:	FN_BIAI_03
Addressed by:	Modules: • GIC • Integration & testing

Requirement ID:	**FN_BIAI_02**	Priority:	**Mandatory**
Requirement title:		Serialised AI models	
Description:		The AI should produce serialisable model outcomes. In the serialised form, the data can be delivered to another data store, application, or other destination.	
Rationale/Goal:		Serialisation for an easily transmittable form.	
Means of verification:		Build a test unit for transmitting and deserializing models	
Dependencies:		FN_BIAI_01	
Addressed by:		Modules: • GIC • Integration & testing	

Requirement ID:	**FN_BIAI_03**	Priority:	**Mandatory**
Requirement title:		AI models and analytics input data	
Description:		The input data for AI models should be structured files, such as JSON, CSV files. The imported data within the Gateway should have a hierarchical structure, such as JSON/XML format.	
Rationale/Goal:		Input data.	
Means of verification:		By design.	
Dependencies:		FN_BIAI_01, FN_BIAI_09	
Addressed by:		Modules: • GIC • CSB	

Requirement ID:	**FN_BIAI_04**	Priority:	**Optional**
Requirement title:		Use efficient models	
Description:		AI Models should be optimised such as not to be computational expensive.	
Rationale/Goal:		Efficiency of the computational costs.	
Means of verification:		Compare training times versus prediction accuracy	
Dependencies:		FN_BIAI_01	
Addressed by:		Modules: • GIC	

Requirement ID:	**FN_BIAI_05**	Priority:	**Mandatory**
Requirement title:		Trustworthiness of models	
Description:		Models should be, verifiable and trustworthy.	

Rationale/Goal:	Offering and verifiable decision-making capabilities that leverage the evidence produced by the underlying data analysis and augment clinical studies targeting HF and other CVDs.
Means of verification:	Present results in meetings and validate with other technical partners
Dependencies:	n/a
Addressed by:	Modules: • GIC

Big Data Platform:

Requirement ID:	**FN_BIAI_06**	Priority:	**Mandatory**
Requirement title:		Data structure	
Description:		Data should be easy to be retrieved and easy to be integrated within AI, BI, DSS and other applications, for example able to be retrieved easy and fast, in e.g., a tabular form (data frame).	
Rationale/Goal:		Data should be easy to read and interpret.	
Means of verification:		Testing.	
Dependencies:		FN_BIAI_07, FN_BIAI_09	
Addressed by:		Modules: • GIC • CSB • Integration & testing	

Requirement ID:	**FN_BIAI_07**	Priority:	**Optional**
Requirement title:		Data structure type	
Description:		Data should be homogeneous for an efficient processing, meaning same data structure across clinical centres	
Rationale/Goal:		Input data.	
Means of verification:		Acceptance Testing.	
Dependencies:		FN_BIAI_06	
Addressed by:		Modules: • GIC • CSB • EDGE • Integration & testing	

Requirement ID:	**FN_BIAI_09**	Priority:	**Mandatory**
Requirement title:		FAIR	
Description:		Data should respect FAIR principles, such as findable, accessible, interoperable, reusable	
Rationale/Goal:		By respecting the FAIR principles data can be easily used by the RETENTION framework	
Means of verification:		Certified by technical partners	

Dependencies:	FN_BIAI_03, FN_BIAI_06
Addressed by:	Modules: • GIC • CSB • EDGE • Integration & testing

Requirement ID:	**FN_BIAI_09**	Priority:	**Mandatory**
Requirement title:		Get metadata of a data base schema	
Description:		The Big Data Platform should access a REST functionality to enable the retrieval of information regarding a DB schema. This will allow to retrieve the list of corresponding tables/indices, the tables' column names and data types, the primary/foreign key constraints.	
Rationale/Goal:		Data Visualisation Dashboard.	
Means of verification:		Querying database tables/indices of interest	
Dependencies:		FN_BIAI_10	
Addressed by:		Modules: • GIC	

Requirement ID:	**FN_BIAI_10**	Priority:	**Mandatory**
Requirement title:		API access to data	
Description:		Big Data Platform should access a REST functionality to allow the Data Analytics components to retrieve intermediate query results of their execution	
Rationale/Goal:		Real-time access to data	
Means of verification:		Querying the provided REST API	
Dependencies:		FN_BIAI_06	
Addressed by:		Modules: • GIC • CSB	

BI (Business Intelligence) / Analytics:

Requirement ID:	**FN_BIAI_11**	Priority:	**Mandatory**
Requirement title:		AI Design	
Description:		With respect to HF management, including prediction and progression, the goal is to investigate patient features and how they correlate with outcomes, providing the means for key factors identifications that affect patient health status. This can be achieved through a combination of classification, process mining and pattern mining techniques, and visual analytics.	
Rationale/Goal:		Build models to diagnose based on certain KPIs read from the patient	

Means of verification:	Validate by clinician
Dependencies:	FN_BIAI_01
Addressed by:	Modules: • GIC • Integration & testing

Requirement ID:	**FN_BIAI_12**	Priority:	**Mandatory**
Requirement title:		Big Data Processing	
Description:		AI models and analytics should be able to handle big amounts of data well.	
Rationale/Goal:		Capability to work with large amount of data	
Means of verification:		By testing	
Dependencies:		FN_BIAI_011	
Addressed by:		Modules: • GIC • Integration & testing	

Requirement ID:	**FN_BIAI_13**	Priority:	**Mandatory**
Requirement title:		Validate data	
Description:		Input data for AI models and BI/Analytics should be consistent, as complete as possible, unique (no duplicates), and the data must be accurate to correctly represent the recorded events (no missing timestamp or measurement information).	
Rationale/Goal:		Filter out redundant data	
Means of verification:		Build a validation system for these types of scenarios	
Dependencies:		FN_BIAI_03	
Addressed by:		Modules: • GIC	

Requirement ID:	**FN_BIAI_14**	**Priority:**	**Mandatory**
Requirement title:		Alert System	
Description:		AI models results and analytics should support corresponding alerts necessary towards the clinical level.	
Rationale/Goal:		Build an alert decision support systems with multiple alert levels	
Means of verification:		Validate by clinician	
Dependencies:		FN_DI_05	
Addressed by:		Modules: • GIC • CSB	

Requirement ID:	**FN_BIAI_15**	Priority:	**Optional**

Requirement title:	Recurring update of models
Description:	AI models should be generated/updated on a regular interval. Once new data is added into system, the models need to take that into consideration
Rationale/Goal:	Update models regularly with new data. Raise alert if a model stagnates
Means of verification:	By design
Dependencies:	FN_DI_04
Addressed by:	Modules: • GIC • CSB

Requirement ID:	**FN_BIAI_16**	Priority:	**Mandatory**
Requirement title:		Causal analysis through monitoring of policies' KPIs.	
Description:		KPIs monitoring is essential in the assessment or development of health policies. In this context, causal analysis refers to the association of potential changes in specific KPIs with certain interventions or with other available patient related data. Such associations can facilitate the identification of factors that influence policy impact. A KPI monitoring dashboard is required for this process, available for public health experts.	
Rationale/Goal:		Help improving existing policies	
Means of verification:		Validate by clinician	
Dependencies:		FN_BIAI_17	
Addressed by:		Modules: • GIC • CSB	

Requirement ID:	**FN_BIAI_17**	Priority:	**Mandatory**
Requirement title:		Conceptual analysis of policies' KPIs.	
Description:		conceptual framework for the KPIs and their relationships could help in the design of public health policies. Public health experts will assess the final evaluation of the policies based on the given evidence. The outcome can be in the form of acceptance/non-acceptance along with recommendations for improvement.	
Rationale/Goal:		Policy analysis and evaluation	
Means of verification:		Validate by clinician	
Dependencies:		FN_BIAI_16	
Addressed by:		Modules: • GIC • CSB	

Applications:

Requirement ID:	**FN_BIAI_18**	Priority:	**Mandatory**
Requirement title:		Data and model sharing	
Description:		AI & BI models should provide an open data sharing specification and model which will enable new partners to leverage RETENTION platform, bringing new clinical trial data, new AI algorithms, as well as new types of smart devices into the platform, and linking it to additional domains and relevant piloting activities.	
Rationale/Goal:		Exploit the validated RETENTION intervention and decision-making models in pertinent applications.	
Means of verification:		Evaluate using feedback formulars	
Dependencies:		FN_BIAI_11	
Addressed by:		Modules: • GIC	

Appendix 6: co-design workshop report #1

Introduction

The following document is a report of the internal co-design workshop -held on March 3, 2022- aimed at the **assessment and refinement of the patients' Mobile App mockups.**

Below is the list of participants and their respective roles in the workshop:

Name	Organisation	Role
George Del Toro	DATAMED	Technical Partner
Angeliki Gkouziouta	ONASSIS CARDIAC SURGERY CENTRE	Clinical Partner
Stamatis Adamopoulos	ONASSIS CARDIAC SURGERY CENTRE	Clinical Partner
Mercedes Rivas-Lasarte	SERVICIO MADRILEÑO DE SALUD	Clinical Partner
Luciano Potena	ALMA MATER STUDIORUM UNIVERSITA' DI BOLOGNA	Clinical Partner
Laura Borgese	ALMA MATER STUDIORUM UNIVERSITA' DI BOLOGNA	Clinical Partner
Bastian Schmack	UNIVERSITY HOSPITAL ESSEN	Clinical Partner
Petros Nikolopoulos	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	Clinical Partner
Yorgos Goletsis	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	Observer
Mary Roumpi	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	Observer
Maria Haritou	INSTITUTE OF COMMUNICATION & COMPUTER SYSTEMS	Observer
Matteo Colombo	i2GROW	Moderator
Mattia Pirani	i2GROW	Observer
Gianluca Gambatesa	i2GROW	Facilitator

Workshop's structure

The purpose of the workshop was the assessment and refinement of patients' mockups.

The workshop took place on zoom and, for what concerns visuals and images, on mural (a professional whiteboard).

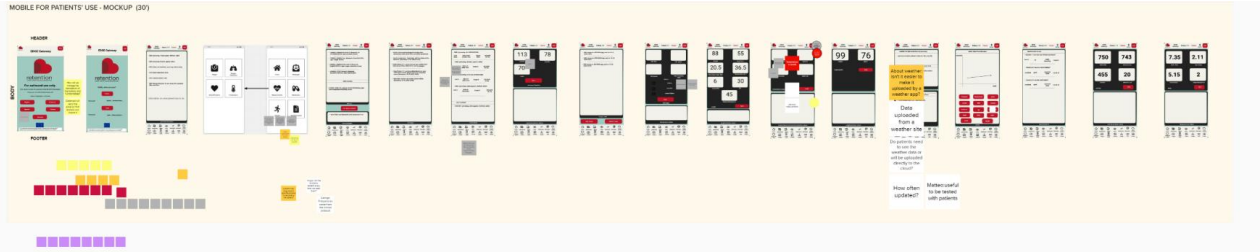
It lasted 3 hours, divided as follows:

- Mockups' introduction
- Q&A session
- Feedback session

- Doctors' suggestions (via stories)
- Insight harvesting and next steps
- Feedback and greetings

Mockups' Introduction

During the first part of the workshop, Mr. George Del Toro has introduced the Mobile Application's General Overview and has shown the mockups to participants; all the mockups have been hosted on the whiteboard, allowing participants to follow the explanation and to see with their eyes the user interface and the philosophy behind it.



Patients' Mobile App mockups' sequence

Q&A Session

At the end of the mockups' description phase, the participants were able to formulate questions relating to the user experience and, in general, to the design choices.

Patients' effort

Question 1 (UNIBO):

How long would it take the process to be done by the patient? Are we maybe asking too many things to patients? Have you already tested it?

Answer:

It depends on the patient and it must be discussed from the clinical side.

UNIBO suggests that there must be a balance between what is good from the engineering/scientist point of view (collecting as much data as they wish) and the willingness of patients to fill in the data.

From the developer point of view, it is doable to make the system show requests to the patients as many times as the doctors like (FORTH suggestion). It really depends on the protocol itself.

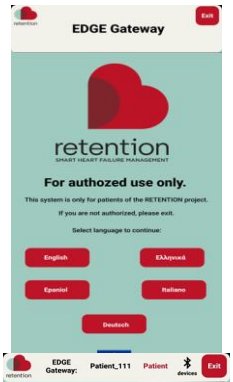
Languages

Question 2 (UNIBO):

How will we manage the translations of the buttons and functionalities?

Answer:

Datamed will send the excel in english so that doctors can import it and then translate it.



Buttons

Question 3 (Who?):

Will the buttons on the footer always be present? They seem too small.

Answer:

There are two alternatives, a version with 14 buttons, and another one with 5 buttons that will enable pop-ups. In any case, the buttons are easy to be recognised on a smartphone interface.

From the doctors' point of view, maybe there are too many icons and it would be useful to simplify.

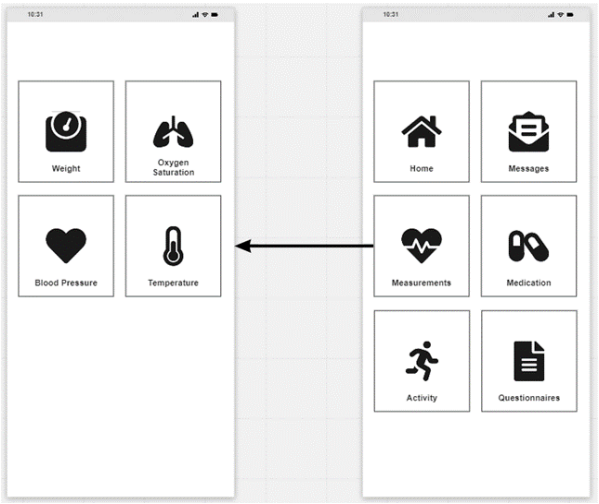
FitBit Sync

Question 4 (SERMAS):

How is information about daily activity, continuous HR and variability and sleep synchronised from the Fitbit?

Answer:

Fitbit is open - fitbit gets you everything you need via the tracker, everything the tracker is getting.



There is no specific screen dedicated to FitBit; sleep and activity data will come from the FitBit tracker.

UNIBO points out that FitBit overestimates the steps.

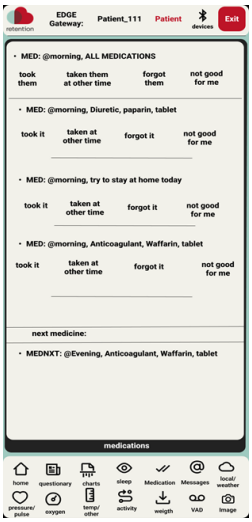
Medications' screen

Question 5 (SERMAS):

The screen looks too crowded. Could we simplify?

Answer:

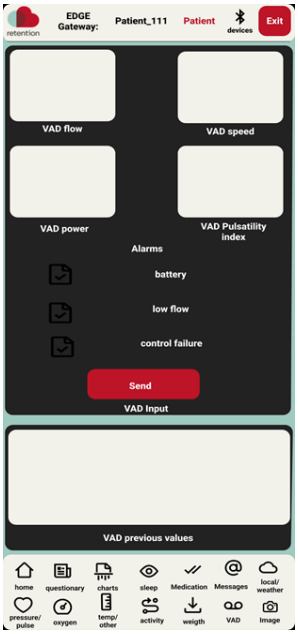
It is customisable and the system will focus on the questions that matter and the messages will be correlated to the patient's answer. The system will keep asking what it needs to know.



VAD Screen

Suggestion (SERMAS)

When a patient gets an alarm, the system should highlight the type, time and duration



Temperature, calories, fluids

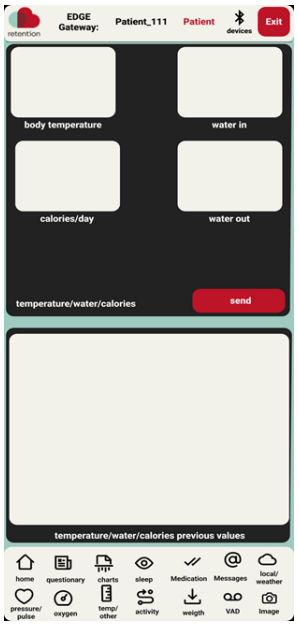
UKESSEN suggests that temperature must not be skipped completely, but it must be introduced depending on the conditions of the patients (temperature is a useful parameter, specially in a VAD patient). It must not be asked by default, regularly, but only when it's necessary.

FORTH suggests making the temperature screen available so that it could be activated when doctors need it. SERMAS suggests a button "I'm not feeling well" so that doctors could eventually ask for a temperature parameter.

UKESSEN asks if it is better to activate the process via chat or by an algorithm (automatically).

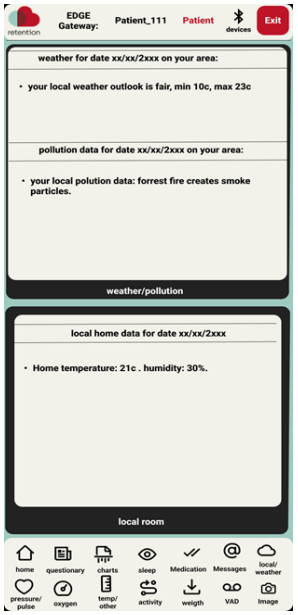
FORTH says there are two ways: the system collects the data related to temperature and it extracts the information/patterns useful to design an algorithm, otherwise doctors suggest the process to design an algorithm that - in certain conditions - makes the temperature interface pop up.

We need some kind of rule, developers say, to train the model with consistent data.



Weather data

Data will be uploaded by a weather website. Do patients need to see the weather conditions coming from the raspberry Pi getting the information from Copernicus? Is the daily average enough? This is something that could be part of the tests to be done with patients (i2Grow's suggestion).



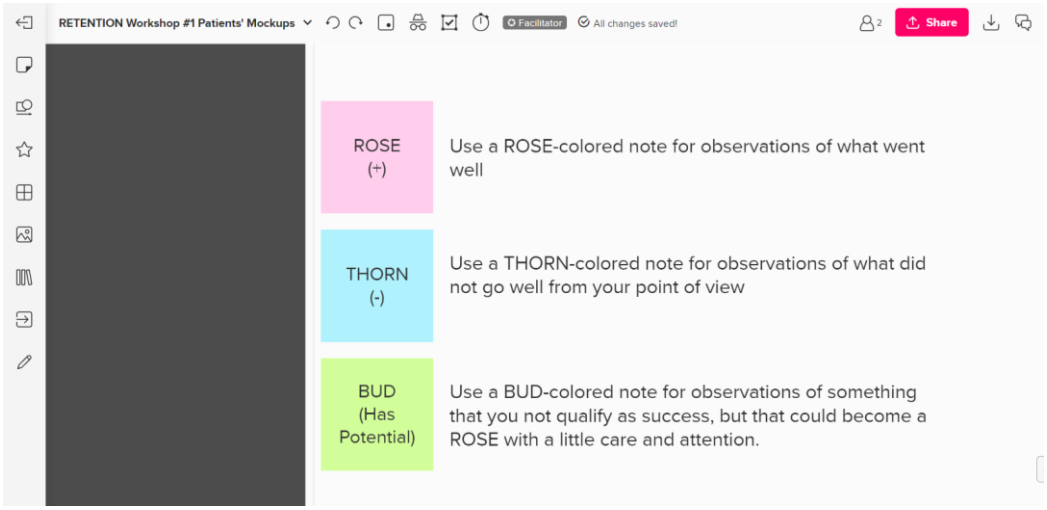
Feedback Session

Feedback sessions allowed participants to share, first individually, and then in group their opinions concerning the mockups.

Thanks to a color sticky legenda, participants have shared:

- observations of what went well (rose - pink sticky)

- observations of what did not go well (thorn - blue sticky)
- observations of something they do not consider success but, with a little care and attention, could become a success



What went well

Participants say that the overall design is nice, same for screens. Most of them have no observations to add, they are fine with the design.

What did not go well

Having clear in mind that their comments were constructive feedbacks and not judgements, participants have highlighted a few things:

- we should synchronise the screens with the clinical protocol content; seems like a few screens are missing (e.g. symptoms)
- We have patients distributed in a test group (they interact with the system and they share suggestions) and a control group (they don't interact, they only contribute to data. They will have the chance to send messages, but they'll not receive answers). Will the control group get any

feedback from the clinicians? We need to avoid the chance for the control group to see what the test group will see on the screen. We need to take care, not revealing who's in the control group and who's not (FORTH). DATAMED's proposal is letting the system know what group the patient belongs to, so that the app will only show what is pertinent to the profile. DATAMED suggests taking a decision about this topic. FORTH highlights the risk that patients could interact outside of the system, discovering that the experiences are different. i2Grow suggests taking the two groups separated during the patients' workshop and to explore the topic further in the meetings to come.

What needs care and attention

Participants have highlighted a few things/questions:

- Is the screen the same for patients and caregivers (UNIBO)? We need to pay attention.
- Is it possible to have a version to be tested? (DATAMED answers that it is not already a beta version, it is a test application to test the data).
- What's the size of the screen? I'm afraid it is too small for patients; the interface must be as simple as possible and as big as possible (UKESSEN); DATAMED answers it works well with smartphones. For sure we'll focus on bigger buttons. The navigation will focus on the few information that patients and doctors will need in a certain moment.
- Weather data must leverage on free, available weather apps, without too much effort in developing a system from scratch (UKESSEN).
- It'd be better having the blood pressure written as on the pressure meter (e.g. 140/90), instead of two different boxes to be filled with the two values (NKUA).

Doctors' suggestions (via stories)

Participants had a chance to share their stories related to previous experiences with apps developed for patients. A few insights, useful for the developers, have emerged:

- Be careful on the fit-bit step counter bias, tested against Google phone since the phone is not on the wrist but in the pocket (UNIBO).
- Oxygen saturation might be imprecise, especially for VAD patients (e.g., devices like garmin are not effective); UKESSEN suggests testing the oximeter device too with VAD patients (this must be part of a future workshop with patients, FORTH suggests).
- From previous experiences (with cancer patients) i2Grow says that it is crucial that patients find a value in using the app- not just adding data for the clinicians.
- Do we analyse Heart rhythm or "just" heart rate? Does the fit bit support ECG? (UKESSEN). DATAMED says FitBit is not a medical device, it is only a tracker. The Apple watch is a medical device. FitBit can track heart rate. UNIBO adds that we could choose a medical device, for sure expensive, but reliable - or a simple tracker that will not be reliable. Is it worth spending more for accuracy? Medical decisions from data shared by fitbit are tricky - we can look at other devices than the Apple watch, less expensive but reliable.

From insights to next steps

In the last part of the workshop, participants made a leap from insights to next steps.

What happened during the workshop? What did you notice?

The answers were:

- The overall app design is very good
- App functionalities should be uploaded according to clinical protocol
- We need to finally agree on smart devices. There are still questions with regard to the Smartphone
- Some critical issues on the alignment with the latest clinical protocol version. Some pending decisions on critical issues such as the heart rate monitoring system, the way intervention and control groups interact with the app, motivational messages

What patterns or conclusions are emerging?

- We must pay attention to the accuracy of the data
- Smart devices are crucial because they define the accuracy of the variables
- The RETENTION app will be the key point to make this project a successful project. The app should be improved
- There are still some important decisions that have to be taken by the clinical board.

What actions make sense?

- We need a version of the app to be tested, a beta version
- We need to review the final version of the protocol and make final comments
- We need to consider double checking with open source measurements like Google Fit/Samsung Health or Weather app
- We need to agree on the devices with regard to budget, clinicians' needs/wishes and IT infrastructure
- We need to synchronise with the final version of the protocol and refine the requirements!

Feedback related to the workshop

Participants shared some feedback:

- Mural was an effective tool to share ideas
- It was nice, I enjoyed it! Reluctant about the use of it with patients
- Very cool way to interact, but a bit time consuming and people need to be informed beforehand about the kind of meeting (point for attention)
- Shorter meetings sometimes are more efficient (point for attention)

Appendix 7: co-design workshop report #2

Introduction

The following document is a report of the internal co-design workshop -held on March 17, 2022- aimed at the **assessment and refinement of the Clinical Site Backend (CSB) and Global Insights Cloud (GIC) mockups.**

Below is the list of participants and their respective roles in the workshop:

Name	Organisation	Role
Angeliki Gkouziouta	ONASSIS CARDIAC SURGERY CENTRE	Clinical Partner
Mercedes Rivas Lasarte	SERVICIO MADRILEÑO DE SALUD	Clinical Partner
Laura Borgese	ALMA MATER STUDIORUM UNIVERSITA' DI BOLOGNA	Clinical Partner
Bastian Schmack	UNIVERSITY HOSPITAL ESSEN	Clinical Partner
Petros Nikolopoulos	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	Clinical Partner
Ioannis Basdekis	STS	Technical Partner
Michalis Vakalellis	AEGIS	Technical Partner
Andreas Alexopoulos	AEGIS	Technical Partner
Gabriel Danciu	SIEMENS	Technical Partner
Maria Haritou	INSTITUTE OF COMMUNICATION & COMPUTER SYSTEMS	Observer
Matteo Colombo	i2GROW	Coordinator and Moderator
Natalia Allegretti	i2GROW	Coordinator
Gianluca Gambatesa	i2GROW	Facilitator

Workshop's structure

The purpose of the workshop was the assessment and refinement of CSB and GIC mockups.

The workshop took place on zoom and, for what concerns visuals and images, on mural (a professional whiteboard).

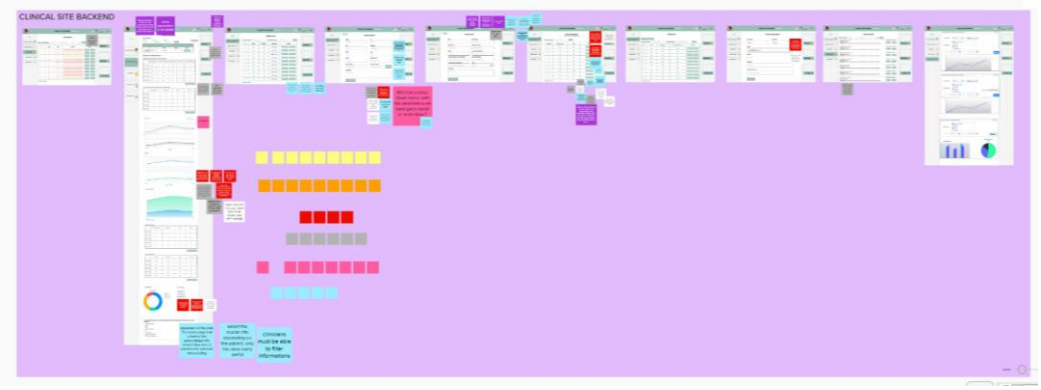
It lasted 3 hours, divided as follows:

- Mockups' introduction
- Q&A session
- Next steps

- Feedback and greetings

Mockups' Introduction

During the first part of the workshop, Mr. Michalis Vakalellis (AEGIS) and Mr. Gabriel Danciu (SIESRL) have explained the mockups inviting the participants to have a look at the user interface and the design ideas behind it.

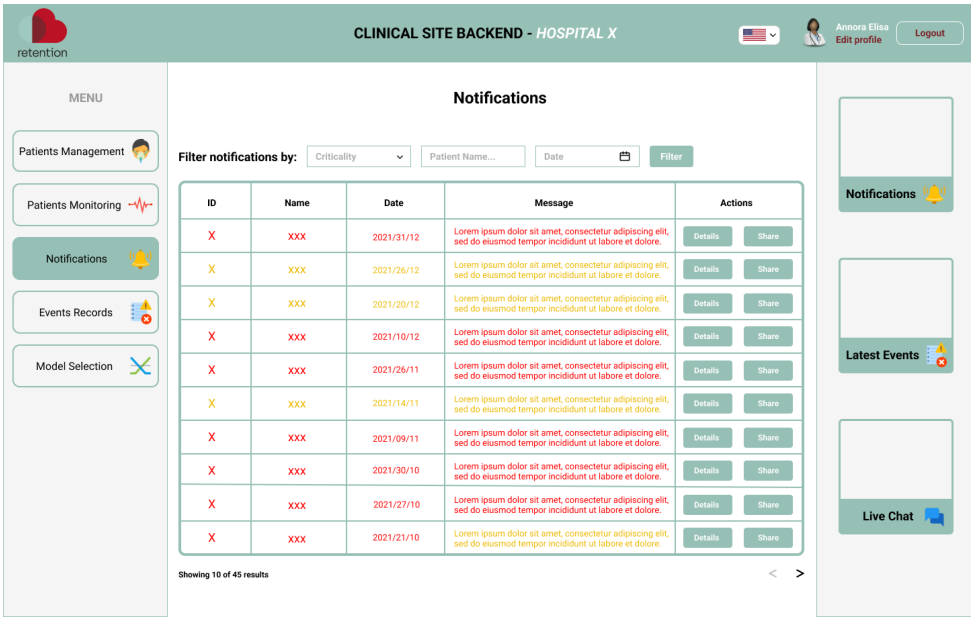


Clinical Backside mockups sequence

Q&A Session for Clinical Site Backend

At the end of the mockups' description phase, the participants were able to formulate questions relating to the user experience and, in general, to the design choices.

Notifications



SERMAS suggests there should be a button to allow actions like

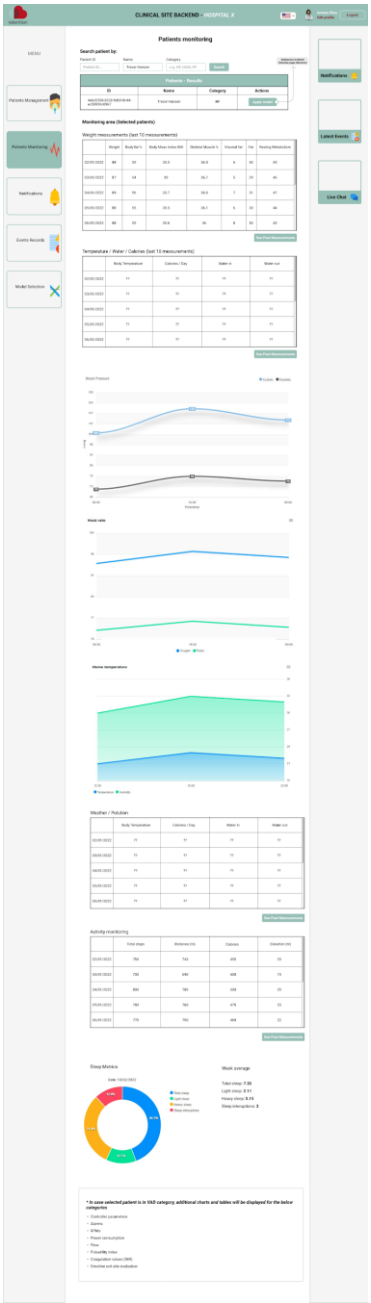
- dismiss
- schedule an in person visit
- schedule a telephone call visit

If doctors click on schedule a visit, they should have other options, like “change medication” or “reinforce health advices”

Patients Monitoring

i2Grow asks if the monitoring area parameters are already aligned with the ones discussed in the patient Age session.

STS answers that more parameters will be added.



The mockup has been useful to clarify the difference between notifications and events.

Notifications are automatically created by the system; events need to be created by clinicians (e.g. hospitalisation), events already shared via excel within the partners.

SERMAS adds that, for what concerns the scale, it is a simple one and neither calories nor water intake must be added (all the variables needed from patients have been listed in the excel file).

UKESSEN asks if there will be certain times during which clinicians will be notified about HR and SO2. The smartphone is measuring all day long. Should clinicians tell patients when to have rest so as to have comparable results? How do they get along with all that data? HR must be continuously monitored. Do clinicians need from the software any kind of average or other intervals/values? Max/Min/Average?

SERMAS adds that, for what concerns patient monitoring, there are two kinds of variables - the ones clinicians will use to manage the patients, the ones which clinicians don't know how to use yet (not so much literature related to them).

First of all clinicians should choose the device, depending on it they’ll have different variables. Once the variables are finally known, clinicians will ask for a certain kind of visualisation.

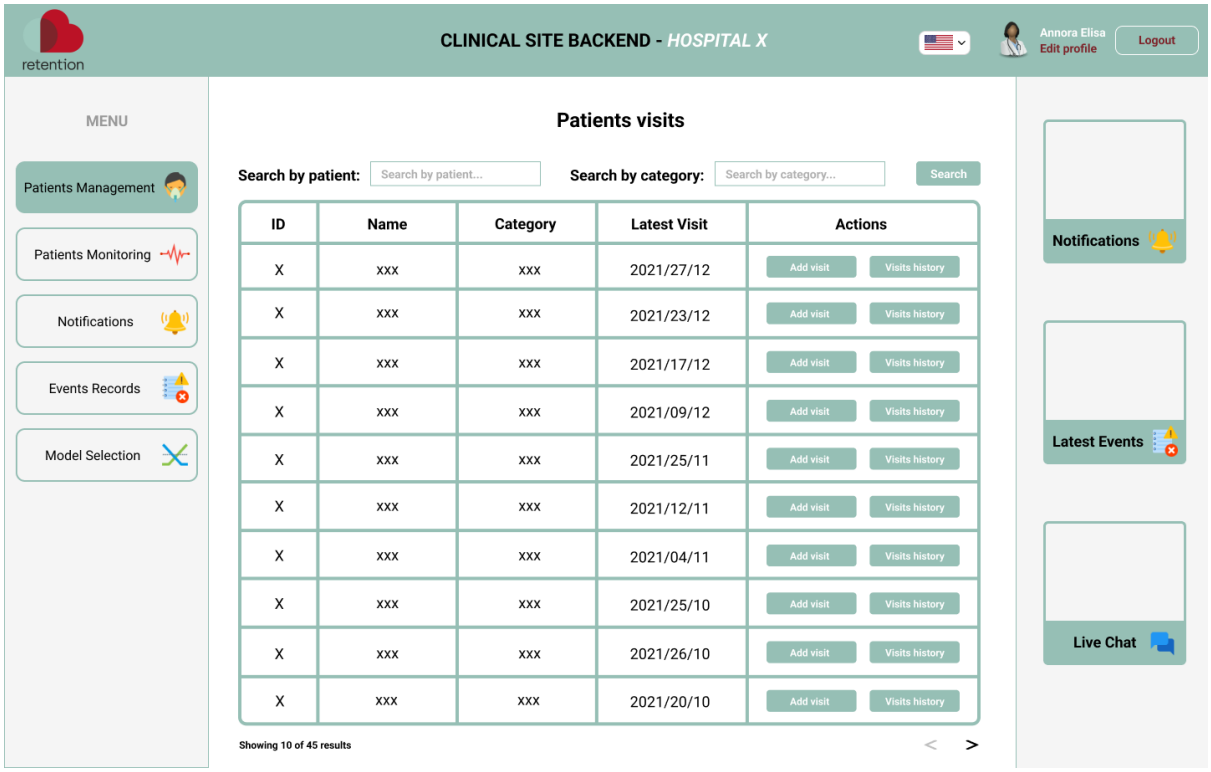
AEGIS is ok with showing the data the way doctors prefer.

AEGIS and **STS** highlight that the charts are placeholders, useful to understand if there's something missing.

Depending on the type of patient, there will be certain info useful to be viewed (by filtering).

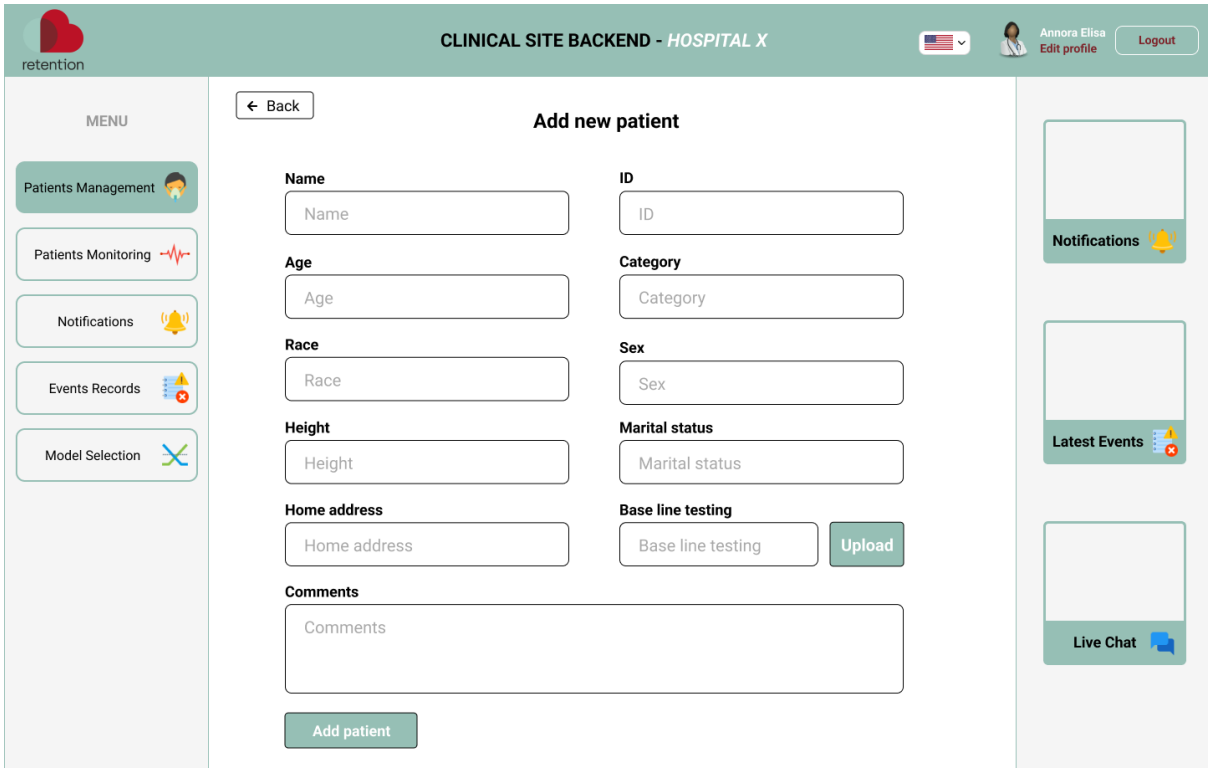
The home page that presents the personalised info should have less to prevent info overload and scrolling.

Patients Visits



STS says that, at first, clinicians should be allowed to view and later on to edit. By filtering the kind of visits, they'll be able to edit the parameters. A two step process: viewing and editing.

Add New Patient



For what concerns patients' data, **SERMAS** asks if clinicians will be allowed to upload patients' PDFs.

STS suggests to leverage a specific format for data sharing, unless there's a common way for information to be represented. An excel file will be useful to easily map the parameters.

Systems need to talk to each other (the hospitals' ones and the RETENTIONn one). Hospital system traces patients via an id, same for Retention (a different id).

A match between ids is necessary to make the automatic import doable. The hospital system needs to give a sort of an API to digest data.

Patients' creation has two steps: during the 1st one, personal data and PI are being inputted (sensitive data, encrypted), while during the 2nd, personal health record data, device assignment(s) and visit info are managed.

This is an interoperability issue and - as **i2Grow** reminds - from the RETENTION side there is a specific task leader in the interoperability area.

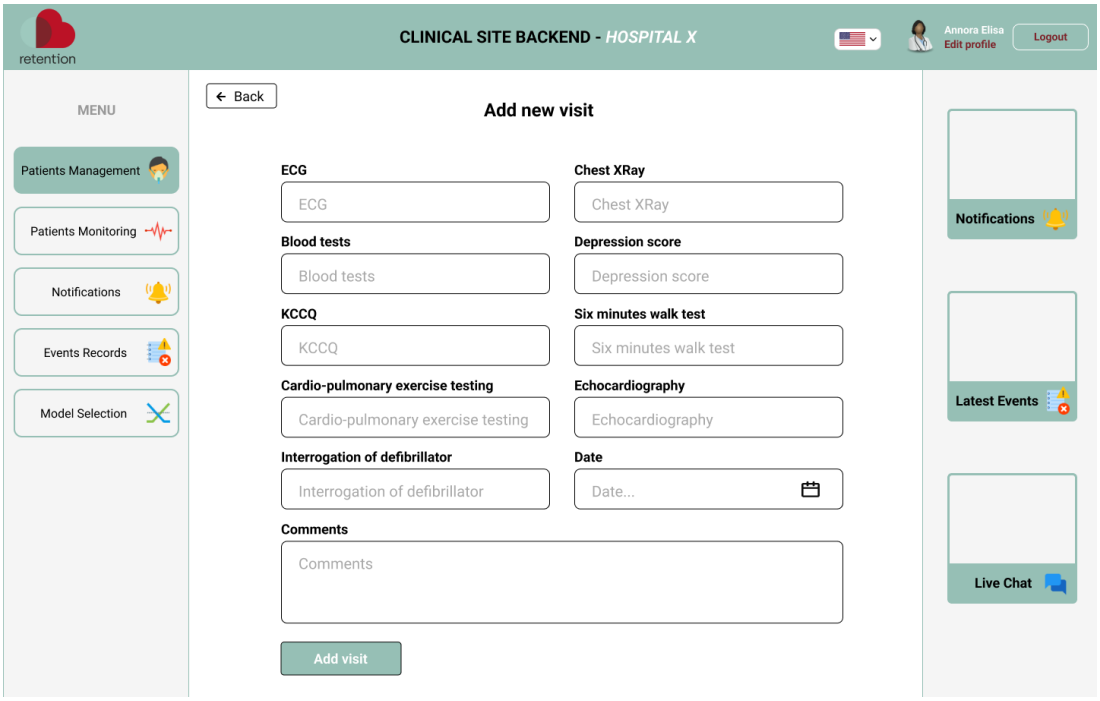
In any case, for what concerns data input, **STS** suggests avoiding free type.

i2Grow asks why, since there is interoperability, there is a need to create new patients into the CBS and not to import. Why mockups with data entry if it is an automatic process?

STS answers that not all the pilots have systems in place allowing the transmission of the data. In those cases, we need to allow a manual import.

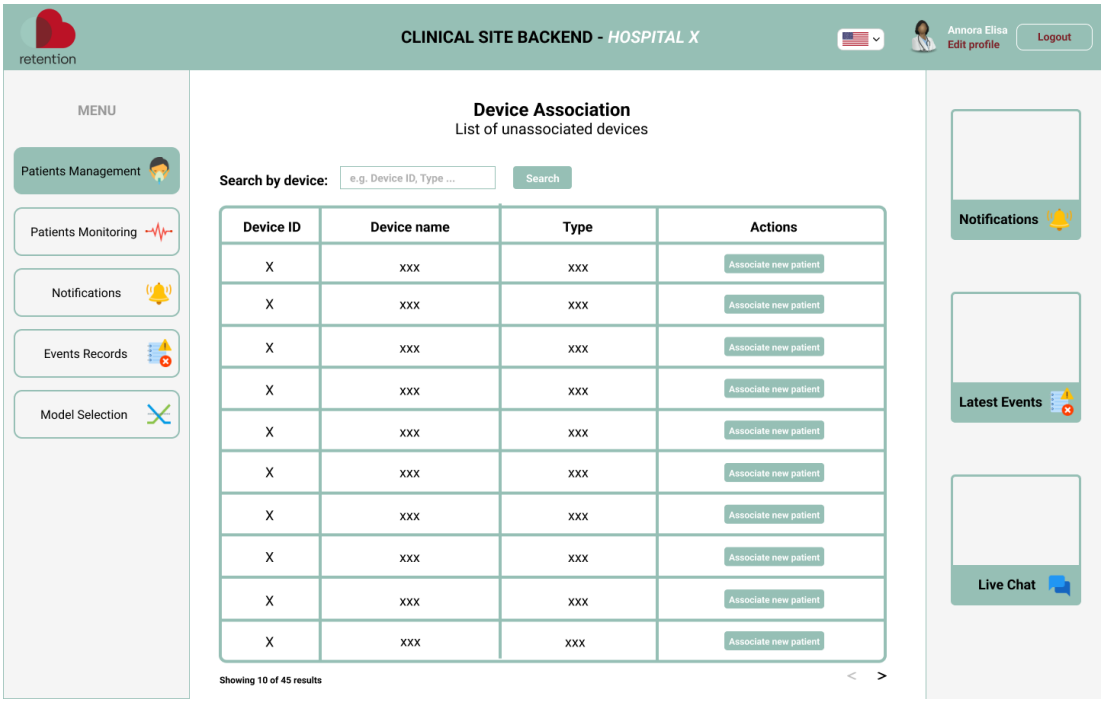
Mapping+API to directly get the data (not all the hospitals have the same way to collect and show data).

Add New Visit



STS highlights that, in the first instance, id must be created by the hospital team. Next step is identifying patients and allowing the Hospital System to share data with RETENTION.

Device Association



Unassociated devices mean devices in stock that could be matched with brand new patients.

STS reminds the group that an alternative Device association/allocation design mockup has been suggested (basecamp).

For what concerns device association, two roles are needed:

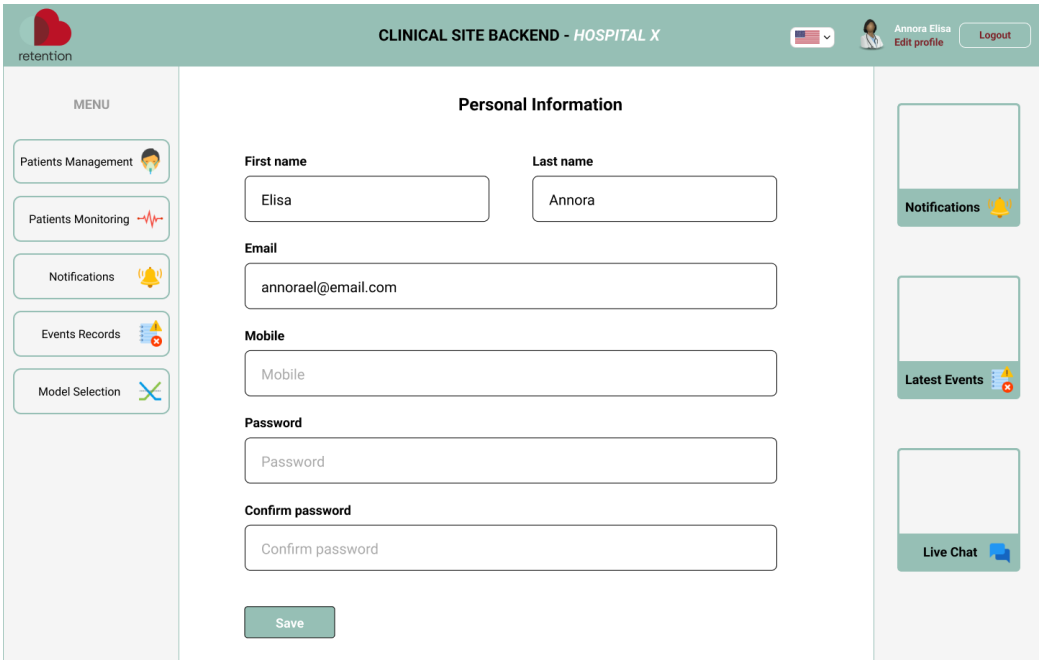
- the clinicians decide what devices are associated to whom
- a technician matches the device with the patient (technicians are not allowed to read sensitive data)

SERMAS says that there are no resources inside the hospital to be invested in a technician to manage this part of the flow and invites the technical partners to make this step as easy as possible.

ICCS says that in any case, if you monitor patients remotely, it is mandatory having technicians responsible for the process (installation and management) and it could be worth trying asking the Hospital IT dept for support. Tech partners build the system, technical support is required locally at pilot (clinical) site.

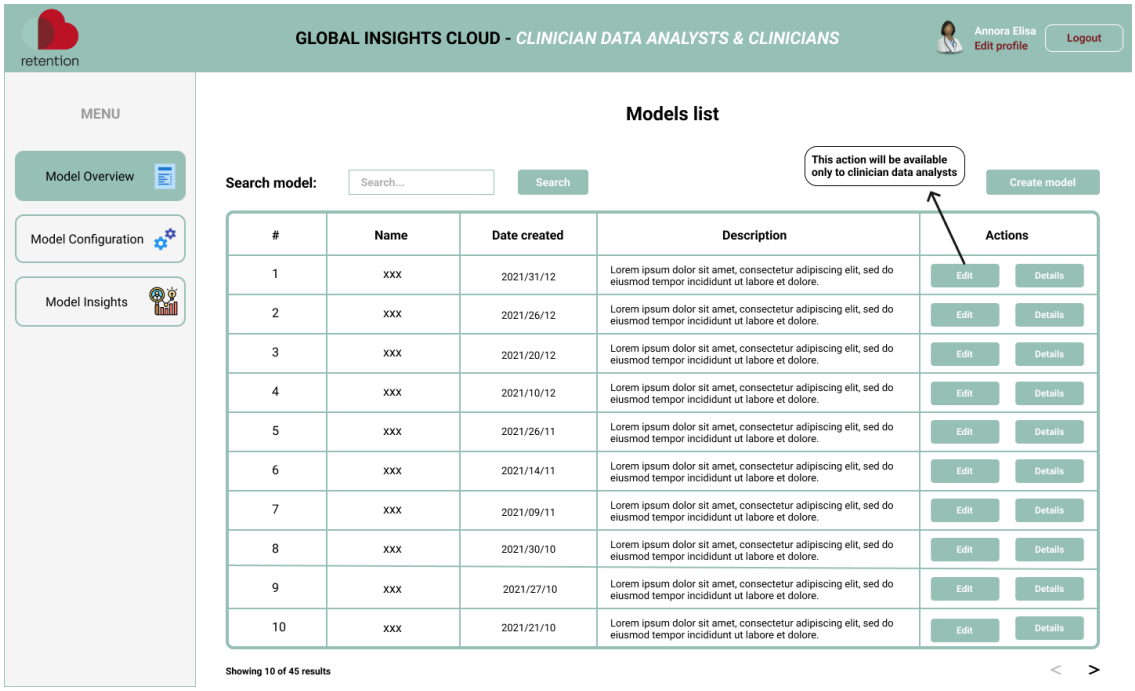
i2Grow suggests discussing the issue in the following meetings.

Personal Information



This screen is related to clinicians. Forgot my password functionality is available.

Q&A Session for Global Insights Cloud



SIESRL starts the presentation with a brainstorm invitation that will take place in the next few months: What are the use cases that the clinicians need from tech guys in this project? There will be data collected over a period of time. How might tech partners help clinical partners understand the data? This is something that needs cooperation.

STS highlights that there will be more models for the same scenario, and different scenarios.

i2Grow: if models are made and edited by data analysts, what's the action expected from clinical partners? Shouldn't clinicians be simply allowed to apply the model to a specific patient or selection of patients data sets? If so, where is the function to do so?

SERMAS adds there are no comments related to the mockups. As clinicians, they need to define what kind of models they want to be created. Who is going to create a specific model?

SIESRL answers that they will create models. Their question is “what do you need to find out from the models?”

From **SERMAS’s** point of view clinicians don’t need to apply the model but to receive info from the system that, leveraging the model, could send messages like “be aware that this patient is at risk of…”

The system allows the creation and administration of models, says **STS**. There will be another interface that will allow clinicians to apply the model to a set of patients.

In the excel file clinicians have shared all the events to be aware of; what is needed as an information is the risk for the patient to live those events (**SERMAS**).

STS adds that to start modeling there is no need for real data.

Clinicians and Technicians need to work in parallel mode, trying to define the models and later on these models will be applied to real data. Dummy data will be necessary in the beginning to accurately configure

the model. There are a few models from literature (e.g. the Seattle Heart Failure Model) that could be a starting point, as suggested by **i2Grow.**

The major outcome of the RETENTION Project is being able to define and execute models that differentiate (adding more important predictors) from the ones already present in the literature (**STS**).

SERMAS reminds the group that “every variable that we put in the excel could be a potential predictor”.

In the end of the conversation related to GIC a few points stand out:

- clinicians need a model able to predict the events (**SERMAS**)
- it is an ongoing process, later we’ll be able to refine models introducing new ones who target different variables (**STS**)
- it is a joint effort (**ICCS**)

Next steps

What actions make sense?

OCSC: we need to select the devices

SERMAS: we need to select the devices. When is it expected to happen?

UKESSEN: we need to put our hands on the system, understand how it works, work with the system to understand what’s established and what’s missing. I find it difficult to really understand the usability of the app leveraging mockups.

We need to get some “hands on”

NKUA: Will we be able to use a dummy version at the Madrid meeting?

A few considerations from the non-clinical partners:

AEGIS: we need to build the interface in order to use it; we'll incorporate your suggestions to build the dashboard.

ICCS: model development is a joint work, a collaborative work, between techs and clinicians, and it is a continuous collaboration. We need to understand if the model provides the answers to clinicians.

Feedback related to the workshop

i2Grow: Clinical partners should ensure availability and continuity to these kind of meetings, we need continuous interaction. It will be an iterative process.

Is Figma a good way to evaluate the mockups?

STS: we need to leverage Figma to show not only the screenshots but the sequence of actions necessary for each use case (e.g. device assignments).