D6.2

Software requirements and architecture specification of a S-EHR - V2

ABSTRACT

Fundamental technical results of InteropEHRate will be composed of two aspects. The first one will be a set of open specifications, implementable by any vendor or institution. The second technical result will be a reference implementation composed of reusable software components, which will implement the specifications and will be interoperable with any other implementation of the same specifications. This document focuses on the requirements and the reference implementation of one of the components; the S-EHR mobile app (S-EHR-A). This document provides architecture specifications, screens and screen mock-ups, description of workflow and technology used for the S-EHR-A.

Delivery Date	May 29th, 2020
Work Package	WP6
Task	T6.1
Dissemination Level	Public
Type of Deliverable	Report
Lead partner	Andaman7

InteropEHRate project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106.

This document has been produced in the context of the InteropEHRate Project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106. All information provided in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose.

CONTRIBUTORS

	Name	Partner
Contributors	Martin Marot, François Sevrin, Lucie Keunen	A7
Contributor	Juan Fernandez	EFN
Reviewer	Chrysostomos Symvoulidis	BYTE
Reviewer	Marcel Klötgen	FRAU

LOG TABLE

Version	Date	Change	Author	Partner
0.1	2020-02-06	First draft of ToC	Martin Marot	A7
0.2	2020-02-10	First draft of ToC	Martin Marot	A7
0.3	2020-02-17	Review and feedback on ToC	Lucie Keunen	A7
0.4	2020-02-17	Comments and input	Juan Fernandez	EFN
0.5	2020-03-12	Second draft of ToC	Martin Marot	A7
0.6	2020-03-13	Second draft of ToC	Martin Marot	A7
0.7	2020-04-06	Update content	Martin Marot	A7
0.8	2020-04-07	Update content	Martin Marot François Sevrin	A7
0.9	2020-04-08	Update content	Martin Marot François Sevrin	A7
0.10	2020-04-09	Update content	Martin Marot François Sevrin Julien Henrard	A7
0.11	2020-04-14	Update content	Martin Marot François Sevrin	A7
0.13	2020-04-23	Review of wording and formatting	Lucie Keunen	A7
0.14	2020-04-24	Review of wording and	Lucie Keunen	A7

		formatting		
1.0	2020-04-28	First internal review	Chrysostomos Symvoulidis	BYTE
1.1	2020-04-29	Second internal review	Marcel Klötgen	FRAU
1.2	2020-05-06	Correction following review	Francois Sevrin	A7
1.3	2020-05-07	Correction following review	Francois Sevrin	A7
1.4	2020-05-11	Correction of acronym usage based on last comment received	Lucie Keunen	A7
1.5	2020-05-12	Correction following review	Francois Sevrin	A7
1.6	2020-05-12	Minor corrections regarding the naming of figures and titles + slight reordering of subsections + update of section "updates regarding previous version"	Lucie Keunen	A7
1.7	2020-05-12	Quality review	Argyro Mavrogiorgou	UPRC
1.8	2020-05-12	Fixed numbering of figures	Lucie Keunen	A7
1.9	2020-05-18	Addressed new comments from ENG review	François Sevrin	A7
1.10	2020-05-21	Final review	Laura Pucci Francesco Torelli	ENG
1.11	2020-05-26	Addressed few comments regarding consistency of wording with other deliverables and accuracy of some paragraphs	Lucie Keunen	A7
1.12	2020-05-27	Updated sections "Process to define software requirements" and "Conclusion"	Lucie Keunen	A7
VFinal	2020-05-29	Final check and submission	Laura Pucci	ENG

ACRONYMS

Acronym	Term and definition
API	Application Program Interface
CA	Certification Authority
CEF	Connecting Europe Facility
D2D	Device to Device
eCOA	Electronic Clinical Outcome Assessment
EHR	Electronic Health Record
eID	Electronic identification
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HCP	Healthcare Professional
HQ	Headquarter
HR	Health Record
IRS	InteropEHRate Research Service
IT	Information Technology
QR code	Quick Response code
R2D	Remote to Device
S-EHR	Smart Electronic Health Record
S-EHR-A	Reference implementation of S-EHR
TEE	Trusted Execution Environment

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. Scope of the document

This document provides the software requirements specification of the S-EHR-A, which is the reference implementation of a S-EHR, able to import/share data from/with EHRs and with research centres, using short-range wireless D2D (device to device) communication or remote communication protocols.

This document presents the design of the S-EHR-A based on the user requirements defined for the first year of the InteropEHRate project. It will also describe the design of future features to be implemented in the S-EHR-A.

1.2.Intended audience

The document is intended for all people interested in having an overview of the design, workflow and ideas of improvement of the S-EHR-A and core application.

1.3.Structure of the document

This document is structured into seven sections:

1. **Introduction**: description of the purpose and objectives of this document, the intended audience that can be interested to read it, and the structure of the document;
2. **Software requirements of a S-EHR**: definition of the purpose and objectives of a S-EHR and the S-EHR-A;
3. **Andaman7 as the core app for the S-EHR-A (reference implementation of a S-EHR)**: description of the application used as a base to create the S-EHR-A, and the user requirements that are already covered by this application;
4. **Definition of the user requirements not yet implemented for the S-EHR-A**: definition of the user requirements not covered by the core application, and explanation of how it will be through the wireframe model. This section also contains explanations on the interactions between each feature;
5. **Improvement of the S-EHR-A**: ideas to improve the user experience and the design of the S-EHR-A;
6. **Design of the S-EHR-A**: visual mockups for each wireframe described in the previous section;
7. **Conclusions and next steps**: conclusion of this document.

1.4.Updates with respect to previous version

- Update of the section “Process to define software requirements”;
- Addition of the section “User requirements for version 2 of the S-EHR-A”;
- Addition of the section “New features of the S-EHR-A” to include:
  - The addition of the new section “User flow of S-EHR R2D protocol”;
  - The addition of the new section “Security of the S-EHR-A”;
- Update of the section “User requirements already implemented by the core application”;
- Update of the section “New user requirements for the S-EHR-A already implemented”:

- Section renamed “Requirements integrated in existing features of the core app”
    - Update of the section “R2D import of data from national EHR on S-EHR”;
    - Addition of the section “Consultation of auditing health data sharing for citizen on S-EHR”;
- Update of the section “New user requirements for the S-EHR-A not yet implemented”:
    - Section renamed “Requirements integrated as new features of the core app”;
    - Update of the section “D2D visualization of the healthcare organization by the citizen”;
    - Addition of the section “Enabling of citizen identification from S-EHR (with CA)”;
    - Addition of the section “Invitation of candidate citizens to participate to a research study”;
    - Addition of the section “Activation of automatic backup of S-EHR content on selected S-EHR Cloud”;
    - Addition of the section “Sharing of health data with qualified HCPs for emergency by means of S-EHR Cloud”;
    - Addition of the section “Citizen's consent to be part of InteropEHRate Open Research Network”;
    - Addition of the section “Citizen's access to emergency token”;
    - Addition of the section “Citizen's withdrawing from research network”;
    - Addition of the section “Citizen's consent to share health data for a research protocol”;
    - Addition of the section “Reception and storage of consent, digitally signed from research organisation, on citizen's S-EHR”;
- Update of the section “Visual Mockup of S-EHR-A based on user requirements”:
    - Section renamed “Screens and mockups of the S-EHR-A based on user requirements”
    - Update of the section “D2D visualization of the healthcare organization by the citizen”;
    - Update of the section “D2D consent by the citizen to healthcare organization for temporary S-EHR access”;
    - Addition of the section “Consultation of health data sharing audit by the citizen on his/her S-EHR”;
    - Addition of the section “Citizen's consent to be part of InteropEHRate Open Research Network”;
    - Addition of the section “Invitation of candidate citizens to participate to a research study”;
    - Addition of the section “Citizen's withdrawing from research network”;
    - Addition of the section “Citizen's consent to share health data for a research study”;
- Update of the section “CONCLUSIONS AND NEXT STEPS”;
- Small changes in other sections such as rephrasing, without changing the meaning.

2. SOFTWARE REQUIREMENTS OF A S-EHR

2.1. S-EHR overview

A S-EHR is an application installed on a personal mobile device (smartphone or tablet), that is able to store the personal health data of a user in a secure (encrypted) way according to the constraints specified by the conformance levels [D3.1] and that supports the InteropEHRate protocols [D4.1][D4.8].

The S-EHR is able to exchange health data with any application that adopts the standard protocols specified by the InteropEHRate project. More specifically, the S-EHR uses the so called Remote to Device (R2D) protocol to exchange health data remotely (with the use of the internet) with healthcare organizations while the Device to device (D2D) protocol allows to exchange health data with healthcare organizations during face to face encounters (without the use of the internet, but adopting short range communication technologies like bluetooth).

The reference implementation of the S-EHR (S-EHR-A) will be used for experimenting with the approach during the validation phases. Starting from the user requirements specified in collaboration with final users and focus groups, a first version of mockups of the S-EHR-A is presented.

Details on the architecture of the S-EHR-A can be found in the design deliverable [D2.4].

2.2. Process to define software requirements

In order to develop new software and create a new product, such as a S-EHR mobile application in this case, the solution has to be designed first.

To begin with, a person or a group of people need to decide what is the general purpose of the project and what kind of solution they seek to achieve this purpose. The general purpose of this project has been depicted in the Grant Agreement of InteropEHRate and addresses issues such as the lack of access and control from the citizens on their own health data. Therefore, this health data, currently locked in silos, cannot be fully exploited for healthcare and research. InteropEHRate aims to address those issues by developing new solutions, based on an innovative citizen-centred, bottom-up approach, and supported by new specifications and standard protocols.

To briefly summarize it, the solution proposed by InteropEHRate project consists of several applications, used by several actors (citizens, also sometimes referred to as patients, healthcare professionals and researchers), that are interoperable. The main specificity of the solution however, is that it is citizen-centred. The citizen is the centrepiece of all data exchanges. He/she is acting as the hub of his/her own data, and is offered the possibility to exchange his/her data with other actors or organisations, such as hospitals, research centres, etc. In this document, the focus is on the application used by the citizen, referred to as the S-EHR (Smart-Electronic Health Record).

Once this general purpose and solution have been agreed on, the requirements need to be further defined, in a more granular way. As anyone can imagine, a S-EHR can be packed with a tremendous amount of different features. To get started and help focus the work, the project consortium started from three different use case scenarios: “Medical visit abroad”; “Emergency access”; and “Health research study”. Then, each of these scenarios is broken down into different steps: the user requirements. This work requires the participation of many stakeholders. Especially that in this project, the consortium opted for a "co-design" approach, involving the final users in the design of the different versions of the solution. More details on the description of the user requirements for each scenario can be read in the deliverables dedicated to this topic [D2.1] [D2.2].

It is only after all those discussions and decisions that we can achieve the next steps: translating the user requirements into software requirements. The user requirements are expressed as "user stories[1]", for example: "a European citizen should be able to download the S-EHR application on his/her smartphone". The software requirements consist of all technical specifications required to achieve that goal, for example, the steps needed to create the application and make it available for download on the Play Store and/or the App Store (platforms to download applications for Android and iOS respectively).

Most of the time, the process of translating user requirements into software requirements requires back and forth discussions with the final users or the other partners involved in the development of the solution. Thus, the software requirements of the S-EHR-A evolve as new versions of the solution are designed and developed, and that the consortium refine its understanding of how the project's solutions can best tackle the challenges addressed by the InteropEHRate project. In this document, we will present software requirements as they are at month 15 of the InteropEHRate project[2].

2.3. User requirements for version 1 of the S-EHR-A

At the end of the first requirements gathering cycle, the following requirements were identified (here are presented the requirements that were implemented within the first version).

User requirement title	User requirement description
S-EHR download from the Android store	The S-EHR is downloadable from the Android store (aka the Play Store). The citizen downloads the S-EHR from the Play Store and installs it on its Android device.
S-EHR download from the iOS store	The S-EHR is downloadable from the iOS store (aka the App Store). The citizen downloads the S-EHR from the App Store and installs it on its iOS device.
S-EHR runs on Android smartphone	The S-EHR is a mobile app that can run on Android version X
S-EHR runs on iOS smartphone	The S-EHR is a mobile app that can run on iOS version X
Consent to S-EHR data management	At installation, the S-EHR app obtains from the citizen his/her consent (informed consent) to store and manage his/her personal health data on the smart device.
Enabling of Citizen identification from S-EHR (without CA)	The S-EHR stores and sends to the HCP App the identification data of the citizen (the identification data allows the HCP to confirm the identity of the citizen by comparing them with the ID card of the Citizen).

[1] User stories are part of an agile approach that helps shift the focus from writing about requirements to talking about them. All agile user stories include a written sentence or two. User stories are short, simple descriptions of a feature told from the perspective of the person who desires the new capability, usually a user or customer of the system.

[2] March 2020.

R2D import of (a portion of) the Patient Summary from a national EHR on the S-EHR	Citizen health data (a portion of the Patient Summary) can be imported from the citizen’s national EHR on the citizen’s S-EHR.
R2D import of (a portion of) the prescriptions from a national EHR on the S-EHR	Citizen health data (a portion of the prescriptions) can be imported from the citizen’s national EHR on the citizen’s S-EHR.
D2D device pairing	The citizen connects/pairs his/her smart device to the HCP computer/device.
D2D visualization of the healthcare organization by the citizen	The citizen sees on the S-EHR the data describing the identity of the healthcare organization.
D2D access consent to healthcare organization by the citizen	The citizen gives his/her consent to the healthcare organization to get his/her identifying data
D2D consent by the citizen to a healthcare organization for temporary S-EHR access	The citizen may give his/her temporary consent, to all HCP belonging to a specific healthcare organization and involved in a specific care/treatment, to download data from the S-EHR and upload the updated/acquired data back to the S-EHR.

Table 1 - User requirements for the first version of the S-EHR-A

2.4. User requirements for version 2 of the S-EHR-A

At the end of the second requirements gathering cycle, the following requirements were identified (here are presented the requirements that will be implemented within the second version).

User requirement title	User requirement description
R2D import of (a portion of) Laboratory result from the national health care system on the S-EHR	Citizen’s health data (a portion of Laboratory results) can be imported from the citizen's national health care system on the citizen’s S-EHR.
R2D import of (a portion of) Medical images and reports from the national health care system on the S-EHR	Citizen’s health data (a portion of reports and Medical images) can be imported from the citizen's national health care system on the citizen’s S-EHR.
R2D import of (a portion of) Prescription from the national health care system on the S-EHR	Citizen’s health data (a portion of Prescriptions) can be imported from the citizen's national health care system on the citizen’s S-EHR.
R2D import of (a portion of) Patient Summary from the national health care system on the S-EHR (with security)	Citizen’s health data (a portion of Patient Summary) can be imported from the citizen's national health care system on the citizen’s S-EHR.
Consultation of health data sharing audit by the citizen on the S-EHR	Any audited sharing operation on health data (sharing, authorization) is consultable from the citizen that is the owner of the data.
Enabling of citizen identification from the S-EHR (with CA)	The S-EHR asks the citizen his identity and stores on the device a qualified certificate that identifies the citizen. The certificate is released by a CEF eID trusted certification authority.
Invitation of candidate citizens to participate to a research study	The S-EHR, upon receiving a notification of the publication of a research study, executes a check to verify if the citizen's profile

	matches with research study enrolment criteria. If the matching is positive, the citizen is invited to share his/her health data for the research study.
Activation of automatic backup of the S-EHR content on a selected S-EHR Cloud	Citizens can activate by means of explicit consent the automatic backup of all the health records stored on their S-EHR, on their preferred S-EHR Cloud service (selected in the list of certified S-EHR Cloud services provided by the S-EHR).
Sharing of health data with qualified HCPs for emergency by means of the S-EHR Cloud	Citizens can consent to the access, by HCPs of Healthcare organisations, only for emergency reasons, to their health data stored on the S-EHR Cloud. Giving the consent activates the automatic backup of the health data from the S-EHR to the preferred S-EHR Cloud (selected in the list of certified S-EHR Cloud services provided by the S-EHR). The consent authorises the HCP to access health data using an emergency token or the identification data of the citizen.
Citizen's consent to be part of InteropEHRate Open Research Network	Using their S-EHR, and signing a digital consent, citizens can become part of the InteropEHRate Open Research Network. From that moment, the S-EHR will receive the details of new research studies and will be authorised to match the health data of the citizen with the enrolment criteria of the study (without sending any health data to any party).
Citizen's withdrawal from research network	A citizen may withdraw at any moment, using the S-EHR, his/her participation in the InteropEHRate Research Protocol.
Citizen's consent to share health data for a research protocol	Using the S-EHR, a citizen may give an electronic consent to participate in a specific research protocol, accepting the conditions described within the published formal specification of that research protocol.
Reception and storage of consent, digitally signed by the research organisation, on the citizen's S-EHR	After a consent to participate in a research protocol has been signed on paper by the citizen, an electronic copy of it, digitally signed by the research centre where the consent has been given, is sent to and received by the S-EHR of the citizen, and will be stored permanently within his/her S-EHR.
Citizen's access to emergency token	A citizen may use a S-EHR to access and exchange with other applications an image with his/her "emergency token". The emergency token allows a qualified HCP (authorised by his/her organization) to identify the citizen and access his/her emergency dataset stored on the S-EHR Cloud also if the citizen is unconscious or the S-EHR is not available. To this end the citizen will have to print, preferably on a medal or bracelet, and wear the emergency token produced by the S-EHR.
Storage and download of medical images on S-EHR	A citizen can also enable the storage, and import/download of Medical Images from the EHR or the S-EHR Cloud, on his/her S-EHR if the smart device has enough memory.
Citizen's access to Medical images from S-EHR	A citizen may access from the S-EHR his/her Medical images stored on the S-EHR Cloud or on the S-EHR.

Table 2 - User requirements for the second version of the S-EHR-A

2.5. Software requirements of the S-EHR-A

Each user requirement identified in previous paragraphs needs to be translated into software requirements in order to be implemented in the S-EHR-A.

Before actually starting the implementation, the global architecture for the project and the different technical components have to be defined. It is important so that the S-EHR-A can be nicely integrated with other developed components, and all the components can actually interact with one another. For more details on the global architecture, refer to the document on the subject [D2.4].

After setting up the development environment to start the coding of the S-EHR-A, the consortium decided to work in an "agile" way[3]. What it implies, is that user requirements are not translated into software requirements all in one shot. Instead, user requirements are considered one at a time. This allows the developers to work in a more incremental way, more adapted to software development, and have the advantage to provide the concrete results faster. It is also very efficient to respond rapidly to potential unpredicted difficulties. This is why, in the rest of this document, some of the requirements will not be described in much detail, even though their implementation is foreseen for the second S-EHR-A version, due end of 2020.

[3] The Agile Method is a particular approach to project management that is utilized in software development. This method assists teams in responding to the unpredictability of constructing software. It uses incremental, iterative work sequences that are commonly known as sprints. Definition from Team Linchpin (https://linchpinseo.com/the-agile-method/).

3. ANDAMAN7 AS THE CORE APP FOR THE REFERENCE IMPLEMENTATION OF A S-EHR

For the reference implementation of the S-EHR (S-EHR-A), the InteropEHRate consortium decided not to start from scratch. Instead, it will start from an existing application called Andaman7. Therefore, few user requirements identified by the consortium and not specific to the InteropEHRate protocols were already implemented:

- S-EHR download from iOS store;
- S-EHR runs on iOS smartphone;
- S-EHR download from Android store;
- S-EHR runs on Android smartphone;
- Consent to S-EHR data management.

Also, Andaman7 goes beyond the InteropEHRate specifications on many features, as it is currently the result of approximately 30 man years of development. On the other end, most user requirements needed for the three use case scenarios the project focuses on are not yet implemented in Andaman7.

This section presents the Andaman7 mobile application and briefly describes what it initially already offers. Further in the document, some of the new requirements that will be implemented in the existing core app are described.

3.1. Core application

Andaman7 is a free app designed by patients for patients. Citizens can integrate their complete health history and decide what to share and with whom. They can manage their health with the ones they trust.

Patients and healthcare providers can now access, collect and share their personal and patient's health records. As a citizen you can collect and store your electronic health records, vitals, allergies, medications, vaccinations, hospital admissions, lab results, emergency contacts, health history, medical imaging and more. The app connects with other Apple Health enabled apps and smart devices such as iWatch, weighing scale, glucose meter, blood pressure monitor, medical devices and others.

You can securely share part or all of your records with family members and other healthcare providers. By default, no data is stored in the cloud. Data is stored locally and exchanged directly, from person to person. No one other than you and the people you trust will have access to your data.

All healthcare providers can connect and share health records with patients, outpatient facilities, hospitals, organizations active in clinical studies or research with explicit consent from patients, to participate in patient reported outcomes or experience initiatives.

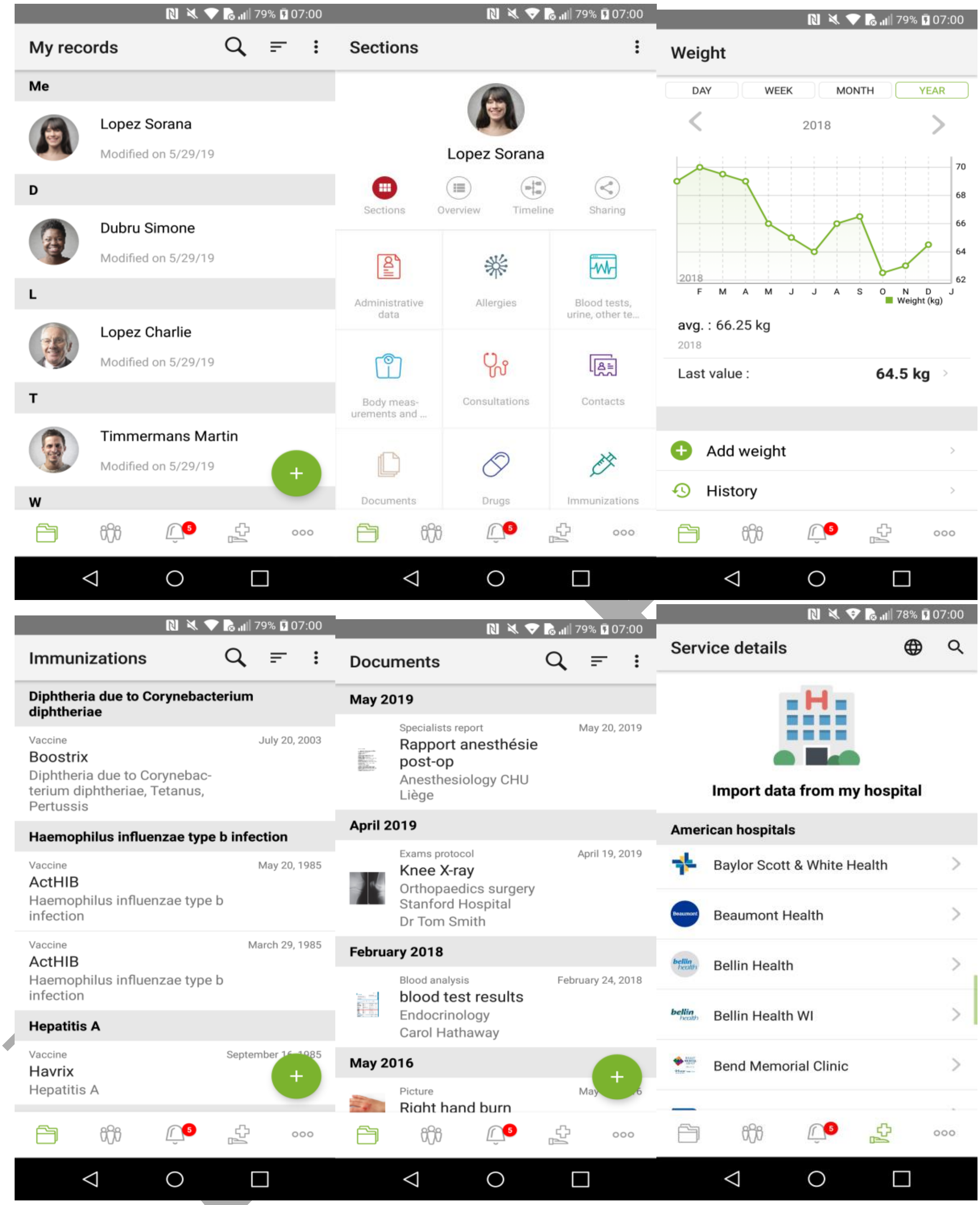


Figure 1 - Screenshots of the core application

3.2. User requirements already implemented by the core application

3.2.1. S-EHR download from Android / iOS store

First of all, citizens need to acquire the application, either via the Play store for Android users, or the App store for iOS users. Once one of these 2 stores is opened, users can simply search for « Andaman7 » and will be able to click a button to download the application.

Users will start using their application with an authentication part. Based on their email address, the core application server will determine if a new account needs to be created or if an account already exists. In the first case, the user will be redirected to the registration part of the application. In the second one, the user will complete the login with his/her password. Now the user can start using the application.

Even if a user already has an account, he/she will not automatically retrieve his/her data because data is not stored on the cloud; everything is stored on the device. There are two ways to retrieve his/her data:

- **Use a backup**: The application provides the possibility to the user to create a backup of his/her data, and to use it to transfer data from his/her old to his/her new device.
- **Share his/her data with a trusted user**: with this option, the application will automatically call a share back of shared data to this trusted user.

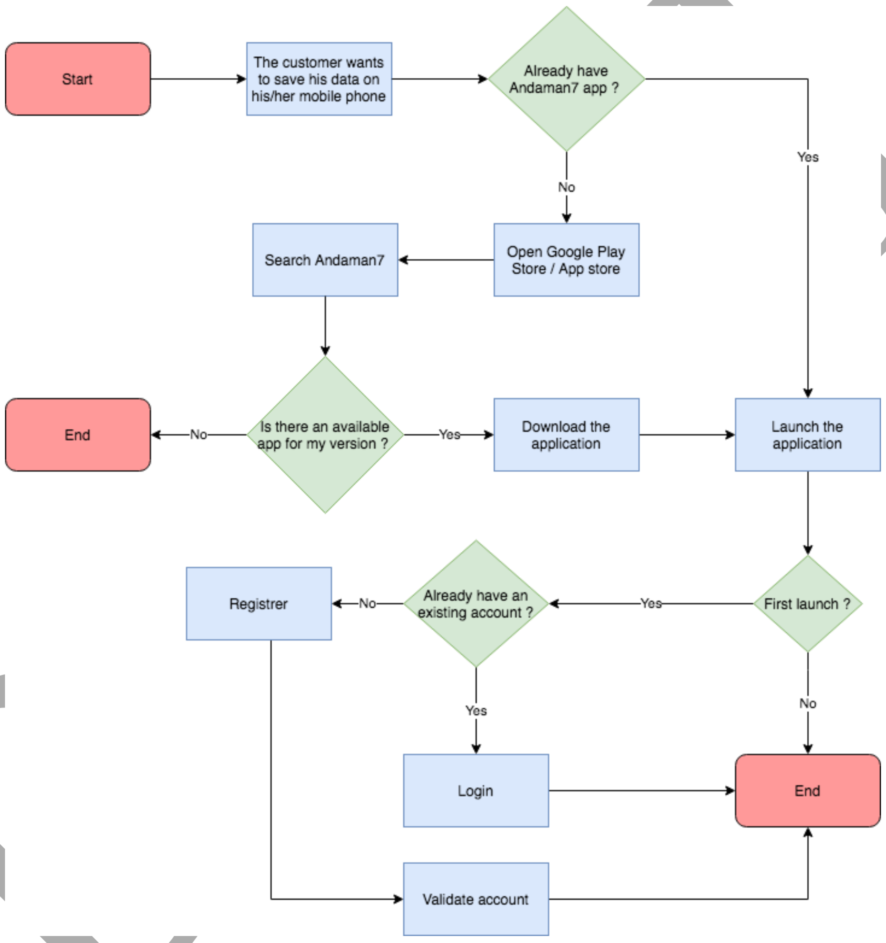

Start
The customer wants to save his data on his/her mobile phone
Already have Andaman7 app ?
Yes
No
Open Google Play Store / App store
Search Andaman7
Is there an available app for my version ?
No
End
Yes
Download the application
Launch the application
First launch ?
Yes
Already have an existing account ?
No
Registrer
Yes
Login
No
End
Validate account

Figure 2 - User flow diagram: Download and launch of the core application

3.2.2. S-EHR runs on Android / iOS smartphone

The S-EHR must be able to run on both Android and iOS smartphones, each application on both operating systems must define the minimum version managed by the application.

For Android, the version is fixed through the properties “minimum sdk version” defined in the properties files of each Android application. At this moment (March 2020), the version goes from 1 to 29 and represents each commercial version of the Android software. For the S-EHR-A, the version will be the one already fixed by the core Android application (16) which corresponds to the Android commercial version “Android 4.1 Jelly Bean JRO03D”.

For iOS, the version is fixed through the properties “iOS deployment target” defined in the project properties of each iOS application. At this moment, the version goes from 1 to 12. For the S-EHR-A, the version will be the one already fixed by the core iOS application (9). The version 9 is the last one supported by Apple. Each year, Apple stops to support the oldest version, and releases a new one.

3.2.3. Consent to S-EHR data management

When the citizen registers to the application (as shown in figure 2), he/she must check a widget to give his/her consent to the core application for the storage and management of his/her data. After the consent is given, and the account is validated, the core application provides some useful functionalities for the S-EHR-A:

- **Add / Update data**: The main functionality of the chosen core application is to store health data on the mobile phone. Data types are sorted in different sections; for example, the data type «Weight» is available in the «Body and measurement» section.
  To add new data, the user must go to the right section and select the type of data he/she wants to add. Then he/she will have the choice to add new data or update an older one.
  In this application, data is never erased. The app keeps in memory every change about a data point. Users have the possibility to see the history of their modifications in a view provided for this purpose.

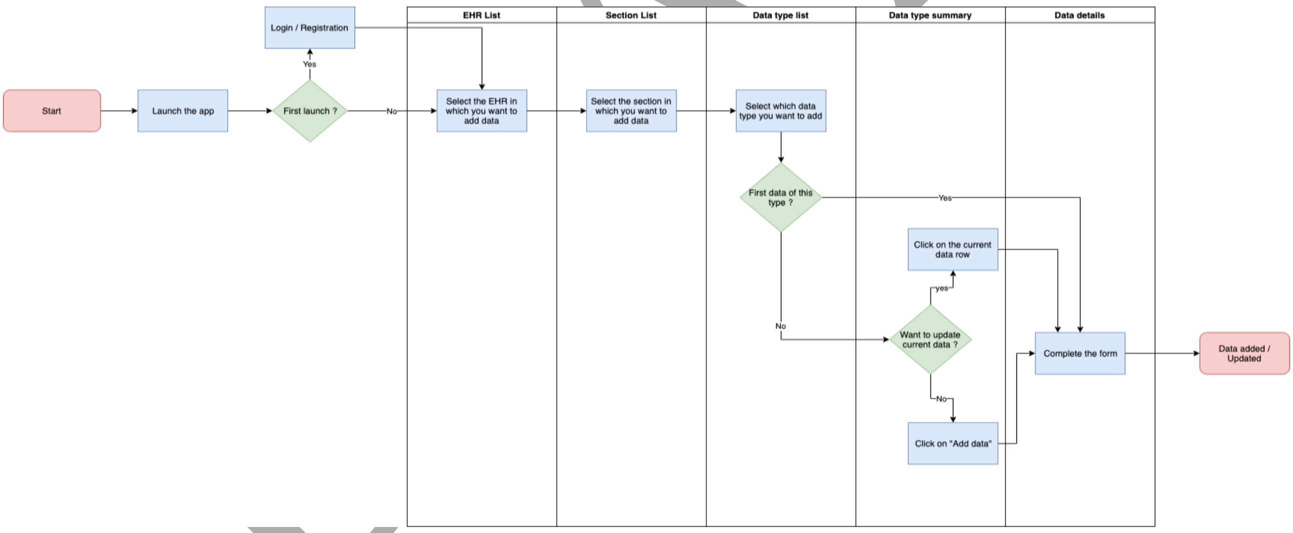

Login / Registration
EHR List
Section List
Data type list
Data type summary
Data details
Yes
Start
Launch the app
First launch ?
No
Select the EHR in which you want to add data
Select the section in which you want to add data
Select which data type you want to add
First data of this type ?
Yes
Click on the current data row
yes
No
Want to update current data ?
Complete the form
Data added / Updated
No
Click on "Add data"

Figure 3 - User flow diagram: Add / Update a data

- **Share data**: Users have the possibility to share their EHR folder to other users. This functionality gives the user two possibilities:
  - The first one is to share his/her health data with his/her healthcare provider (he/she needs to have the application too). The HCP can complete the user’s EHR with new data and share it back to the user. So the user doesn’t need to update his/her data himself.
  - The second one is to share his/her EHR with a trusted user. If the user loses or changes his/her mobile, he/she would have the possibility to easily retrieve his/her data.

Once the user has chosen a trusted user to share his/her data with, he/she can decide which data type he/she wants to share through a selection list.

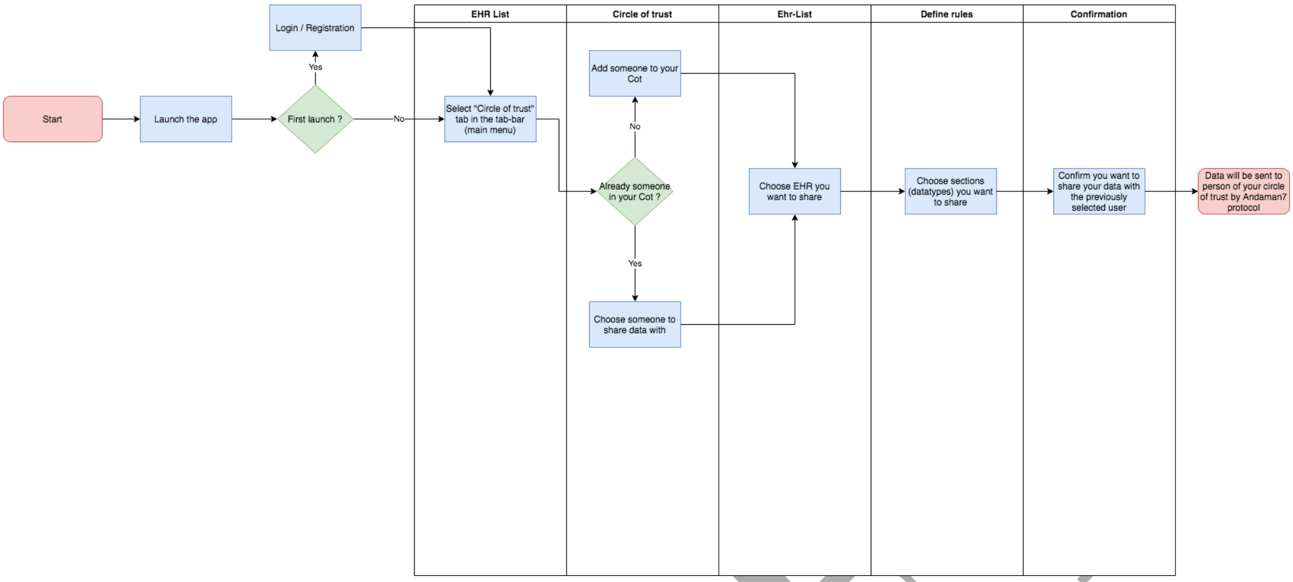

EHR List
Circle of trust
Ehr-List
Define rules
Confirmation
Start
Launch the app
First launch ?
Yes
Login / Registration
No
Select "Circle of trust" tab in the tab-bar (main menu)
Add someone to your Cot
No
Already someone in your Cot ?
Yes
Choose someone to share data with
Choose EHR you want to share
Choose sections (datatypes) you want to share
Confirm you want to share your data with the previously selected user
Data will be sent to person of your circle of trust by Andaman7 protocol

Figure 4 - User flow diagram: Share data

3.3. Integration of new functionalities to the core application to implement the S-EHR-A

The S-EHR-A is divided into two parts, the first one is the core application, which already contains all the necessary features to manage and store the citizen's data. In the case of the InteropEHRate project, this part is managed by the existing Andaman7 application.

The second part contains all the necessary features to connect the mobile application with other actors or organizations, such as hospitals, research centres, etc. It implements the two mobile side protocols of this project:

- the mobile D2D protocol that allows to connect directly with the web EHR app via Bluetooth;
- and the mobile R2D protocol that allows to connect to different actors through the internet.

This part will be provided as libraries to integrate into the core application.

The D2D library provides to the core application two views: one to have access to a scanner, and the second one to have access to the HCP information. The first one is used to scan the QR code, and returns a healthcare provider. The second one is to show information about the healthcare provider that is given in parameters. The next step will be called automatically.

Once the connection is established, health data is shared with the HCP application from the core application through the library. When the web application has finished receiving the data, each change is shared back to the S-EHR in the opposite way. The mobile application can display a message to inform the citizen that the connection is complete, and what changes have been received.

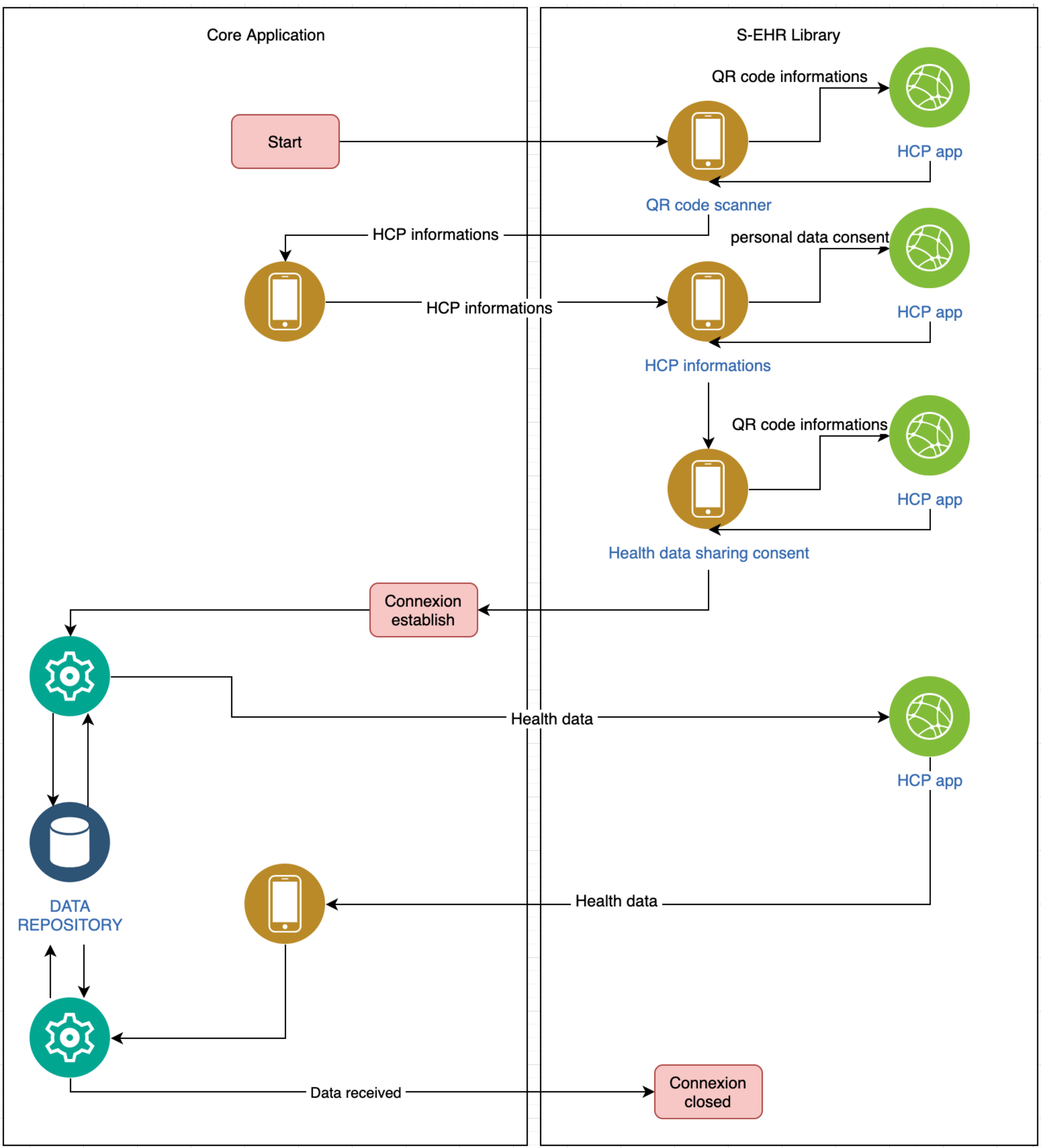


Figure 5 - Diagram: Integration of new functionalities to the core application to make the S-EHR-A

4. NEW FEATURES OF THE S-EHR-A

4.1. User flow of S-EHR D2D protocol

Here is one of the main user flows provided by the S-EHR, each step is made to establish a connection between the citizen and the HCP. The technology selected to make the connection is «Bluetooth». This will allow an easy connection, but over a short distance.

The Bluetooth connection is established when a valid QR code is scanned by the user. However, the Connection is considered fully established when the user has accepted the temporary consent request received from the HCP app. Otherwise, if the user refuses or cancels one of these steps, the connection is closed.

Once all steps are done and the connection is fully established, the HCP app can use, modify and add data. At the end, each modification is shared back to the user into his/her S-EHR.

If the connection is interrupted (example: if the user moves too far away from the connection source), the user will be automatically reconnected when he/she approaches again.

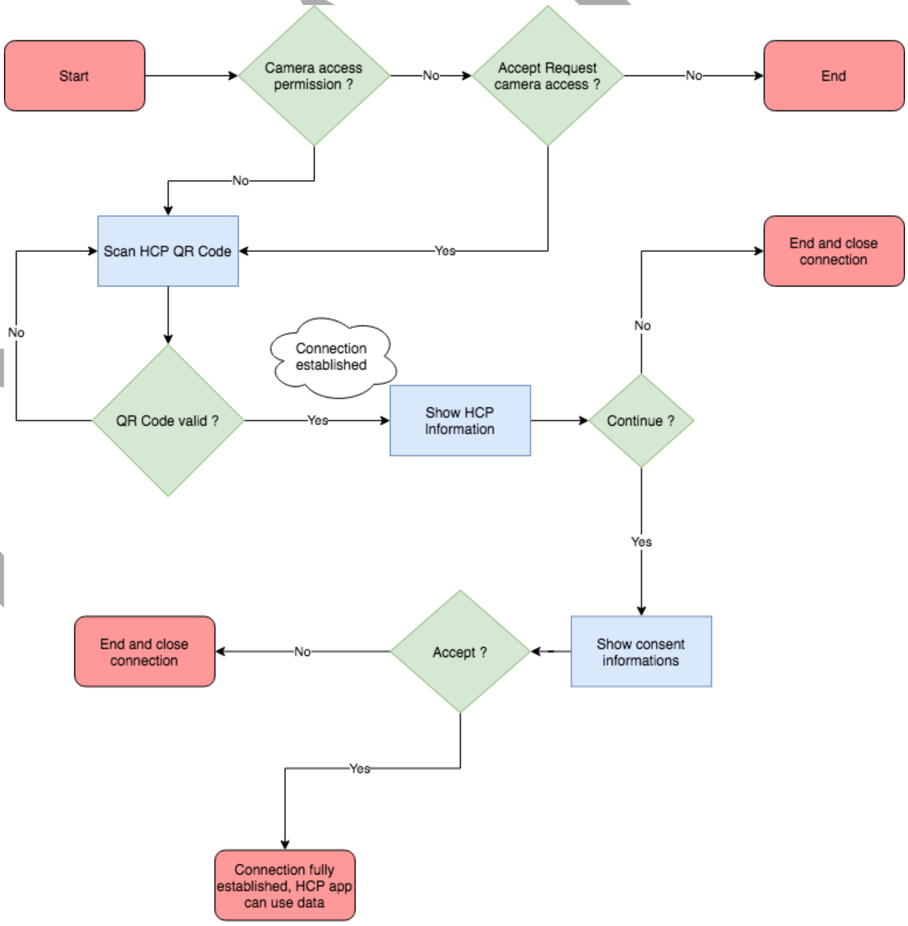


Figure 6 - User flow diagram: S-EHR D2D protocol

4.2. User flow of S-EHR R2D protocol

The R2D protocol is a protocol that orchestrates the data exchange from any EHR or S-EHR Cloud with the usage of the internet. It provides the S-EHR the possibility to retrieve health data from eHDSI National Contact Point.

The first step is the identification of the citizen using trusted user certificates, this will be done by using an open source Identity and Access Management solution called "Keycloak" [Keycloak]. Once the citizen is correctly identified with "Keycloak", the citizen will retrieve health data from eHDSI National Contact Point. This data will be inserted into his/her personal EHR stored on his/her S-EHR.

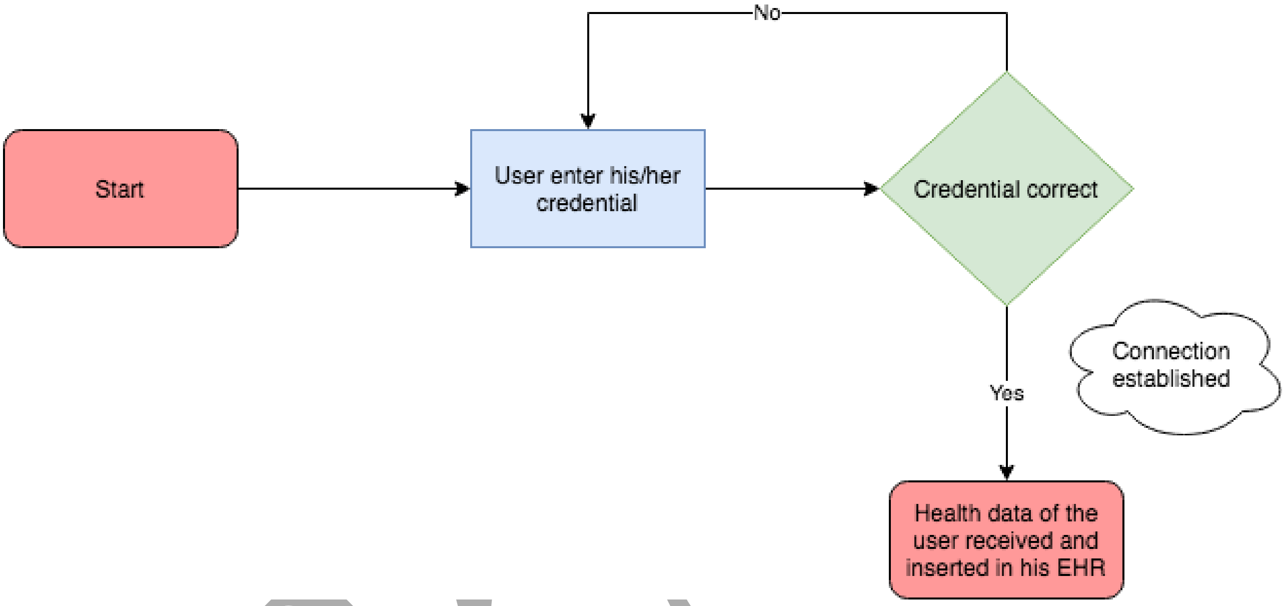

No
Start
User enter his/her credential
Credential correct
Yes
Connection established
Health data of the user received and inserted in his EHR

Figure 7 - User flow diagram: S-EHR R2D protocol

4.3. Security of the S-EHR

In the context of the S-EHR, confidentiality is a necessary security requirement and both encryption/decryption functionalities will be provided in both the D2D and R2D protocols through the security library. More information regarding the encryption/decryption functionalities are provided in the deliverable D3.5 [D3.5]. In addition, as already introduced in the deliverable D3.3 [D3.3], the QR code scanned by the user with his/her mobile device also includes the digital signature of the message and verifies the integrity of the message and the HCP identity. Last but not least, all the necessary sensitive credentials are stored safely in the user's TEE (Trusted Execution Environment): the Android keystore.

5. NEW USER REQUIREMENTS FOR THE S-EHR-A

5.1. Requirements integrated in existing features of the core app

5.1.1. R2D import of data from national EHR on S-EHR

The core application already provides the possibility for the user to register to different kinds of services.

The main types are:

- **Clinical Study**: part of the application is dedicated to clinical studies. Once the user is registered to a study (the enrolment is carried out by an external party, through the Andaman7 web application), he/she has access to the related service. After giving consent to the terms of the service, the user will have access to the concerning study section and its surveys;
- **Hospital Service:** the core application is already linked to numerous hospitals. It allows Andaman7 to give users access to their health data which was for the moment only stored in their hospital.

The R2D (Remote to Device) protocol implementation will be added to the existing features as a hospital service.

Here are the different sections in which the citizen will be able to retrieve data from his/her national EHR at the end of the development of the S-EHR-A:

- Patient summary;
- Laboratory result;
- Medical image;
- Prescription.

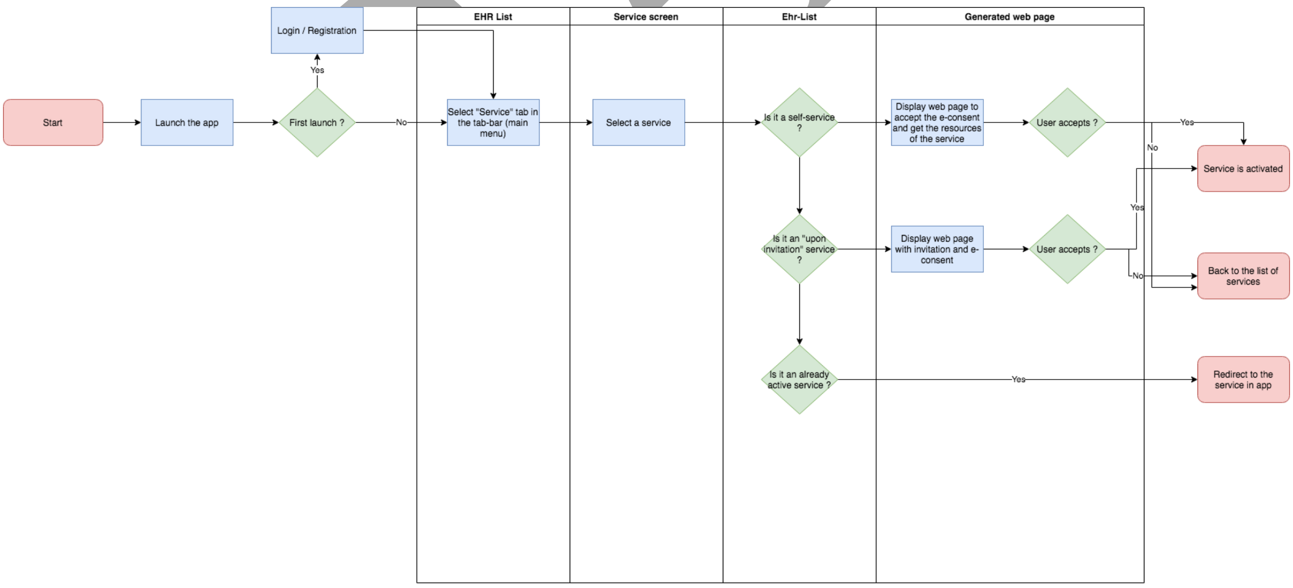

EHR List
Service screen
Ehr-List
Generated web page
Login / Registration
Yes
Start
Launch the app
First launch ?
No
Select "Service" tab in the tab-bar (main menu)
Select a service
Is it a self-service ?
Display web page to accept the e-consent and get the resources of the service
User accepts ?
Yes
No
Service is activated
Is it an "upon invitation" service ?
Display web page with invitation and e-consent
User accepts ?
Yes
No
Back to the list of services
Is it an already active service ?
Yes
Redirect to the service in app

Figure 8 - User flow diagram: register to service

5.1.2. Consultation of health data sharing audit by the citizen on his/her S-EHR

The citizen should be able to consult the history of his/her sharing operations, whether the sharing was performed by means of the D2D protocol, R2D protocol or research protocol.

The most relevant information that the citizen will have access to regarding those sharing operations will be:

- **Date:** When the exchange occurred;
- **Who:** Who was the other side;
- **Type:** Type of exchange (receive data, send data, both) from the point of view of the citizen;
- **Section(s):** Which section(s) of the patient's EHR has/have been exchanged.

This sharing information will be shown as a list (one row by sharing operation).

The citizen should have access to a more detailed view of each exchange, which will show which data of each section has been exchanged.

5.2. Requirements integrated as new features of the core app

5.2.1. D2D device pairing

The purpose of this requirement is to start the connection between the citizen and the HCP application. This is done through the scan of a QR code that contains all data necessary to establish the connection between the two actors.

To satisfy this need, a simple screen is provided, which contains a scanner that can read the HCP QR code information. It is shown as a dialog. To be able to use the scanner, the user must give his/her permission to the application to use the camera. So the first time this screen is launched, it will start by a permission request.

Once a valid QR code is scanned, a message pop-up will be shown to the user to inform him/her that the connection to the HCP has started.

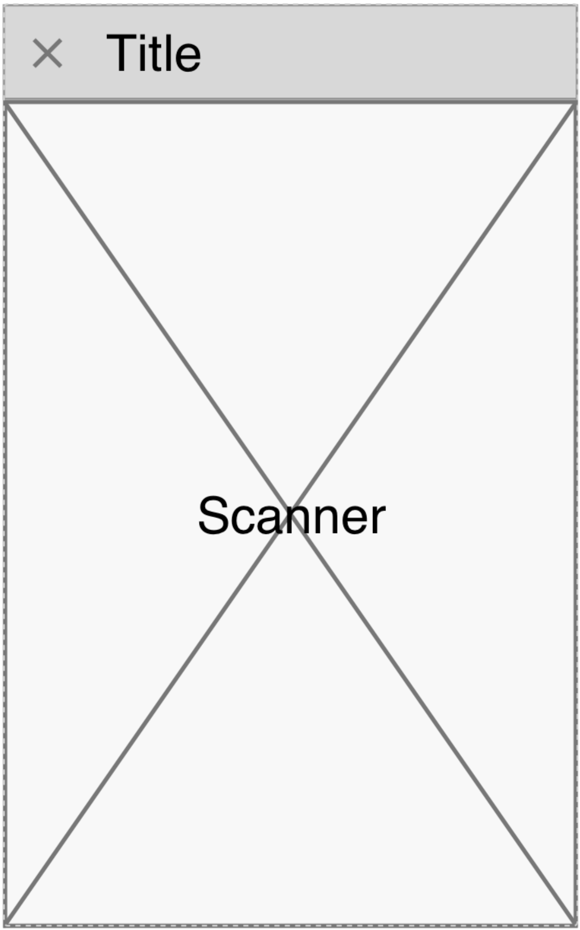


Figure 9 - Wireframe: D2D device pairing

5.2.2. D2D visualization of the healthcare organization by the citizen

Here is the screen about the HCP information. It will regroup essential information that will allow the user to easily identify who they are connecting to.

After discussions during co-design meeting sessions with final users, it was agreed that the most relevant information that should be shown to the citizen about the HCP were the name of the practitioner, his/her qualification and the name of the current location (hospital, research centre, ...). It was also agreed that a picture of the practitioner could be shown.

Consent management regarding the sharing of identification data was subsequently removed to simplify the workflow, since this consent has been declared as not mandatory. Indeed, the identification data can be shared since it is necessary to the performance of a contract (the contract here refers to the consent that will be asked to share health data).

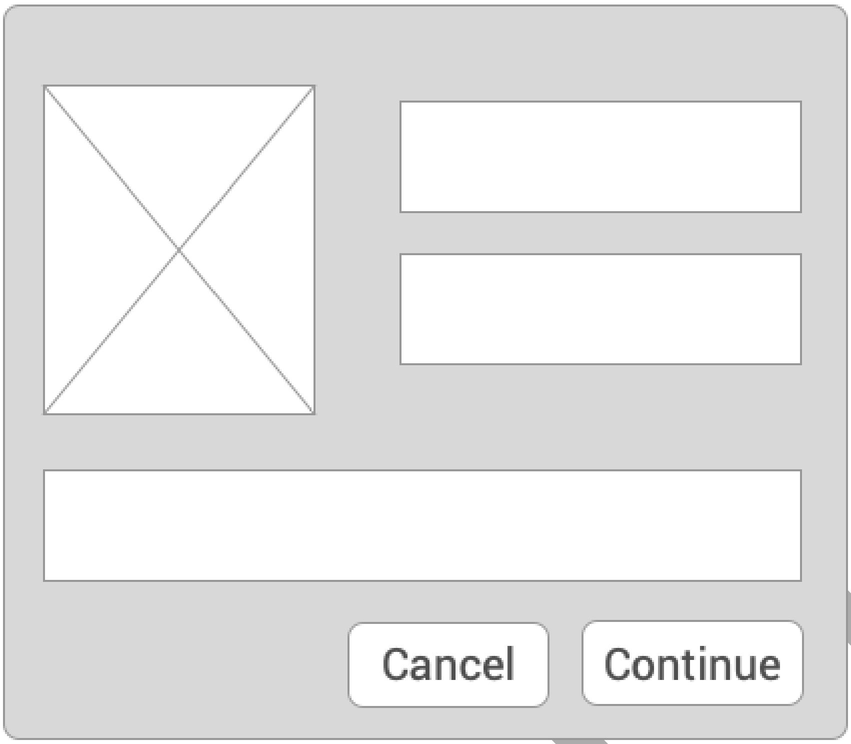


Figure 10 - Wireframe: D2D visualization of the healthcare organization by the citizen

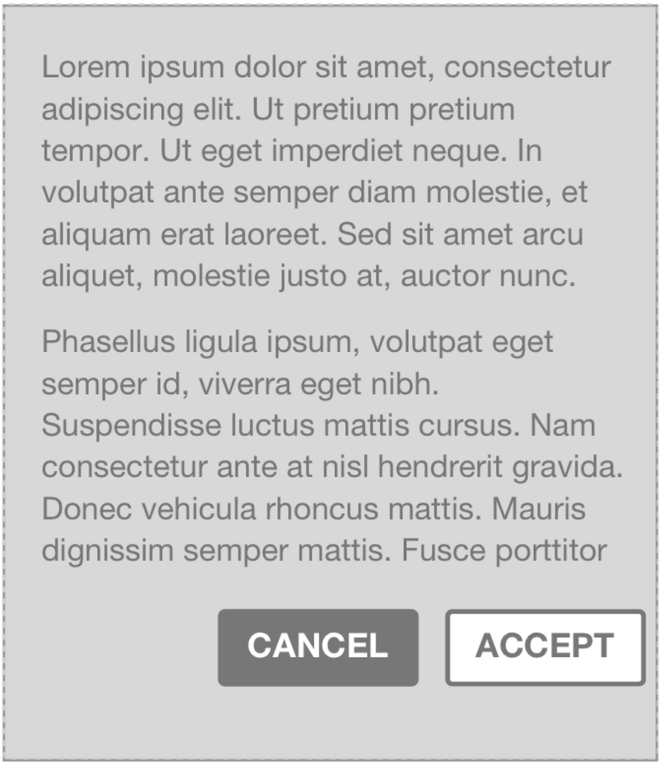
5.2.3. D2D access consent to healthcare organization by the citizen

Following a co-design meeting sessions decision, the consent management has been removed to simplify the workflow. When the user clicks on the « continue » button on the screen of the HCP information [Figure 9] the user gives his/her consent for sharing his/her personal data with the HCP application.

5.2.4. D2D consent by the citizen to the healthcare organization for temporary S-EHR access

The last step of the connection for the user is to give his/her consent for sharing his/her health data with the HCP application. This will allow the HCP app to read the user's data, modify it and add new data to the user's EHR.

After this step, the connection will be fully established. The user will come back to the core application.



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut pretium pretium tempor. Ut eget imperdiet neque. In volutpat ante semper diam molestie, et aliquam erat laoreet. Sed sit amet arcu aliquet, molestie justo at, auctor nunc.

Phasellus ligula ipsum, volutpat eget semper id, viverra eget nibh. Suspendisse luctus mattis cursus. Nam consectetur ante at nisl hendrerit gravida. Donec vehicula rhoncus mattis. Mauris dignissim semper mattis. Fusce porttitor

Figure 11 - Wireframe: D2D consent by the citizen to the healthcare organization for temporary S-EHR access

5.2.5. Enabling of citizen identification from the S-EHR (with CA)

Related to the security, each citizen should have a certificate that will identify him/her. This certificate will be used during the sharing of data through the D2D protocol, R2D protocol and research protocol.

The certificate is released by a CEF eID trusted certification authority.

5.2.6. Invitation of candidate citizens to participate to a research study

The S-EHR, upon receiving a silent notification of the publication of a research study, executes a check to verify if the citizen's profile matches with research study enrolment criteria. If the matching is positive, then the citizen is invited to share his/her health data for the research study.

If the citizen agrees to share his/her health data, a signed consent is sent to the InteropEHRate Research Service and InteropEHRate Open Research Network who both store the consent.

5.2.7. Activation of automatic backup of S-EHR content on selected S-EHR Cloud

The citizen has the choice to activate or not an automatic backup of his/her data on a certified S-EHR Cloud. That means that all of his/her health data will be transferred to a S-EHR Cloud storage, and it will be updated when a modification on his/her data has been made. This feature gives him/her the possibility to retrieve his/her data in case of problems with his/her device.

The citizen can choose which one of the certified S-EHR Cloud services he/she wants to use in a list of available services.

5.2.8. Sharing of health data with qualified HCPs for emergency by means of S-EHR Cloud

Citizens can consent HCPs of Healthcare organisations to access, only for emergency reasons, to their health data stored on the S-EHR Cloud. Giving the consent activates the automatic backup of the health data from the S-EHR to the preferred S-EHR Cloud (selected by the list of certified S-EHR Cloud services provided by the S-EHR).

The consent authorises the HCP to access health data using an emergency token or the identification data of the citizen.

5.2.9. Citizen's consent to be part of InteropEHRate Open Research Network

The citizen can subscribe to his/her S-EHR to be part of the InteropEHRate Open Research Network. The S-EHR sends the subscription to the Open Research Network and includes a signed consent to receive studies on his/her S-EHR. The Open Research Network adds the citizen to the list of subscribers who can receive a notification for a research.

5.2.10. Citizen's access to emergency token

A citizen may use a S-EHR to access and exchange with other applications an image with his/her "emergency token". The emergency token allows a qualified HCP (authorised by his/her organization) to identify the citizen and access his/her emergency dataset stored on the S-EHR Cloud.

This token will be used if the citizen is not able to give access directly to his/her data (e.g.: unconscious citizen).

5.2.11. Citizen's withdrawing from research network

A citizen can opt out from the Research Network. When he/she chooses to opt out, the S-EHR sends the request to the Research Network where the citizen is removed from the subscriber list.

5.2.12. Citizen's consent to share health data for a research protocol

If the citizen's demographic and health data match a study criterion, he/she receives an invitation to participate in this study. In this invitation, the citizen is asked his/her consent to share data.

This demand includes:

- a description of the research;
- by which hospital/centre this research is conducted;
- the benefits and objectives;
- which data will be shared;
- when it will be shared;
- and the period for how long the data will be kept.

5.2.13. Reception and storage of consent, digitally signed from research organisation, on citizen's S-EHR

Once the consent is digitally signed by the two parts, it is stored on the citizen’s device (it is also stored by the research organisation).

6. DESIGN OF THE S-EHR-A

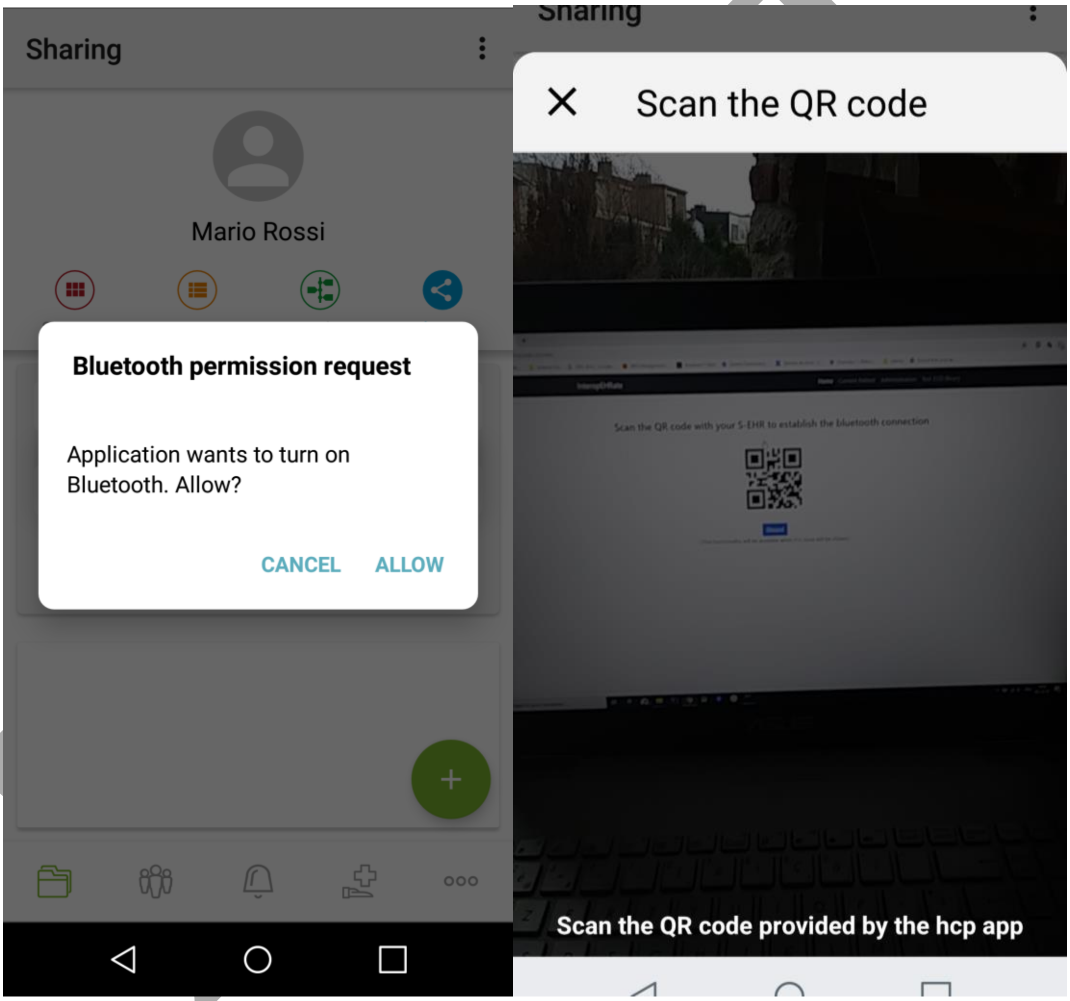
6.1. Screens and mockups of the S-EHR-A based on user requirements

Based on the wireframe, here are the visuals for the implementation of each screen.

6.1.1. D2D device pairing

The screen will be shown in a bottom sheet view. In practice, a bottom sheet is a component that slides up from the bottom of the screen to reveal more content.

For the scanner, the bottom sheet provided by the Mobile Vision API from Google is used. The framework provides a lot of camera functionalities, including a barcode detector.



Bluetooth permission request

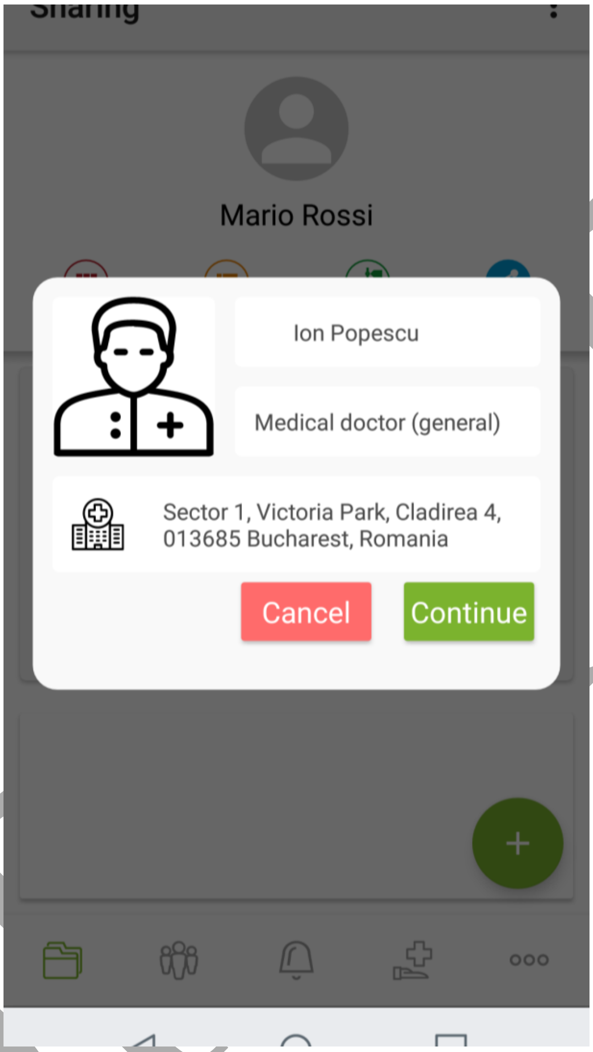
Application wants to turn on Bluetooth. Allow?

Scan the QR code provided by the hcp app

Figure 12 - GUI: D2D device pairing

6.1.2. D2D visualization of the healthcare organization by the citizen

The HCP information is shown in a dialog.



Ion Popescu

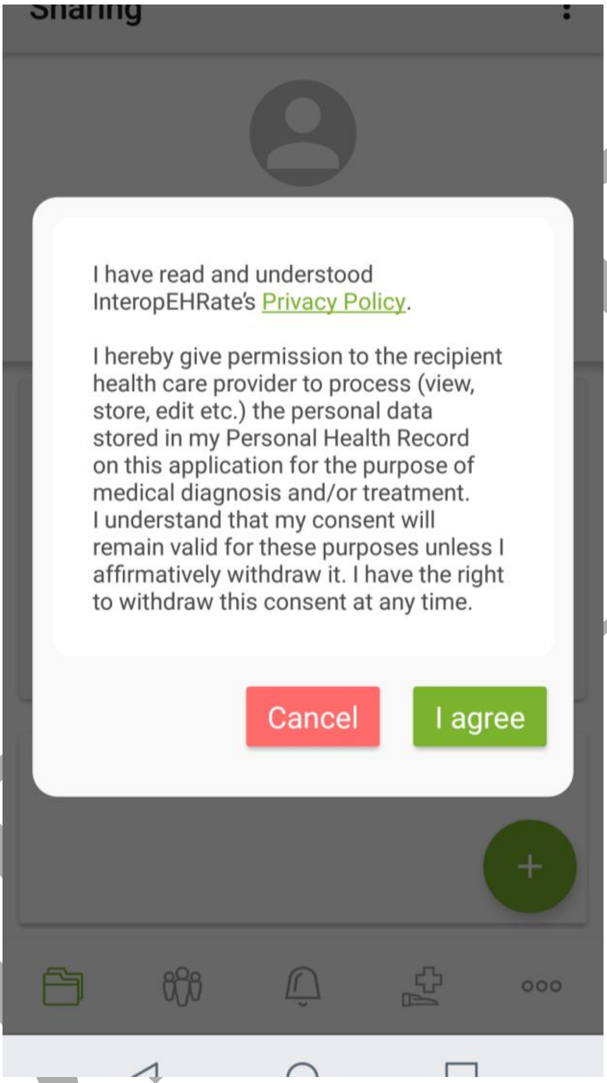
Medical doctor (general)

Sector 1, Victoria Park, Cladirea 4,
013685 Bucharest, Romania

Figure 13 - GUI: D2D visualization of the healthcare organization by the citizen

6.1.3. D2D consent by the citizen to the healthcare organization for temporary S-EHR access

The consent for health data sharing is shown in a dialog.



I have read and understood InteropEHRate's Privacy Policy.

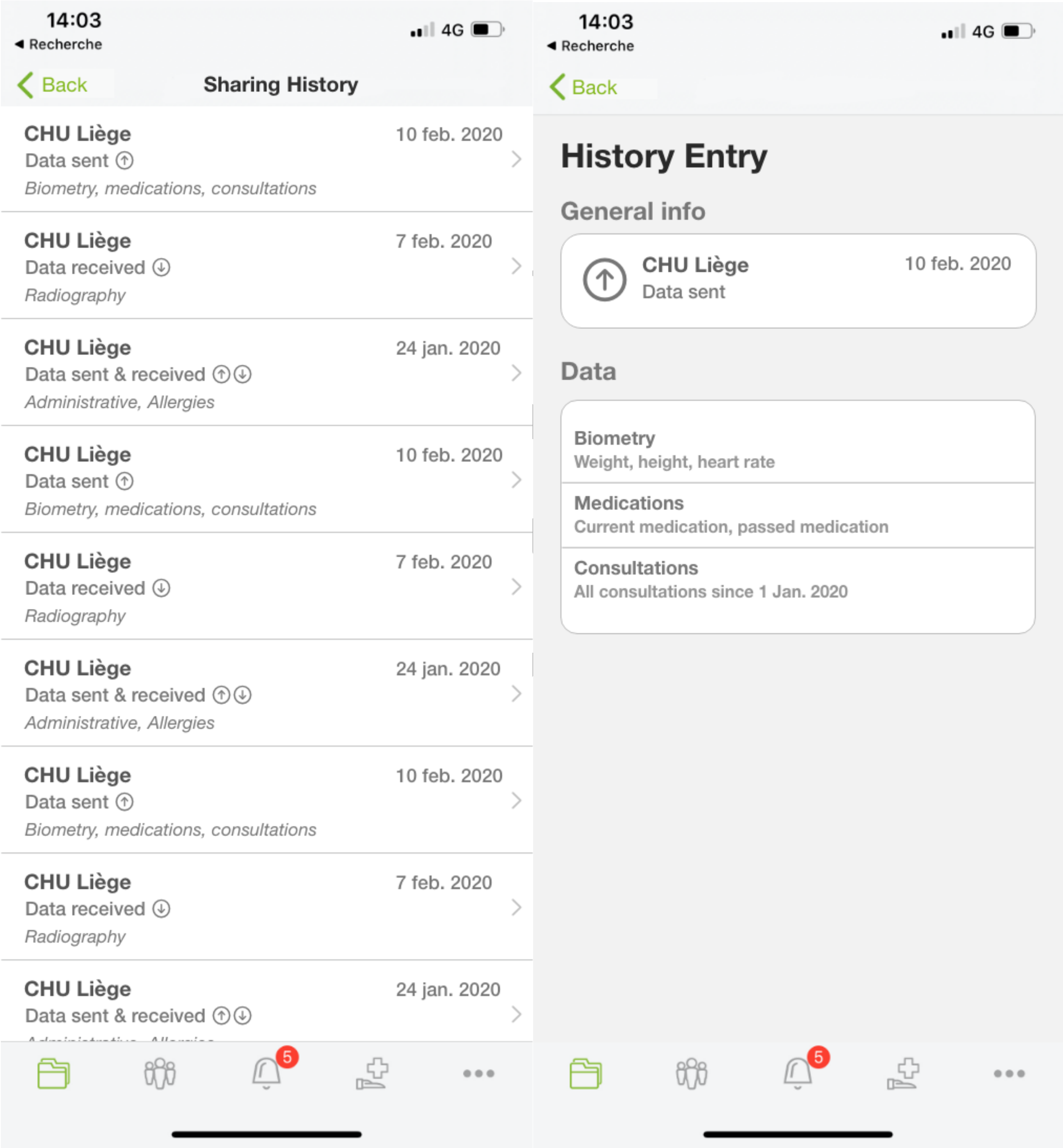
I hereby give permission to the recipient health care provider to process (view, store, edit etc.) the personal data stored in my Personal Health Record on this application for the purpose of medical diagnosis and/or treatment. I understand that my consent will remain valid for these purposes unless I affirmatively withdraw it. I have the right to withdraw this consent at any time.

Figure 14 - GUI: D2D consent by the citizen to the healthcare organization for temporary S-EHR access

6.1.4. Consultation of health data sharing audit by the citizen on his/her S-EHR

In the first view, the citizen can see the full history of his/her sharing operations through D2D protocol, R2D protocol and research protocol.

When clicking on a row, the citizen accesses the second view, a more detailed view of a sharing operation.



14:03
◂ Recherche
4G

‹ Back Sharing History

CHU Liège 10 feb. 2020
Data sent
Biometry, medications, consultations

CHU Liège 7 feb. 2020
Data received
Radiography

CHU Liège 24 jan. 2020
Data sent & received
Administrative, Allergies

CHU Liège 10 feb. 2020
Data sent
Biometry, medications, consultations

CHU Liège 7 feb. 2020
Data received
Radiography

CHU Liège 24 jan. 2020
Data sent & received
Administrative, Allergies

CHU Liège 10 feb. 2020
Data sent
Biometry, medications, consultations

CHU Liège 7 feb. 2020
Data received
Radiography

CHU Liège 24 jan. 2020
Data sent & received

14:03
◂ Recherche
4G

‹ Back

History Entry

General info

CHU Liège 10 feb. 2020
Data sent

Data

Biometry
Weight, height, heart rate

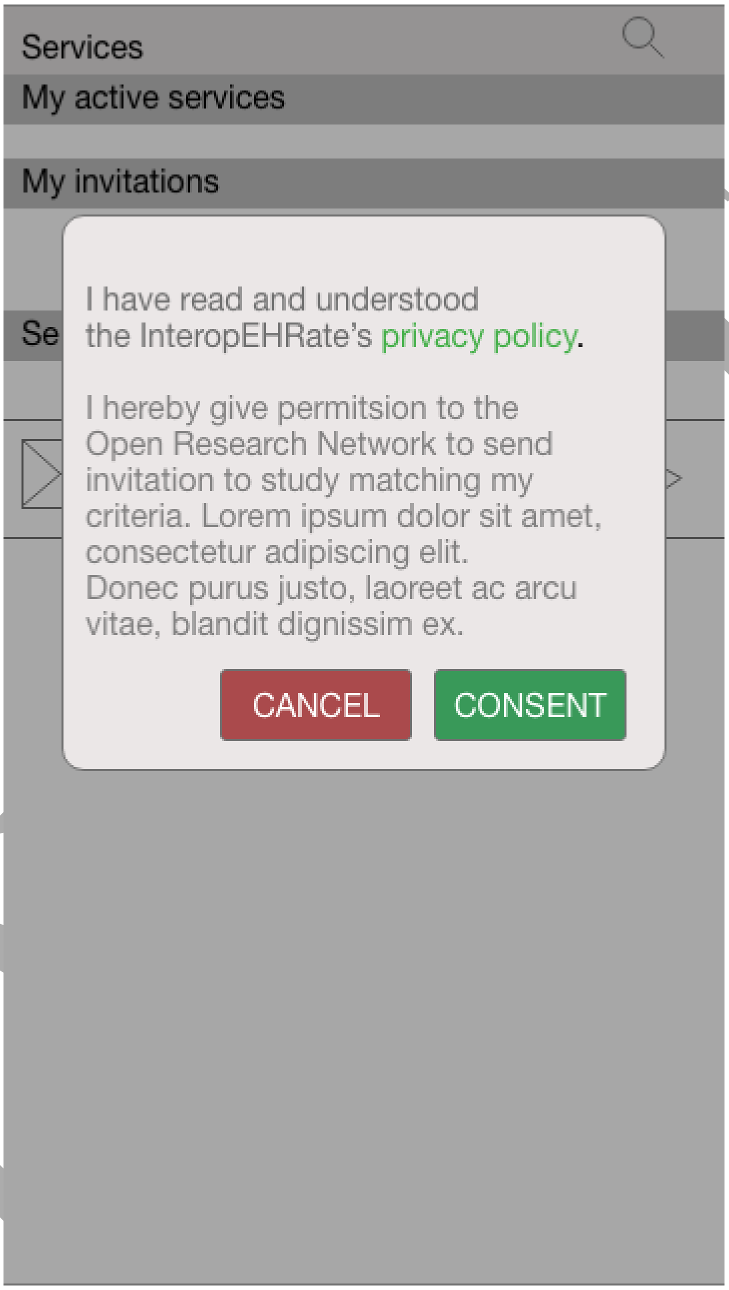
Medications
Current medication, passed medication

Consultations
All consultations since 1 Jan. 2020

Figure 15 - Mockup: Consultation of auditing health data sharing for Citizen on S-HER

6.1.5. Citizen's consent to be part of the InteropEHRate Open Research Network

The consent to be part of the InteropEHRate Open Research Network will be shown in a dialog.



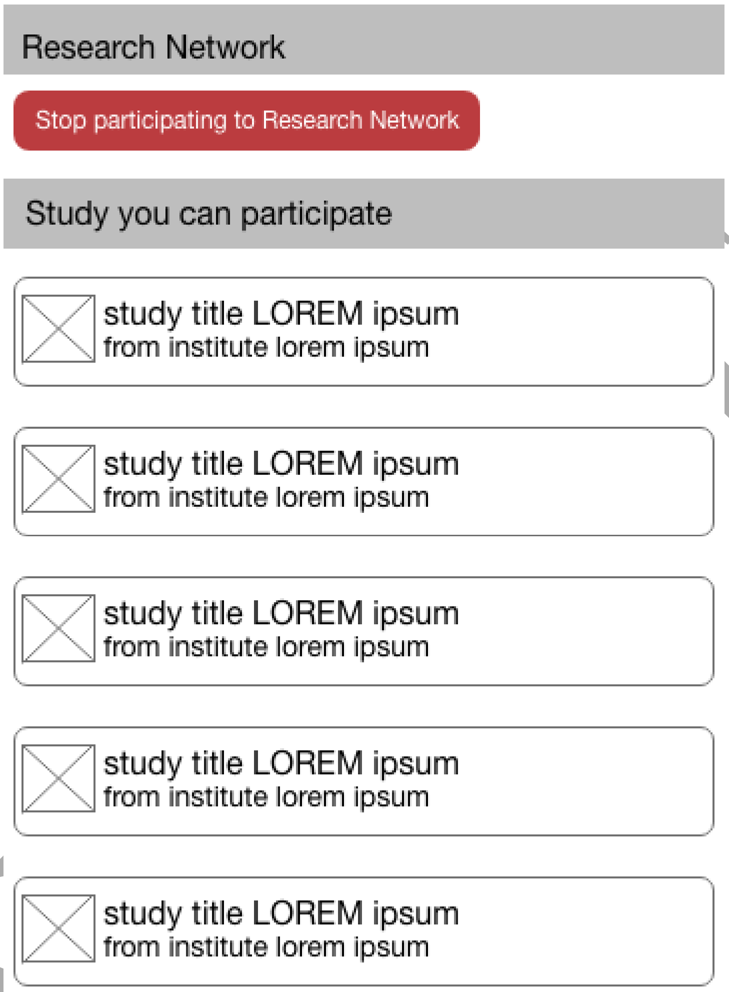
I have read and understood the InteropEHRate's privacy policy.

I hereby give permitsion to the Open Research Network to send invitation to study matching my criteria. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec purus justo, laoreet ac arcu vitae, blandit dignissim ex.

Figure 16 - Mockup: Citizen's consent to be part of InteropEHRate Open Research Network

6.1.6. Invitation of candidate citizens to participate to a research study

Citizens can see, as a list, the studies that they can participate in.



Research Network

Stop participating to Research Network

Study you can participate

study title LOREM ipsum
from institute lorem ipsum

study title LOREM ipsum
from institute lorem ipsum

study title LOREM ipsum
from institute lorem ipsum

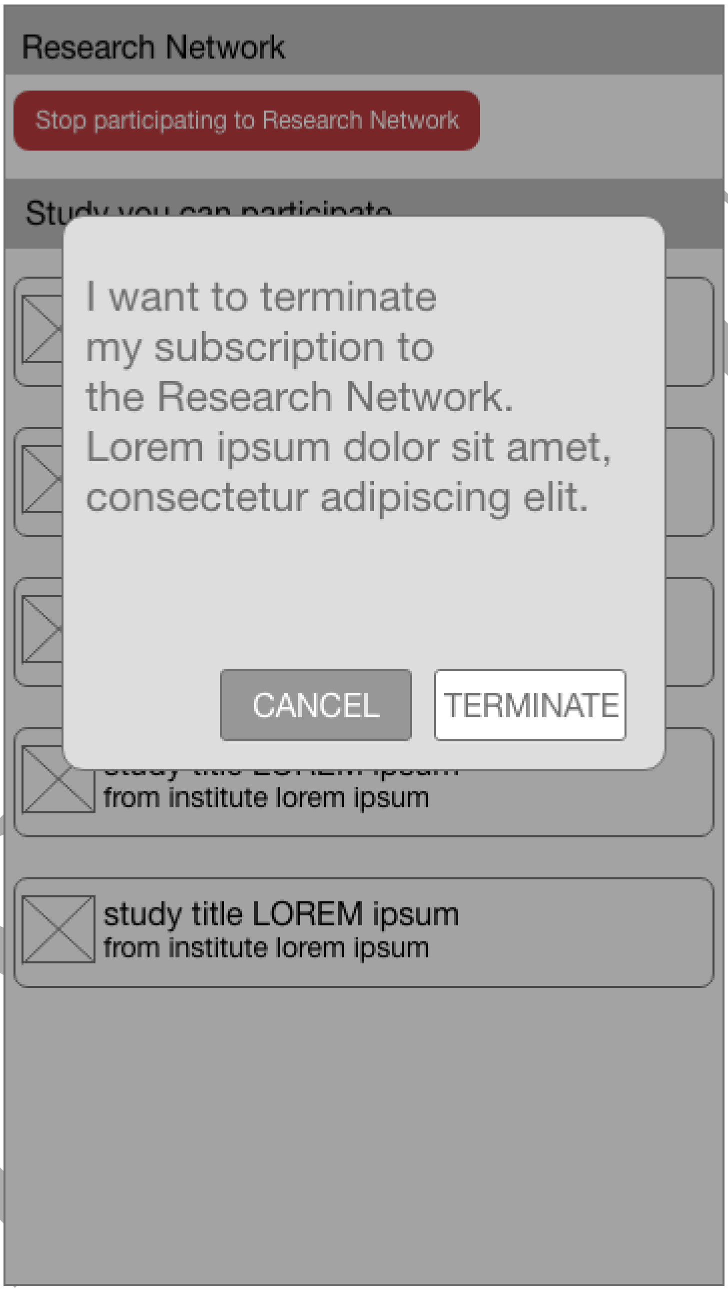
study title LOREM ipsum
from institute lorem ipsum

study title LOREM ipsum
from institute lorem ipsum

Figure 17 - Mockup: Invitation of candidate citizens to participate to a research study

6.1.7. Citizen's withdrawing from research network

A citizen can stop his/her participation in the research network by clicking on the button “Stop participating in the Research Network”.


Research Network
Stop participating to Research Network
Study you can participate
CANCEL
TERMINATE

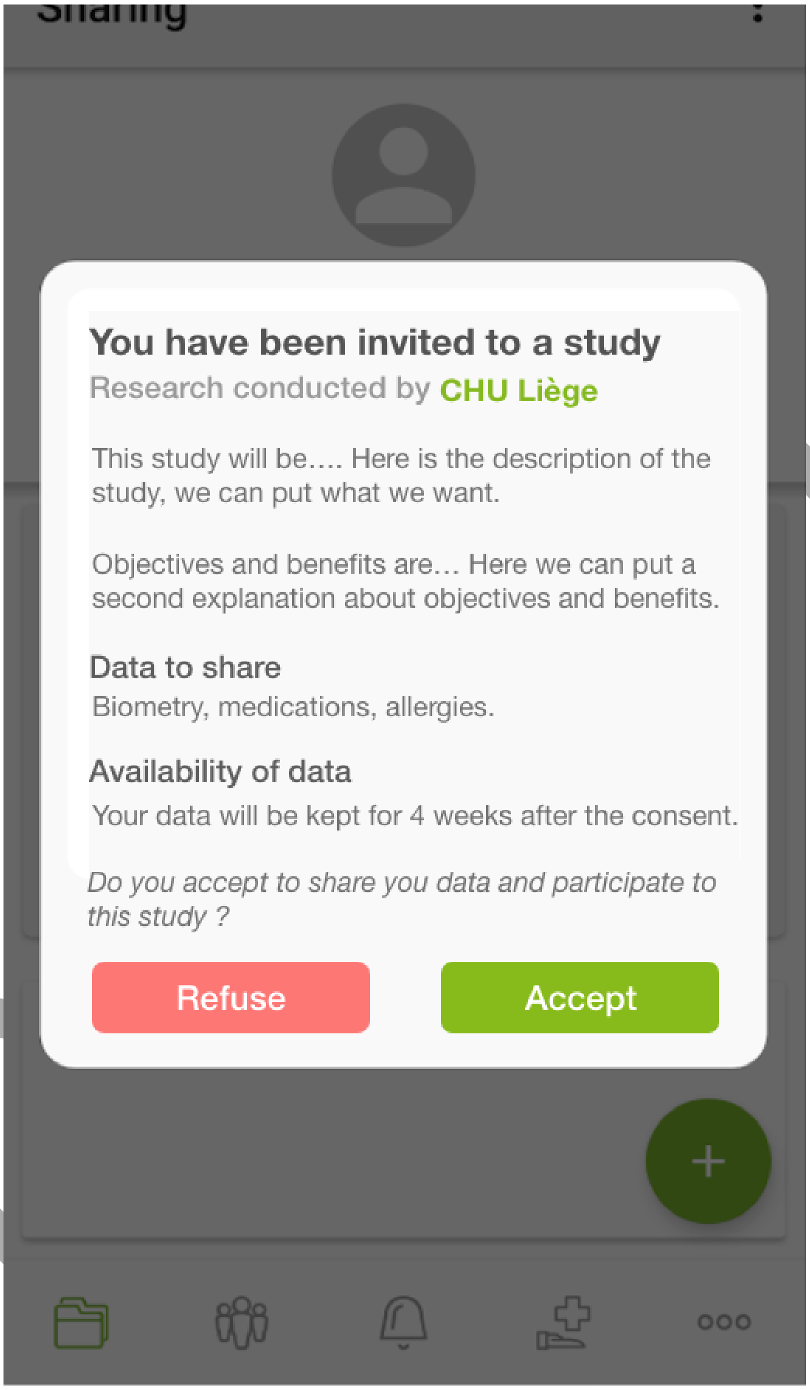
I want to terminate my subscription to the Research Network. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

study title LOREM ipsum
from institute lorem ipsum

study title LOREM ipsum
from institute lorem ipsum

Figure 18 - Mockup: Citizen's withdrawing from research network

6.1.8. Citizen's consent to share health data for a research study



Sharing

You have been invited to a study

Research conducted by CHU Liège

This study will be…. Here is the description of the study, we can put what we want.

Objectives and benefits are… Here we can put a second explanation about objectives and benefits.

Data to share

Biometry, medications, allergies.

Availability of data

Your data will be kept for 4 weeks after the consent.

Do you accept to share you data and participate to this study ?

Figure 19 - GUI: Citizen's consent to share health data for a research study

7. CONCLUSIONS AND NEXT STEPS

This deliverable outlines the software requirements designed for the versions 1 and 2 of the reference implementation of a S-EHR in the context of the InteropEHRate framework.

In the first version of this deliverable [D6.1], the grounds of the S-EHR-A were described. It explained that the Andaman7 application would be used as the core application for the reference implementation of a S-EHR and how the new software requirements specific to the InteropEHRate project would be designed and added to that core. A few of those new requirements were already depicted, which were to be implemented in the first version of the S-EHR-A. They were all related to the first scenario of the project: “Medical visit abroad”, and presented a first draft of the user interface for the usage of D2D protocol by the citizen using a S-EHR application. The early stages of the R2D protocol were also introduced.

The current version of the deliverable (D6.2) is built on top of the version 1 and its content is expanded to new software requirements designed since the first version.

On one hand, it displays the updated requirements of version 1, with actual interfaces developed rather than mock-ups. Those interfaces have been subject to the feedback of final users.

On the other hand, it describes some requirements of scenario 1 in further details as well as new requirements for the two other scenarios, namely “Emergency access” and “Health research study”. Those requirements of course focus on the citizen side, the citizen being the actor of the scenarios using the S-EHR. In that regard, this deliverable shows how the citizen will use the R2D protocol to retrieve his/her health data, how he/she will use the D2D protocol to share his/her health data with a HCP without the use of the internet, how he/she will have the possibility to use a S-EHR Cloud of his/her choice for additional services, how he/she will be offered to participate to some research studies, etc.

It is to be noted that some security aspects have also been added in this second version, even though such aspects are not always visible from a “user interface” point of view.

A third and last version of this deliverable (D6.3) is planned in March 2021. It will present in more detail the software requirements and user interfaces implemented in the version 2 of the S-EHR-A, including improvements resulting from co-design sessions. It will also describe the last software requirements required to develop the third and last version of the S-EHR-A, covering fully the 3 scenarios of the InteropEHRate project.

REFERENCES

- **[D2.1]** InteropEHRate consortium. *D2.1: User Requirements for cross-border HR integration - V1*, June 2019. www.interopehrate.eu/resources/#dels

- **[D2.2]** InteropEHRate consortium. *D2.1: User Requirements for cross-border HR integration - V2*, March 2020. www.interopehrate.eu/resources/#dels

- **[D2.4]** InteropEHRate consortium. *D2.4 InteropEHRate Architecture - V1*, June 2019. www.interopehrate.eu/resources/#dels

- **[D3.1]** InteropEHRate consortium. *D3.1: Specification of S-EHR mobile privacy and security conformance levels*, March 2020. www.interopehrate.eu/resources/#dels

- **[D3.3]** InteropEHRate consortium. *D3.3 – Specification of remote and D2D IDM mechanisms for HRs Interoperability,* March 2020*.* www.interopehrate.eu/resources/#dels

- **[D3.5]** InteropEHRate consortium. *D3.5: Specification of data encryption mechanisms for mobile and web applications,* March 2020. www.interopehrate.eu/resources/#dels

- **[D4.1]** InteropEHRate consortium. *D4.1: Specification of remote and D2D protocol and APIs for HR exchange - V1,* June 2019. www.interopehrate.eu/resources/#dels

- **[D4.8]** InteropEHRate consortium. *D4.8: Specification of protocol and APIs for research health data sharing - V1*, March 2020. www.interopehrate.eu/resources/#dels

- **[Keycloak]** Open Source Identity and Access Management. Website: https://www.keycloak.org/.
- **[D6.1]** InteropEHRate consortium. *D6.1: Software requirements and architecture specification of a S-EHR - V1*, June 2019. https://www.interopehrate.eu/resources/#dels