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 of Communication and Computer Systems

Deliverable ID.:	**6.2**	
Deliverable title:	**RETENTION Security & Privacy by design enabling mechanisms v1**	
Planned delivery date:	31/12/2022	
Actual delivery date:	23/12/2022	
Deliverable leader:	STS	
Contributing partners:	DM, SIESLR, ICCS	
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.

This deliverable reflects only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.

Document information and history

Deliverable description (from DoA)
Delivery of the first version of the RETENTION Security and Privacy by design enabling mechanisms.

Version N.	Date	Author [Person and Organisation]	Reviewer [Person and Organisation]	Milestone*	Notes
V. 0.1	*31/10/2022*	*Ioannis BASDEKIS (STS)*		*Creation of ToC*	
V. 0.7	*14/12/2022*	*Emmanouil SPANOUDAKIS (STS), Georgios SPANOUDAKIS (STS), Ioannis BASDEKIS (STS)*		*1st draft version*	
V. 0.99	*18/12/2022*	*Emmanouil SPANOUDAKIS (STS), Georgios SPANOUDAKIS (STS), Ioannis BASDEKIS (STS)*		*2nd final draft version*	*For Review*
V. 0.99	*21/12/2022*		*Yiannis Kouris, Nikos Vasileiou, Maria Haritou (ICCS)*	*Final review*	*Minor comments*
V. 1.0	*22/12/2022*	*Emmanouil SPANOUDAKIS (STS), Georgios SPANOUDAKIS (STS), Ioannis BASDEKIS (STS)*		*final version*	
V. 1.0	*23/12/2022*		*Maria Haritou (ICCS)*	*Deliverable Approved*	*Deliverable Submitted*

Table of Contents

1 Executive Summary 9
2 About this Document 10
2.1 Role of deliverable 10
2.2 Relationship to other RETENTION deliverables 10
2.3 Structure of the document 11
3 RETENTION Security Component 12
3.1 Introduction 12
3.2 Prerequisites and Building Blocks 12
3.2.1 OAuth 2.0 14
3.2.2 OpenID Connect 16
3.2.3 API Manager 16
3.2.4 Hardware and Software requirements for the Security Component 17
3.3 Adhering to Privacy by Design Principles in the context of RETENTION 18
3.3.1 Choosing an appropriate Policy-Based Access Control 21
3.3.2 RETENTION Pseudonymisation 24
3.4 RETENTION Application and Home Gateway Secure Transmissions 28
3.5 Security Component: Main functionality 29
3.5.1 End-users' management 29
3.5.2 Patients' management 32
3.5.3 GDPR Requests management 36
4 Continuous monitoring of the Security and Privacy Posture 39
4.1 Elicitation analysis to address healthcare security management standards 39
4.2 RETENTION Continuous Security and Privacy Assurance Platform 41
4.2.1 Key Features 42
5 Operations 45
5.1 Keycloak - KrakenD Initialisation 45
5.1.1 End-User Roles Creation 47
5.1.2 Configuring Role-Based Access Control of CSB APIs 48
5.1.3 Security and Privacy Assessments Planning 51
6 Conclusion 55
7 References 56
8 Annexes 58

8.1 OpenApi.Json 58
8.2 Detailed Design of CSB@SecurityComponent Functionality 68

Table of Figures

Figure 1: RETENTION platform logic architecture overview. 13
Figure 2: OAuth 2 flow. 15
Figure 3: Upon a Access token is been issued by Keycloak issuing, KrakenD allows the triggering of an end-point assuming that role policy permits this. 16
Figure 4: Aspects of the "Privacy by Design" principle of GDPR 19
Figure 5: The CSB@SecurityComponent replaces Pseudo-Id1 to Pseudo-Id2 by which pseudonymised data record is stored in CSB@Repository and vice versa. In a similar way, CSB@SecurityComponent replaces Pseudo-Id1 to Pseudo-Id3 by which pseudonymised data record is stored in GIC@Repository. 26
Figure 6: Sequence diagram of the patient creation process suppotred by CSB@SecurityComponent. 33
Figure 7: Sequence diagram of the of the pseudonymisation process suppotred by CSB@SecurityComponent. 34
Figure 8: RETENTION Architecture overview: the RETENTION Continuous Security and Privacy Assurance Platform will perform security and privacy assessments. 42
Figure 9: The RETENTION Continuous Security and Privacy Assurance Platform's Architecture. 44
Figure 10: Keycloak login. 45
Figure 11: Realm creation. 46
Figure 12:User creation. 46
Figure 13: Step 1/3: Keycloak login. 47
Figure 14: Step 2/3: Role addition. 48
Figure 15: Step 3/3: Roles added. 48
Figure 16: Data and events of predefined components (CSB Repository, CSB Dashboard/webserver, CSB REST API manager log, CSB Security component log, and others) will be collected by lightweight data shippers (namely Beats, such as Filebeat, MetricBeat, PacketBeat, Logstash), and then send them to ElasticSearch which centralises log data and transforms them for later proccessing. 53
Figure 17: Design mock-up: end-user's login requires also a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to be performed to protect RETENTION platform from spam and login-password repeated attemprs by bots. 68
Figure 18: Design mock-up: home page of a previously authenticated CSB end-user. 68
Figure 19: Design mock-up: CSB administrator views existing end-users and can create a new one. 69
Figure 20: Design mock-up: End-user creation form: CSB administrator fills nessesary profile information (fullname, email, and granded role) to trigger the creation. 69
Figure 21: Design mock-up: End-user edit form: CSB administrator may also alter end-user's profile information and reset his/her password. 69

Figure 22: Design mock-up: CSB Clinical Case Manager manages existing study participants (of the particular pilot) and may initiate the creation process. 70

Figure 23: Design mock-up: Create a study particiopant: CSB Clinical Case Manager fills in the nessesary information (fullname, birthday, home address details, phone), inserts an Gmail email account to be used for login to a Google account in order to download newer version(s) of RETENTION mobile application (if occur), along with reqruitment details and those to be conducted in case of an emergency. Upon triggering the creation, all 3 identifiers to be created, while the group (remote patient monitoring and interventions – RPMI, or remote patient monitoring and usual care - RPMUC group) is randomly selected. 70

Figure 24: Design mock-up: CSB Clinical Case Manager (or Help Desk Operator) may assign devices to a previously created study participant. 71

Figure 25: Design mock-up: CSB Clinical Case Manager (or Help Desk Operator) can monitor latest trasmitions per device type. 71

Figure 26: Design mock-up: CSB Clinical Case Manager (or Help Desk Operator) can view metadata of all device usage data trasmitions. 72

Figure 27: Design mock-up: CSB Clinical Case Manager can view and manage screenshots (photos of the Left Ventricular Assist Devices monitor) providing daily measurements (e.g., pump flow, pump speed, pulsatility index, pump power, alarrm) sent to the CSB by the study participant via a RETENTION mobile application mechanism. 72

Figure 28: Design mock-up: CSB Clinical Case Manager can view measuremet indicated by screenshots, review the correctness of the measurments values inputed by the study participant and (if nessesary) correct them. 73

List of Tables

Table 1. Security Component system requirements 17
Table 2. GDPR requirements and corresponding precaution 20
Table 3. RBAC vs. ABAC: Limitations/Cons to RETENTION 22
Table 4. End-user management: REST service definitions 30
Table 5. End-user management: My profile: REST service definitions 31
Table 6. Patient management: REST service definitions 34
Table 7. GDPR request management: REST service definitions 37

List of Abbreviations

Essential abbreviations used in the document:

(HL7) FHIR	Fast Healthcare Interoperability Resources
AAA	Authentication, Authorisation and Accounting
ABAC	Attribute-based Access Control
AES-256	Advanced Encryption Standard
API	Application programming interface
CIA	Confidentiality – Integrity – Availability
CIG	Global Insights Cloud – GIC
CSB	Clinical Site Backend – CSB
cSPAP	RETENTION Continuous Security and Privacy Assurance Platform
EHR	Electronic health record
GDPR	General Data Protection Regulation
HF	Heart Failure
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Identity	International Mobile Equipment
IETF	Internet Engineering Task Force
ISMS	Information security management system
JSON	JavaScript Object Notation
JWT	JSON Web Token
KCCQ	Kansas City Cardiomyopathy Questionnaire
LVAD	Left Ventricular Assist Device
MIT	IT-networks
ML	Machine Learning
MNA	Mini Nutritional Assessment
MOCA	Montreal Cognitive Assessment
NIST	National Institute of Standards and Technology
PD	Participant Devices
PE	Patient Edge

PETs	privacy measures and enhancing technologies
PHDs	Personal health devices
PHQ	Patient Health Questionnaire
PII	Personal Identifiable Information
PKI	Public key infrastructure
RBAC	Role-based Acess Control
REST (RESTfull)	REpresentational State Transfer
RPMI	remote patient monitoring and interventions group
RPMUC	remote patient monitoring and usual care group
RPO	Recovery Point Objective
SDK	Software development kit
SSH	Secure Shell
TLS	Transport Layer Security
TLS	Transport Layer Security
VAD	Ventricular assist device
VPN	Virtual Private Network

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 for the healthy and independent living of the study participants. As a technical prerequisite for this result, RETENTION will leverage big data analytics and learning capabilities, allowing for large scale analysis of the above-mentioned collected data, to generate the evidence required for making such decisions and in turn to trigger personalised interventions. Within this context, privacy-preserving and secure by design data handling mechanisms, covering data at rest, in processing, and in transit, will cover comprehensively all the components and connections utilised by the RETENTION platform (consisting of the following blocks: i) the Global Insights Cloud – GIC, ii) the Clinical Site Backend – CSB one instance for each pilot, iii) the Patient Edge (PE) and Participant Devices (PD) for each study participant.

The RETENTION Architecture that adheres to the "Privacy by Design" principle of the 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 centres in Germany, Greece, Italy 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 (Machine Learning models and their applicability) to be produced can be made available to RETENTION Pilots, can be applied to subsets or specific patients, and assist clinicians in their activities. In this context, this deliverable covers the development, modelling, configuration, and execution of mechanisms to guarantee the security and privacy of data held in the RETENTION platform, with an emphasis on the mechanisms concerning the CSB, given that data collected and managed within this scope may lead to the identification of study participants. As such, the developed safeguards support the effective protection of them (e.g., pseudonymisation, limitation of access, encryption, data minimisation), while in parallel 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 assessments mechanism. All mechanisms are built on top of open-source software and have been selected to maximise the prevention of possible security and privacy incidents. Initially, we provide the platform security and privacy requirements, and afterwards descriptions of its functionality. Lastly, we provide a roadmap of the integration of the mechanisms and processes needed to guarantee the security (confidentiality, integrity and availability) of all RETENTION assets via the RETENTION Continuous Security and Privacy Assurance Platform.

2 About this Document

The aim of the RETENTION project is to integrate heterogeneous sensors, assistive medical and mobile devices to enable the continuous data collection from the everyday life of the RETENTION study participants (Heart Failure patients), which will be analysed to obtain the evidence needed to offer personalised interventions promoting their healthy and independent living. Privacy-preserving and secure by design data handling mechanisms, covering data at rest, in processing, and in transit, will cover comprehensively all the components and connections utilised by the RETENTION platform.

2.1 Role of deliverable

Task 6.5 is associated with designing and developing of mechanisms to ensure the security and privacy of the data held in the RETENTION platform (i.e., CSB instances, GIC, PE) and the integrity of the platform itself. The security properties focus on the integrity, confidentiality and availability of data at rest, in transit and in processing for data flows (KPI-3.1, KPI-3.2) acquired by the interactions with external (m)IoT devices, home sensors and RETENTION services (deployed within CSB, GIC and PE). Thus, by definition, the implemented mechanisms that handle data acquired (i.e., medical records, devices/sensors usage, questionaries) and data generated (i.e., descriptive analytics, ML models, interventions) comply with the privacy and security-by design principles, 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 GDPR, data minimisation, pseudonymisation, transparency in processing of personal data, and other appropriate technical and organisational measures have been considered at early stage of the platform design to ensure that privacy and security requirements are met.

This deliverable covers the fundamentals, the development, the modelling, the configuration, and execution of mechanisms to guarantee the security and privacy of data held in the RETENTION platform. These mechanisms are built on top of open-source software and have been selected to maximize the prevention of possible security and privacy incidents. In conformance to the legal framework for privacy (General Data Protection Regulation - GDPR), it elaborates on how those data will be curated in order to preserve the privacy of individuals participating in the RETENTION study and reused (anonymised) in the context of research activities even beyond this project's lifecycle.

2.2 Relationship to other RETENTION deliverables

Privacy-preserving and secure by design data handling mechanisms, covering data at rest, in processing, and in transit, will cover comprehensively all the components and connections utilised by the RETENTION platform. This deliverable relates to end-user requirements analysis and outcomes (presented in D3.1), and the arcitectute of the RETENTION solution (in D3.2) and covers the development, modelling, configuration, and execution of mechanisms to guarantee the security and privacy of all data generetad, held and managed.

The mechanisms supported by the Security Component (i.e., data minimisation, authentication, pseudonymisation, API management, end-users management, devices management, Ids management, patiens management, GDPP requests management) protect the transmission of any (sensitive or not) data utilised in the context of all components (presented in D4.2, D5.1, D.6.1 and others), and provides evidence for assessing the project's workings regarding compliance with

research ethics principles and corresponding legal obligations, as enunciated by the European Commission (EC) (defined in D1.2 and in D10.2).

2.3 Structure of the document

This document presents the first version of the mechanisms that safeguard the security and privacy posture of the RETENTION platform and describes: i) fundemental blocks of the Security Component, and provides more details on the privacy and security provisions in accordance to the Privacy by Design principle and in consideration of the tentative list of user requirements (defined in D3.1) and new ones (e.g., micro-adjustments and improvements) requested by clinicians (during the 3rd PCC meeting in Madrid, May 12-13, 2022), including core mechanisms for preserving the anonymity of the data; and ii) how monitoring of CSB instances and GIC will be performed.

3 RETENTION Security Component

To support the aim of the RETENTION, the technical solution (including the CSB, the GIC and the PE) as a prerequisite must support the integration of heterogeneous (m)IoT devices and home sensors, later to enable the continuous data collection from the study participants operate them, and to analyse the collected data using novel data analytics' technologies. Within such context, the Security Component, that resides in both CSB instances and GIC, supports: a) the monitoring the security of all operations, preserving the privacy, and providing the data subjects and b) the 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 and privacy mechanisms implemented, to fulfil the user requirements (defined in D3.1).

3.1 Introduction

In order to support the aim of the RETENTION, the technical solution (RETENTION platform consists of five CSB instances responsible for managing raw data of Heart failure (HF) study participants for each of the five hospital, and the GIC that supports the management of ML analytics and the decision-making capacity) will support the integration of heterogeneous sensors, medical and mobile devices (PE consists of the RETENTION application and the Home Gateway), later on to enable the continuous data collection from the everyday life of HF study participants outside hospitals, and to analyse the collected data using novel data analytics and artificial intelligence technologies, while preserving the privacy and providing the data subjects with the control of knowing who and how their data are been 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 presents the fundamentals of the Security Component (a component that resides with some variations in both CSB and CIC) and encompasses the security and privacy mechanisms supported.

3.2 Prerequisites and Building Blocks

Protection of personal data is a critical issue, and particularly within the context of this project, where management of three (3) categories of data (A , B, and C as defined bellow) will take place (during the clinical pilot sites of the RETENTION study):

- Category A: Personal private data and personal identifiers: full name, date of birth, home address, phone number, and associated identifiers;
- Category B: Sensitive private data: personal health record (demographics, baseline medical history, medications, clinical data, labs exams, VAD measurements), questionaries scores (of the Mini Nutritional Assessment – MNA, the Montreal Cognitive Assessment – MOCA, the Kansas City Cardiomyopathy Questionnaire - KCCQ, the Patient Health Questionnaire - PHQ-9, and the Caregiver Burden Questionnaire for Heart Failure - CBQ-HF ver. 1), and devices/sensors usage measurements (i.e., blood pressure, heart rate, deep/light sleep time, sleep interruptions, weight, peripheral capillary oxygen saturation, steps (distance), calories, body temperature, heart rate variability, resting heart rate, arrhythmia alarms);
- Category C: aggregations (descriptive analytics), ML structures (models and analytics).

To support the secure management and transferring of such information without compromising the privacy the privacy of the data-subjects, the RETENTION platform introduces secure ways to handle, distribute, and show information, to the correct set of 'eyes' (i.e., CSB and GIC end-users with appropriate access rights based on Role-based Acess Control - RBAC), without compromising usability or speed. Particular attention was given to some elements of these data (Category A), information which can identify a single individual. Those data will be 'hidden' and protected as much as possible, and even at the event of security leak the design of the system (RETENTION architecture presented in D3.2, and depicted in Figure 1) such a way that any correlation of the data to identify an individual requires the cooperation of several technical participants with different access levels. As can be noticed from the submission of the architecture deliverable to the present status, there have not been any notable updates on the logic architecture of the RETENTION platform, thus confirming the maturity of the construction.

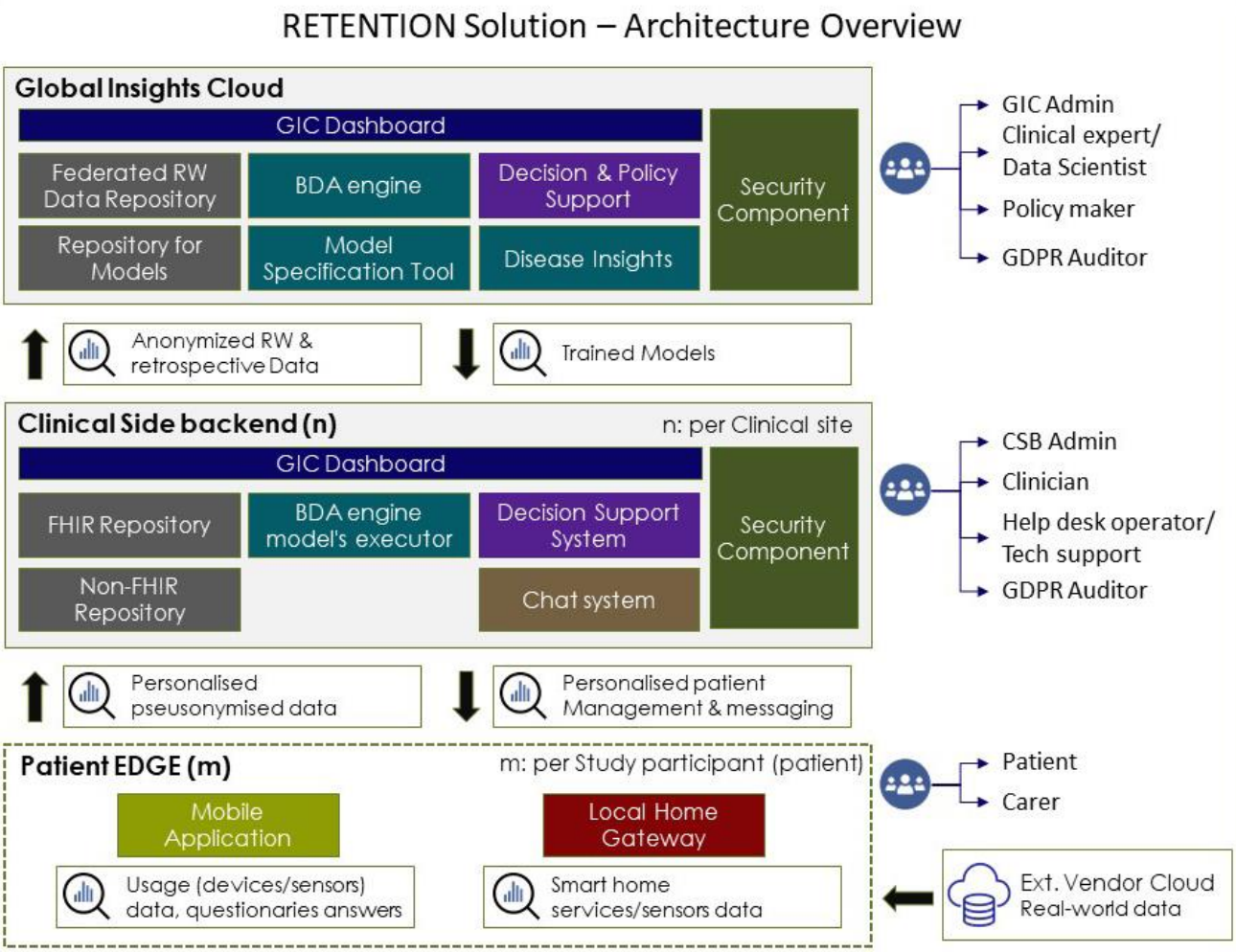

Figure 1: RETENTION platform logic architecture overview.

As a fundamental requirement, the platform was designed in such a way that the full length of the collected or produced Big data (i.e., usage data, medical data, resulted analytics and interventions) should be kept in a fully anonymised fashion, while a small subset consisting of IDs and Personal Identifiable Information (PII) as far as it concerns participants and login-profile information of the CSB and GIC end-users, to be stored with high security safeguards (i.e., encrypted, logged and

limited access to specific role(s)). In this respect, CSB@SecurityComponent allows via configurable rules (RBAC) RESTful application programming interface (API) access to records of Ids associations, to ensure that RETENTION organisational measures are in place to comply with the GDPR.

3.2.1 OAuth 2.0

OAuth 2.0[1] is a widely adopted protocol for authorisation. This specification and its extensions are being developed within the IETF OAuth Working Group[2]. The OAuth 2.0 authorisation framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. OAuth 2 is an authorization framework that enables applications (such as Facebook[3], GitHub[4], and Basecamp[5]) to obtain limited access to user accounts on an HTTP service. The OAuth 2.0 authorisation framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

In OAuth2 jargon there are four (4) different roles specified:

1. Resource owner: An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end-user.
2. Resource server: The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.
3. Client: An application making protected resource requests on behalf of the resource owner and with its authorisation.
4. Authorisation server: The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorisation.

Moreover, it should also be mentioned that OAuth 2 defines 4 different Authorisation Grants as well as an extensibility mechanism for defining additional types which is out of scope of this deliverable. An authorisation grant is a credential representing the resource owner's authorisation (to access its protected resources) used by the client to obtain an access token:

- authorisation code: The authorisation code is obtained by using an authorisation server as an intermediary between the client and resource owner. Instead of requesting authorisation directly from the resource owner, the client directs the resource owner to an authorisation server which in turn directs the resource owner back to the client with the authorisation code;

[1] OAuth 2.0 is the industry-standard protocol for authorization: https://oauth.net/2/

[2] OAuth -- OAUTH WG: https://www.ietf.org/proceedings/82/slides/oauth-0.pdf

[3] Facebook online social media and social networking service: https://en.wikipedia.org/wiki/Facebook

[4] GitHub Inc. Internet hosting service for software development and version control: https://en.wikipedia.org/wiki/GitHub

[5] Basecamp web-based project management tool: https://basecamp.com/

- implicit: In the implicit flow, instead of issuing the client an authorisation code, the client is issued an access token directly. The grant type is implicit, as no intermediate credentials (such as an authorisation code) are issued (and later used to obtain an access token).
- resource owner password credentials: The resource owner password credentials (i.e., username and password) can be used directly as an authorisation grant to obtain an access token;
- client credentials: The client credentials (or other forms of client authentication) can be used as an authorisation grant when the authorisation scope is limited to the protected resources under the control of the client, or to protected resources previously arranged with the authorisation server;

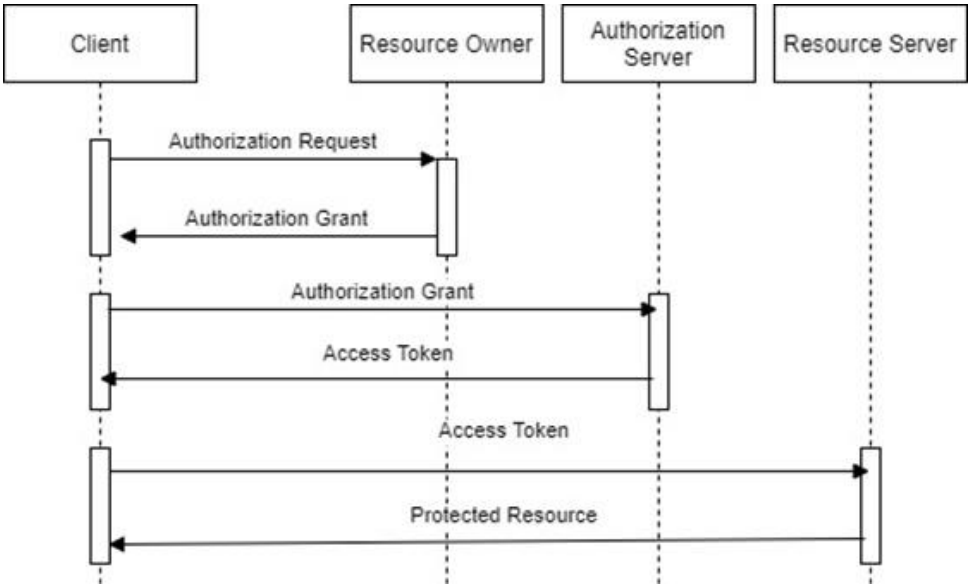

Figure 2: OAuth 2 flow.

An abstract OAuth2 flow is depicted in **Error! Reference source not found.**. This flow describes the nteraction between the four (4) different roles and includes the following six (6) steps:

1. The client requests authorisation from the resource owner.
2. The client receives an authorisation grant, which is a credential representing the resource owner's authorisation, expressed using one of the four authorisation grant types.
3. The client requests an access token by authenticating with the authorisation server and presenting the authorisation grant.
4. The authorisation server authenticates the client and validates the authorisation grant, and if valid, issues an access token.
5. The client requests the protected resource from the resource server and authenticates by presenting the access token.
6. The resource server validates the access token, and if valid, serves the request.

3.2.2 OpenID Connect

The OAuth 2.0 Framework describes overarching patterns for granting authorisation but does not define how to perform authentication. OpenID Connect[6] is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It uses straightforward REST/JSON message flows. OpenID Connect lets developers authenticate their users across websites and apps without having to own and manage password files. OpenID Connect allows for clients of all types, including browser-based JavaScript and native mobile apps, to launch sign-in flows and receive verifiable assertions about the identity of signed-in users. OpenID Connect uses the ID token data structure that enable end-users to be authenticated. The ID token has a JSON Web Token (JWT) format, which is a standard way to generate authentication tokens. The JWT contains various user information which are called claims. Also, it contains information about the validity of the token, such as issue datetime, expiry period etc. The token is normally signed by the token issuer with the issuer's public key to be easily verified using Public key infrastructure (PKI). So, in the context of RETENTION, OpenID connect will be used.

3.2.3 API Manager

The API management of CSB and GIC is accomplished through a combination of two (2) open-source tools to support provisioning, securing, and maintainiwith ng REST APIs. The Keycloak integration with KrakenD was selected since it allows one of the many possible OpenID Connect different security options available in KrakenD, and relies internally on the JWT validation component. JWT are an open standard (RFC 7519) that define a way for securely transmitting information between parties. JWT tokens are compact, secure (digitally signed), and have become an industry-standard used at internet scale. KrakenD supports any system using this open standard, including Keycloak.

Considering also that the RETENTION endpoints are been triggered by both end-users (machine-to-human) and devices (machine-to-machine), the following workflow (Figure 3) is the same.

Figure 3: Upon a Access token is been issued by Keycloak issuing, KrakenD allows the triggering of an end-point assuming that role policy permits this.

[6] OpenID Connect 1.0: https://openid.net/connect/

Having this setup:

- End-Users use their applications to log in to Keycloak who provides an access token for the session.
- Machine-to-machine communication also uses a token from Keycloak after providing a client_id and a client_secret.
- With the token generated by Keycloak, the client passes it to KrakenD in each request inside an HTTP header or cookie
- KrakenD authorises or not the usage of the specific endpoint according to the rules you have configured.
- As KrakenD can validate the Keycloak signature by itself, it does not need to call the Keycloak server to validate the token every time. Instead, KrakenD queries Keycloak every 15 minutes (configurable) to ensure the key has not rotated.

3.2.4 Hardware and Software requirements for the Security Component

The RETENTION project is motivated by the need for personal data management and services that comply with the GDPR, which has already been imprinted during the requirements stage (presents in D3.1). Furthermore, appropriate organisational measures and procedures have been provisioned by all RETENTION partners involved in any kind of personal data processing activity, to ensure full compliance with the GDPR. Specific details on addressing GDPR compliance issues within the RETENTION study were provided (in D1.2 POPD - Requirement No. 2) in accordance with the respective post-grant requirements, as well as in the Data Management Plan (in D2.2). The system requirements mentioned below (in Table 1) are requirements to run the CSB@SecurityComponent and the GIC @SecurityComponent.

Table 1. Security Component system requirements

	Component	Requirement
Hardware	RAM	The minimum RAM proposed is 4GB
	CPU	the recommended number of cores is 2
	Hard disk	20 GB of storage is sufficient
Software	Operating system	It is recommended to run the installation on a Linux operating system
	Keycloak, KrakenD, Patient Manager, SC Database	The deployment of SB@SecurityComponent is based on a Docker compose file for easier deployment and management. The official website of Docker[7] provides detailed installation instructions. Docker is used to create the components that are needed to run, and thus all dependencies are included in each component's container.

[7] Docker docs: https://docs.docker.com/

	Component	Requirement
		The entire suite of the Security Component is lightweight, and thus Docker's minimum requirements of 4GB RAM and a 64-bit kernel are sufficient for running it.
	API manager	Keycloak: Java 8 JDK, at least 512M of RAM, and at least 1GB of diskspace
	Connectivity	A stable internet connection is required in the initial deployment, since the docker-compose needs to download software from global repositories

End-users management API specification (Administrator's functionality) is provided by Keycloak (Admin REST API), available online at: https://www.keycloak.org/docs-api/15.0/rest-api/index.html

End-users management API specification (End-user's functionality) is provided by Keycloak (Admin REST API), available online at: https://www.keycloak.org/docs-api/15.0/rest-api/index.html#_users_resource

The complete list of REST APIs supported is provided in Annex 8.1.

3.3 Adhering to Privacy by Design Principles in the context of RETENTION

According to several organisations and authorities responsible for the monitoring of GDPR (e.g., [UK ICO, 2018]), the notion of "data protection by design and default", which GDPR legislation (Art. 25) leaves somehow open to which exact protective technical measures are to be taken, is all about embedding processes and safeguards during early design stages of a project along with the lifecycle of the relevant data process data protection throughout all your processing operations. Basically, it ideally entails to design an information system in such a way that personal data do not need protection (since all operations involved, they have no security gaps or privacy loopholes). In addition to those, those human responsible for operating them have also in place organisational precautions that in tandem strengthen the protection to such an extent that it makes it practically impenetrable.

Considering the overall scope (i.e., nature, purpose, and context of the data processing activities and their implications) of a platform that collects personal information about study participants, as well as medical information and health-related measurements associated with them, the RETENTION platform was designed in such a way that the major part of the collected or produced data (i.e., devices/sensors usage data, medical data, resulted analytics and interventions) will be kept in a practically fully anonymised fashion, while a small subset consisting of personal data, identifiers and Personal Identifiable Information (PII) as far as it concerns study participants (and secondarily login-profile information of the CSB and GIC dashboard end-users), are stored with high security safeguards (i.e., encrypted, in a separated repository, logged and providing limited access to specific role(s)). Taking into consideration the essence of the RETENTION user requirements analysis (defined in D3.1) that presuppose the use of some type of identifiers for supporting the association of a study participant collected information and (later on) results of ML prognosis, which

requires bidirectional communications, adopting pseudonymisation is a one-way road. Down this road, additional technical measures such as utilising state-of-the-art authentication protocols and a policy-based access control, deploying cryptographic channels for communications between clients and services such as the latest Transport Layer Security 1.2 (TLS1.2), as well as the Secure Shell (SSH) protocols, applying basic encryption in databases (focusing on those storing personal data makes the difference is whose privacy is being sought [ENISA, 2014].

Data accuracy, integrity and confidentiality 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. In addition, to abide by the GDPR's principle of accountability, a specific mechanism (GDPR requests management) supports the collection and management of privacy-related requests, handled by System Administrators for processing. Study participants may issue a request via the mobile application (alternatively via the CSB@Dashboard by the Clinical Care Manager on their behalf) and receive appropriate answer. A GDPR Auditor may track the progress of the request and see who is currently working on it.

Figure 4: Aspects of the "Privacy by Design" principle of GDPR

In parallel to the integration of appropriate mechanisms for securing the platform's operations (precautions mechanisms to be developed in Table 2), adherence to the "Privacy by Design" entails the operation of continuous monitoring mechanisms and processes to guarantee the security (confidentiality, integrity and availability) of all RETENTION assets and the security and privacy of all data being aggregated, generated and processed by the platform in all forms (at rest, in transit, and in processing) increases overall protection and immediacy in responding to any potential cybersecurity risks. To this extend, the RETENTION Continuous Security and Privacy Assurance Platform (cSPAP) is scheduled to perform monitoring at CSB instances and the GIC. The cSPAP is a model driven platform that can make hybrid security and privacy assessments that involve threat and vulnerability analysis, static analysis, penetration testing and continuous runtime monitoring, to provide a comprehensive analysis of the security and privacy posture of a system.

Table 2. GDPR requirements and corresponding precaution

GDPR requirement	Precaution
Security	Devices and sensors MAY collect data using non-permanent buffer or addressing privacy and security if permanent
Security Local de-identification and anonymisation	Devices and sensors transmission SHOULD be protected by state-of-the-art security and privacy technologies and methods (e.g., secure channels, token-based access, validation of pseudo-Id1 and smartphone's IMEI)
Security	Devices and sensors transmission WILL be low range to avoid enlarging the attack surface
Authentication/Authorisation	Devices and sensors MUST transmit to authorized/authenticated recipients only
Security	Recipients of devices and sensors transmission MUST keep the data received and data further elaborated as confidential (e.g., pseudonymisation)
Security Aggregation of data	Behavioural and environmental data SHOULD treat confidentially
Authentication/Authorisation	Systems holding personal data MUST provide authentication mechanism ensuring access by authorised person only (e.g., protected repository)
Aggregation of data Local de-identification and anonymisation	The privacy and security of structured data MUST be kept in all circumstances
Authentication Authorisation	Access to structured data MUST allowed only to authorized persons (e.g., RBAC)
Security	Personal data SHOULD not be saved locally in a permanent buffer (e.g., encrypted in separated repository)
Authentication/Authorisation	Web interface MUST provide Authentication, subject to Authorisation policy (e.g., RBAC)
Security Monitoring data access Accountability	Logging features MUST be protected (e.g., introduce logging mechanisms, security assessments)
Minimize personal data Aggregation of data	Stored data SHOULD be limited to those needed by analytics (e.g., pseudonymisation)
Monitoring data access	platform as a whole MAY adopt continuous compliance monitoring approach access supporting auditability. Automated regular checking of the accuracy of data, including updating, is an absolute necessity because of the potential damage which might be caused to the patient heath if data were to remain inaccurate

GDPR requirement	Precaution
Data breach	If a personal data breach occurs, Data controllers shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of stroke survivors. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification of a personal data breach to the supervisory authority shall at least: describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the personal data breach; describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. When the personal data breach is likely to result in a high risk to the rights of a participant, the controller will communicate the personal data breach to the data subject without undue delay, describing in clear and plain language the nature of the personal data breach.
Fail-safe setup	All the data of the pilot sites will be stored and served from a single location (CSB intance). Start times and completion times for all regular backups to defined on evening/weekend timeperiods (outside of Pilots production schedules), while incrementan backup to occur on daily basis. The schedule includes all data backup activities and include testing activities as needed. Restore files that are accidentally deleted. It's happened to all of us at some time and it helps to have a safety net in case work files or other critical data are erased. Recovery Point Objective (RPO) is: 1 day Same scheduling as for the GIC.

3.3.1 Choosing an appropriate Policy-Based Access Control

In terms of data minimisation, some well-define technical implementations for organising sets of permissions are available. Authentication and authorisation present the basic logic of how an end-user can login into the system, as well as on how we can get the user info, but also define an access control mechanism of how we apply this information (Policy-based Access Control). The Attribute-

based Access Control (ABAC), and the Role-based Access Control (RBAC), (along with some variations of theirs e.g., Purpose-based Access Control) were the one considered for the RETENTION platform, since not only end-uses (via dashboards) are the ones triggering services but also machines (m2m connectivity between CSB and smartphones/Raspberry Pi, or between GIC and CSB instances). A brief introduction for those considered is the following (detailed definitions provided by NIST ([NIST, 2016] and [NIST, 2014]):

- Attribute Based Access Control (ABAC): A logical access control methodology where authorisation to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes, which creates is a dynamic matrix to which policies can be determined and applied:
    - Attributes are characteristics that define specific aspects of the subject, object, environment conditions, metadata in the system, and/or requested actions that are predefined and preassigned by an authority;
    - A subject is an active entity (generally an individual, process, or device) that causes information to flow among objects or changes the system state;
    - An object is a passive information system-related entity containing or receiving information;
    - An operation is the execution of a function at the request of a subject upon an object;
    - Policy is the representation of rules or relationships that define the set of allowable operations a subject may perform upon an object in permitted environment conditions.
- 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 (in comparison to ABAC) because of its simplicity and manageability instead of assigning each end-user permissions. Based on their requirements, end-users are grouped and then each group is assigned a role. Afterward, each user is assigned on or more roles and each role is assigned with one or more permissions. This method of access control has system administrators assign roles to end-users as they are added to the system. Consequently, roles need to be predetermined within the system in order to be applied by administrator who in turn are then able to create policies that make access decisions based on the roles that are connected to each user. Benefits of RBAC:
    - create 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.

Table 3. RBAC vs. ABAC: Limitations/Cons to RETENTION

RBAC	ABAC
Widely adopted and allows small- to medium-sized projects to eliminate implementing access controls on an individual basis - manual role creation (small number or roles, reasonable number of endpoints)	Complex roles can be defined and applied (not applicable to RETENTION)
Static approach: All policy must be predetermined (compatible with RETENTION requirements) - Can't set up a rule using parameters that are unknown to the system and cannot scale (not applicable to RETENTION)	Multidimensional approach: can leverage multiple dimensions of data attributes to determine whether to grant or deny data access - more work to establish but easier to scale (not applicable to RETENTION)
As basic, easy to establish and assign in the particular case of limited set of end-user roles - Easy to establish roles and permissions and manageable (technical personnel of clinical partners to uptake CSB administrative duties, Role explosion is not anticipated)	Requires more processing power, time- and labour-intensive up-front work and technical knowledge of the technical personnel to undertake this role - Assignment of a business rule of any complexity can be done but with high cost

Based on the above comparison, and since RBAC is considered simpler to implement, less prone to administrative errors and suited RETENTION needs, it is decided this access control model to be implemented (end-user roles supported were defined in section 3.1 "RETENTION actors" of D3.2). Via the Security Component access of each end-user on REST permitted to be triggered by the specific role is appointed to. In that sense, CSB end-users of each pilot site will be able to have access to pseudonymised data (i.e., clinicals the full set, while help desk operators only to devices pairing records and transmissions metadata), while GIC end-user are able to manage anonymised data (in the context of ML pipelines). In the context of the supported operations:

- CSB (and GIC) system administrators are registering and managing end-users and performing actions such as system monitoring, services health checks and responding to GDPR requests.
- CSB Clinicians have access only to relevant views of the CSB@Dashboard that relate to the pseudonymised medical history of study participants they monitor, while they can view resulted general and personalised analytics, apply available ML predictive models and trigger personalised interventions.
- CSB Help Desk Operators (Technicians) of each CSB are supporting the specific pilot by managing the paired devices/sensors and monitoring their inactivity periods (that might trigger communicating to an individual without knowing the real identity).
- Study participant (associated to a pilot) refers to the HF patient that gave consent to participate to the RETENTION study (RETENTION study participant), who interacts via the RETENTION Mobile application via secure transmission channels to transmit devices measurements and sensors data. Half of those (remote patient monitoring and interventions group - RPMI) are also able to acquire guidance or information about the treatment and the trajectory of personalised care plans (while those of remote patient monitoring and usual care group - RPMUC), will not receive those.

- Carer (Caregiver) it refers to health professional (family caregiver, a respite caregiver, a home caregiver, or a primary caregiver) who provides care for the patient who needs extra help and utilises the RETENTION application on his/her behalf.
- GIC Data Scientist refers to a professional responsible for collecting, analysing, and interpreting the overall amount of data collected by the GIC. For that purpose, he/she utilises open-source tools (i.e., Jupyter Notebook[8], ML Flow[9]) via a VPN access to compile ML pipelines.
- GIC Healthcare policy maker 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.
- CSB Auditor refers to the role that is responsible for administering privacy-related audits to the RETENTION platform (by monitoring responses of GDPR requests and security and privacy assessments results performed by the RETENTION Continuous Security and Privacy Assurance Platform).

Study participants IDs associations records (elaborated in detailed in the following section) can be used by semi-automated processes in accordance with GDPR rights, and with the involvement of responsible-for-monitoring clinicians under specific conditions (e.g., medical protocol, GDRP rights, privacy audits), and as study participants identification is accessible only to this end-user role. Access to those -necessary data for RETENTION research activities only- data is limited via RBAC, and in relation to the purposes of the RETENTION clinical study and not further processed in a manner that is incompatible with those purposes (data types, frequency of data collection, provisions on access limitation and other processing details defined in the RETENTION clinical protocol D8.2). Secondary to the clinical study end-user roles (such as help desk operators, GDPR auditors, policy makers, data analysts) have limited access depended on specific needs related to the respective role and only to processing operations on pseudoanonymised of anomimised data.

3.3.2 RETENTION Pseudonymisation

In particular for the pseudonymisation, ENISA [ENISA, 2018] provides a technical definition which entails “the process of de-associating a data subject's identity from the personal data being processed for that data subject”. Pseudonymisation is defined in detail in (GDPR art. 4(5), 2016) as:

> *“pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;’.*

In practice, the pseudonymisation process ensures that a record after-the-fact can no longer be attributed to a specific data subject, without having previously been associated with additional

[8] https://jupyter.org/

[9] https://mlflow.org/

information. Consequently, as long as this additional key information (i.e., a subset of the data) that may lead to subject's identification is kept separately, and its usage is subject to technical and organisational measures, the original data set cannot lead to subject's identification by any means (provided for instance that one has previously removed all direct identifiers and other not essential indirect identifiers with high disclosure risk, or unusual unique characteristics have been merged into data groups). Still this small critical dataset, is the one that allows Data Controllers to meet specific GDPR obligations. Subsequently, its existence (during project's lifecycle) allows the exercise of all GDPR Individual rights (such as subject's request as to who viewed his/her pseudonymised data aka 'Right to be informed') or the Data controller's obligation to keep records, while its absence will convert all RETENTION big data collected and produced to a fully anomimised dataset and as such it can be used under specific conditions ('appropriate safeguards') even beyond the duration of the RETENTION project ('storage limitation'). Notably, privacy audits to be conducted will assert these claims (via the use of the RETENTION Continuous Security and Privacy Assurance Platform).

As stated, the Security Component which resides in both CSB and GIC, is a component which provides mechanisms and services to secure communication between all platform's components (intranet), to allow access based on a policy (as aforementioned in previous section), equally importantly to perform pseudonymisation by altering identifiers (associated to study participants and devices they are utilising) and filtering out PII, to validate usage records based on specific requirements (i.e., valid pseudo-id1 and IMEI pair), to allow access to endpoints provided by CSB instances and GIC, and to log activities when required (e.g., for security assessments, for GDPR related audits/assessments). As such, is used to perform data pseudonymisation and deidentification by switching back and forth the identifiers associated with every study participant.

Having the 1st version of the RETENTION platform operating in a production environment (five CSB instances, one GIC instance) and the functionality in place to support the initial data collection and monitoring of the five pilots planned, considering the aforementioned data categories. During their first, baseline appointment with RETENTION Clinicians team of the specific pilot, and after having signed the Informed Consent Form (ICF), they will have a complete medical history examination. By then, a record is created containing his/her personal and medical data (via the CSB@Dashboard), while the system associates the study participant to three unique RETENTION pseudo identifiers (pseudo-Id1, pseudo-Id2, and pseudo-Id3 utilised in various stages), used in various tasks (e.g., pseudo-Id1 for usage data transmission from RETENTION Mobile application – Edge App to the CSB). The data from this initial visit will be collected creating an individualised profile, while (in the background) access to them will be logged (providing evidence for GDPR-related audits). Upon the completion of setting up and configuration of appropriate (based on the 3 types of patients supported: patients with HF not enlisted for transplant at the time of their recruitment, patients with Left Ventricular Assist Device (LVAD), and heart transplant recipients) wearable devices and sensors, the data collection process begins. The raw usage data eventually will be resided in CSB@Repository (2 types: FHIR and nonFHIR), while to support the production of ML analytics (the ML pipeline is supported by tools been operated withing the context of the GIC) big usage data and medica will be transferred to the GIC after having previously undergone a transformation of the pseudo identifiers to preserve the anonymity. The following image (Figure 5) illustrates this process. In a nutshell:

- GIC: data stored and utilised for analytics in the context of the GIC will be irreversibly anonymised;

- CSB: personal data and PIIs will be stored encrypted in a separate repository (Security Component). Those can be used as input to various activities, still never shared publicly;
- The anonymised and the pseusonymised raw/aggregated data can be used for analysis in publications.

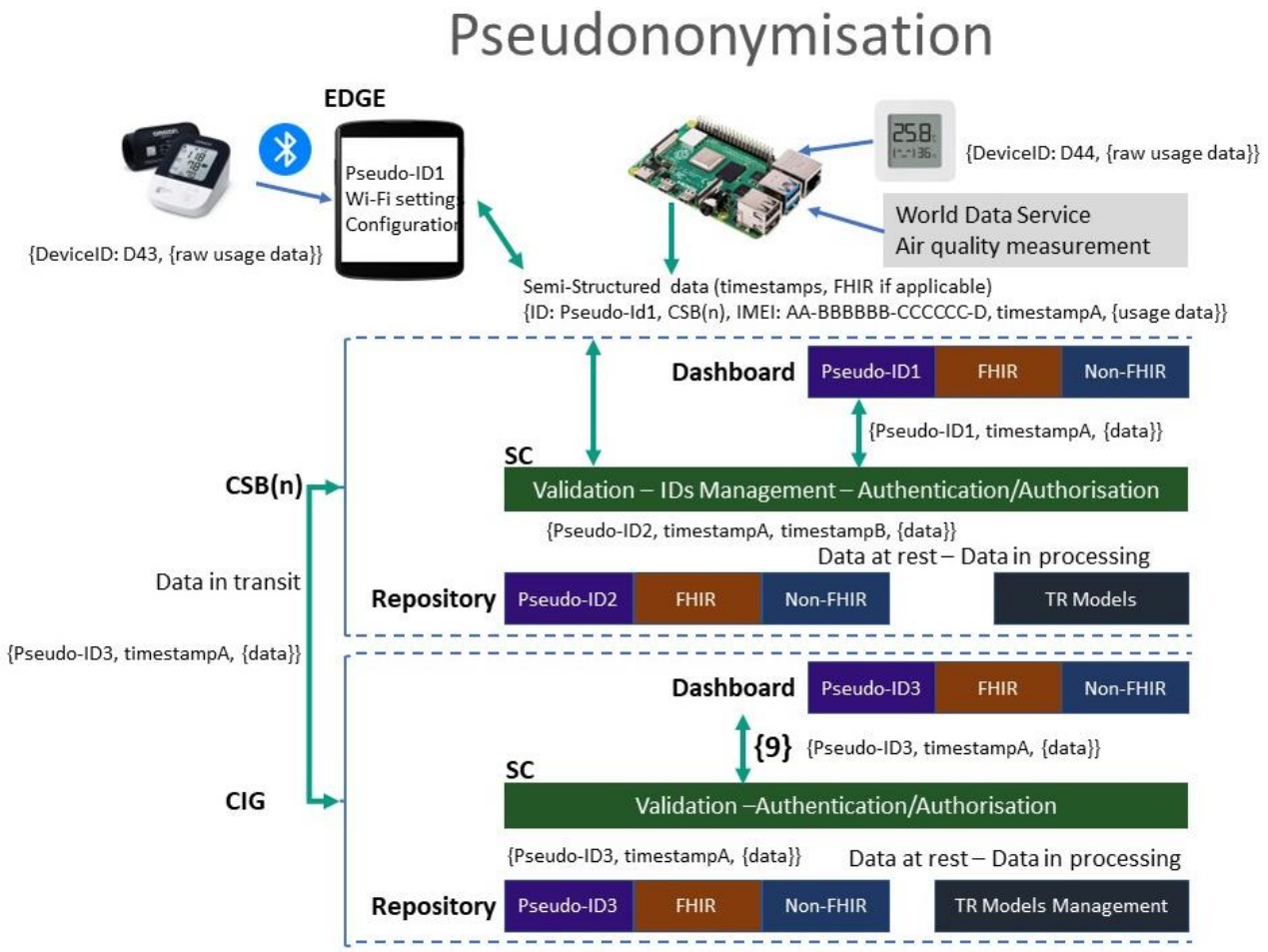

Figure 5: The CSB@SecurityComponent replaces Pseudo-Id1 to Pseudo-Id2 by which pseudonymised data record is stored in CSB@Repository and vice versa. In a similar way, CSB@SecurityComponent replaces Pseudo-Id1 to Pseudo-Id3 by which pseudonymised data record is stored in GIC@Repository.

3.3.2.1 Ids management

- For data arriving from RETENTION Application or Home Gateway, records contain a non-identifiable External pseudo Id (pseudo-Id1) associated with a unique study participant, as well as potential PII (e.g., device identifiers). Those Ids will be replaced to a CSB-generated Id (Pseudo-Id2), while PIIs will be removed.
- The association of this identifier (Pseudo-id1) with study participant's real identity is known only to CSB clinicians. This Id (Pseudo-Id1) utilised for associating and pairing all (m)Iot devices and sensors handed over to each individual, while all analyses are utilising different ones (pseudo-Id2 or pseudo-id3), with the correlation record been stored encrypted within the CSB@SecurityComponent. The way the Id stored in smartphone's 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.

- Similarly, micro-aggregated sensors data transmitted via the Home Gateway or world data from External Vendor's cloud are also associated on creation with the same Pseudo-Id1, later to be replaced via the SB@SecurityComponent mechanism.
- The Pseudo-Id1 that provided by the CSB@SecurityComponent is used to configure all devices/sensors. Whenever the CSB receives data through the RETENTION application or the Home Gateway it will not store the data (in the CSB@Repository) under Pseudo-Id1. Instead, it will first replace Pseudo-Id1 with Pseudo-Id2, remove any identifiers contained and then it will store the relevant data record. Thus, the data in the SB@Repository will be pseudonymised at rest. Such Id replacement process is performed by the CSB@SecurityComponent during every REST trigger that transmits or retrieves data into/from the SB@Repository respectively.
- The way CSB handles usage data digestion support interoperability over (m)IoT devices, as long as those provide an open API (SDK) and connectivity via Bluetooth.

Notably, even if in the unlikely event of malicious access to both CSB@Repository and CSB@SecurityComponent is achieved, still will not be possible to reidentify study participants since data stored encrypted within the later, and consequently cannot correlate Pseudo-Ids.

3.3.2.2 API Gateway

A strong, dynamic and seamless Authentication, Authorisation and Accounting (AAA) mechanism is in place for the protection of all machine-2-machine and machine-2-human interactions involved. Security (i.e., confidentiality, integrity, and availability) of data at all states (i.e., at rest, in processing and in transit) will be provided, leveraging industry best practices and standardized mechanisms, along with the definition of a secure-out- of-the-box configuration for all deployed components. The aim will be to provide a trustworthy platform with accountability provisions, as this is not only a prerequisite for its wide adoption, but also mandatory from a regulatory, legal, and ethical perspective.

CSB and GIC endpoints are protected with Keycloak tokens, to allow single sign-on with Identity and Access Management. Keycloak[10] supports three different authentication protocols (namely - OpenID Connect, OAuth 2.0 and SAML 2.0), and also has full support for Single Sign-On and Single Sign-Out to secure the access to the REST API (Application Programming Interface). In the particular context of RETENTION, the OAuth 2.0 protocol is utilised via JWT, a JSON format scheme for the exchange of information between services in a secure way by allowing the client (i.e., CSB and GIC Dashboards, RETENTION application, Home Gateway) to send an authentication request to the server, and in turn a signed token is created and been sent to the client which, from that moment, uses it to authenticate subsequent requests. To trigger any of the available RESTful APIs (presented in Annex 8.1), the client needs to first obtain a secure token from Keycloak. Then, the component utilises the KrakenD API Gateway, which sits between the end-user's client and the backend services. To ensure access in an authorized manner, KrakenD directly communicates with Keycloak to verify the validity of the JWT contained in each API call's Authorisation Header. Upon verifying the signed token's validity, KrakenD then checks that the specific end-user for whom the JWT has

[10] https://www.keycloak.org/

been issued holds the necessary permissions, and only then proceeds with forwarding the request to the corresponding backend service.

Conclusively, in the context of RETENTION, pseudonymised data stored in the five CSB instances are subjected to different types of analysis, including statistical analysis techniques (e.g., descriptive statistics, statistical testing and inferencing), while complex Machine Learning techniques (e.g., prediction), to be performed in the context of GIC. Both CSB and GIC, by virtue of its design, support privacy. Personal data and PII stored encrypted in CSB@SecurityComponent and not be transferred to the GIC For stored data, PII for the subject of the data is masked or removed from it altogether. Regarding the type of personal information contained in transmitted data, there are three (3) different origins of data collected and associated types: a) data manually inputted by CSB clinicians, b) (m)IoT and sensors usage measurements and answers to questionaries and world data (associated to a study participant) transmitted via the RETENTION Application or the Home Gateway, and c) aggregated data or ML models composed and managed within the GIC. IDs management and Personal Identifiable Information removal techniques used were introduced in (Basdekis et al, 2019) and properly enhanced to meet RETENTION needs.

3.4 RETENTION Application and Home Gateway Secure Transmissions

Both the RETENTION Application and the Home Gateway act as a gateway concerning the usage data (devices/sensors measurements) flow from the various medical, wearable devices and home sensors integrated either through their SDK (Bluetooth connection) or via the direct API exposed by the device itself. These in turn store temporarily all collected usage data in their internal databases, and periodically transmit them to their corresponding hospital CSB via a secure channel. In addition to such precautions, the validity of the pair (pseudo-Id1 and smartphone's IMEI or Raspberry pi device identifier) it will be checked by a CSB@SecurityComponent mechanism for digestion of the transmitted data to be allowed. In this respect, data protection mechanisms are implemented to provide security both while data are flowing between these clients and the CSB (data in transit) as well as while usage data stay temporarily in the devices internal database (data at rest).

Data in transit is secured using the OAuth 2.0 protocol. By following the protocol, a unique cryptographic token is generated which identifies the user of the application and is then used to perform valid data transfers to the CSB through the REST API exposed by the CSB. If the token is not valid, the transaction cannot be not valid as well. For every transaction, a new key is generated. Each key has a specified time-to-live period, after which it expires and becomes useless. All keys generated and used by the application are logged. This ensures that no valid keys remain unused and all transactions between devices and the CSB can be traced by the keys used. For every transaction, the data transmitted is secured using the generated key, which creates a cryptographically secure hash of the data. The transaction happens over a secure channel established by the HTTPS protocol using Transport Layer Security (TLS) certificates which uniquely identify the servers used. If the secure channel is compromised, the contents of a message remain cryptographically secure and even if the key generator is compromised so that a message could be decrypted, the contents of the actual message are anonymized.

Concerning data at rest, symmetric key encryption, based on the Advanced Encryption Standard (AES-256) algorithm, is applied to all transmitted data. A cryptographic key is generated while it is installed and registered for the first time (RETENTION Application initial configuration). The cryptographic key is then stored in a keystore based on the Android Keystore system, which is an

embedded security feature that protects key material from unauthorized use by preventing extraction outside the application processes. Moreover, it enforces the restrictions imposed by the authorized uses outside of the application's processes. The authorized uses are specified when the key is generated, and authorizations cannot be changed afterwards. This way, the smartphone's application process is the only one that can access the cryptographic key, ensuring also that the key cannot be extracted from the smartphone at all. In any case, all data stored in the application's internal database are pseudo anonymized and are also transmitted as such, making the actual linking between any data to an identifiable user as hard as much as possible.

The proper management of the Android permission model highly affects the application's privacy. A privacy policy, that allows the client users to be adequately informed and consent for any type of personal data processed, is attached to the application. The main privacy design strategy followed is to minimize the personal data as much as possible.

Data transfers from the CSB are also encrypted under the HTTPS protocol. Communication over HTTPS are also applied whenever the CSB@Dashboard requests data, or whenever GIC retrieves or transmits data (e.g., anonymized data, ML models). As for the data transmitions occuring:

- Token-based access to RESTfull APIs allowing data transmission from/to the CSB. Each component will need to obtain a security token prior to the communication with any of the CSB or GIC components;
- Encrypted connections (HTTPS) will protect the contents of data in transit, as well as all RESTfull calls;
- Protected logging system for monitoring data access.

3.5 Security Component: Main functionality

The Security Component (in both CSB and GIC) provide interface (REST API endpoints) to be used by:

- CSB@SecurityComponent (instance)
  - CSB components (of specific instance)
  - RETENTION Mobile Application (of study participants associated with specific pilot/instance)
  - Local Home Gateway (of study participants associated with specific pilot/instance)
  - GIC (for transferring ML models)
- GIC@SecurityComponent
  - GIC components
  - CSB (for transferring anonymised data)

3.5.1 End-users' management

CSB and GIC end-users' management is supported by Keycloak[11], which provides a single sign on solution for web apps and RESTful web services. Security features that developers normally have to

[11] Keycloak: https://www.keycloak.org/

write for themselves are provided out of the box and are easily tailorable to the individual requirements of a specific project.

For each CSB instance a login page will allow access to previously registered by the CSB Administrator end-user. The authentication flow uses OpenId-Connect as provided by Keycloak.

To grand access to a production CSB instance or GIC, the following procedure will be applied:

- Each Pilot (hospital) to compile a list of individuals and associated supported-by-the-platform role(s) (full name, role, and email);
- Access is approved by Responsible for granting access (RGA) per CSB instance;
- Approved access list (and any future updates) forwarded by RGA to the CSB Administrator;
- Whenever a new registration happens, the Administrator compares the registration info of the registrant against those of this list (of the related organization) and acts accordingly.

The end-user management service allows the management of CSB@Dashboard and GIC@Dashboard end-user accounts. Access is not granted automatically, but via a moderation mechanism the CSB or the GIC Administrator creates an account and selected upon a predefined end-user role to gain access according to it. Administrator may assign a different role that the one originally requested (during the creation process), and as such different privileges and access to the services supported. In addition, an account can be temporary cancelled or suspended.

Following this, to login in a GIC instance or a GIC, an end-user will use the credentials provided by the CSB Administrator (or the GIC Administrator respectively). Upon first login will be required to modify the password. Via a login form, end-user will enter his/her credentials in order to access the GIC services. Upon this triggering, the REST authentication service communicates with the Security Component:

- to verify whether the end-user has an active account status, and if it does, whether the password he/she typed is correct or not:
    - if credentials used are the correct ones, a valid TOKEN is generated and used throughout the end-user's session until the web browser is closed or he/she chooses to log out;
    - in case of rejection: end-user will be notified that his/her login has been declined;
- Whenever a signed-in end-user wishes to exit, trigger of logout service will logout and make the access token deprecated.

Table 4. End-user management: REST service definitions

Method	Params	Response
Method: Get all		
GET	UserId	JSON records of all end-users containing UserId, fullname, organisation, role, and last update of account status
Method: Get		
GET	UserId	JSON record of specific end-user ID containing UserId, fullname, organisation, role, status, last update of

Method	Params	Response
		account status and associated action(s) (JSON: type, assigned to, status and timestamp)
Method: Edit		
POST	UserId, first name, last name, organisation, role, email and status	JSON record containing UserId, fullname, organisation, role, status, last update of account status and associated action (JSON: type, assigned to, status and timestamp)
Method: Create		
POST	UserId, type, and assigned to	JSON record containing UserId, fullname, organisation, role, status, last update of account status and associated action (JSON: type, assigned to, status and timestamp)
Method: Edit		
POST	UserId, type, assigned to, and status	JSON record containing UserId, fullname, organisation, role, status, last update of account status and associated action (JSON: type, assigned to, status and timestamp)

End-users management API specification (Administrator's functionality) is provided by Keycloak (Admin REST API), available online at: https://www.keycloak.org/docs-api/15.0/rest-api/index.html

End-users management API specification (End-user's functionality) is provided by Keycloak (Admin REST API), available online at: https://www.keycloak.org/docs-api/15.0/rest-api/index.html#_users_resource

3.5.1.1 End-user's profile

My Profile service enables registered end-users to manage their personal details and login credentials. The end-user can click on a link named by his/her first name to view and edit his/her profile information, with the option to edit those, or to alter the password.

Table 5. End-user management: My profile: REST service definitions

Method	Params	Response
Method: My profile		

Method	Params	Response
GET	UserId	JSON record of specific end-user ID containing UserId, fullname, organisation, role, status, last update of account status and associated action(s) (JSON: type, assigned to, status and timestamp)
Method: Edit		
POST	UserId, first name, last name, organisation, role, email and status	JSON record containing UserId, fullname, organisation, role, status, last update of account status and associated action (JSON: type, assigned to, status and timestamp)

End-users management API specification (End-user's functionality) is provided by Keycloak (Admin REST API), available online at: https://www.keycloak.org/docs-api/15.0/rest-api/index.html#_users_resource

3.5.2 Patients' management

CSB patients' (study participants) management is also supported by Keycloak[12]. According to the predefined clinical protocol (presented in D8.1) during first visit (i.e., baseline assessment), the study participant has previously signed the (paper-based) Informed Consent Form (ICF), the signature date of which later will be inserted during the creation process operated by a clinician.

The subset of the electronic health record (EHR) of each study participant that holds all personal information (Category A, in section 3.2) is stored and managed by the Security Component. During each creation, 3 different identifiers are generated:

1. pseudo-Id1 that CSB clinicians can view, in knowledge also to those responsible for associating devices and sensors. This identifier also used whenever usage data are transmitted to the CSB by the RETENTION Mobile application or the Home Gateway;
2. pseudo-Id2 is the second identifier replacing pseudo-Id1. Prior to storing the transmitted data to CSB Repository, pseudo-Id1 is replaced by pseudo-id2 and then are stored under the latter identifier (Figure 6). Hence, the end-users of the RETENTION platform and those able even for direct manipulation of the data stored in the repository have only access to the pseudo-id2 and there is no way for them to retrieve the pseudo-id1 (as this association

[12] Keycloak: https://www.keycloak.org/

record is stored encrypted with the repository of the Security Component, depicted in Figure 7). The relation between pseudo-id1 and pseudo-id2 is maintained in encrypted form separately from the patient data and were accessible only under special administrative access rights;

3. the pseudo-id3 is automatically assigned as well during the creation and is utilised whenever usage data from CSB instances are to be transmitted to the GIC for big data ML analysis.
4. During the study participant creation process, a random assignment is performed on how the particular participant will be assigned to either the remote patient monitoring and interventions group (RPMI group), or to the remote patient monitoring and usual care (RPMUC group) groups. The randomisation functionality divides the set of patients into two subgroups: a) RPMI, b) RPMUC. This is done at random, giving each patient a 50-50% probability of belonging to either group. However, some additional checks are in place. In particular:
    a. No more than three consecutive patients can be placed in the same subgroup. For example, if patient 1 is placed in the RPMI group, and then subsequent patients 2, 3, and 4 are placed in the RPMUC group, patient 5 cannot be placed in the RPMUC group again (as a hard constrain). With 100% probability, patient 5 to be placed in the RPMI group.
    b. For each pilot, the ratio of RPMI and RPMUC patients will be 1:1. To ensure this, the total number of patients that each pilot will have needs to be known beforehand. Then, the total number of patients in each subgroup is tracked. If at some point the current total number reaches 50% of the total number of patients, then henceforth all created patients will be placed in the other subgroup. For example, consider a pilot involving 20 HF patients. By chance, 10 out of the 15 first created HF patients registered by the platform belong to the RPMI subgroup. In this case, all subsequent HF patients will no longer be assigned to this group by chance. Instead, they will all be assigned to the RPMUC subgroup, so that in the end they have 10 HF patients each.

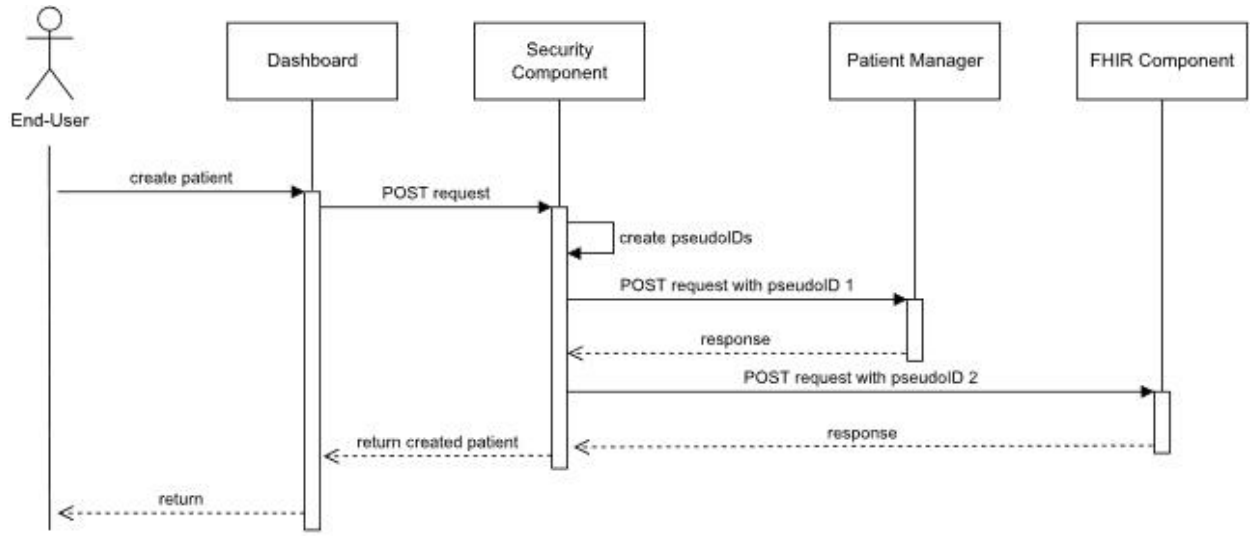

Figure 6: Sequence diagram of the patient creation process suppotred by CSB@SecurityComponent.

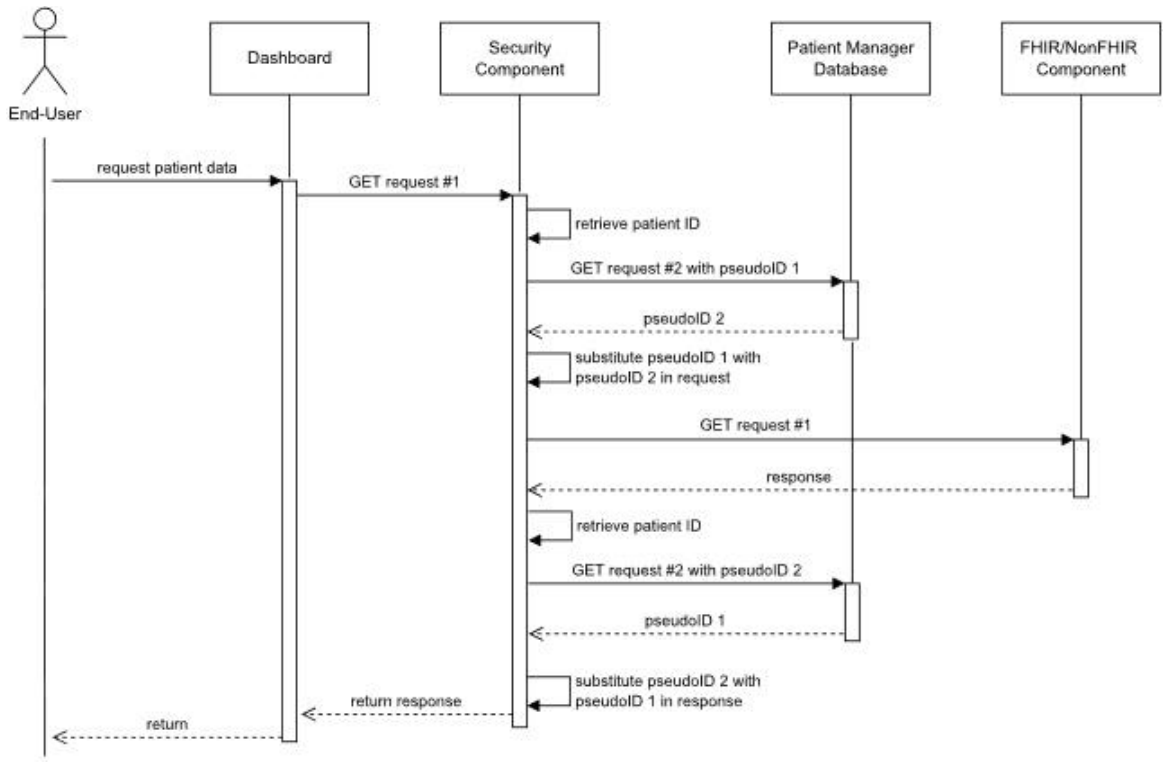

Figure 7: Sequence diagram of the of the pseudonymisation process suppotred by CSB@SecurityComponent.

Table 6. Patient management: REST service definitions

Method	Params	Response
Method: Get all	Params	Response
GET	UserID	JSON records of all patients containing Pseudo-Id1, RecruitmentStatus-ID, Group-Id, Last Transmission date, Createdby UserId, Last updated timestamp
Method: Get		
	UserID, Pseudo-Id1	JSON record containing Pseudo-Id1, PilotID, OrganisationID, Fullname, Birthday, Home address, PO, Phone, email, RecruitmentStatus-ID, Group-Id Date of participant's consent Withdraw consent date, Reason-ID, End-user1-ID, End-user2-ID, End-user3-ID, email1, email2, email3
Method: Edit		
POST	UserId, Pseudo-Id1, Fullname, Birthday, Home address, PO, Phone, email,	JSON record containing UserId, Pseudo-Id1, Fullname, Birthday, Home address, PO, Phone, email, RecruitmentStatus-

Method	Params	Response
	RecruitmentStatus-ID, Group-Id Date of participant's consent Withdraw consent date, Reason-ID, End-user1-ID, End-user2-ID, End-user3-ID, email1, email2, email3	ID, Group-Id Date of participant's consent Withdraw consent date, Reason-ID, End-user1-ID, End-user2-ID, End-user3-ID, email1, email2, email3
Method: Create		
POST	UserId, Fullname, Birthday, Home address, PO, Phone, email, RecruitmentStatus-ID, Group-Id Date of participant's consent Withdraw consent date, Reason-ID, End-user1-ID, End-user2-ID, End-user3-ID, email1, email2, email3	JSON record containing UserId, Pseudo-Id1, Fullname, Birthday, Home address, PO, Phone, email, RecruitmentStatus-ID, Group-Id Date of participant's consent Withdraw consent date, Reason-ID, End-user1-ID, End-user2-ID, End-user3-ID, email1, email2, email3
Method: Assign device		
POST	UserId, Pseudo-Id1, Device ID, DeviceCategory-ID, Status-ID, Number	JSON record containing Pseudo-Id1, Device ID, DeviceCategory-ID, Status-ID, Number
Method: View devices		
	UserId, Pseudo-Id1	JSON record containing Pseudo-Id1, Device ID, DeviceCategory-ID, Status-ID, Number
Method: Edit device		
POST	UserId, Pseudo-Id1, Device ID, DeviceCategory-ID, Status-ID, Number	JSON record containing Pseudo-Id1, Device ID, DeviceCategory-ID, Status-ID, Number
Method: View Last usage data transfers		
GET	UserId, Pseudo-Id1	JSON record containing Pseudo-Id1, Device ID, DeviceCategory-ID, LastTransmition timestamp
Method: View usage data transfers (of particular device type)		

Method	Params	Response
GET	UserId, Pseudo-Id1, DeviceCategory-ID	JSON record containing Pseudo-Id1, Device ID, DeviceCategory-ID, LastTransmition timestamp
Method: Upload photo		
POST	Pseudo-Id1, IMEI, Speed, Flow, Pulse index, Power, Alarm, filename	JSON record containing Pseudo-Id1, Pseudo-Id1, Speed, Flow, Pulse index, Power, Alarm, filename, CreatedTimestamp
Method: view all photos		
GET	UserId, Pseudo-Id1, Image-ID	JSON record containing Pseudo-Id1, Pseudo-Id1, Speed, Flow, Pulse index, Power, Alarm, filename, CreatedTimestamp
Method: view photo		
GET	UserId, Pseudo-Id1, Image-ID	Image filename

Swagger Supported by SMARTBEAR

Patients management API specification is within Patient Manager API ./openapi.json swager, available online at: http://147.102.33.191:58081/

The complete list of REST APIs supported is provided in Annex 8.1.

3.5.3 GDPR Requests management

Collecting and managing privacy-related requests (i.e., exercising a GDPR right) been handled by the GDPR requests management service, which accept requests and forwards them to CSB Administrators for processing. Study participants may issue a request via the RETENTION Mobile application (alternatively via the CSB@Dashboard by the Clinical Care Manager on their behalf) by which can also track status, follow-up, and provide feedback to those handling their requests. In addition, an Auditor may track the progress of the request and see who is currently working on it. The following roles are assigned to this service to support request creation, handling and tracking:

- CSB Administrator
  - View GDPR request(s) created by study participant(s) (or by Clinical Case Managers in their behalf)
  - View notification(s) for pending action(s)
  - View GDPR request details and associated actions
  - Respond to a request (may also attach a file)
- CSB Auditor
  - View GDPR request(s) created by study participant(s) (or by Clinical Case Managers in their behalf)

  - View notification(s) for pending action(s)
  - View GDPR request details and associated actions
  - View action details
- Clinical Case Manager
  - View GDPR request(s) created by him/her on behalf of a study participant
  - Create GDPR request (on behalf of a study participant)
- Patient (or study participant)
  - View GDPR request(s) created by him/her
  - Create GDPR request
  - Receive response via the RETENTION Mobile application

Table 7. GDPR request management: REST service definitions

Method	Params	Response
Method: View all		
GET	UserID	JSON records of all GDPR requests containing requestID, participantID/UserId, category, status, and last update of request status
Method: View		
GET	UserID, requestID	JSON record of specific GDPR request containing requestID, participantID/UserId, category, status, and last update of request status and associated action(s) (JSON: type, assigned to, status, priority and timestamp)
Method: Edit		
POST	UserID, requestID, participantID/UserId, category, status	JSON record of specific GDPR request containing requestID, participantID/UserId, category, status, and last update of request status and associated action(s) (JSON: type, assigned to, status, priority and timestamp)
Method: Create		
POST	UserID, participantID/UserId, category	JSON record containing requestID, participantID/UserId, category, status, and last update of request status and associated action(s) (JSON: type, assigned to, status and timestamp)
Method: Respond		

Method	Params	Response
POST	UserID, requestID, action type, assigned to, and priority	JSON record containing requestID, participantID/UserId, category, status, and last update of request status and associated action(s) (JSON: type, assigned to, status, priority and timestamp)

GDPR requests management API specification is within Patient Manager API ./openapi.json swager, available online at: http://147.102.33.191:58081/

The complete list of REST APIs supported is provided in Annex 8.1.

4 Continuous monitoring of the Security and Privacy Posture

An overarching objective of RETENTION is to provide a trustworthy platform with security and privacy provisions considered by design and maintained throughout the development, testing and refinement of all components comprising the proposed solution. The provisions adhering to the "Privacy by Design" principle presented in the previous chapter (secure communication channels, RBAC, pseudonymisation, IDs management, encryption, etc.) are proportionate to the highly sensitive personal data involved in the operation of the RETENTION platform and the relevant safety, regulatory, legal and ethical issues stemming from said data and the healthcare environment (involving ethics approvals by five hospitals).

Although the state-of-the-art controls and processes adopted in RETENTION ensure that all security, privacy and regulatory compliance requirements, as identified by the comprehensive risk and compliance assessment carried out at the early stages of the project, are compellingly addressed, the notion that GDPR is a continuous process rather than a specific goal to be achieved should not be overlooked. Human errors, technical bugs, programming languages vulnerabilities are among the factors that might cause data breaches even on the most secure information systems. To cope with this aspect, the real-time operational compliance of the RETENTION platform to said requirements will be provided in an evidence-based manner through the integration of the RETENTION continuous Security and Privacy Assurance Platform (cSPAP), which will enable security and privacy assessments based on vulnerability analysis, penetration testing and continuous monitoring of the RETENTION assets.

4.1 Elicitation analysis to address healthcare security management standards

In parallel with the processes concerning the medical dimension of the RETENTION project, the under development framework supports as well those responsible for operating the RETENTION platform (e.g., technicians in the healthcare ecosystem) to realise security and privacy risks and address related implications arising from the detection and analysis of potential vulnerabilities cyber-attacks on the respective Health Care Information Infrastructures (HCIIs). Therefore, upon completion of the core infrastructure of the RETENTION platform, will provide the corresponding mechanisms and software components for conducting continuous monitoring of assets and enabling security controls against known threats and vulnerabilities. The RETENTION Continuous Security and Privacy Assurance Platform (based on the Assurance Platform of STS) will be tailored to and integrated into RETENTION platform to enable the real-time, continuous security and privacy posture assessment of the RETENTION deployment, with the aim to support management procedures for securing IT infrastructure from a technical perspective, tailored to the healthcare ecosystem. To this, a brief description of international and national security management standards is provided, including the ISO/IEC 27000 family of standards, which is the main international standard for information security management systems and the National Institute of Standards and Technology (NIST) SP 800 publication, which provides guidelines for securing IT infrastructure from a technical perspective. The most relevant to RETENTION standards of the ISO 27000 and NIST SP 800 families and are outlined below.

- **ISO/IEC 27001:2013**: it specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation, and outlines how stakeholder should manage information

security risk by creating an information security management system (ISMS). A guide for creating an ISMS, such as the structures an organization has in place to manage data, including technology, physical security, personnel policies, and organisational hierarchy that delegates responsibility for these issues.

- **ISO/IEC 27000:2018**: (as with previous) it provides the overview of ISMS, including terms and definitions commonly used in the ISMS family of standards. This standard is applicable to all types and sizes of organisations which intend to manage risks that could compromise the organisation's information security.
- **ISO/IEC 27005:2022**: is a guide to risk management, and provides inspiration for assessing and managing risks related to the organisation's information, based on an assessment of the likelihood of occurrence of an incident, together with the impact of the incident on the organisation. Thus, a guidance on how to carry out a risk assessment via tools for prioritising risks, that provide an overview of the organisation’s threats and vulnerabilities, and how risks can be addressed based on the organisation's risk acceptance. As suggests, risk management is an ongoing process that is to be maintained continually. However, it does not support any specific technique for this purpose or any computational method to analyse and combine the assessment information.
- **ISO / IEC 27002**: not a certifiable standard per se but rather a collection of information security guidelines that are intended to help an organization implement, maintain, and improve its information security management, including implementation guidance based on internationally recognised best practices. It provides hundreds of potential controls and control mechanisms that are designed to be implemented with guidance and is tailored to the specific information risks and needs of any organisation, irrespective of size or type and offers recommendations on standard security practices that enable an organisation to meet audit, regulatory and legal requirements. By its adopting, an organisation can be able to assess its information risks, set control objectives and implement appropriate controls.
- **ISO / IEC 27035**: is a standard that focuses on information security incident management and presents basic concepts and phases of information security incident management and principles in a structured approach to support the detection, reporting, assessing, and responding to incidents, and applying lessons learnt. The guidelines consist of phases for planning and preparing security incident management policies, security policies, establishing incident response team, incident management awareness training, and incident management plan testing.
- **ISO 27799:2016**: offers guidance on how best to protect the confidentiality, integrity, and availability of personal health data for anyone working in the health sector or its unique operating environments information security management and information security controls, taking into consideration the organisation's information security risk environment.
- **NIST SP 800-30 (revision 1**): is used to provide risk assessment guidelines for organisation and government information systems (critical infrastructures including health care infrastructures) and as a complement to NIST SP 800-39, including identifications of threat source, event threats, vulnerability, and determining the likelihood, the impact, and the level of risk.
- **ISO 14971:2019**: it specifies terminology, principles and a process for risk management of medical devices including software and intends to assist manufacturers of medical devices

to identify the hazards associated with the medical device, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls. concerns itself with the application of risk management to medical devices including software. The standard covers the whole product lifecycle including post-production. One of the prerequisites it sets for manufacturers is to establish, implement, document, and maintain a risk management process, to delegate risk management to experienced staff and to define a policy of risk acceptance criteria, which are based upon relevant regulatory demands.

- **ISO/TR 22696:2020**: it provided guidance for managing healthcare service security with connectable personal health devices (PHDs) and is applicable to identification and authentication between the bidirectionally connected PHDs and gateway by providing possible use cases and the associated threats and vulnerabilities. It uses the "CIA concept" (confidentiality, integrity, and availability) to define cybersecurity focus, and considers all three equally important in the healthcare domain.
- **IEC 80001-1:2010**: it defines the roles, responsibilities and activities that are necessary for risk management of IT-networks (MIT) incorporating medical devices to address safety, effectiveness and data and system security. Having as main objective to find, assess, control and evaluate risks throughout the life cycle of MIT incorporating medical devices.
- **ISO 13606-1:2019**: is a standard with the main objective to define a rigorous and stable information architecture for communicating part or all of the Electronic Health Record (EHR) of a single subject of care (i.e. patient), or between EHR systems and a centralized EHR data repository. It may also be used for EHR communication between an EHR system and clinical applications or middleware components (such as decision support components) that need to access EHR data, or as the representation of EHR data within a distributed (federated) record system.
- **ISO 81001-1:2021**: it targets manufacturers of "Health Software" and other software used in the health sector (i.e., specifically for managing, maintaining, or improving health of individual persons), excluding medical devices (as defined by the EU Medical Device Regulation) (e.g., fitness apps for sports purposes, general nutrition counselling for healthy individuals). Its requirements are specifically tailored to the field of health software.
- **ENISA Cloud Security for Healthcare Services:** a set of general practices aims to help IT professionals in the healthcare security contexts to establish and maintain Cloud security while selecting and deploying appropriate technical and organisational measures. The report includes relevant data protection aspects, to be considered when procuring Cloud services for the healthcare industry, allowing in this way the identification of the main incident sources, and suggesting the correct handling procedures for them.

4.2 RETENTION Continuous Security and Privacy Assurance Platform

The cSPAP is an integrated framework of models, processes, and tools to enable the certifiable view of security properties of services. The cSPAP (in Figure 8) is scheduled to perform security and privacy assessments that involve threat and vulnerability analysis, static analysis, penetration testing and continuous runtime monitoring, to provide a comprehensive analysis of the security and privacy posture of a system. It will, through an Event Captor Module to be developed for the purpose of the RETENTION platform, audit critical components and processes of the CSB and GIC infrastructures while leveraging monitoring mechanisms developed in the context of the project.

Based on the input (e.g., log files, event captors to be produced via data probes) scheduled to be collected, the cSPAP will provide an evidence-based, certifiable view of the security posture of the RETENTION platform, 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 metrics. To support this evidence collection, the platform will have interoperability with various components of the GIC and the CSB and programmatic connectivity to some of their core components through appropriate probes (e.g., event captors, test tools), enabling it to obtain the monitoring and/or test the evidence required for the assessments. Also, the methodology and procedures for the automation of security certification are also 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). Within this context, several 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. This section presents a detailed description of the cSPAP, while relative information regarding the forthcoming integration process to the RETENTION platform will be also described.

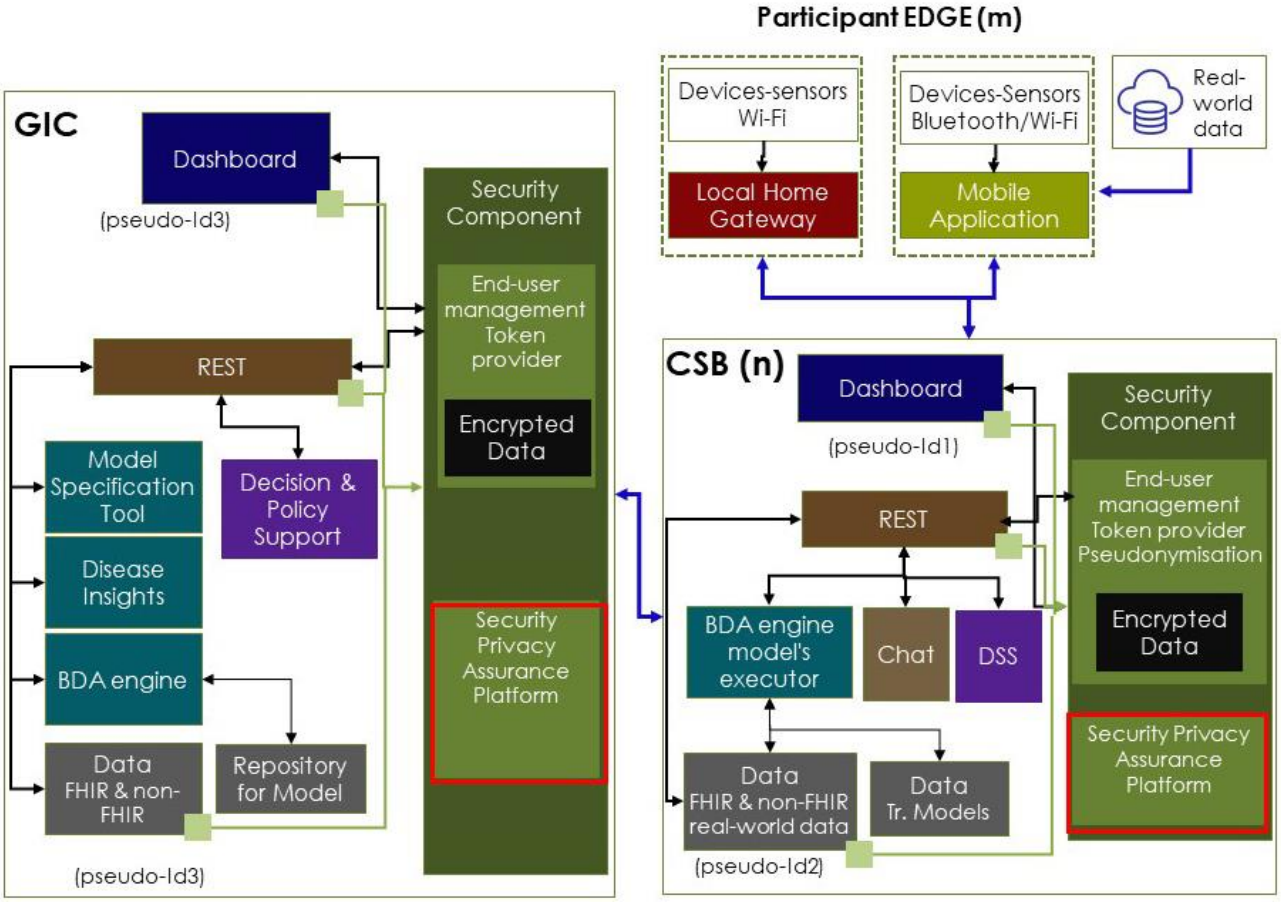

Figure 8: RETENTION Architecture overview: the RETENTION Continuous Security and Privacy Assurance Platform will perform security and privacy assessments.

4.2.1 Key Features

The cSPAP is comprised of five basic software modules:

1. Asset Loader Module: The component responsible for receiving the cyber system's asset model for the target organisation (in particular the assets of the CSB and GIC). This model includes This model includes the assets of the RETENTION, security properties for these assets, threats that may violate these properties, relations between assets in the model, and the security controls that protect the assets. The latter data are defined by the target organization using an excel file, which is is parsed by the Asset Loader Module, and in turn automatically constructs the respective model for the target organisation.
2. Vulnerabilities Loader Module: The component responsible for loading the known vulnerabilities of the identified assets and updating the cSPAP depending on the organisation's assets included in the assurance model. It is composed of two subcomponents, (a) the Vulnerabilities Loader, and (b) the Vulnerabilities Database. Vulnerabilities Loader Module uses OpenVas , an open-source vulnerability assessment framework/scanner, while the known vulnerabilities are loaded through a daily update feed provided by Greenbone.
3. Monitoring - Auditing Module: This component is 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. The latter are stored to the monitor database while the monitor submodule. Monitor is the core submodule of the auditing module that reasons if a monitoring rule is violated or satisfied.
4. Evidence collection - Event Captor Module: 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, and PacketBeat), which centralises log data. Data can also be collected via open server-side data processing pipelines (such as Logstash) that ingests data from a multitude of sources, which transforms and then sends them to ElasticSearch. The Event Captor is initiated through the respective REST API calls from the monitoring module.
5. Dynamic Testing Module: 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.

The cSPAP forms the basis of this component (in Figure 9) and is used for monitoring, testing, and assessing the under protection RETETION platform, ensuring and assuring the proper functioning of the whole framework. The types of evidence foreseen include monitoring data and testing data, while additional sources may be added as the development progresses in order to combine runtime monitoring and dynamic runtime testing to ensure correct and effective operation of security controls.

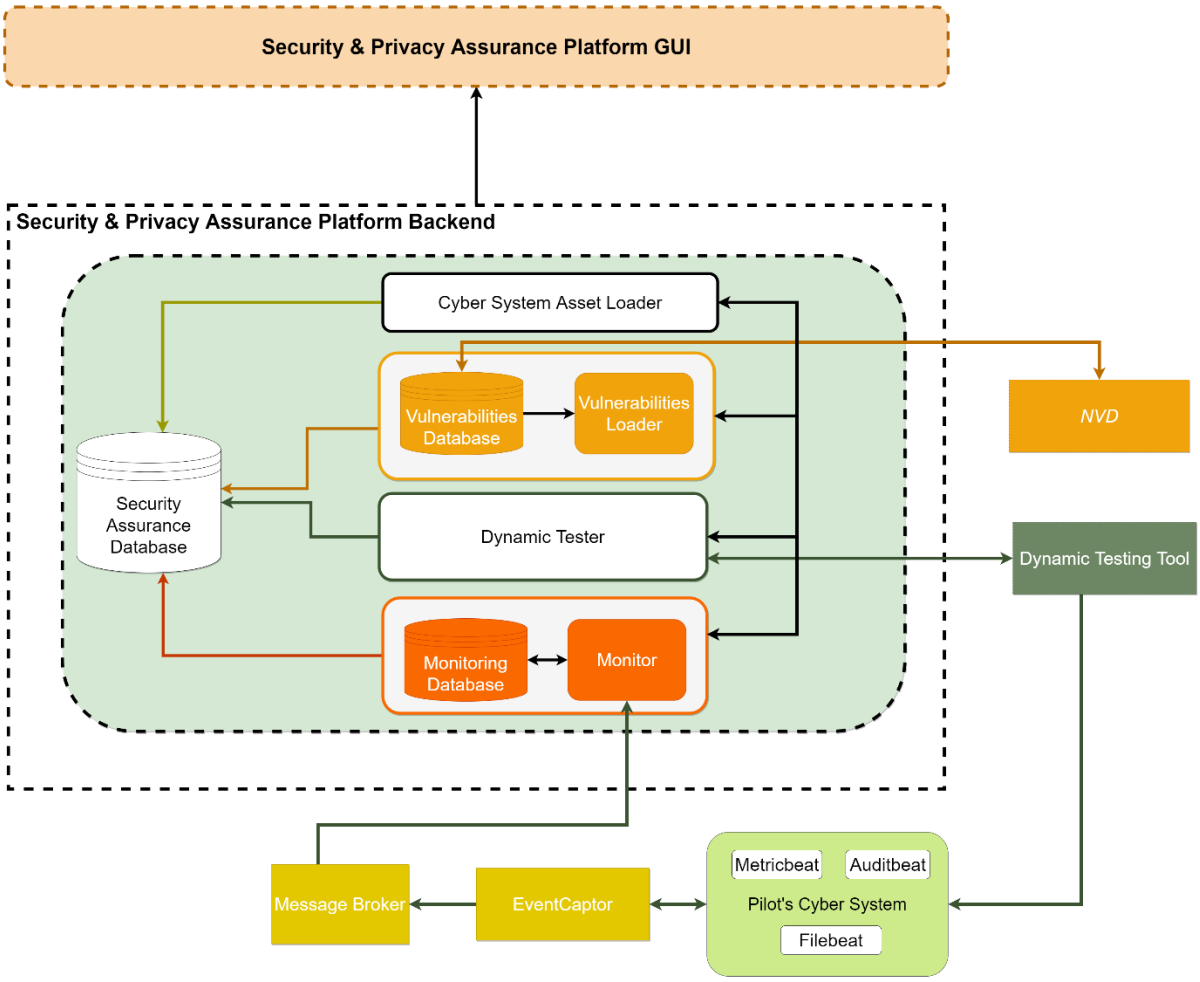

Figure 9: The RETENTION Continuous Security and Privacy Assurance Platform's Architecture.

In RETENTION two variants of the cSPAP will be deployed; one tailored to the CSB environment and one to the GIC. More specifically, the CSB instances will integrate a variant tailored to monitoring the secure and privacy-aware operation of each component comprising the CSB instance, while the variant to be integrated into the GIC will monitor and assess the security and privacy posture of critical components comprising the GIC.

Pending to be started activity: Since at this point the testing of all core components of the integrated RETENTION platform v1 has not competed (D7.1 is due on M22), aspects regarding the integration, configuration and operation of the cSPAP will be updated in accordance with the project's progress and presented in D6.4.

.

5 Operations

5.1 Keycloak - KrakenD Initialisation

Upon a fresh Keycloak installation[13], proper configuration must take place to ensure end-users utilising the RETENTION mobile application (i.e., study participants) and the CSB@Dashboard (CSB end-uses) can login, receive their token, and KrakenD can validate their tokens against the Keycloak configuration.

By default, Keycloak is installed with an admin user, and a “master” realm. A realm is the logical collection of a set of users, credentials, roles, and groups. A single user belongs and logs into a realm. For example, the “admin” account, which is present by default, belongs to the “master” realm. To keep the Keycloak administrator and the RETENTION application’s administrator separate, a new realm needs to be created, titled "retention”. This realm will hold all end-user accounts, credentials, and roles.

To create the new realm, the system administrator:

1. Logs in at the Keycloak administration dashboard.
2. From the menu (on the left) hovers over the “Master” dropdown and clicks on “Add realm” (Figure 10).
3. Inputs the new realm name and clicks “Create” (Figure 11).

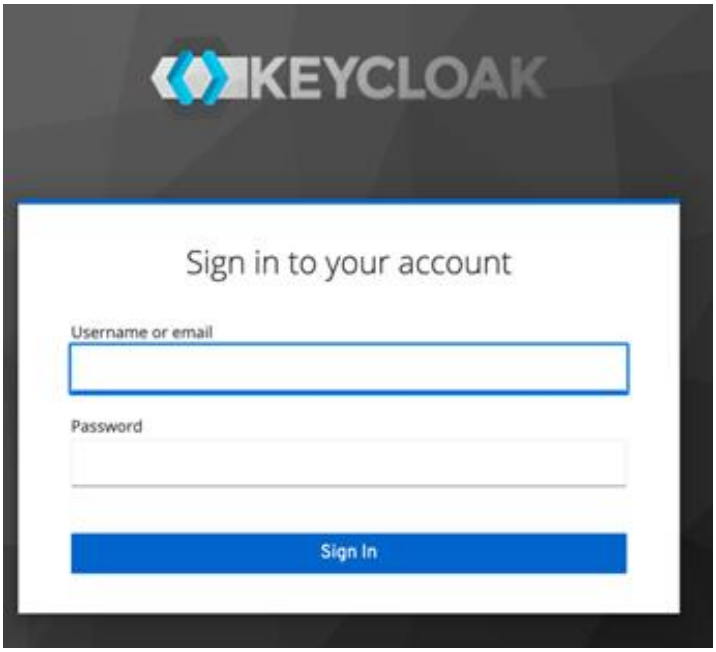

Figure 10: Keycloak login.

[13] Keycloak installation: Using standalone mode: https://www.keycloak.org/docs/16.1/server_installation/#_standalone-mode

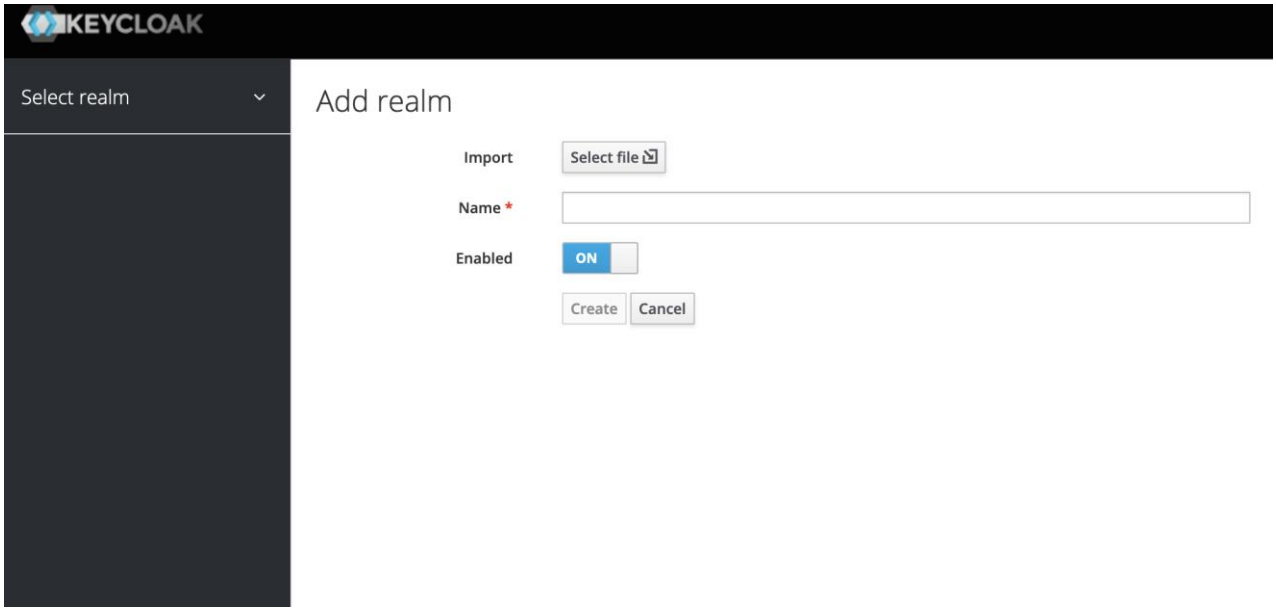

Figure 11: Realm creation.

Following the realm creation, users can be created by selecting “Users” on the sidebar, then clicking on “Add user” (Figure 12).

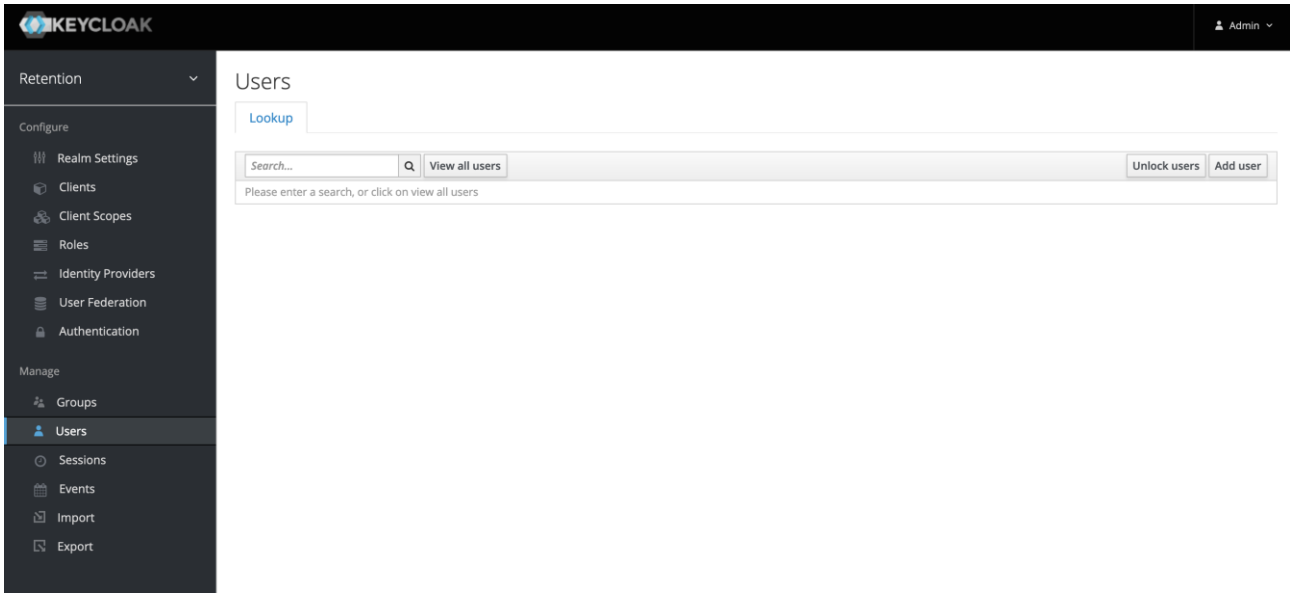

Figure 12:User creation.

For a user to login however, one needs to create the appropriate clients. Clients are entities that can request Keycloak to authenticate a user; as such, the mobile application or the web dashboard are clients and need to be created. To create such clients:

1. The Keycloak administrator clicks on “Clients” in the sidebar.
2. Clicks on “Create”.
3. Inputs a client id (e.g. “dashboard” or “mobile”), and clicks on “Save”.
4. Additional settings may be configured. For example, Access Token lifespan, or Access Type.

Now, the exact realm and client combination can be used to integrate Keycloak’s provided login page to any GUI. Alternatively, a direct API call can be used to retrieve the token at

"/auth/realms/{realm-name}/protocol/openid-connect/token" where {realm-name} is the name of the keycloak realm. The payload of the request depends on the grant_type. For parameter. A value of "password" means that a username and a password must be sent to the endpoint, along with the client's id. Alternatively, a grant_type of "client_credentials" allows the admin user to login using the client id as username, and the client's secret as the password – but only when the access type is set to "Confidential".

5.1.1 End-User Roles Creation

The following images (Figure 13 and Figure 14) depict the process by which CSB end-user roles (defined in D3.1) are created. To create a role the system administrator:

1. Logs in at the Keycloak administration dashboard;
2. From the menu (on the left) select "Roles" and then "Add Role";
3. Inserts the role's name and optionally a description;
4. Repeats steps 2 and 3 until all roles are created (Figure 15).

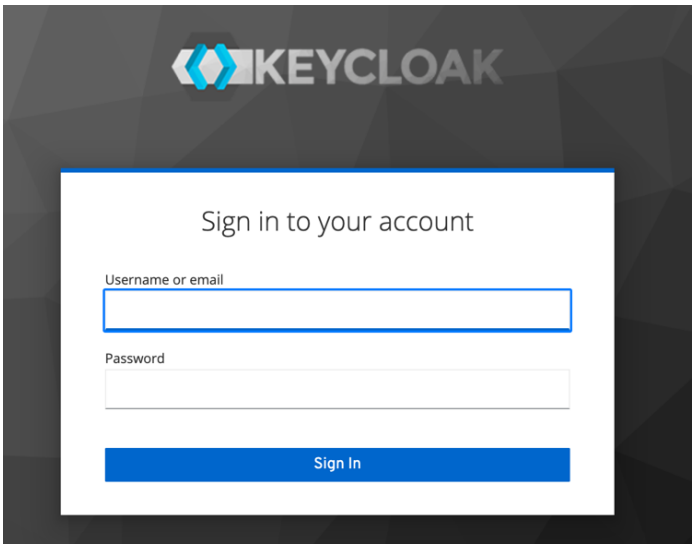

Figure 13: Step 1/3: Keycloak login.

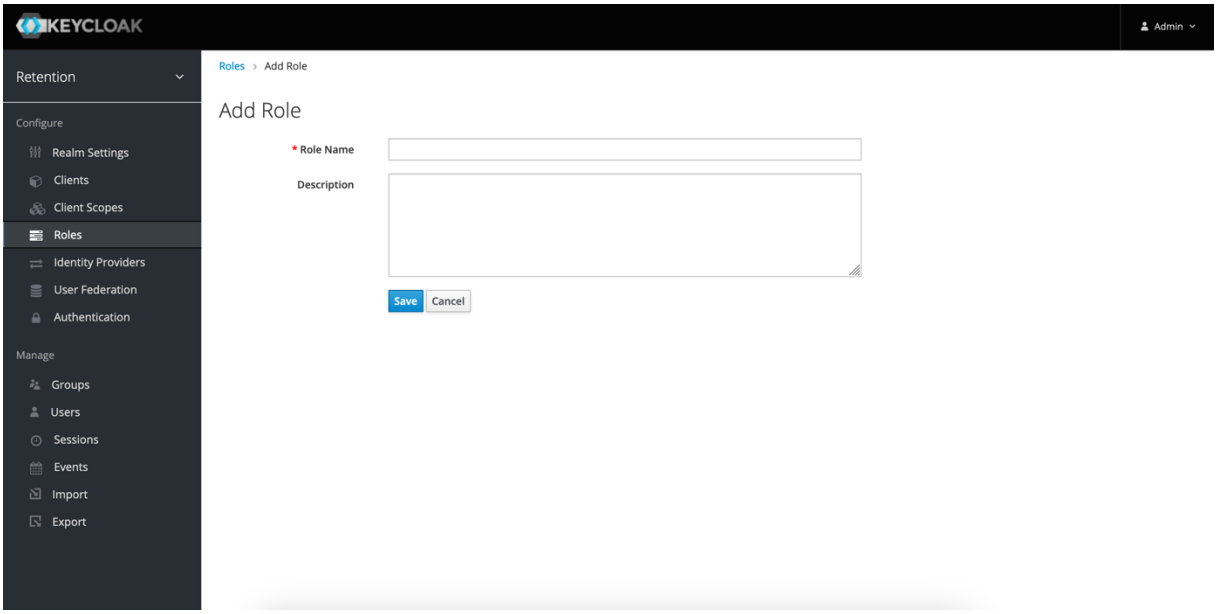

Figure 14: Step 2/3: Role addition.

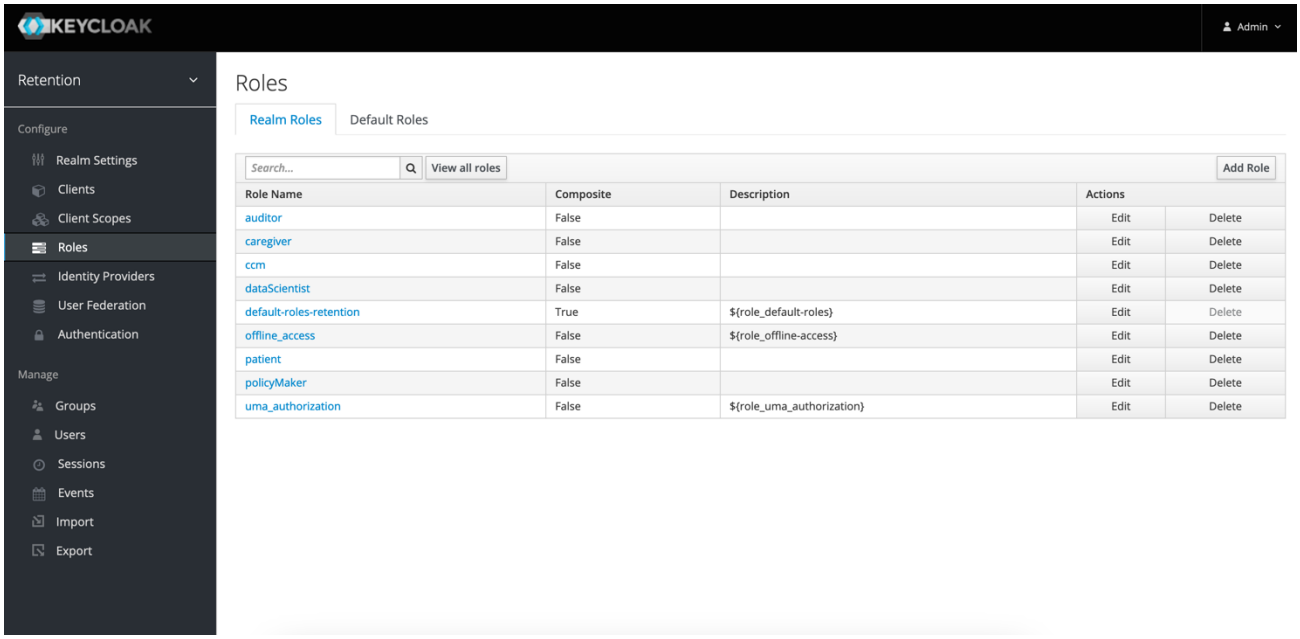

Figure 15: Step 3/3: Roles added.

5.1.2 Configuring Role-Based Access Control of CSB APIs

Within CSB, a REST layer is used for retrieving, saving or analysing the data stored in the CSB@Repository.

To protect this REST layer, the KrakenD high-performance open-source API gateway is used, which sits between the user client and the backend services and can handle all authorization aspects. Additionally, KrakenD is highly extendable using plugins written in GoLang – these plugins can be used to transform both requests and their responses, thus providing an excellent way to implement RETENTION's pseudoanonymization functionality.

KrakenD's basic functionality can be configured entirely through a single configuration file in JSON format. This provides a very convenient way to handle versioning and automated deployment. To create endpoints that forward requests to backend services, one needs to specify them in the configuration file with details such as the URL pattern, the HTTP method, and the backend service that will handle the request.

An example of a simple endpoint definition in KrakenD follows below:

```
{
    "endpoints": [
        {
            "endpoint": "/patients",
            "method": "GET",
            "backend": [
                {
                    "url_pattern": "/patients",
                    "method": "GET",
                    "host": [
                        "http://localhost:8080"
                    ]
                }
            ]
        }
    ]
}
```

In the above example, the endpoint is defined as "/patients" and it will handle "GET" requests. The request will be forwarded to the backend service at "http://localhost:8080/patients". This configuration however is currently insecure; it does not handle any kind of authorization to the service as all requests will be routed to the backend.

To secure the previous endpoint with Keycloak, additional configuration is needed. More specifically, for each endpoint, the administrator needs to define how KrakenD will validate any JWTs present in the Authorisation header of the request, and which roles to authorize. This is very easy to define using KrakenD's built-in Keycloak integration.

```
{
    "endpoints": [
        {
            "endpoint": "/patients",
            "method": "GET",
            "extra_config": {
                "auth/validator": {
```

```
                    "alg": "RS256",
                    "jwk_url":    "http://keycloak:8080/auth/realms/healthcare/protocol/openid-
connect/certs",
                    "roles_key": "realm_access/roles",
                    "roles": [
                        "ccm", "admin"
                    ]
                }
            },
            "backend": [
                {
                    "url_pattern": "/patients",
                    "method": "GET",
                    "host": [
                        "http://localhost:8080"
                    ]
                }
            ]
        }
    ]
}
```

In this configuration, the “auth/validator” property is added under the “extra_config”. This property specifies that this endpoint will be protected with a validator, that the token is expected to be signed using the RS256 algorithm, and that the public key to verify its validity can be found at the address specified as “jwk_url”. In addition, KrakenD is aware that the token will include the user’s roles under the “realm_access/roles” key, and will only forward the request if the token is valid and the roles in the JWT include either “ccm” or “admin”.

In addition to the authorisation, KrakenD needs to incorporate the pseudoanonymisation functionality. As such, a custom KrakenD plugin needs to be written that performs the following functions:

- Recognize all requests that include a patient ID in their payload. These can be present anywhere in their “body”, or as a query parameter that extends the endpoint location. For example: a GET request at “/patient/28”, with 28 being the patient’s ID.
- Extract the patient ID (pseudo-id 1) and match it against SC’s database to retrieve its corresponding pseudo-id 2 (or 3 depending on the request’s destination).
- Reconstruct the request using the pseudo-id 2, taking care to overwrite any auto-generated headers. For example, the “Content-Length” header which specifies the body’s size in bytes needs to be recalculated after pseudoanonymisation as pseudo-id 2 may contain more digits than pseudo-id 1.
- Recognize any responses that include a patient ID in their body. If these responses originate from the FHIR and Non-FHIR databases, this patient ID will correspond to the pseudo-id 2 in case of a clinical site backend, or pseudo-id 3 in case of the cloud repository.

The patient ID then needs to be swapped with pseudo-id 1, and the response to finally be forwarded back to the user.

For all endpoints where the pseudoanonymisation functionality needs to be enabled, this must be defined explicitly in the KrakenD configuration file.

```
{
    "endpoints": [
        {
            "endpoint": "/patients",
            "method": "GET",
            "extra_config": {
                "auth/validator": {
                    "alg": "RS256",
                    "jwk_url":      "http://keycloak:8080/auth/realms/healthcare/protocol/openid-
connect/certs",
                    "roles_key": "realm_access/roles",
                    "roles": [
                        "ccm", "admin"
                    ]
                }
            },
            "backend": [
                {
                    "url_pattern": "/patients",
                    "method": "GET",
                    "host": [
                        "http://localhost:8080"
                    ],
                    "plugin/req-resp-modifier": {
                        "name": ["pseudoanonymization-request", "pseudoanonymization-response"]
                    }
                }
            ]
        }
    ]
}
```

In the above example, the pseudonymisation-request and pseudonymisation-response are two different functions that are to be applied only on the request and the response side of the endpoint respectively.

5.1.3 Security and Privacy Assessments Planning

This section describes the Privacy and Security Assessment (PSA) methodology, schedule, and requirements that the <Security Control Assessor> will use to evaluate the <RETENTION Platform> (CSB instances and the GIC). The goal of this plan is to clearly define the components of the RETENTION Platform upon which checks will be performed, and explain the information that <Security Control Assessor> expects to obtain prior to the assessment(s), the areas that will be examined and the specific types of assessment(s) to be performed, the time periods these assessments will take place, and the proposed scheduled activities the <Security Control Assessor>

expects to perform during or after the assessment(s). The methodology relies on the availability (locally integrated) of the cSPAP, a suite responsible for monitoring, testing, and assessing the security and privacy posture of the platform's assets, in a real-time, continuous manner. Within this context, several built-in security assessments addressing the Confidentiality – Integrity – Availability (CIA) principles can be utilised, or other tailored to the specific needs (e.g., software/hardware specifications) leveraging an evidence-based approach, to provide security assurance assessments with certifiable results.

5.1.3.1 Evaluation target

The RETENTION platform's architecture is based on a 3-Layer model, consists of: i) the Global Insights Cloud - GIC, which functions as the main Big Data repository that hosts the Big Data analytics engine and services to support the Machine Learning pipelines upon anonymised data stored with the GIC@Repository (a FHIR and a nonFHIR one), as well as the policy making (via the same analytic engine), offering to the registered end-users (i.e., Data scientist, clinical expert, or healthcare policy maker) the tools to conduct ML analytics resulting in prognostic prediction models that (later on) assist clinicians in making necessary decisions about a medical disease management (in particular Heart Failure). Upon completion of best (performance-wise) trained models, those will be "pushed" to the Clinical Site Backend instances for application; ii) the Clinical Site Backend - CSB that offers to the registered end-users (mainly clinicians) tools to monitor their patients (RETENTION study participants), in terms of gathering their medical and usage data (evidence) and take "informed" decisions about them. CSB@Repository (FHIR and nonFHIR) stores pseusonymised information about those patients, while the CSB@SecurityComponent manages their personal data, PII and identifiers by having a separate encrypted repository. The same component provides API management mechanism and RBAC features to allow REST API endpoints to be triggered via the CSB@Dashboard or several mobile applications and Raspberry Pi (token-based access); iii) Patient EDGE consists of a mobile application (Android smartphone) and a home gateway (Raspberry Pi), and supports the continuous monitoring of patients and the collection of real-world data associated to them. The Mobile application support bidirectional secure connectivity to a predefined CSB instance for managing the devices'/sensors' usage data, questionnaires' answers and receive personalised notifications and alerts by the CSB.

Target of evaluation

During the initial assessment, the following subcomponents or processes are considered candidates for conducting the assessments:

- CSB@Repository and GIC@Repository, built upon open-source Java & MariaDB (access logs can provide evidence for assessments);
- CSB@SecurityComponent and GIC@SecurityComponent, built upon open-source PostgreSQL (access logs can provide evidence for assessments) and Java;
- REST API that supports the CSB and GIC FHIR specification;
- Keycloak, that supports the end-user management of both CSB@Dashboard end-users and GIC@Dashboard end-users (via an access token for the session);
- Machine-to-machine communications between CSB and Mobile applications/Raspberry Pi;
- CSB@Dashboard (web browser log file or SecurityComponent log file may provide evidence for assessments).

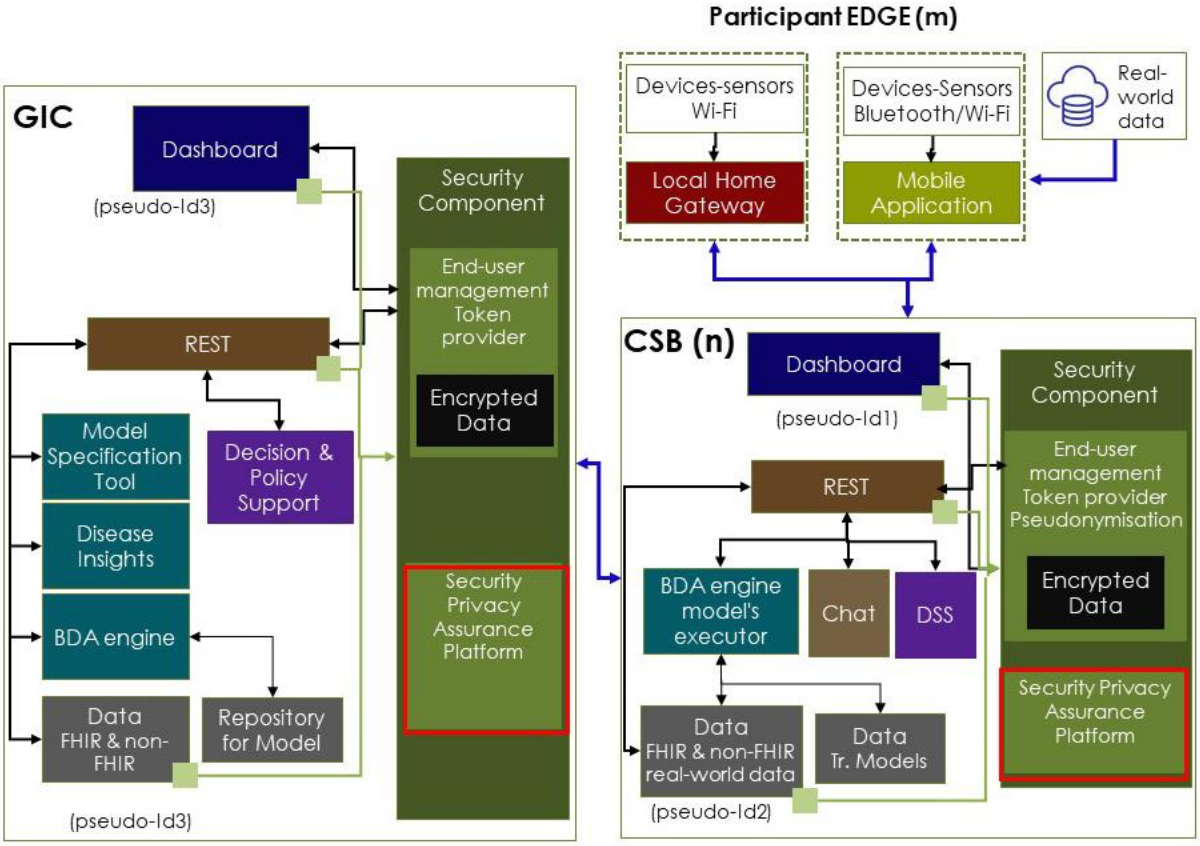

Figure 16: Data and events of predefined components (CSB Repository, CSB Dashboard/webserver, CSB REST API manager log, CSB Security component log, and others) will be collected by lightweight data shippers (namely Beats, such as Filebeat, MetricBeat, PacketBeat, Logstash), and then send them to ElasticSearch which centralises log data and transforms them for later proccessing.

Phases:

1. Customisation, integration, and deployment of the cSPAP for the purposes of the RETENTION project;
    a. (if required) Development of appropriate event logging mechanisms for the integration of the cSPAP with the rest of the proposed solution;
    b. Set up and deployment of event logging mechanisms for continuous monitoring of assets and security controls against known threats and vulnerabilities;
    c. Forming rules (e.g., *Log shipper (X) to deployed on component/service (Y) to capture events (Z) and transmit them to the cSPAP obfuscating parts (A, B, C, D) prior to transmittion*)
2. Comprehensive modelling and dependencies of [the assets of the target of evaluation system], including the computational infrastructure (computers, networks, devices); software (system software, firmware, middleware, and application software); data assets and their collection, and data flow processes).
3. Vulnerability analysis, i.e., Identification of potential vulnerabilities and association of them with specific [assets of the target of the evaluation system] according to continually updated international standards.

4. Penetration testing (detection of actual vulnerabilities of [assets of the target of the evaluation system] recommendations for response actions).

Pending to be started activity: Operations related to cSPAP required the integration of the platform and deployment of data snifers, scheduled to be carried out with the completion of the functionality (ver1.0) to support the main pilots.

6 Conclusion

This document provides the initial version of the privacy and security mechanisms of the RETENTION platform, to encompass detailed descriptions of assets developed, as well as their rationale and interoperability. The implemented solution is based on security-by design approach and comply with GDPR, providing anonymity, confidentiality, privacy and integrity of the data, and the integrity of the platform itself. This relates to end-user requirements analysis and outcomes (presented in D3.1), and the arcitectute of the RETENTION solution (in D3.2) and covers the development, modelling, configuration, and execution of mechanisms to guarantee the security and privacy of all data generetad, held and managed.

The mechanisms supported by the Security Component protect the transmission of any (sensitive or not) data utilised in the context of all components and provides evidence for assessing the project's workings regarding compliance with research ethics principles and corresponding legal obligations, as enunciated by the European Commission (EC).

7 References

ENISA, 2018. Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation, online: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provision

ENISA, 2014. Privacy and Data Protection by Design – from policy to engineering, online: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/

GDPR, 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Basdekis I., Pozdniakov K., Prasinos M., and Koloutsou K, 2019. Evidence Based Public Health Policy Making: Tool Support, 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 272-277, doi: 10.1109/SERVICES.2019.00080

UK Information Commissioner's Office (ICO), 2018. Guide to the General Data Protection Regulation (GDPR), online: https://ico.org.uk/for-organisations/guide-to-data-protection/

NIST, 2014. SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, online: https://csrc.nist.gov/publications/detail/sp/800-162/final

NIST, 2016. Role Based Access Control, online: https://csrc.nist.gov/projects/role-based-access-control/faqs

ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements, online: https://www.iso.org/standard/54534.html

What Is ISO 27001:2013? A Guide for Businesses, online: https://auth0.com/blog/what-is-iso-27001-2013-a-guide-for-businesses/

ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary, online: https://www.iso.org/standard/73906.html

ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks, online: https://www.iso.org/standard/80585.html

ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls, online: https://www.iso.org/standard/75652.html

ISO/IEC 27035-1:2016. Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management, online: https://www.iso.org/standard/60803.html

ISO 27799:2016. Health informatics — Information security management in health using ISO/IEC 27002, online: https://www.iso.org/standard/62777.html

National Institute of Standards and Technology, (2012). NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments 1 (2): 1-95.

ISO 14971:2019. Medical devices — Application of risk management to medical devices, online: https://www.iso.org/standard/72704.html

ISO/TR 22696:2020. Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs), online: https://www.iso.org/standard/73696.html

IEC 80001-1:2010. Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities, online: https://www.iso.org/standard/44863.html

ISO 13606-1:2019. Health informatics — Electronic health record communication — Part 1: Reference model, online: https://www.iso.org/standard/67868.html

ISO 81001-1:2021. Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts, online: https://www.iso.org/standard/71538.html

ENISA, 2021. Cloud Security for Healthcare Services, online: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services

8 Annexes

8.1 OpenApi.Json

------ Start of code ---------

{"openapi":"3.0.1","info":{"title":"Patient Manager API","version":"v0"},"servers":[{"url":"https://147.102.33.191:8180/patientmanager","description":"Patient Manager SC Base Path"}],"paths":{"/api/patient/{id}":{"get":{"tags":["patient-controller"],"summary":"Get patient by id","operationId":"getPatientById","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Patient"}}}}}},"put":{"tags":["patient-controller"],"operationId":"updatePatient","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Patient"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Patient"}}}}}},"delete":{"tags":["patient-controller"],"operationId":"deletePatient","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/patient/{id}/contact-phone/{contactPhoneId}":{"put":{"tags":["patient-controller"],"summary":"Update patient's contact phone","operationId":"updatePatientContactPhone","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"contactPhoneId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/ContactPhone"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418

I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}},"delete":{"tags":["patient-controller"],"summary":"Delete patient's contact phone","operationId":"deletePatientContactPhone","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"contactPhoneId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/caregiver/{id}":{"get":{"tags":["caregiver-controller"],"summary":"Get caregiver by id","operationId":"getCaregiver","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Caregiver"}}}}}},"put":{"tags":["caregiver-controller"],"summary":"Update caregiver","operationId":"updateCaregiver","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Caregiver"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Caregiver"}}}}}},"delete":{"tags":["caregiver-controller"],"summary":"Delete caregiver","operationId":"deleteCaregiver","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Caregiver"}}}}}}},"/api/patients/{id}/clinician/{clinicianId}":{"post":{"tags":["patient-controller"],"summary":"Assign a clinician to a patient","operationId":"assignClinicianToPatient","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"clinicianId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/ClinicianAssignment"}}}}}},"delete":{"tags":["patient-controller"],"summary":"Unassign patient from a clinician","operationId":"unassignClinicianFromPatient","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"clinicianId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303

SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}}},"/api/patient":{"post":{"tags":["patient-controller"],"summary":"Create a patient","operationId":"createPatient","requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Patient"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Patient"}}}}}}}},"/api/patient/{id}/image":{"post":{"tags":["patient-controller"],"operationId":"addPatientImage","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"title","in":"query","required":false,"schema":{"type":"string"}}],"requestBody":{"content":{"application/json":{"schema":{"type":"object","properties":{"image":{"type":"string","format":"binary"}}}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}}},"/api/patient/{id}/identity":{"post":{"tags":["patient-controller"],"summary":"Add identity to patient","operationId":"addIdentityToPatient","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Identity"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411

LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/patient/{id}/gdpr_request":{"post":{"tags":["patient-controller"],"summary":"Add GDPR request to patient","operationId":"addPatientGdprRequest","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/GdprRequest"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}}},"/api/patient/{id}/device":{"post":{"tags":["patient-controller"],"summary":"Assign device to patient","operationId":"addPatientDevice","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Device"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504

GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/patient/{id}/contact-phone":{"post":{"tags":["patient-controller"],"summary":"Add patient's contact phone","operationId":"addPatientContactPhone","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/ContactPhone"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/patient/{id}/caregiver/{caregiverId}":{"post":{"tags":["patient-controller"],"summary":"Assign a patient to a caregiver","operationId":"assignPatientToCaregiver","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"caregiverId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Patient"}}}}}},"delete":{"tags":["patient-controller"],"summary":"Unassign a patient from caregiver","operationId":"unassignPatientFromCaregiver","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"caregiverId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/gdprrequest/{id}/file":{"post":{"tags":["gdpr-request-controller"],"summary":"Add gdpr request

file","operationId":"addGdprRequestFile","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"title","in":"query","required":true,"schema":{"type":"string"}},{"name":"description","in":"query","required":true,"schema":{"type":"string"}}],"requestBody":{"content":{"application/json":{"schema":{"type":"object","properties":{"file":{"type":"string","format":"binary"}}}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}}},"/api/device/{id}/metrics":{"get":{"tags":["device-controller"],"summary":"Get a device's metrics","operationId":"getDeviceMetrics","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/DeviceMetrics"}}}}}}},"post":{"tags":["device-controller"],"summary":"Add metrics to a device","operationId":"addDeviceMetrics","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/DeviceMetrics"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/DeviceMetrics"}}}}}}},"/api/caregiver":{"post":{"tags":["caregiver-controller"],"summary":"Create caregiver","operationId":"createCaregiver","requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/Caregiver"}}},"required":true},"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/Caregiver"}}}}}}},"/api/gdprrequest/{id}/status/{status}":{"patch":{"tags":["gdpr-request-controller"],"summary":"Add gdpr request status","operationId":"addGdprRequestStatus","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"status","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/GdprRequest"}}}}}}},"/api/patients":{"get":{"tags":["patient-controller"],"summary":"Get all patients in database","operationId":"getPatients","responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Patient"}}}}}}}},"/api/patients/{id}/clinicians":{"get":{"tags":["patient-controller"],"summary":"Get all patient assignments to clinicians by patient id","operationId":"getClinicianAssignmentsByPatientId","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/ClinicianAssignment"}}}}}}},"/api/patients/pilot/{id}":{"get":{"tags":["patient-controller"],"summary":"Get all patients by pilot id","operationId":"getPatientsByPilot","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Patient"}}}}}}},"/api/patients/pilot/{id}/recruitment/{status}":{"get":{"tags":["patient-controller"],"summary":"Get all patients by pilot id and recruitment status","operationId":"getPatientsByPilotAndRecruitmentStatus","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"status","in":"path","required":true,"schema":{"type":"int

eger","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{
"$ref":"#/components/schemas/Patient"}}}}}}}},"/api/patients/organisation/{id}":{"get":{"tags":["patient-
controller"],"summary":"Get all patients by organisation
id","operationId":"getPatientsByOrganisation","parameters":[{"name":"id","in":"path","required":true,"schema":{"typ
e":"integer","format":"int32"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","it
ems":{"$ref":"#/components/schemas/Patient"}}}}}}}},"/api/patients/organisation/{id}/recruitment/{status}":{"get":{"
tags":["patient-controller"],"summary":"Get all patients by organisation id and recruitment
status","operationId":"getPatientsByOrganisationAndRecruitmentStatus","parameters":[{"name":"id","in":"path","req
uired":true,"schema":{"type":"integer","format":"int32"}},{"name":"status","in":"path","required":true,"schema":{"ty
pe":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","
items":{"$ref":"#/components/schemas/Patient"}}}}}}}},"/api/patient/{id}/images":{"get":{"tags":["patient-
controller"],"summary":"Get all patient's images by patient
id","operationId":"getPatientImages","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integ
er","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$
ref":"#/components/schemas/Image"}}}}}},"delete":{"tags":["patient-controller"],"summary":"Delete all patient
images","operationId":"deletePatientImages","parameters":[{"name":"id","in":"path","required":true,"schema":{"typ
e":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","
enum":["100 CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201
CREATED","202 ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205
RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300
MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303
SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308
PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403
FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407
PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411
LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413
REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415
UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418
I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421
DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425
TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431
REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500
INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504
GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507
INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511
NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/patient/{id}/image/{imageId}":{"get":{"tags":["patient-
controller"],"operationId":"getImage","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"inte
ger","format":"int64"}},{"name":"imageId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],
"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"type":"string","format":
"byte"}}}}}}},"delete":{"tags":["patient-controller"],"summary":"Delete patient
image","operationId":"deletePatientImage","parameters":[{"name":"id","in":"path","required":true,"schema":{"type"
:"integer","format":"int64"}},{"name":"imageId","in":"path","required":true,"schema":{"type":"integer","format":"int
64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100
CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202
ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206
PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300
MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303
SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308
PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403
FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407
PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411
LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413
REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415
UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418

I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/patient/{id}/identities":{"get":{"tags":["patient-controller"],"summary":"Get all patient identities by patient id","operationId":"getPatientIdentities","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Identity"}}}}}}}},"/api/patient/{id}/gdpr_requests":{"get":{"tags":["patient-controller"],"summary":"Get all GDPR requests by patient id","operationId":"getPatientGdprRequests","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/GdprRequest"}}}}}}},"/api/patient/{id}/devices":{"get":{"tags":["patient-controller"],"summary":"Get all patient devices by patient id","operationId":"getPatientDevices","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Device"}}}}}}},"/api/patient/{id}/contact-phones":{"get":{"tags":["patient-controller"],"summary":"Get patient's contact phones","operationId":"getPatientContactPhones","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/ContactPhone"}}}}}}},"/api/patient/{id}/caregivers":{"get":{"tags":["patient-controller"],"summary":"Get all patient's caregivers by patient id","operationId":"getPatientCaregivers","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Caregiver"}}}}}}},"/api/gdprrequests":{"get":{"tags":["gdpr-request-controller"],"summary":"Get all gdpr requests","operationId":"getGdprRequests","responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/GdprRequest"}}}}}}},"/api/gdprrequest/{id}":{"get":{"tags":["gdpr-request-controller"],"summary":"Get gdpr request by id","operationId":"getGdprRequest","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"$ref":"#/components/schemas/GdprRequest"}}}}}}},"/api/gdprrequest/{id}/files":{"get":{"tags":["gdpr-request-controller"],"summary":"Get all gdpr request files by gdpr request id","operationId":"getGdprRequestFiles","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/GdprRequestFile"}}}}}}},"/api/gdprrequest/{id}/file/{fileId}":{"get":{"tags":["gdpr-request-controller"],"summary":"Get gdpr request file by file id","operationId":"getGdprRequestFile","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}},{"name":"fileId","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"type":"string","format":"byte"}}}}}}},"/api/devices":{"get":{"tags":["device-controller"],"summary":"Get all devices","operationId":"getAllDevices","responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Device"}}}}}}},"/api/clinician/{id}/notifications":{"get":{"tags":["clinician-assignment-controller"],"summary":"Get all notifications for a clinician","operationId":"getClinicianNotifications","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/Notification"}}}}}}},"/api/clinician/{id}/assignments":{"get":{"tags":["clinician-assignment-controller"],"summary":"Get all assignments for a clinician","operationId":"getClinicianAssignments","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"array","items":{"$ref":"#/components/schemas/ClinicianAssignment"}}}}}}},"/api/caregivers":{"get":{"tags":["caregiver-

controller"],"summary":"Get all
caregivers","operationId":"getCaregivers","responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":
"array","items":{"$ref":"#/components/schemas/Caregiver"}}}}}}}},"/api/patient/{id}/identity/{identityId}":{"delete":{"
tags":["patient-controller"],"summary":"Delete identity from
patient","operationId":"deleteIdentityFromPatient","parameters":[{"name":"id","in":"path","required":true,"schema"
:{"type":"integer","format":"int64"}},{"name":"identityId","in":"path","required":true,"schema":{"type":"integer","for
mat":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100
CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202
ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206
PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300
MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303
SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308
PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403
FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407
PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411
LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413
REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415
UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418
I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421
DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425
TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431
REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500
INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504
GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507
INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511
NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}}},"/api/patient/{id}/gdpr_request/{gdprRequestId}":{"delete":{"tags":[
"patient-controller"],"summary":"Delete GDPR request from
patient","operationId":"deletePatientGdprRequest","parameters":[{"name":"id","in":"path","required":true,"schema"
:{"type":"integer","format":"int64"}},{"name":"gdprRequestId","in":"path","required":true,"schema":{"type":"integer"
,"format":"int64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100
CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202
ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206
PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300
MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303
SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308
PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403
FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407
PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411
LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413
REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415
UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418
I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421
DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425
TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431
REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500
INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504
GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507
INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511
NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}}},"/api/patient/{id}/device/{deviceId}":{"delete":{"tags":["patient-
controller"],"summary":"Delete patient's
device","operationId":"deletePatientDevice","parameters":[{"name":"id","in":"path","required":true,"schema":{"type
":"integer","format":"int64"}},{"name":"deviceId","in":"path","required":true,"schema":{"type":"integer","format":"in
t64"}}],"responses":{"200":{"description":"OK","content":{"*/*":{"schema":{"type":"string","enum":["100
CONTINUE","101 SWITCHING_PROTOCOLS","102 PROCESSING","103 CHECKPOINT","200 OK","201 CREATED","202

ACCEPTED","203 NON_AUTHORITATIVE_INFORMATION","204 NO_CONTENT","205 RESET_CONTENT","206 PARTIAL_CONTENT","207 MULTI_STATUS","208 ALREADY_REPORTED","226 IM_USED","300 MULTIPLE_CHOICES","301 MOVED_PERMANENTLY","302 FOUND","302 MOVED_TEMPORARILY","303 SEE_OTHER","304 NOT_MODIFIED","305 USE_PROXY","307 TEMPORARY_REDIRECT","308 PERMANENT_REDIRECT","400 BAD_REQUEST","401 UNAUTHORIZED","402 PAYMENT_REQUIRED","403 FORBIDDEN","404 NOT_FOUND","405 METHOD_NOT_ALLOWED","406 NOT_ACCEPTABLE","407 PROXY_AUTHENTICATION_REQUIRED","408 REQUEST_TIMEOUT","409 CONFLICT","410 GONE","411 LENGTH_REQUIRED","412 PRECONDITION_FAILED","413 PAYLOAD_TOO_LARGE","413 REQUEST_ENTITY_TOO_LARGE","414 URI_TOO_LONG","414 REQUEST_URI_TOO_LONG","415 UNSUPPORTED_MEDIA_TYPE","416 REQUESTED_RANGE_NOT_SATISFIABLE","417 EXPECTATION_FAILED","418 I_AM_A_TEAPOT","419 INSUFFICIENT_SPACE_ON_RESOURCE","420 METHOD_FAILURE","421 DESTINATION_LOCKED","422 UNPROCESSABLE_ENTITY","423 LOCKED","424 FAILED_DEPENDENCY","425 TOO_EARLY","426 UPGRADE_REQUIRED","428 PRECONDITION_REQUIRED","429 TOO_MANY_REQUESTS","431 REQUEST_HEADER_FIELDS_TOO_LARGE","451 UNAVAILABLE_FOR_LEGAL_REASONS","500 INTERNAL_SERVER_ERROR","501 NOT_IMPLEMENTED","502 BAD_GATEWAY","503 SERVICE_UNAVAILABLE","504 GATEWAY_TIMEOUT","505 HTTP_VERSION_NOT_SUPPORTED","506 VARIANT_ALSO_NEGOTIATES","507 INSUFFICIENT_STORAGE","508 LOOP_DETECTED","509 BANDWIDTH_LIMIT_EXCEEDED","510 NOT_EXTENDED","511 NETWORK_AUTHENTICATION_REQUIRED"]}}}}}}},"/api/clinician/{id}":{"delete":{"tags":["clinician-assignment-controller"],"summary":"Delete a clinician","operationId":"deleteClinician","parameters":[{"name":"id","in":"path","required":true,"schema":{"type":"integer","format":"int64"}}],"responses":{"200":{"description":"OK"}}}}},"components":{"schemas":{"Patient":{"required":["fullName","homeAddress"],"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"fullName":{"type":"string"},"birthDate":{"pattern":"(0[1-9]|1[0-2])/\\d{4}","type":"string"},"homeAddress":{"type":"string"},"homeZip":{"type":"string"},"phoneNumber":{"type":"string"},"email":{"type":"string"},"organisationId":{"type":"integer","format":"int32"},"pilotId":{"type":"integer","format":"int64"},"recruitmentStatus":{"type":"integer","format":"int64"},"consentDate":{"type":"string","format":"date-time"},"createdByClinicianId":{"type":"integer","format":"int64"}}},"ContactPhone":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"phone":{"type":"string"},"dialCode":{"type":"string"},"iso2":{"type":"string"}}},"Caregiver":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"email":{"type":"string"}}},"ClinicianAssignment":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"clinicianId":{"type":"integer","format":"int64"},"accepted":{"type":"boolean"},"assignedAt":{"type":"string","format":"date-time"},"respondedAt":{"type":"string","format":"date-time"}}},"Identity":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"identityId":{"type":"string"},"assigner":{"type":"string"},"scope":{"type":"integer","format":"int64"},"status":{"type":"integer","format":"int64"}}},"GdprRequest":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"requestee":{"type":"string"},"category":{"type":"integer","format":"int64"},"status":{"type":"integer","format":"int64"},"about":{"type":"string"},"inform":{"type":"integer","format":"int64"},"gdprRequestFile":{"uniqueItems":true,"type":"array","items":{"$ref":"#/components/schemas/GdprRequestFile"}}}},"GdprRequestFile":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"title":{"type":"string"},"filepath":{"type":"string"},"description":{"type":"string"},"status":{"type":"integer","format":"int64"}}},"Device":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"serial":{"type":"string"},"endUserId":{"type":"string"},"status":{"type":"integer","format":"int64"},"deviceTypeId":{"type":"integer","format":"int64"},"lastUsed":{"type":"string","format":"date-time","readOnly":true}}},"DeviceMetrics":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"transmissionDate":{"type":"string","format":"date-time","readOnly":true},"valid":{"type":"boolean"}}},"Image":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"title":{"type":"string"},"filepath":{"type":"string"}}},"Notification":{"type":"object","properties":{"id":{"type":"integer","format":"int64","readOnly":true},"message":{"type":"string"}}}}}}

---------- end of code ----------

8.2 Detailed Design of CSB@SecurityComponent Functionality

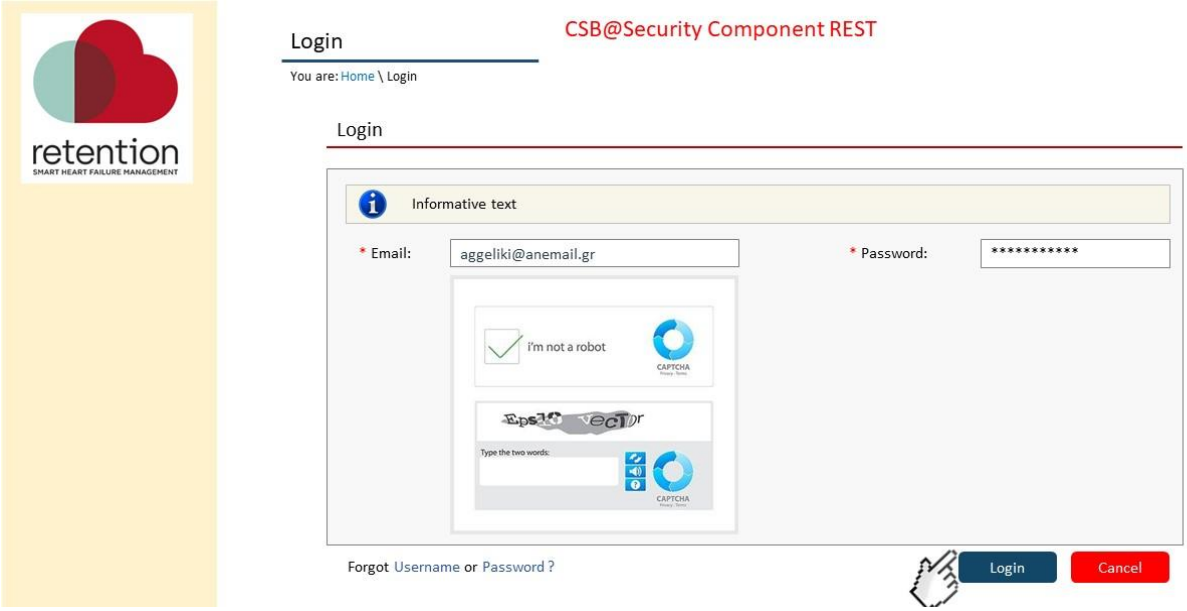

Figure 17: Design mock-up: end-user's login requires also a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to be performed to protect RETENTION platform from spam and login-password repeated attemprs by bots.

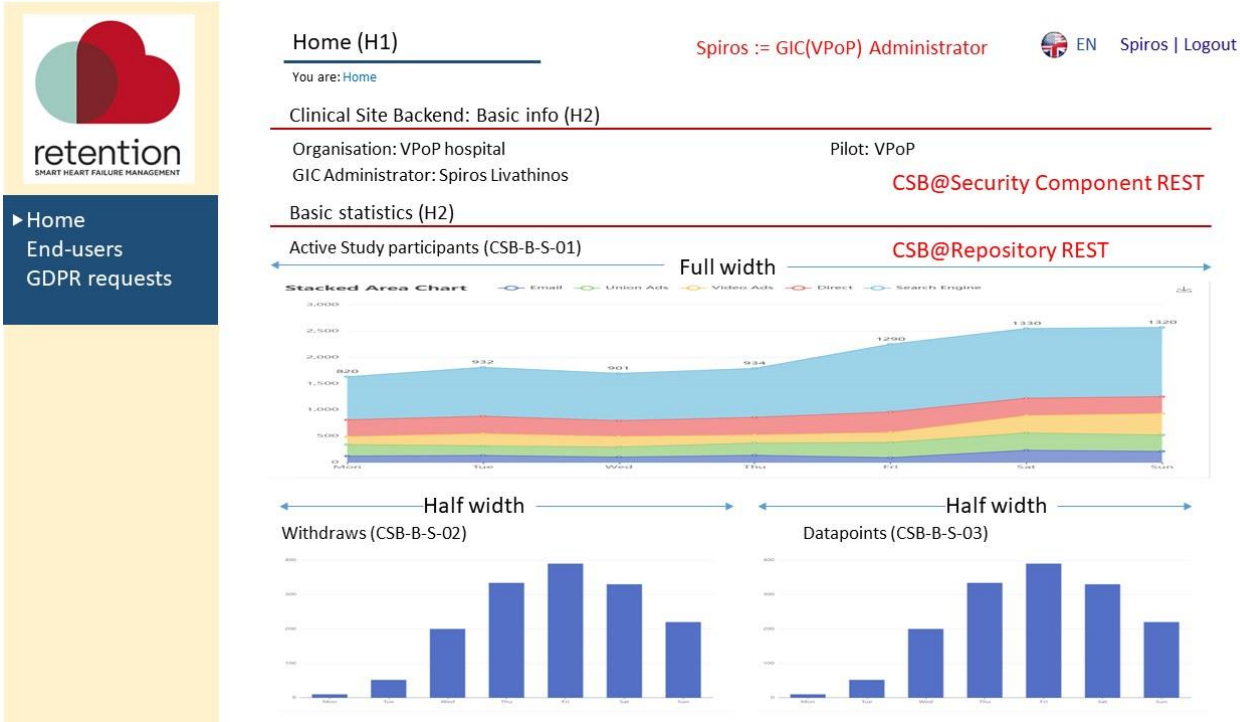

Figure 18: Design mock-up: home page of a previously authenticated CSB end-user.

Figure 19: Design mock-up: CSB administrator views existing end-users and can create a new one.

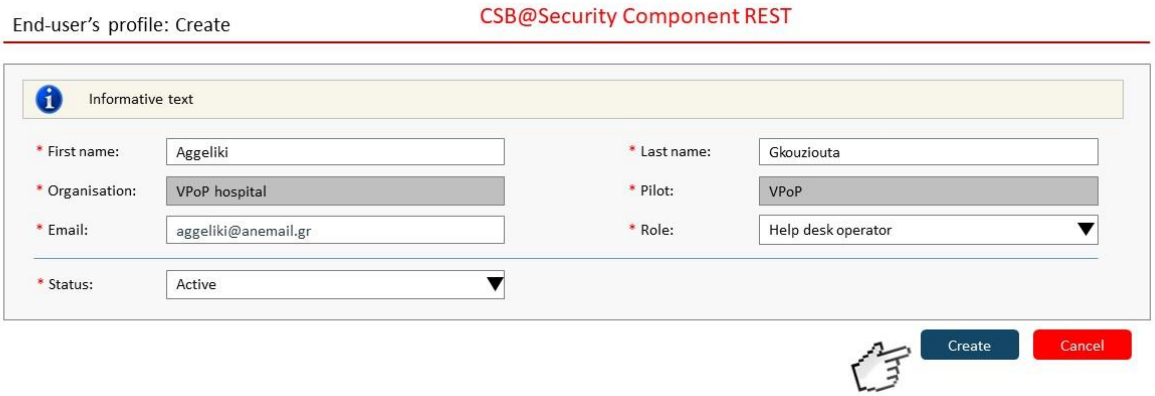

Figure 20: Design mock-up: End-user creation form: CSB administrator fills nessesary profile information (fullname, email, and granded role) to trigger the creation.

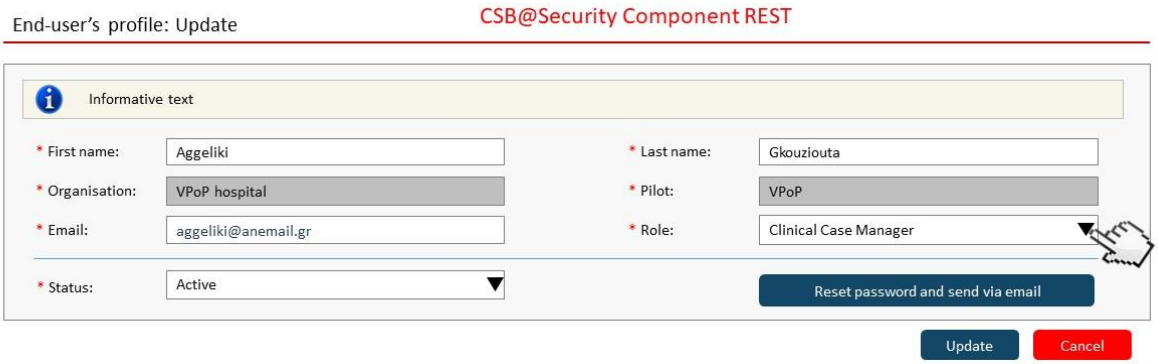

Figure 21: Design mock-up: End-user edit form: CSB administrator may also alter end-user's profile information and reset his/her password.

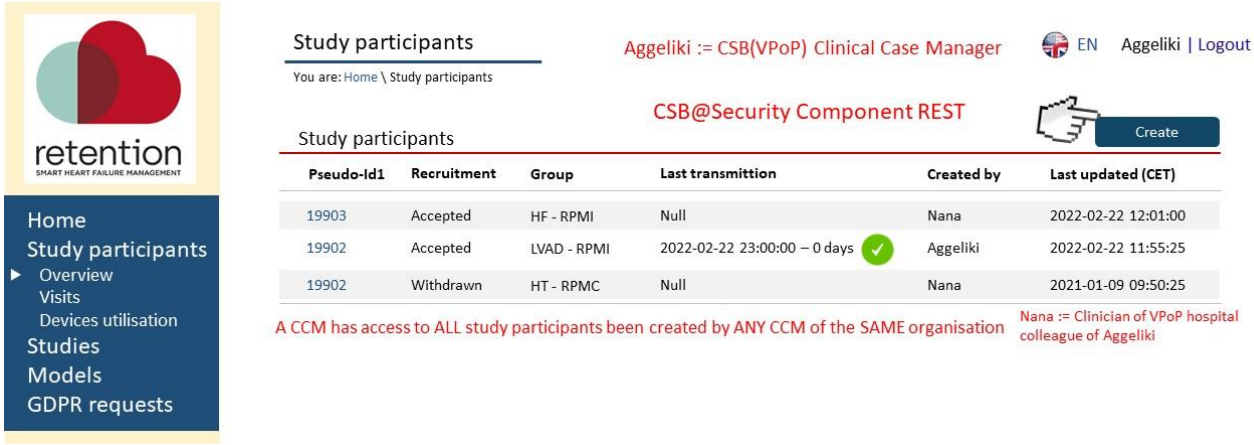

Figure 22: Design mock-up: CSB Clinical Case Manager manages existing study participants (of the particular pilot) and may initiate the creation process.

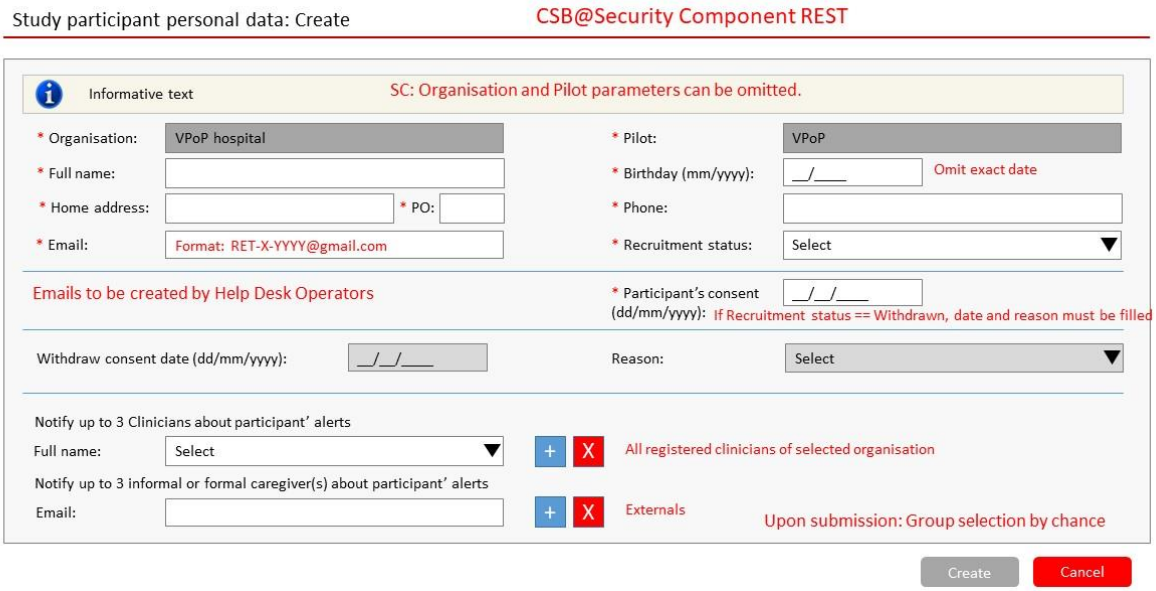

Figure 23: Design mock-up: Create a study particiopant: CSB Clinical Case Manager fills in the nessesary information (fullname, birthday, home address details, phone), inserts an Gmail email account to be used for login to a Google account in order to download newer version(s) of RETENTION mobile application (if occur), along with reqruitment details and those to be conducted in case of an emergency. Upon triggering the creation, all 3 identifiers to be created, while the group (remote patient monitoring and interventions – RPMI, or remote patient monitoring and usual care - RPMUC group) is randomly selected.

Figure 24: Design mock-up: CSB Clinical Case Manager (or Help Desk Operator) may assign devices to a previously created study participant.

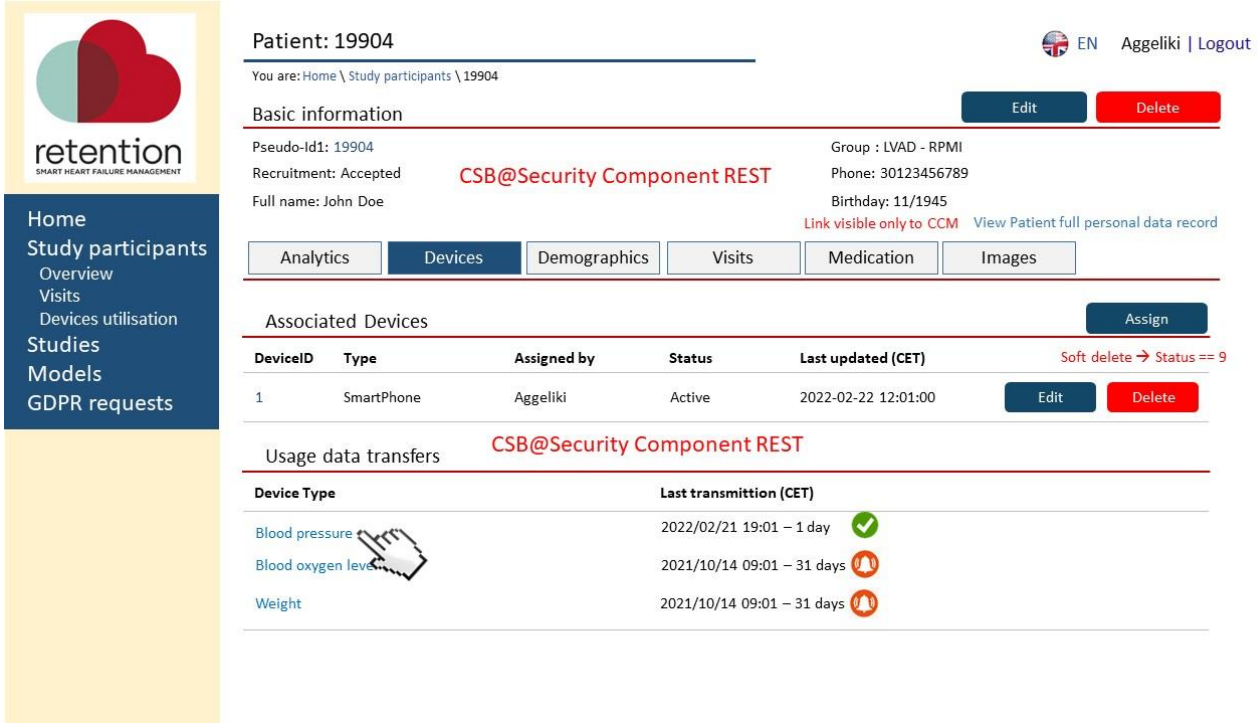

Figure 25: Design mock-up: CSB Clinical Case Manager (or Help Desk Operator) can monitor latest trasmitions per device type.

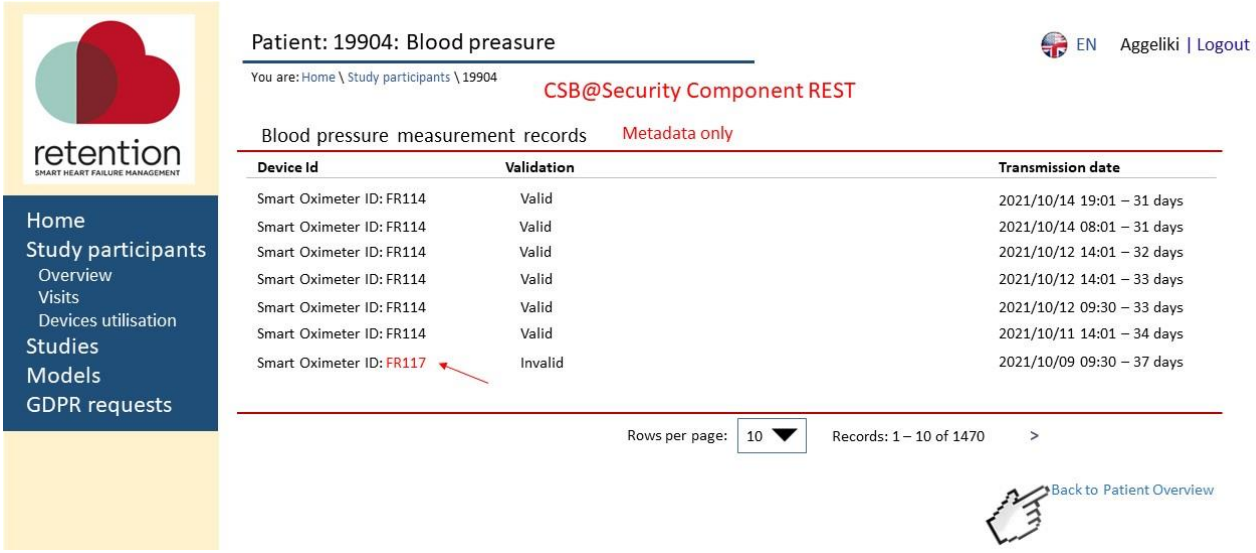

Figure 26: Design mock-up: CSB Clinical Case Manager (or Help Desk Operator) can view metadata of all device usage data trasmitions.

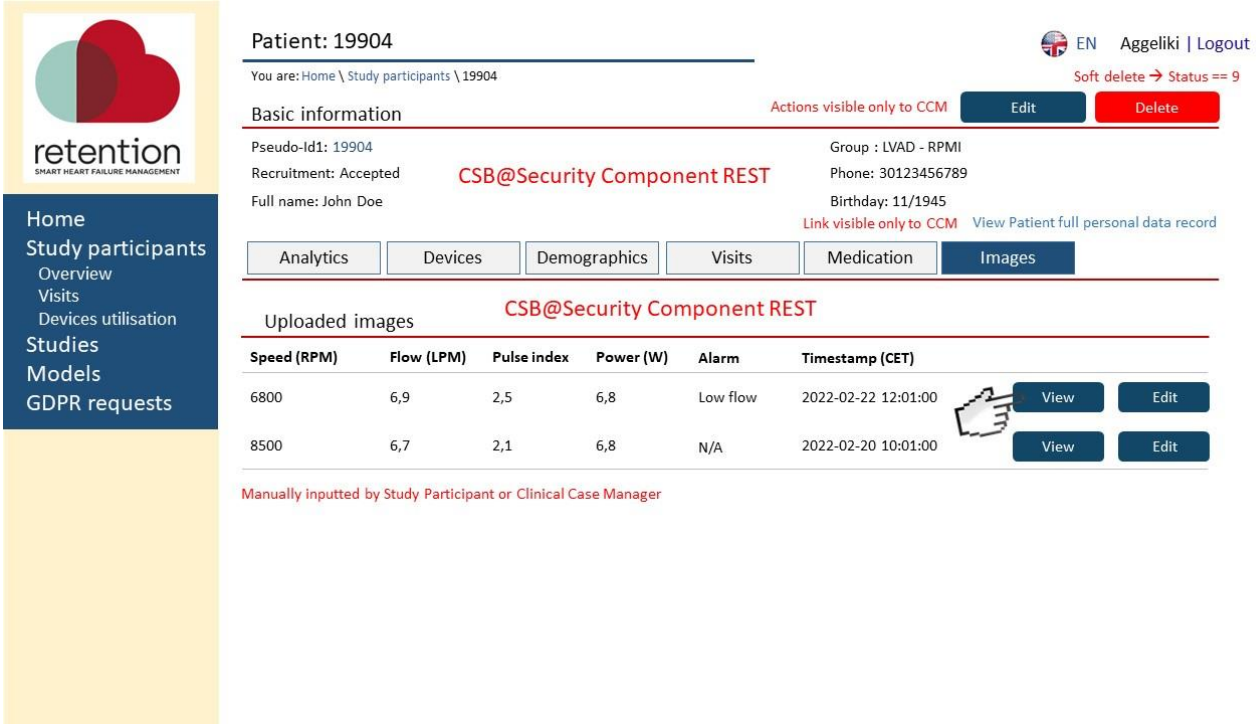

Figure 27: Design mock-up: CSB Clinical Case Manager can view and manage screenshots (photos of the Left Ventricular Assist Devices monitor) providing daily measurements (e.g., pump flow, pump speed, pulsatility index, pump power, alarrm) sent to the CSB by the study participant via a RETENTION mobile application mechanism.

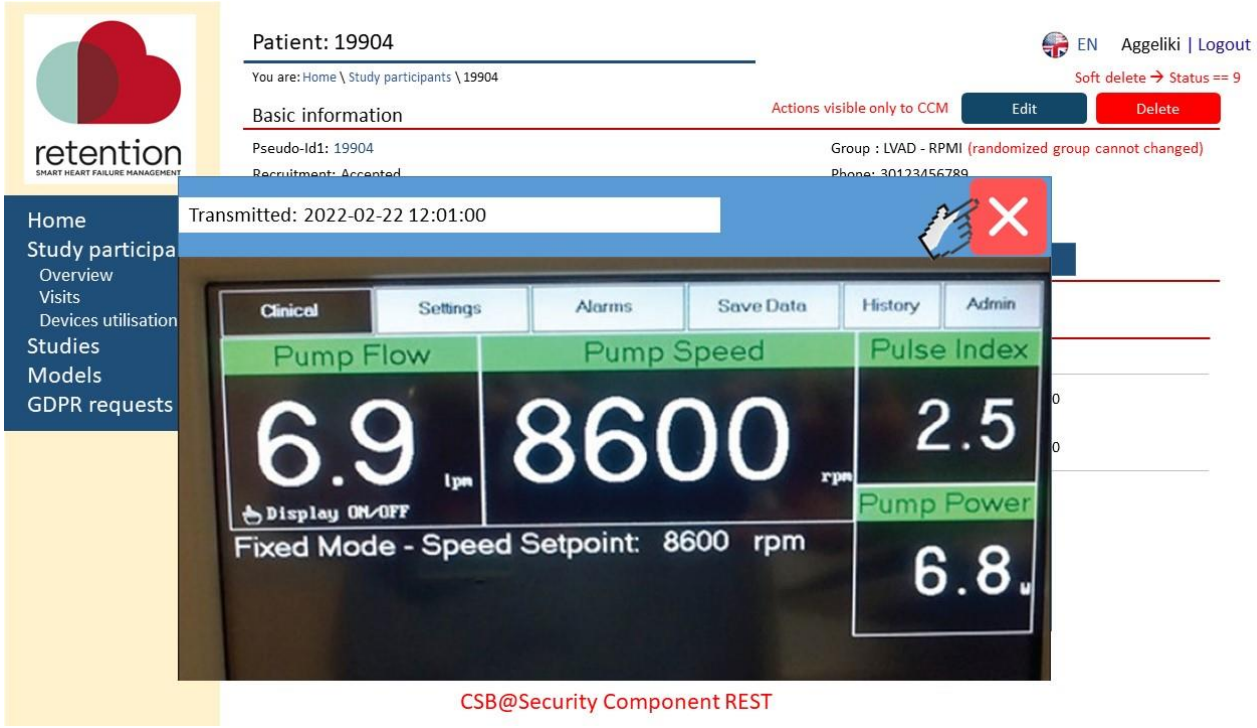

Figure 28: Design mock-up: CSB Clinical Case Manager can view measuremet indicated by screenshots, review the correctness of the measurments values inputed by the study participant and (if nessesary) correct them.