D6.3

Software requirements and architecture specification of a S-EHR - V3

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	30th July, 2021
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, Lucie Keunen	A7
Contributor	Paul De Raeve	EFN
Reviewer	Chrysostomos Symvoulidis	BYTE

LOG TABLE

Version	Date	Change	Author	Partner
0.1	2021-02-06	First draft of ToC	Martin Marot	A7
0.2	2021-06-14	Update of software requirements section	Martin Marot	A7
0.3	2021-06-18	Update wireframe & user requirements section	Martin Marot	A7
0.4	2021-06-23	Update User flow graph	Martin Marot	A7
0.5	2021-06-28	update design section	Martin Marot	A7
0.6	2021-06-30	final update + review	Martin Marot	A7
0.7	2021-07-03	Review	Lucie Keunen	A7
1.0	2021-07-05	First internal review	Chrysostomos Symvoulidis	BYTE
1.1	2021-07-09	Quality check	Argyro Mavrogiorgou	UPRC
1.2	2021-07-29	Addressed comments after ENG tech review	Martin Marot	A7
Vfinal	2021-07-30	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
IEHR	InteropEHRate
IRS	InteropEHRate Research Service
IT	Information Technology
QR code	Quick Response code
R2D	Remote to Device
RDS	Research Data Sharing
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 specifications of the 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 end-user requirements defined during 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. **New features of the S-EHR-A**
5. **New user requirements for 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 3 of the S-EHR-A”;
- Update of the section “New features of the S-EHR-A”:
  - Addition of the section “User flow of S-EHR Research protocol”;
  - Addition of the section “User flow of S-EHR Emergency protocol”;
  - Update of the section “Security of the S-EHR”;
- Update of the section “User requirements already implemented by the core application”;
  - Addition of the section “Translation/Conversion of health data”;
  - Addition of the section “Execution of questionnaire defined by research protocol”;
- Update of the section “Requirements integrated as new features of the core app”:
  - Update of sub-sections order, sorting by scenario;
  - Addition of the section “Selection of healthcare providers for R2D Access”;
  - Addition of the section “Selection of Encounters to download by means of R2D Access”;

    - Update of the section “Activation of automatic backup of S-EHR content on selected S-EHR Cloud”;
    - Update of the section “Citizen's consent to be part of InteropEHRate Open Research Network”;
    - Addition of the section “Invitation of candidate citizens to participate in a research study”;
    - Addition of the section “Citizens' selection of reference research center”;
    - Addition of the section “Citizen's consultation of the details of the research study”;
    - Update of the section “Citizen's consent to share health data for a research protocol”;
- Update of the section “Screens and mockups of the S-EHR-A based on user requirements”:
    - Update of sub-sections order, sorting by scenario;
    - Addition of the section “Selection of healthcare providers for R2D Access”;
    - Addition of the section “Selection of Encounters to download by means of R2D Access”;
    - Addition of the section “Activation of automatic backup of S-EHR content on selected S-EHR Cloud”;
    - Addition of the section “Consent, exchange and storage of Citizens' face (photo) on the S-EHR and S-EHR Cloud”;
    - Addition of the section “Citizen's access to emergency token”;
    - Update of the section “Invitation of candidate citizens to participate to a research study”;
    - Update 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 [D3.2] and that supports the InteropEHRate protocols [D4.3][D4.9].

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 organisations and S-EHR Cloud, The Research Data Sharing protocol (RDS) to exchange health data with research network, and the Device to Device (D2D) protocol to exchange health data with healthcare organisations 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 end-users and focus groups, designed screens or mockups of the S-EHR-A are presented.

Details on the architecture of the S-EHR-A can be found in the design deliverable [D2.6].

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 summarise 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. They act as the hub of their own data, and offer the possibility to exchange their 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 end-users in the design of the different versions of the solution. More details on the user requirements for each scenario can be read in the deliverables dedicated to this topic [D2.3] "User Requirements for cross-border HR integration - V3".

Only after the definition of the requirements can be achieved 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 their 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 defined in the User Requirement deliverable, [D2.3] "User Requirements for cross-border HR integration - V3", in the section "4.2.1 S-EHR App".

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

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, in bold those that will have a visual impact on the UI).

User requirement title	User requirement description
Auditing health data modification for Citizen on S-her	Any modification on health data (creation, reading, updating, deleting) performed by any user is tracked by the S-EHR
Confirmation to enable the S-EHR data management	At first run the S-EHR obtains from the Citizen is informed that: (1) his/her personal health data will be stored and managed by him on the smart device, (2) any data sharing action will require his/her approval. A confirmation is then requested to start to use the S-EHR.
D2D consent by the Citizen for temporary S-EHR access to Healthcare organization	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. The temporary consent of the Citizen for data exchange automatically expires at the end of the day.
D2D device pairing	The Citizen connect/pair his/her smart device to the HCP

[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.

	computer/device
D2D Visualization of Healthcare organization to the Citizen	The Citizen see on the S-EHR the data describing the identity of the Health Organization
Enabling of Citizen identification from S-EHR (without CA)	The S-EHR store and send 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).
R2D import of (portion of) Patient Summary from healthcare provider on S-EHR (without security)	Citizen health data (portion of Patient Summary) can be imported from the Citizen healthcare provider on Citizen S-EHR.
S-EHR download from Android store	S-EHR is downloadable from the Android store. The Citizen downloads the S-EHR from the Android store and installs it on its Android device.
S-EHR runs on Android smartphone	The S-EHR is a mobile app that can run on Android version X
Consultation of auditing health data modification for Citizen on S-EHR	Any audited modification on health data (creation, reading, updating, deleting) performed is consultable from the Citizen that is the owner the data

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

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

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, in bold those that will have a visual impact on the UI).

User requirement title	User requirement description
D2D Identification and Authentication of the citizen from HCP	The citizen's identification data (certificate) is used to create or match the citizen's digital identity in the HCP App. The certificate contains the information of the patient from his/hers ID card. The certificate is displayed to the HCP and he/she can dismiss or accept the consultation. The match can be persistent in the HCP App in order to avoid the manual confirmation for future use. The citizen's digital identity is used for further transactions, e.g. D2D data exchange.
R2D import of (portion of) Laboratory result from healthcare provider on 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 (portion of) Medical images and reports from healthcare provider on 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.
Non repudiable data provenance tracking	The author and data origin of any health data is verified (i.e. non repudiable), tracked, visible to any authorized user and legally valid.
Compliance to IEHR profiles	The S-EHR and HCP App refuse to accept any health data set including a FHIR resource that declares conformance to an IEHR profile but is not actually compliant to it.

R2D import of (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.
Auditing health data sharing for Citizen on S-her	Any sharing operation on health data (sharing, authorization) performed by any user is tracked by the 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.
Citizen's digital signature of consent to share health data for a given study	The Citizen can give his/her consent to participate in a research study he/she has been invited to and digitally sign it (in a legally binding way) directly on his/her S-EHR.
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 their 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, its/her participation in the InteropEHRate Research Protocol.
Support of machine interpretable research protocol for publication.	A research protocol that is publishable on the InteropEHRate Open Network must contain a machine interpretable description of the set of health data that the patient will consent to share, of the enrolment criteria. The representation has to be interpretable by the S-EHR for (1) automatically comparing the enrolment criteria with the content of the S-EHR, to check if the patient can be enrolled; (2) automatically share the required data set with authorised Research Organisations.
Support of name within publishable research protocol.	A formal publishable specification of a research protocol allows to assign a name to the research protocol.
Support of constraints on min and max value of patient's attributes	A formal publishable specification of a research protocol allows to express enrolment criteria based on constraint on the minimum or

within enrolment criteria.	maximum allowed value of a specific attribute of the patient.
Support of constraints on patient's diagnosis within enrolment criteria.	A formal publishable specification of a research protocol allows to express enrolment criteria based on the received diagnosis of the patient.
Support of constraints on patient's drug therapy within enrolment criteria	A formal publishable specification of a research protocol allows to express enrolment criteria based on one or more active ingredients included in the current or past patient's therapy.
Support of description of pseudo-anonymisation (yes/no) within data set definition	A formal publishable specification of a research protocol allows to express if the citizen is asked to share identity information or pseudoanomysed health data has to be shared in order to participate in the described study.
Support of drug treatment plan within data set definition.	A formal publishable specification of a research protocol allows to include the treatment plan (both prescription and consumption of drugs) of the patient among the kind of health data that the citizen is required to share in order to participate in the described study.
Support of specification of prospective period within dataset definition.	A formal publishable specification of a research protocol allows to specify the period of time in the future during which the required health data will be required to be produced and shared by the citizen, in order to participate in the described study.
Support of specification of retrospective period within dataset definition.	A formal publishable specification of a research protocol allows to specify the period of time in the past that the required health data refers to and has to be shared by the citizen in order to participate in the described study.
Support of evaluation data (blood tests, vital signs, visits, instrumental examination) within data set definition.	A formal publishable specification of a research protocol allows to specify the health evaluation data (blood tests, vital signs, visits, instrumental examination) to be shared by the citizen in order to participate in the described study.
Automatic download of health records from S-EHR Cloud to S-EHR	When the citizen authorises the backup on the S-EHR Cloud, any new health data written on the S-EHR Cloud by an authorised application are automatically replied to on the S-EHR of the citizen. The alignment happens automatically each time that the smartphone of the Patient is connected to the internet.
Citizen's access to emergency token	A citizen may use a S-EHR to access and exchange with other applications an image with their "emergency token". The emergency token allows a qualified HCP (authorised by their organization) to identify the citizen and access their 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.
Encryption of S-EHR content exchanged with S-EHR Cloud.	Every data sent by a S-EHR to the S-EHR Cloud is encrypted by the S-EHR, before of the transmission, with a private key unknown to the S-EHR Cloud provider, so that the S-EHR Cloud provider cannot decrypt any stored data, but only the Citizen and the HCP can.
Storage and download of medical images on S-her	A citizen can also enable the storage, and import/download of Medical Images from the EHR or the S-EHR Cloud, on their S-EHR if the smart device has enough memory.

Citizen's access to Medical images from S-her	A citizen may access from the S-EHR their 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

2.5. User requirements for version 3 of the S-EHR

At the end of the third requirements gathering cycle, the following requirements were identified (here are presented the requirements that will be implemented within the third version, in bold those that will have a visual impact on the UI).

User requirement title	User requirement description
R2D import of (portion of) Hospital discharge reports from healthcare provider on S-her	Citizen health data (portion of Hospital discharge reports) can be imported from the citizen's national EHR on the citizen's S-EHR.
R2D import of (portion of) Prescription from healthcare provider on S-her	Citizen health data (portion of Prescriptions) can be imported from the citizen's healthcare provider on the citizen's S-EHR.
Integrity of medical information	Users are guaranteed that the managed health data (stored or transferred) hasn't been modified maliciously or accidentally.
Enabling of Citizen identification from S-EHR (with CA)	The S-EHR asks the Citizen and stores on the device a qualified certificate that identifies the Citizen. The certificate is released by a CEF eID trusted certification authority.
Citizen's consultation of the details of the research study	The citizen can consult the list of received invitations to research studies and see, for each of them, the details of requested health data, the purpose of the research, the data retention periods and the level of anonymization. The citizen may also consult the information document of the research, containing reference contacts of organisation and principal investigator, to be contacted for further details.
Digitally signature by Reference Research Centre of Citizen's consent	The Reference Research Centre digitally counter-signs the consent (to participate in a research study) signed by the citizen, and sends it back to the citizen.
Citizen's digital revocation of consent to share health data for a given study	A Citizen may revoke, directly from his/her S-EHR, a consent previously released to participate in medical research. The revocation of the consent using the S-EHR must be legally binding for the Reference Research Centre also in case the S-EHR does not support the digital signature of the consent by the citizen directly on the S-EHR.
Reminder of invitation to participate in a research study	If there is some invitation to which the citizen has still to answer, a notification is displayed periodically to remind him to decide.
Automatic anonymisation and	After a citizen accepts an invitation to a research study and the study

sharing of citizen's health data for research.	is started according to the specified protocol, the S-EHR automatically queries its content for the data required by the study, once or periodically, depending on the study, and automatically sends the matching data to the IEHR Research Network. The S-EHR anonymises the data before sharing it, if required by the protocol.
Addition of new S-EHR Cloud service to the S-EHR	The citizen adds a new S-EHR Cloud service to the list of certified S-EHR Cloud services of the S-EHR by inputting the URL of the service. Only S-EHR Cloud services that are conformant to the InteropEHRate S-EHR conformance levels may be added to the list of certified Cloud services.
Citizen's selection of reference region for research	After consenting to participate in the InteropEHRate Open Research Network, a citizen may choose, using the S-EHR, a reference region. The reference region is a geographical region that the citizen considers easy to reach and where a research centre is present to assist the citizen during the execution of the research protocol.
Support of specification of Reference Centres within research protocol	A formal publishable specification of a research protocol allows to specify the list of Research Centres (and relative region) that a patient participating in the study can select as a Reference Research Centre for the specific described study. The Research Centres are identified by a simple unique ID and described by name, specialty, address and contact information.
Automatic reception, matching and notification of enrolment criteria on S-EHR.	From the moment that a citizen accepted to participate in the InteropEHRate Open Research Network, the S-EHR will receive any new research protocol and will automatically match the health data of the citizen contained within the S-EHR with the enrolment criteria of the new protocol, without sending any personal data of the citizen to any party. The citizen is notified when a positive match is found.
Inclusion of human readable description of Coordinating and Local Research Centre within research protocol	A formal publishable specification of a research protocol refers to a human readable document (PDF) including a description of the research centre that will coordinate the specific study of the specific research centre (Local Research Centre) that will receive and process the shared health data.
Inclusion of human readable description of data retention period within the research protocol	A formal publishable specification of a research protocol refers to a human readable document (PDF) including a description of the amount of time that the researchers will be authorized to store and use any personal health fata shared by the citizen for that specific research protocol.
Inclusion of human readable description of purpose of research within the research protocol	A formal publishable specification of a research protocol refers to a human readable document (PDF) including a description of the purpose of the described research study.
Inclusion of human readable description of usage restrictions of	A formal publishable specification of a research protocol refers to a human readable document (PDF) including a description of all the

data within the research protocol	allowed and forbidden usages of any personal health data shared by the citizen for that specific 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 study, so accepting the condition described within the formal published specification of that research study.
Citizens' selection of reference research centre	The citizen selects through the S-EHR, the reference research centre, which is one of those centres within the geographical region previously selected by the citizen. The selection is notified to the reference research center.
Reception and storage of consent, digitally signed from research organisation, on Citizen's S-her	After that a consent to participate to a research protocol has been signed ~~on paper~~ form 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 the S-EHR.
Signed consent refers to the research protocol accepted by the patient.	A S-EHR will store the signed consent and will start to share health data on the InteropEHRate Open Research Network only if the signed consent refer to a research protocol already accepted by the Patient on the S-EHR.
Pseudoidentity restricted to single research protocol.	When a citizen gives a digital consent to participate in a research protocol, a specific pseudo-id for that patient will be generated, to be used only for the pseudonymization of data shared within that specific research protocol.
Notification to citizens of data sharing event for research	When the S-EHR of a citizen automatically shares new data as prescribed by a research protocol that the citizen consented to participate in, the citizen will receive a notification.
Citizen's consultation on S-EHR of S-EHR Cloud auditing data	A citizen may consult on the S-EHR the auditing data collected by the S-EHR Cloud.
R2D import from EHR to S-EHR of the vital signs and other measures	The vital signs and other measures taken during previous medical visits can be imported from the EHR of a healthcare provider to the S-EHR of the citizen.
Notification of access to health data on S-EHR Cloud	Whenever someone accesses the health data of the citizen stored on the S-EHR Cloud, the citizen is notified so that he/she can immediately change (i.e. regenerate) the QR code in case that the access was not authorised.
Encryption of health data written on S-EHR App	The personal data of the Citizen are stored on the mobile device by the S-EHR App in an encrypted format, decryptable only by the citizen, to avoid any unauthorized access on the data.
Encryption on anonymised S-EHR content exchanged with the RRC	Every data sent by a S-EHR to the RRC is encrypted by the S-EHR, before the transmission.

Authentication of the S-EHR App to the Pseudonym Provider	In the second variant of the protocol the user has to authenticate him/herself to the Pseudonym Provider in order to retrieve the pseudonym.
R2D import of Patient's Encounters and related health data from hospital EHR with eIDAS login	The citizen can import on the S-EHR app the description of any encounter with selected healthcare providers and related health data.
Treatment plan compilation on HCP App	During a medical visit an HCP can create and compile a new treatment plan for the patient using the HCP App.
D2D upload by HCP of diagnostic conclusions on S-EHR	An HCP can upload an evaluation report on the S-EHR of the subject Citizen using the D2D protocol
D2D upload by HCP of Treatment Plan on S-EHR	An HCP can upload the treatment plan on the S-EHR of the subject Citizen using the D2D protocol
Consultation of treatment plan on S-EHR	The Citizen can consult the treatment plan from the S-EHR
Selection of healthcare providers for R2D Access	The citizen can consult the list of hospitals trusted by the S-EHR that provides an R2D Access Service and can select the ones from which to download his or her health data.
Notice of R2D Access usage terms	When the citizen asks for the import of health data by R2D Access, the S-EHR gives notice that using R2D Access the citizen authorises the healthcare provider to convert/translate and transmit health data to the S-EHR.
Automatic check and download of new health data by R2D Access	If asked by the citizen, the S-EHR will automatically import, without any further user confirmation, any new or updated HR data available from the selected healthcare provider.
Automatic check and manual approval of download of new health data by R2D Access	If asked by the citizen, the S-EHR will automatically check the availability of new or updated health data from the selected healthcare provider, will notify the citizen if there is any and will download them after confirmation by them.
Selection of Encounters to download by means of R2D Access	The citizen can choose to import all the health data available from a selected healthcare provider or just the health data related to specific medical encounters.
Browsing by Encounter of health data on S-EHR	The citizen can browse the health data available on the S-EHR by the associated medical encounter.
Filtering by date and type of health data on S-EHR	When consulting the health data available on the S-EHR the citizen can filter them by date and type.
Deletion of selected health data from S-EHR by the Citizen	The citizen can remove from the S-EHR any selected health data.
Manual input of health data by the citizen on the S-EHR	The citizen can add new health data on the S-EHR.
Import of health data by the	The citizen can import on the S-EHR health data measured by

citizen on the S-EHR from personal devices	personal devices.
Consent, exchange and storing of citizens' face (photo) on the S-EHR and S-EHR Cloud	If the citizen gives explicit consent the S-EHR and S-EHR Cloud are able to store and exchange with the HCPs also a photo of the citizen's face to identify the patient during the emergencies.
Printing of citizen's QR-code	The citizen can print the QR-code generated by the S-EHR app.
Update of citizen's QR-code	The citizen can ask the S-EHR app to generate a new QR-code and update the S-EHR Cloud content accordingly.
Support of multicentric studies within publishable research protocol	A formal publishable specification of a research protocol allows to define a multicentric protocol.
Support of symptoms within dataset definition of publishable research protocol	A formal publishable specification of a research protocol allows to define the information related to citizens' symptoms to be included in the dataset to be retrieved from the S-EHR.
Support of healthcare treatments within dataset definition of publishable research protocol	A formal publishable specification of a research protocol allows to define the information related to citizens' healthcare treatments to be included in the dataset to be retrieved from the S-EHR.
Support of exit criteria within publishable research protocol	A formal publishable specification of a research protocol allows to define the exit criteria for the exclusion of a citizen form the research study.
R2D-Access to DICOM references	The Citizen may receive from the R2D-Access service health data that contains a reference to a downloadable DICOM studies.
Download on S-EHR of referred DICOM Studies	The Citizen can download on the S-EHR any DICOM study referred to by previously downloaded health data.
Support of questionnaire within dataset definition of publishable research protocol	A formal publishable specification of a research protocol allows to define a questionnaire for collecting self-reported health data from the patient (e.g. side effects from anti-hypertensive medications) .which answers must to be included in the dataset to be retrieved from the S-EHR.
Execution of questionnaire defined by research protocol	At the time specified by the formal specification of the research protocol the citizen is invited to answer on the S-EHR to the defined questionnaire and the answers are stored by the S-EHR.

Table 3 - User requirements for the third version of the S-EHR

2.6. 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 [D2.6].

After setting up the development environment to start the coding of the S-EHR-A, the consortium decided to work in an "agile" way[2]. 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 suited to software development, and have the advantage to provide concrete results faster. It is also very efficient to respond rapidly to potential unpredicted difficulties.

[2] 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 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 men/years of development. On the other hand, 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, organisations active in clinical studies or research with explicit consent from patients, to participate in patient reported outcomes or experience initiatives.

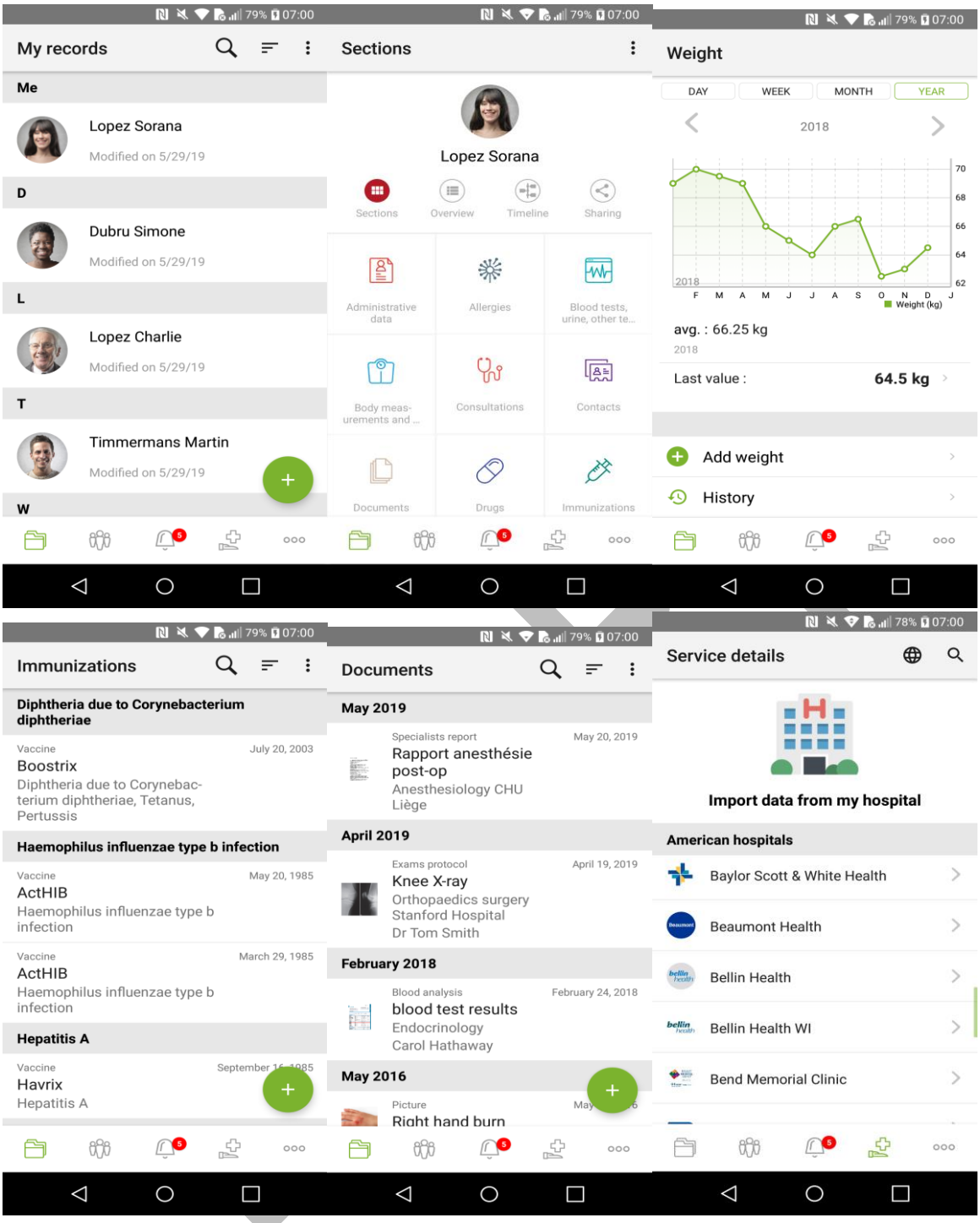

Figure 1 - Screenshots of the core application

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 their password. Now the user can start using the application.

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

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

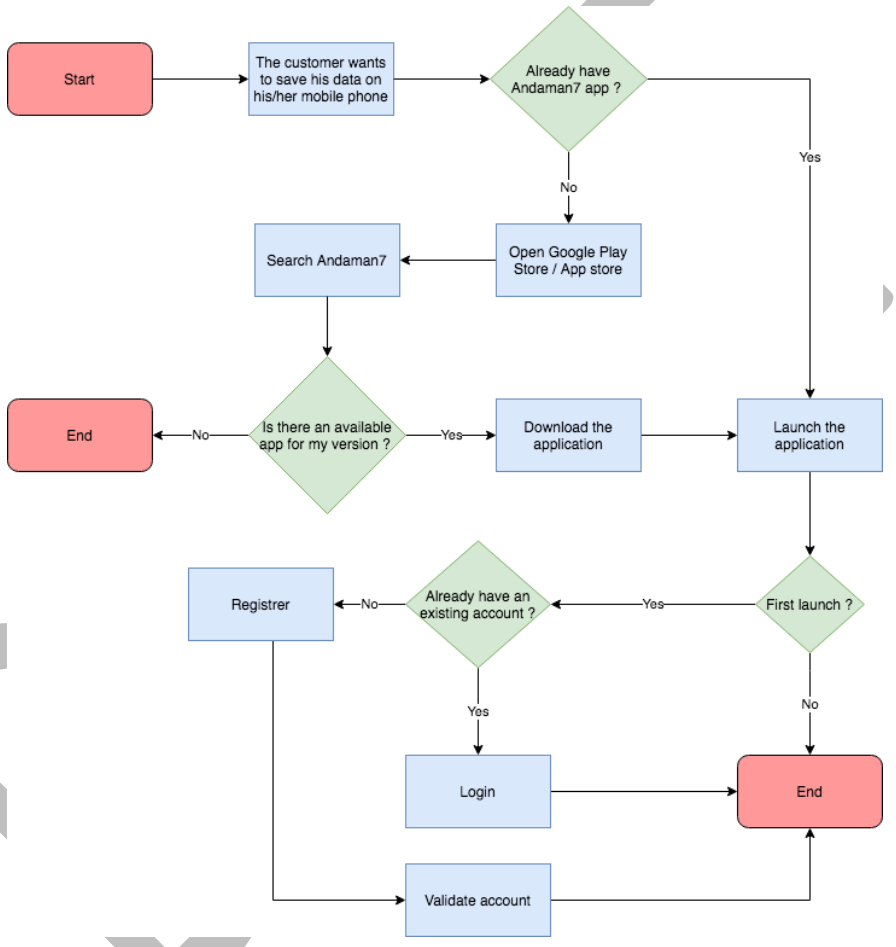

Figure 2 - User flow diagram: Download and launch of the core application

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), they must check a widget to give their consent to the core application for the storage and management of their 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 they wants to add. Then they 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.

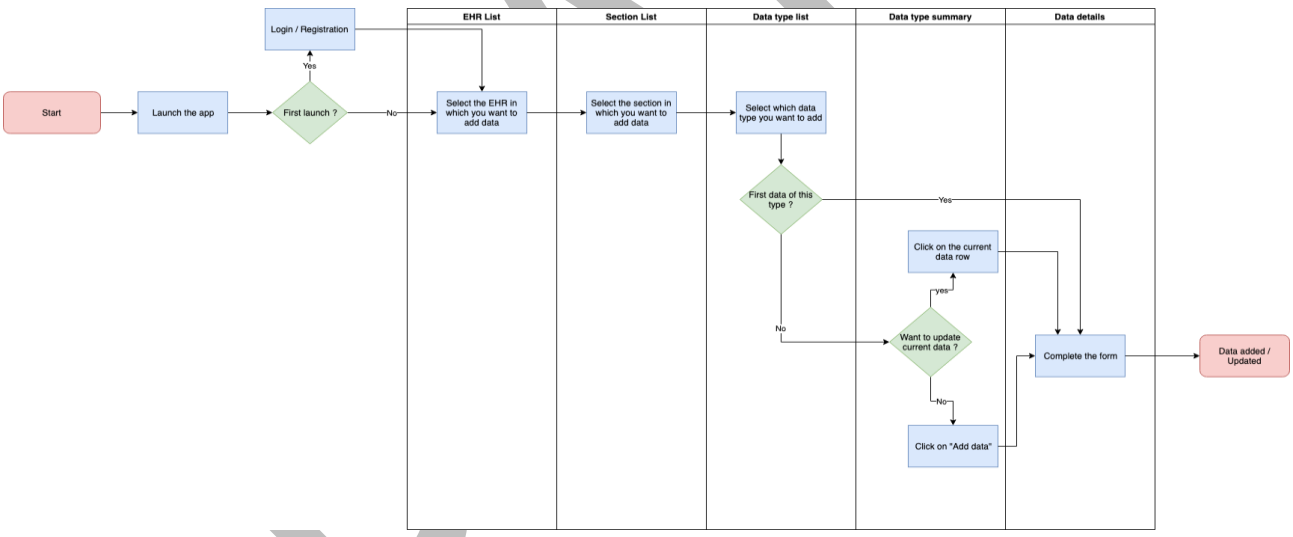

Figure 3 - User flow diagram: Add / Update a data

- **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 their health data with their healthcare professional (they need 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 their data himself.
  - The second one is to share their EHR with a trusted user. If the user loses or changes their mobile, they would have the possibility to easily retrieve their data.

  Once the user has chosen a trusted user to share their data with, they can decide which data type they wants to share through a selection list.

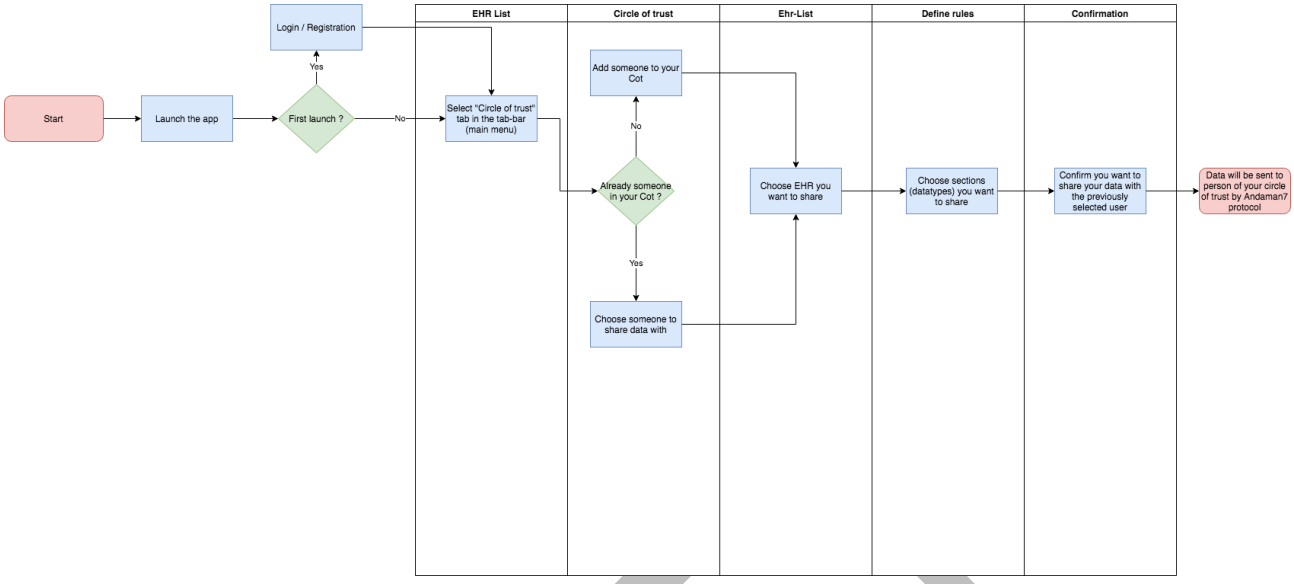

Figure 4 - User flow diagram: Share data

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 three mobile side protocols of this project:

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

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

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 their 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 they approaches again.

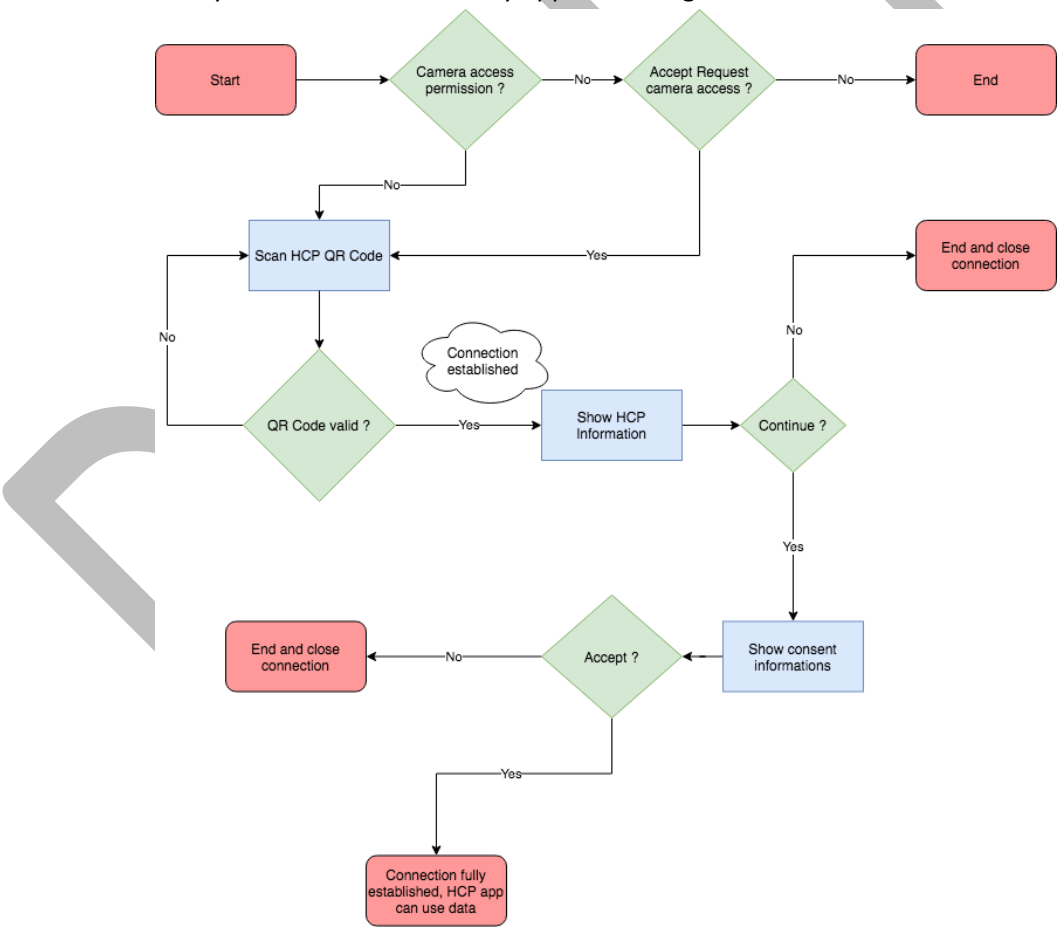

Figure 5 - User flow diagram: S-EHR D2D protocol

4.2. User flow of S-EHR-A R2D protocol

The R2D protocol is a protocol that orchestrates the data exchange from any EHR with the usage of the internet. It provides the S-EHR the possibility to retrieve health data from a hospital.

The first step is the identification of the citizen using trusted user certificates, this will be done by using eIDAS. eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. It is legally binding in the EU and also acts as a blueprint for trust services projects all over the world. Once the citizen is correctly identified, the citizen will retrieve health data from their hospital. Their health data will be inserted into their personal EHR stored on their S-EHR.

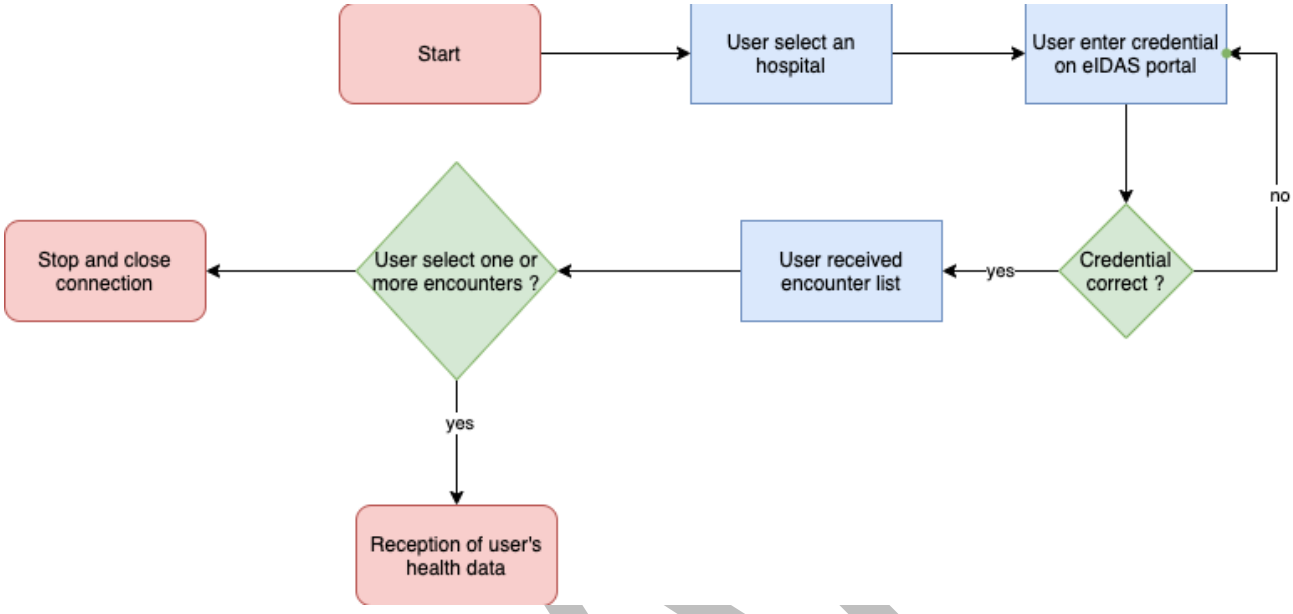

Figure 6 - User flow diagram: S-EHR-A R2D Access protocol

4.3. User flow of S-EHR-A Research protocol

The research protocol is the protocol that will orchestrate the exchange of data between the three parties involved in this scenario:

- The **Central node** that will provide to the S-EHR app the list of potential research studies the citizen can participate in;
- The **S-EHR app** that regroups the health data of the citizen;
- The **Reference research center** that will collect the health data sent by the S-EHR app.

We can highlight three phases during the process. The first one is the opt-in phase, during which the citizen accepts through the S-EHR app to be part of the research network, and receives the studies information. The second one is the enrolment phase, where citizens accept to participate in a dedicated study. The third and final one is the data retrieval phase, during which the health data required by the study is frequently sent from the S-EHR app to the reference center selected by the citizen during the enrolment phase.

The citizen has full control over the process, and can stop it whenever they wants.

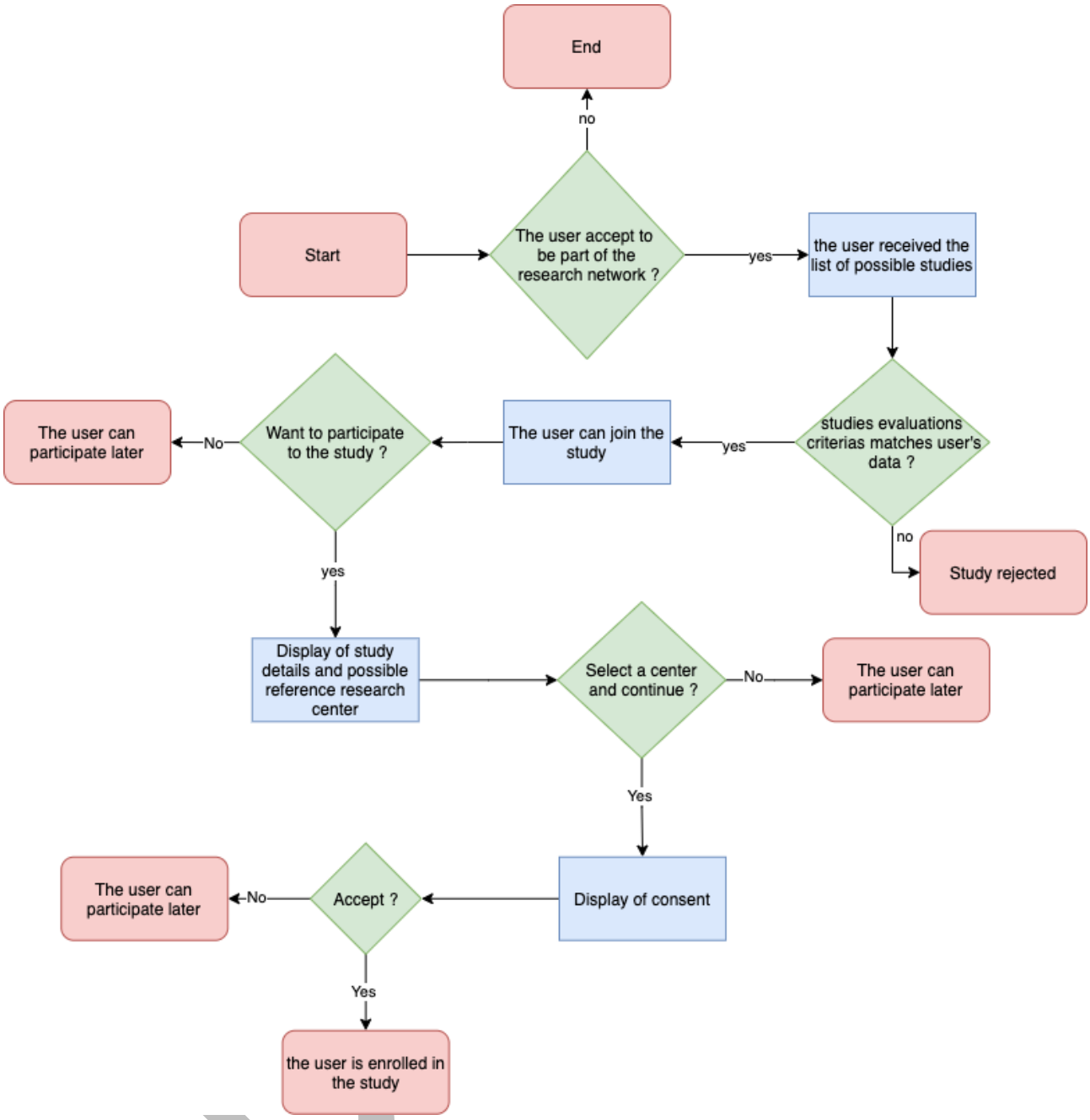

Figure 7 - User flow diagram: RDS protocol

4.4. User flow of S-EHR-A Emergency protocol

The emergency protocol is the protocol that will orchestrate the exchange of data between the S-EHR app and the S-EHR Cloud.

Two features can be highlighted:

- **Data storage**: the citizen can use the S-EHR cloud as an online backup for his health data.
- **Emergency access**: in an emergency situation, an authenticated HCP can access a citizen's health data.

The citizen can use the storage feature, and refuse to allow the access to their health data in emergency situations. But the storage feature is mandatory to use the S-EHR Cloud.

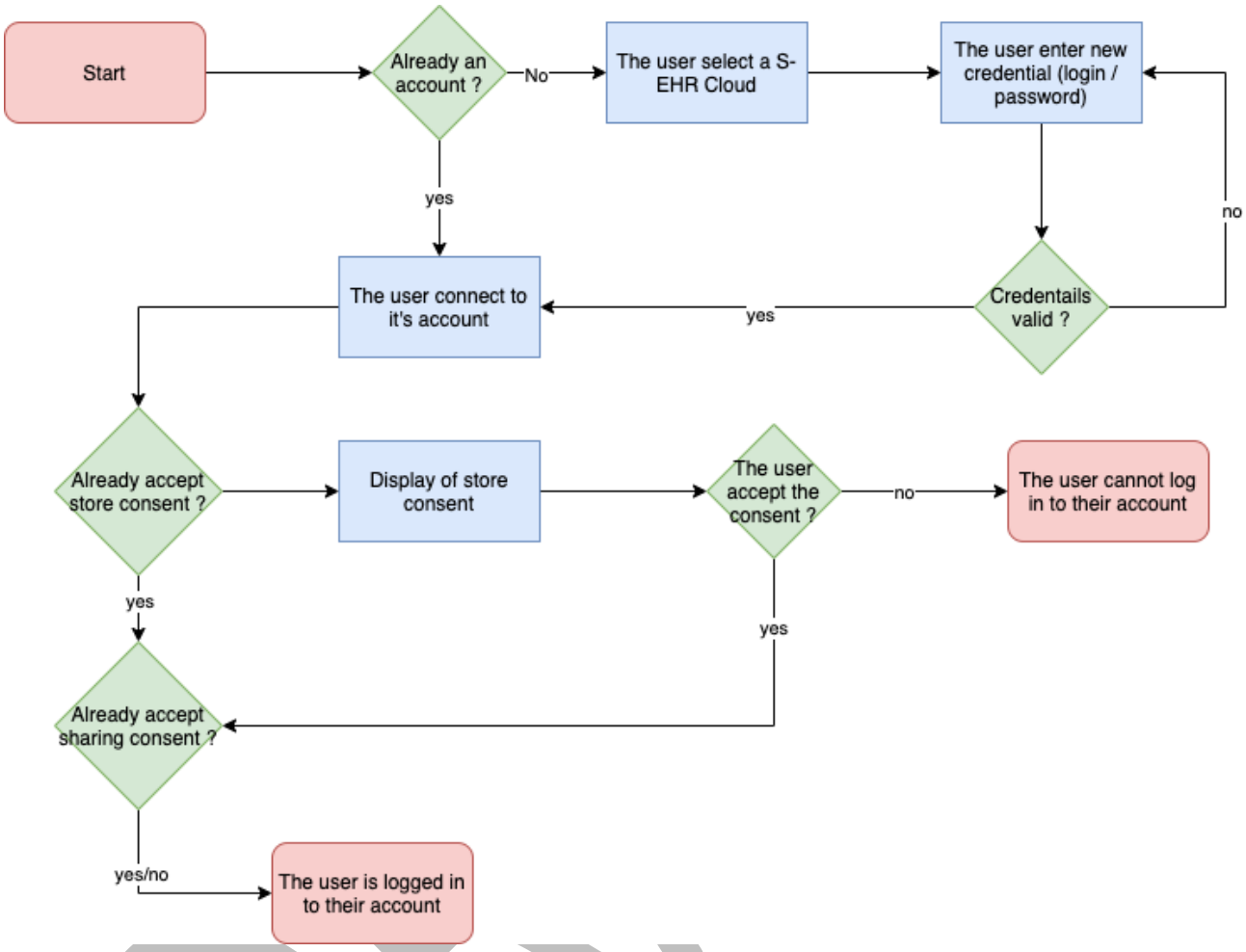

Figure 8 - User flow diagram: R2D Emergency protocol

4.5. 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 all the protocols through the security library. More information regarding the encryption/decryption functionalities are provided in the deliverable D3.6 [D3.6]. In addition, as already introduced in the deliverable D3.3 [D3.3], the QR code scanned by the user with their 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), they has access to the related service. After giving consent to the terms of service, the user will have access to the related 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 their national EHR at the end of the development of the S-EHR-A:

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

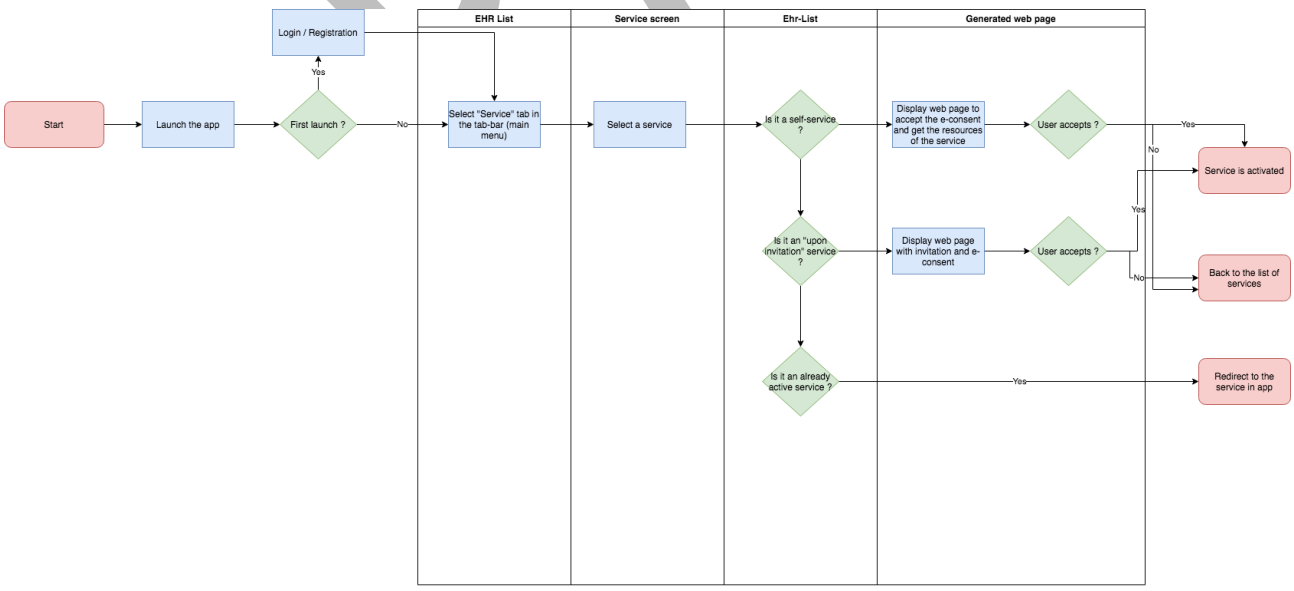

Figure 9 - User flow diagram: register to service

5.1.2. Consultation of health data sharing audit by the citizen on their S-EHR

The citizen should be able to consult the history of their sharing operations, whether the sharing was performed by means of the D2D protocol, R2D protocols 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 on the other side of the exchange;
- **Type:** type of exchange (data reception, data sending, both) from the point of view of the citizen;
- **Section(s):** which section(s) of the citizen'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.

5.1.3. Translation/Conversion of health data

Data retrieved from a hospital will be translated/converted to be understandable by the citizen, but at all times the citizen must be able to see the original value (value before translation/conversion).

This mechanism will be present in the core Andaman7 application, in the interface to see the details of a health data.

5.1.4. Execution of questionnaire defined by research protocol

During a study, in addition to health data collected, the citizen may have to fill in a questionnaire in order to collect additional data such as mental state, etc. Questionnaires should be completed at a frequency defined in the study protocol, citizens should be notified when a questionnaire is to be completed.

The core application used for the pilot already contains a module allowing the citizen to fill in a questionnaire as part of a clinical study, and it is this module that will be used for the reference implementation.

Each questionnaire will be defined by:

- a unique identifier;
- a frequency;
- a list of questions and answers.

The questionnaires will also be linked to a study, which includes a start date and an end date for completion. The questionnaire data will be sent to the reference centre chosen by the citizen during the enrolment phase.

5.2. Requirements integrated as new features of the core app

5.2.1. Scenario 0 - S-EHR feed

5.2.1.1. *Selection of healthcare providers for R2D Access*

The citizen can consult the list of hospitals trusted by the S-EHR that provide an R2D Access Service and can select the ones from which to download their health data. To facilitate the selection of the hospital desired by the citizen, the S-EHR app allows a search on the name of the hospital, and to filter the list according to the country of the hospital.

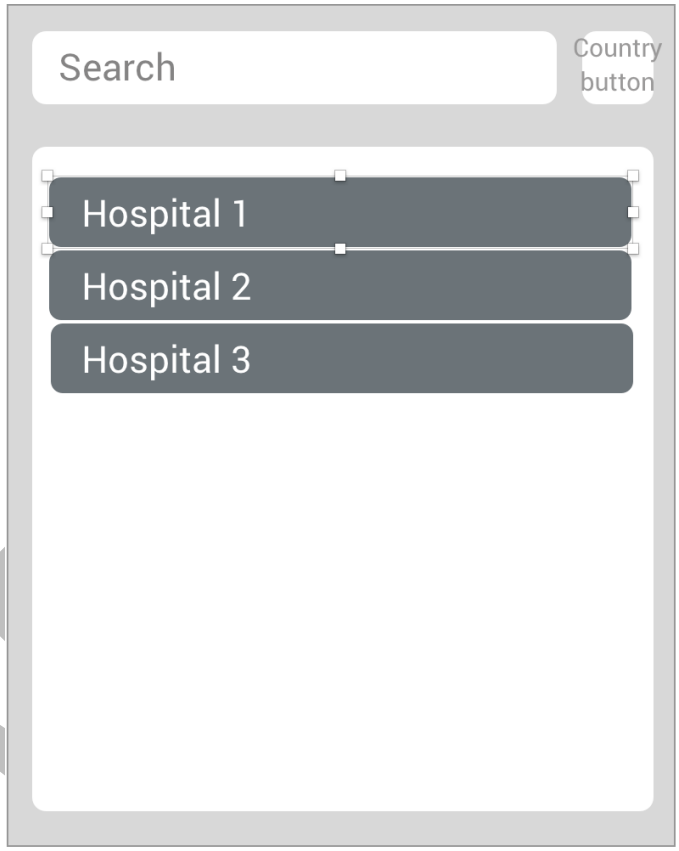

Figure 10 - Wireframe: hospital selection

5.2.1.2. *Selection of Encounters to download by means of R2D Access*

The citizen can choose from which encounter they wish to retrieve their health data. Once one or more encounters are selected, they will receive all the data related to the selected encounter.

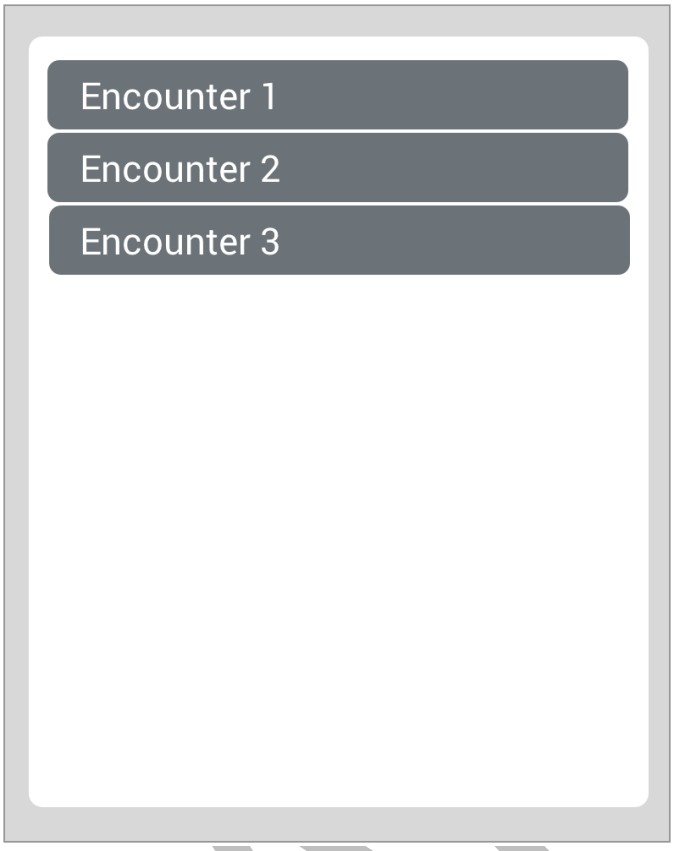

Figure 11 - Wireframe: Encounter selection

5.2.2. Scenario 1 - Medical Visit

5.2.2.1. *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 their 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 them that the connection to the HCP has started.

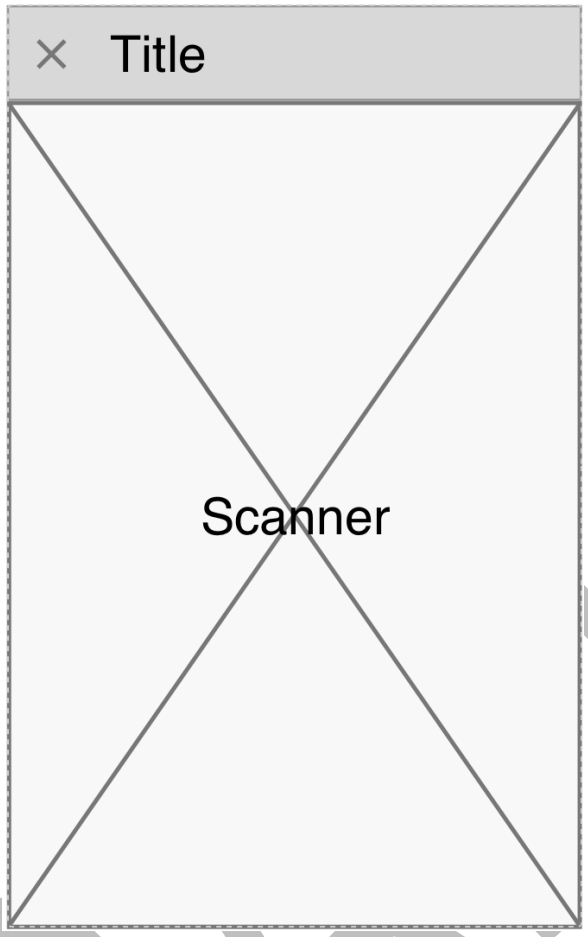

Figure 12 - Wireframe: D2D device pairing

5.2.2.2. *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, their 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).

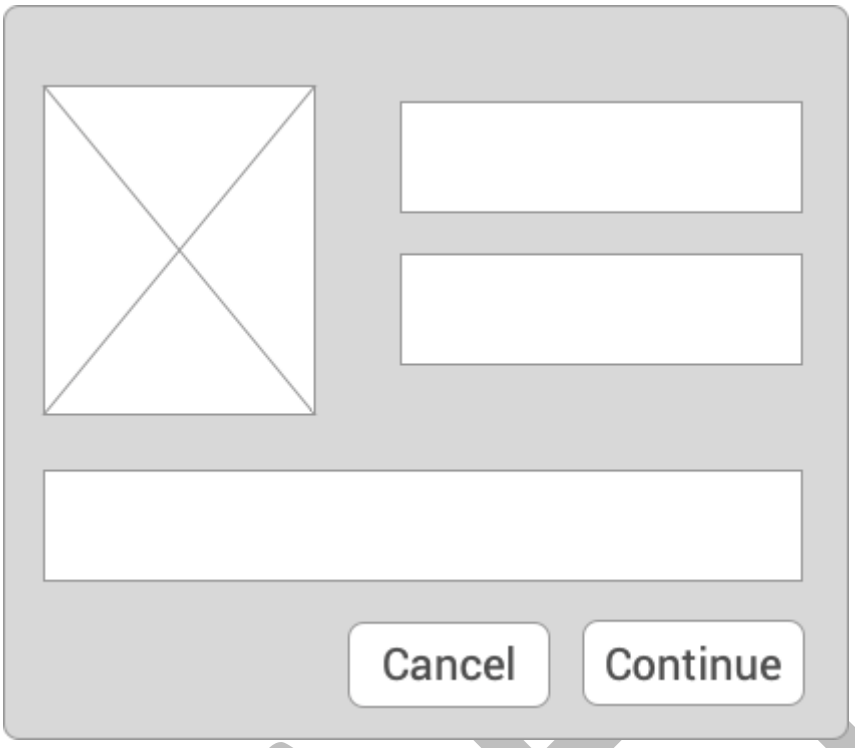

Figure 13 - Wireframe: D2D visualization of the healthcare organization by the citizen

5.2.2.3. *D2D access consent to healthcare organization by the citizen*

Following a co-design session 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 13] the user gives their consent for sharing their personal data with the HCP application.

5.2.2.4. *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 their consent for sharing their 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.

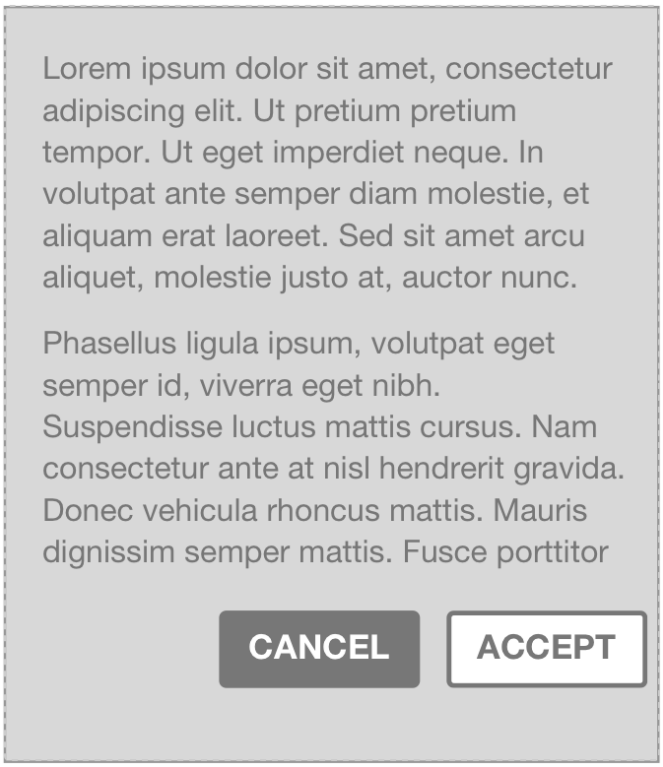

Figure 14 - Wireframe: D2D consent by the citizen to the healthcare organization for temporary S-EHR access

5.2.3. Scenario 2 - Emergency

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

The InteropEHRate project has foreseen the deployment of a S-EHR Cloud to allow access to data in emergency situations. As an extended feature, this cloud storage can also be used by the citizen as a backup of their health data (even if the citizen doesn't want to share their data in emergency situations). These two functionalities will be separated by two different consents that the citizen can accept (or not).

Multiple clouds can be present on the same network. At account creation, the citizen can choose which one they want to use to store their health data. To create an account, the citizen needs to provide a login and a password; the minimum complexity of the password is defined in the cloud (so it could be different for each cloud).

The citizen can connect to the selected S-EHR Cloud with the account they just created, or with an already existing account. Once the citizen is connected, and the storage consent is accepted, the S-EHR app will download the health data already stored on the S-EHR Cloud (if there is any), and upload the health data stored locally on the phone. As long as the citizen is connected to the cloud, the S-EHR app will keep the health data as up-to-date as possible by uploading new/updated data.

The health data type that will be stored on the cloud will be the same that the one managed during the remote to device protocol.

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

Citizens can consent to 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 from 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.

5.2.3.3. *Citizen's access to emergency token*

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

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

5.2.3.4. *Consent, exchange and storing of Citizens' face (photo) on the S-EHR and S-EHR Cloud*

Among the data that will be stored on the Cloud, we will find the data that will allow the party accessing the data to identify a citizen in an emergency situation.

These data will be upload with health data:

- Last name
- First name
- Birth date
- Sex
- Address
- Town
- Country
- Zip Code
- Photo

The data stored on the cloud can be shared only if the citizen allows the sharing feature (by accepting the sharing consent). And only with certified third parties.

5.2.3.5. *Automatic download of health records from S-EHR Cloud to S-EHR*

The first time the citizen will connect to an existing account on the cloud, the application will download the already stored health data, and merge it with the local health data stored on the S-EHR app.

5.2.4. Scenario 3 - Research

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

The citizen can subscribe to their 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 their S-EHR. The Open Research Network adds the citizen to the list of subscribers who can receive a notification for a research.

5.2.4.2. *Citizen's withdrawal from research network*

A citizen can opt out from the Research Network. When they choose to opt out, the S-EHR sends the request to the Research Network where the citizen is removed from the subscriber list.

5.2.4.3. *Automatic reception, matching and notification of enrolment criteria on S-EHR*

Once they are registered to the research network, the app will check at regular intervals of time if there are new research studies the citizen can participate in. This check should be done at least once a day.
The S-EHR app will compare locally stored health data of the citizen with the enrolment criteria of each new study.

If their health data matches the criteria, they will receive a notification in the application, and on the phone. Starting from this point, they will be able to access details of the study, and start the enrolment process if they want.

5.2.4.4. *Reminder of invitation to participate in a research study*

Until a study is marked as seen by the citizen, a notification will be sent to the citizen once a day as a reminder to check it. This notification will remind the citizen that they have one or more studies to check in the application.

5.2.4.5. *Invitation of candidate citizens to participate in a research study*

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

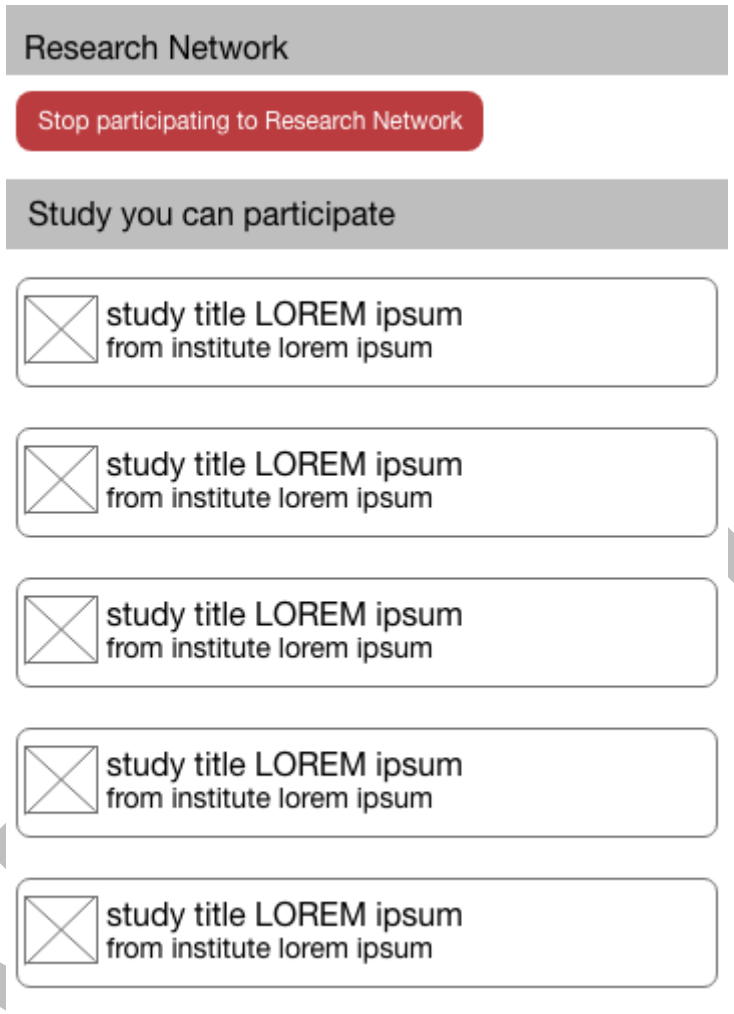

Figure 15 - Wireframe: Invitation of candidate citizens to participate in a research study

5.2.4.6. *Citizen's consultation of the details of the research study*

The citizen will be able to see details of a study before enrolling in it.

These details include:

- A description of the research;
- By which research centers this research is conducted;
- The benefits and objectives;
- Which data will be shared;
- When it will be shared;
- The period for how long the data will be kept.

5.2.4.7. *Citizens' selection of reference research center*

The citizens have the possibility to select which research centers will collect their health data among those defined in the file describing the study.

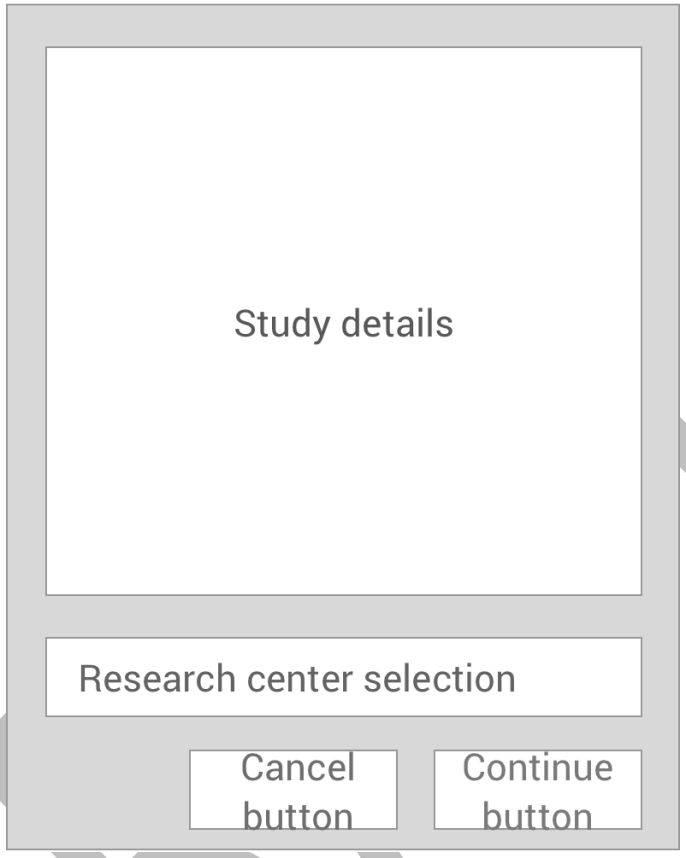

Figure 16 - Wireframe: Study details

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

Before being considered as enrolled in the study, the citizen will have to accept a consent for sharing their health data with the research center, for the purpose of the study. This consent needs to be approved and signed digitally by the two parties .

5.2.4.9. *Citizen's digital revocation of consent to share health data for a given study*

At any time, the citizen can withdraw from a study. From this event, the S-EHR app will stop sharing health data with the selected research center, but the health data already sent to the research center will still be used until the end of the study or until the citizen leaves the research network.

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. Scenario 0 - S-EHR feed

6.1.1.1. *Selection of healthcare providers for R2D Access*

The citizen can consult the list of hospitals trusted by the S-EHR-A that provides an R2D Access Service.

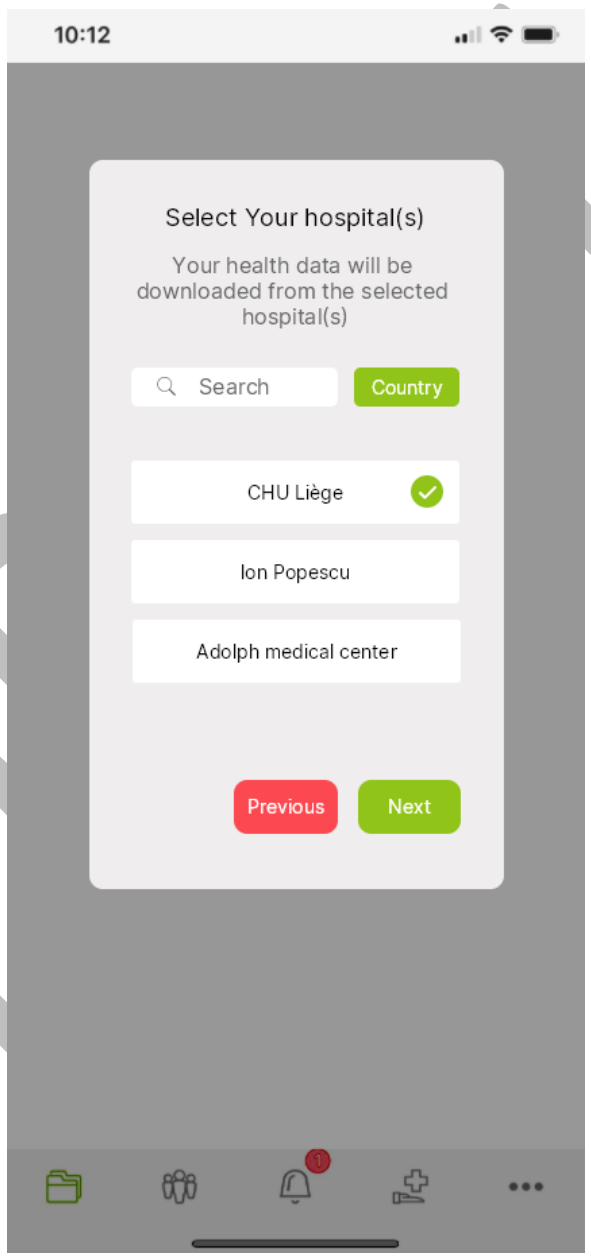

Figure 17 - Mockup: Hospital selection

6.1.1.2. *Selection of Encounters to download by means of R2D Access*

The citizen can choose from which encounter they wish to retrieve their health data.

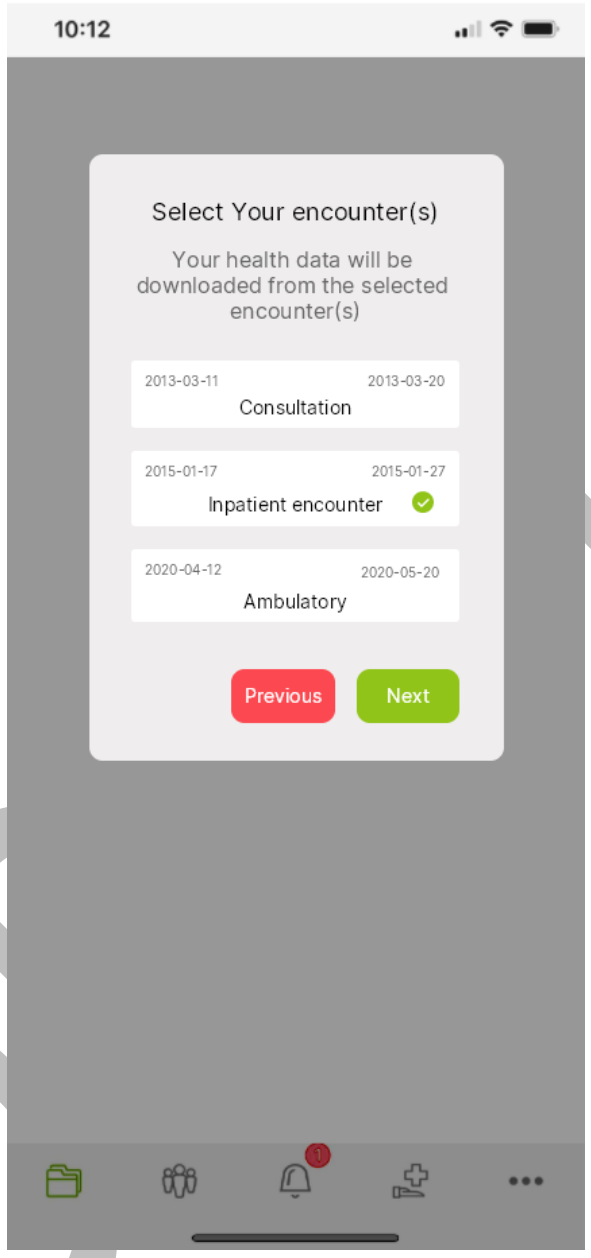

Figure 18 - Mockup: Encounter(s) selection

6.1.1.3. *Consultation of health data sharing audit by the citizen on their S-EHR*

In the first view, the citizen can see the full history of their 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.

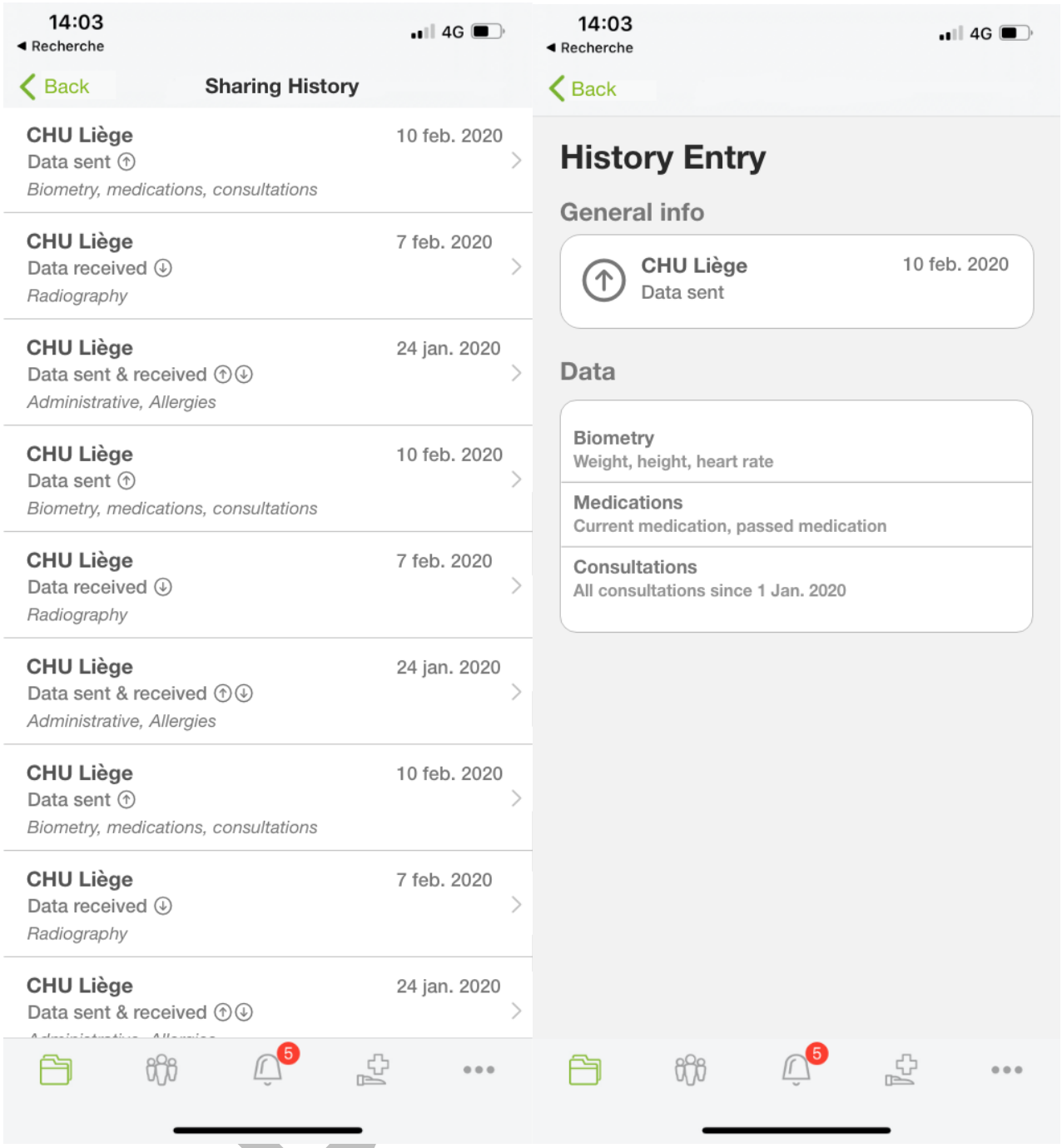

Figure 19 - Mockup: Consultation of health data sharing audit for citizen on the S-EHR

6.1.2. Scenario 1 - Medical Visit

6.1.2.1. *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.

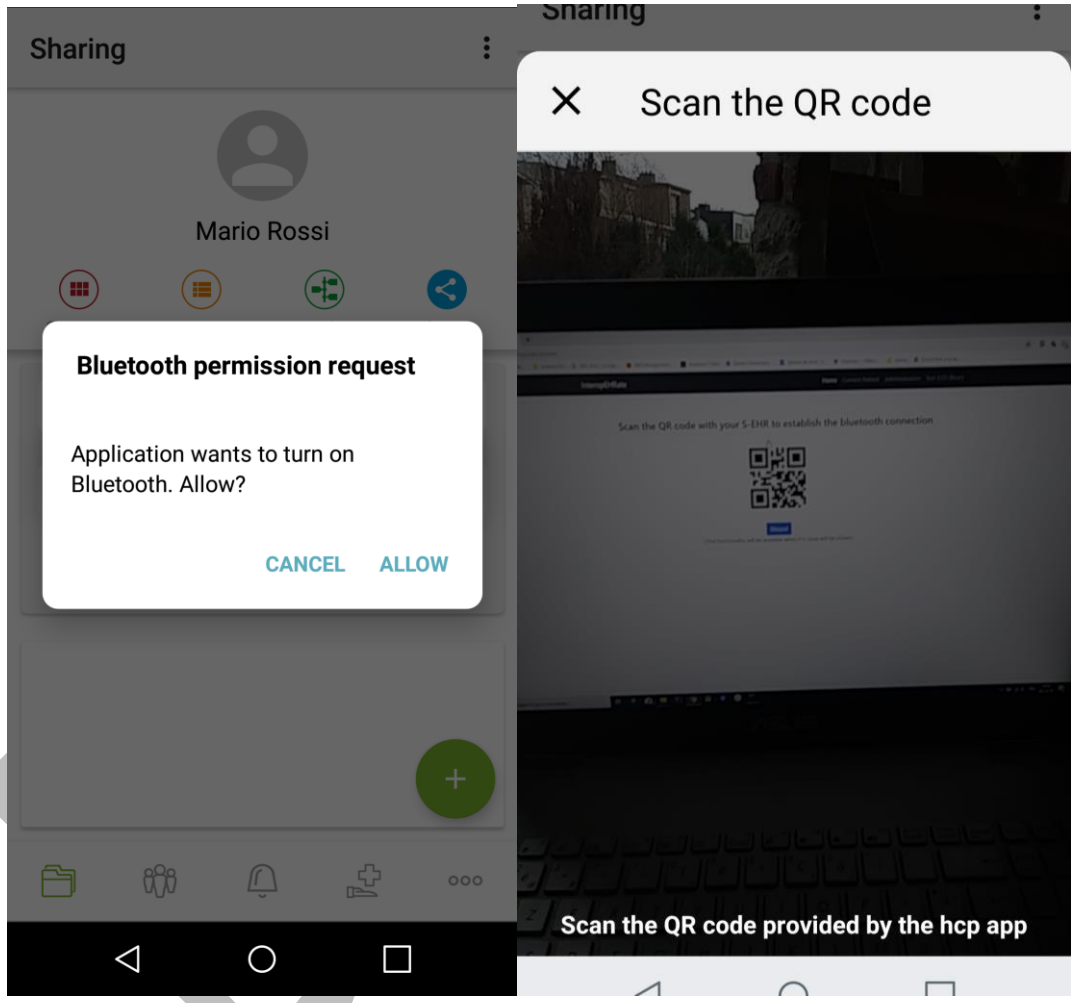

Figure 20 - GUI: D2D device pairing

6.1.2.2. *D2D visualization of the healthcare organization by the citizen*

The HCP information is shown in a dialog.

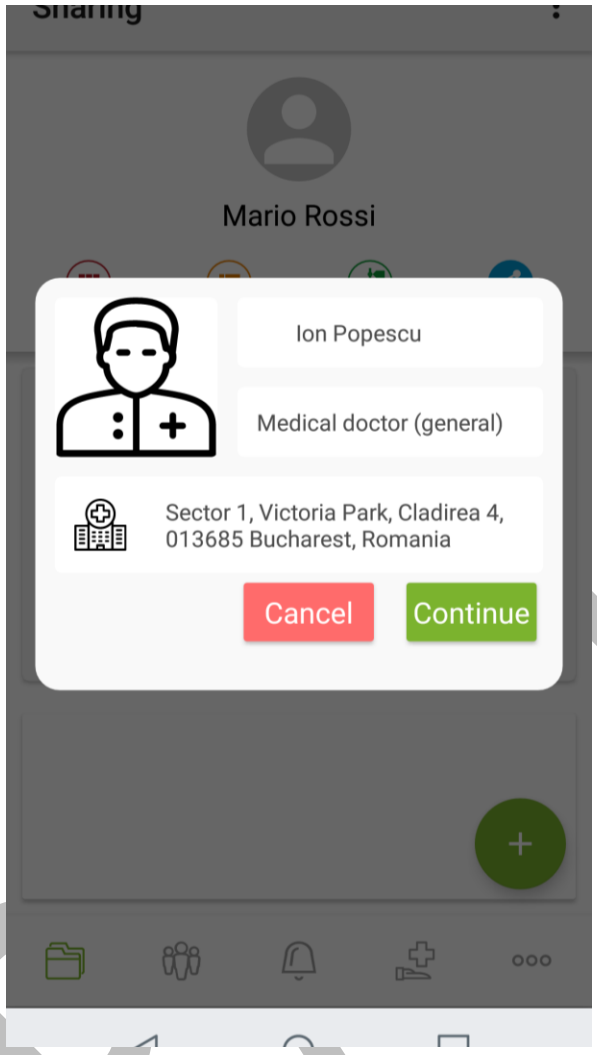

Figure 21 - GUI: D2D visualization of the healthcare organization by the citizen

6.1.2.3. *D2D consent by the citizen to the healthcare organisation for temporary S-EHR access*

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

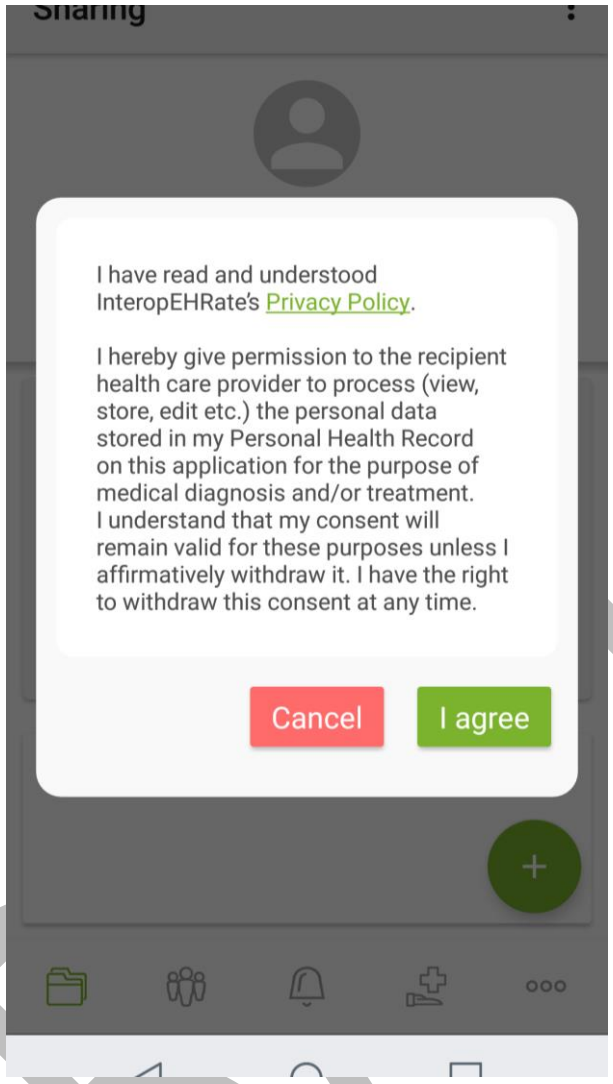

Figure 22 - GUI: D2D consent by the citizen to the healthcare organization for temporary S-EHR access

6.1.3. Scenario 2 - Emergency

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

The citizen can log on to an existing account on a chosen cloud, or create a new account. In the first case, the data already on the cloud will be downloaded and merged with the citizen's health data already on the phone.

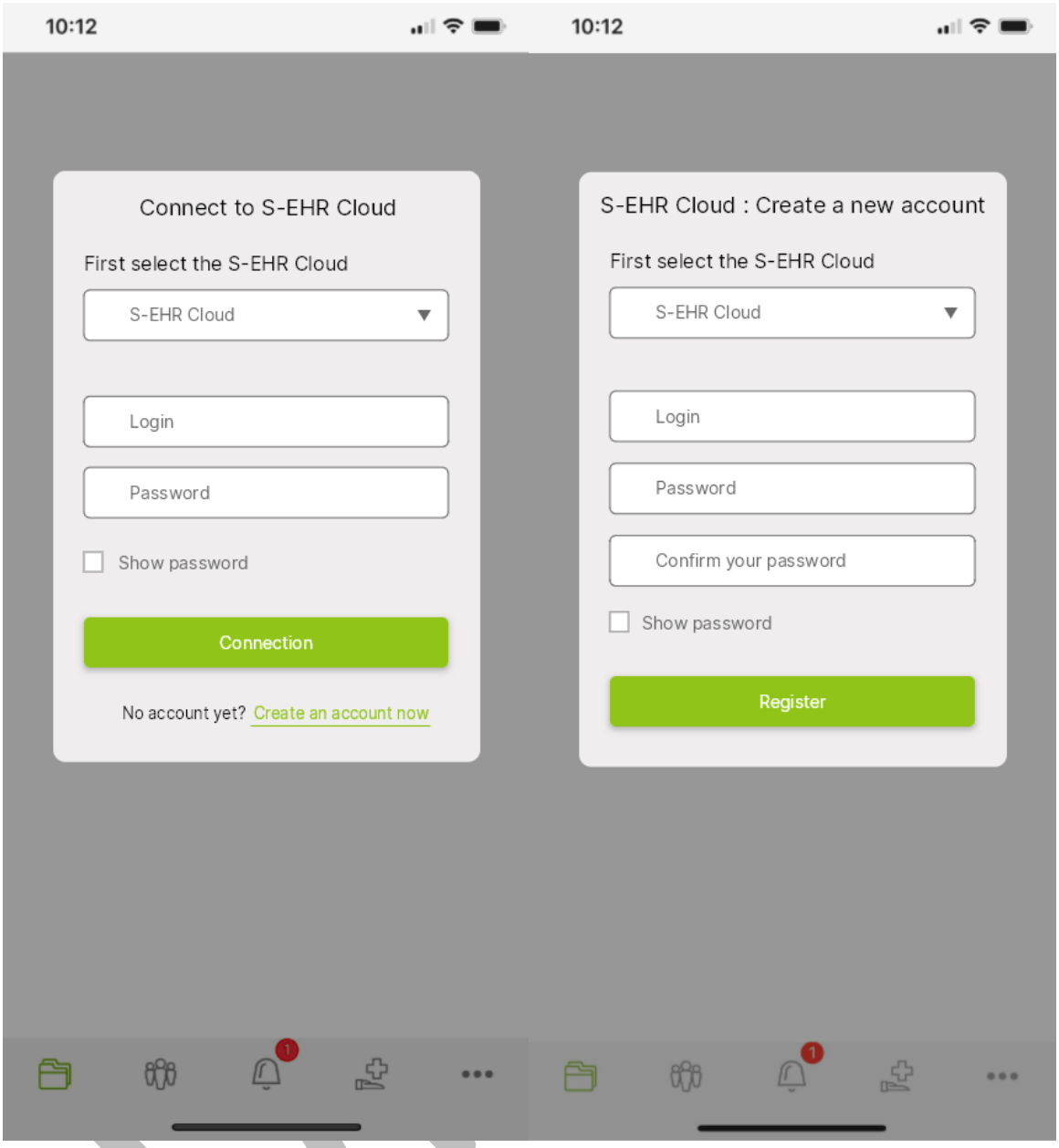

Figure 23 - Mockup: Cloud account creation / login

6.1.3.2. *Consent, exchange and storage of Citizens' face (photo) on the S-EHR and S-EHR Cloud*

The citizen has to accept two consents. The first one is related to the functionality of storage and backup of data on the cloud, this one is mandatory. The second one concerns the functionality of sharing his data stored on the cloud in case of an emergency situation, this one is optional. If the second one is not accepted, the sharing functionality will not be available, but the citizen can at any time revoke or accept this consent while logged into his cloud account.

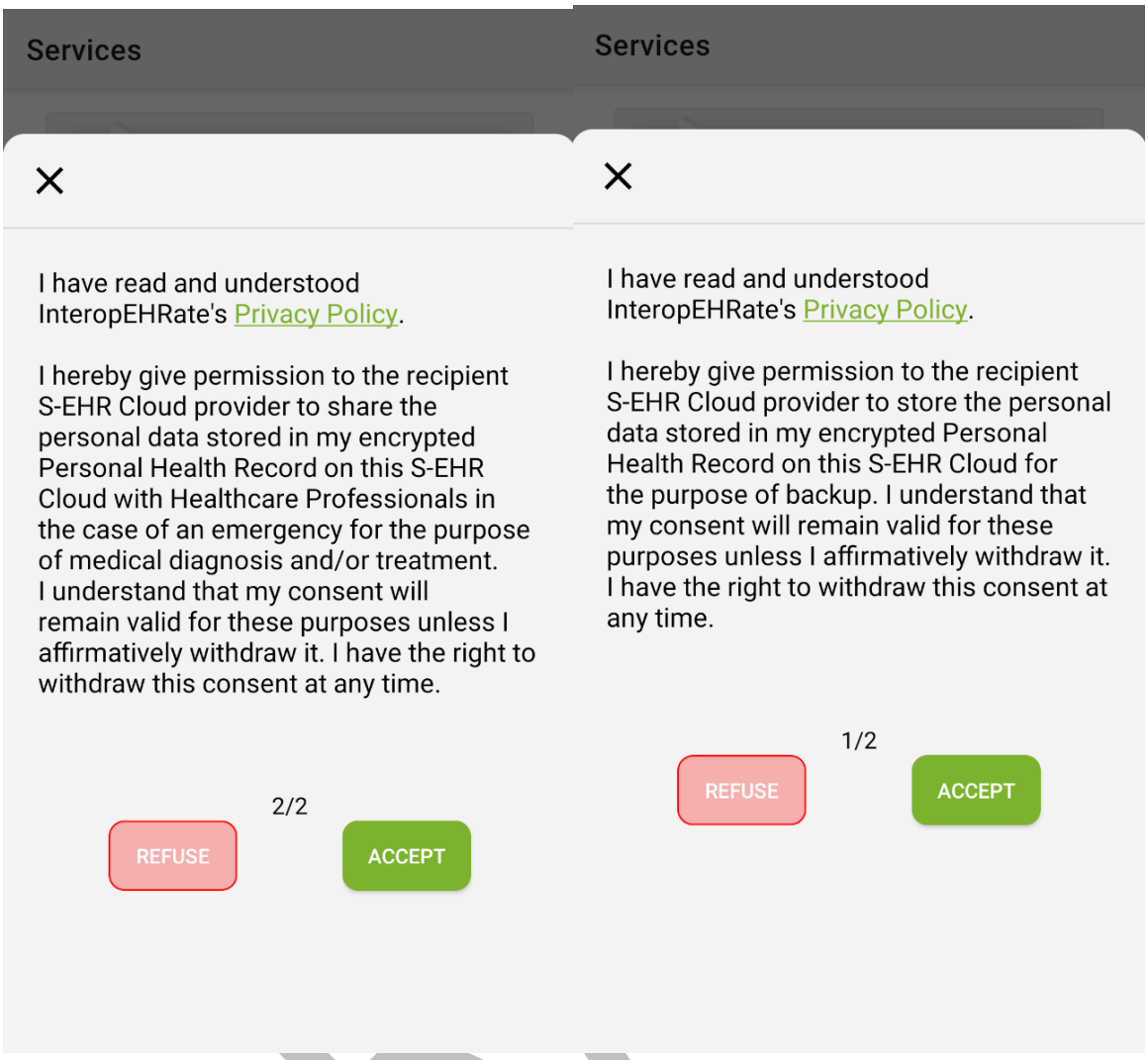

Figure 24 - Mockup: S-EHR Cloud storage consent & emergency sharing consent

6.1.3.3. *Citizen's access to emergency token*

Once logged in, the citizen has access to different possibilities such as logging out, deleting the account or revoking/accepting data sharing. They also have access to the QR code used to share their data. This QR code is only displayed if the sharing consent is accepted.

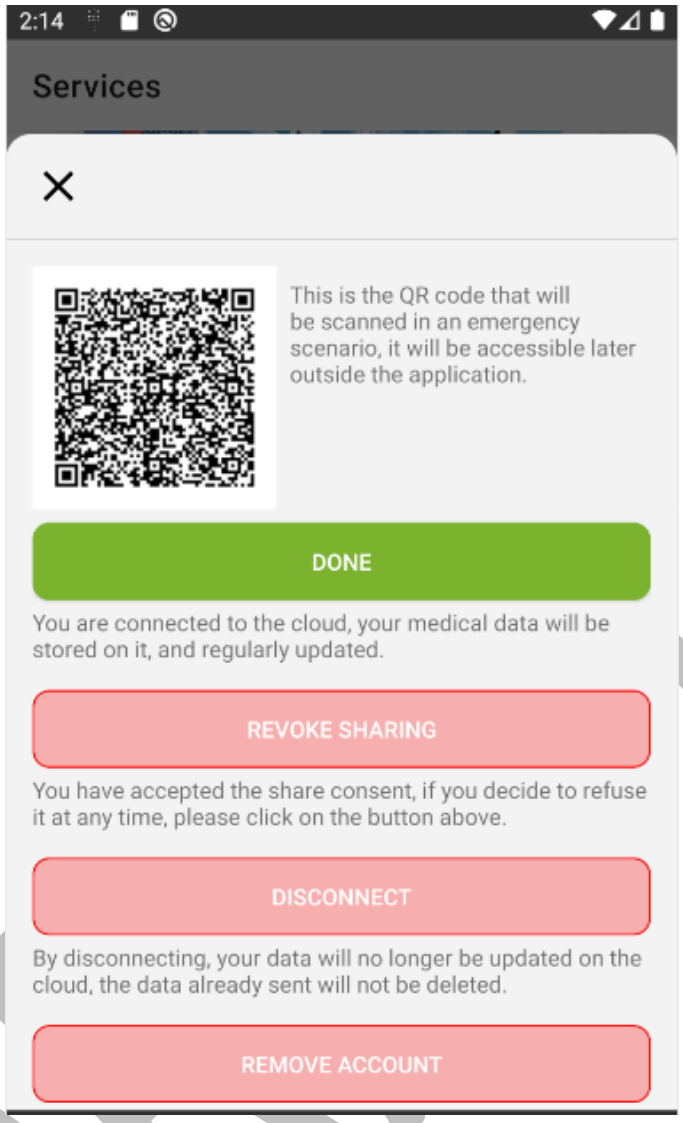

Figure 25 - Mockup: S-EHR Cloud account details

6.1.4. Scenario 3 - Research

6.1.4.1. *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.

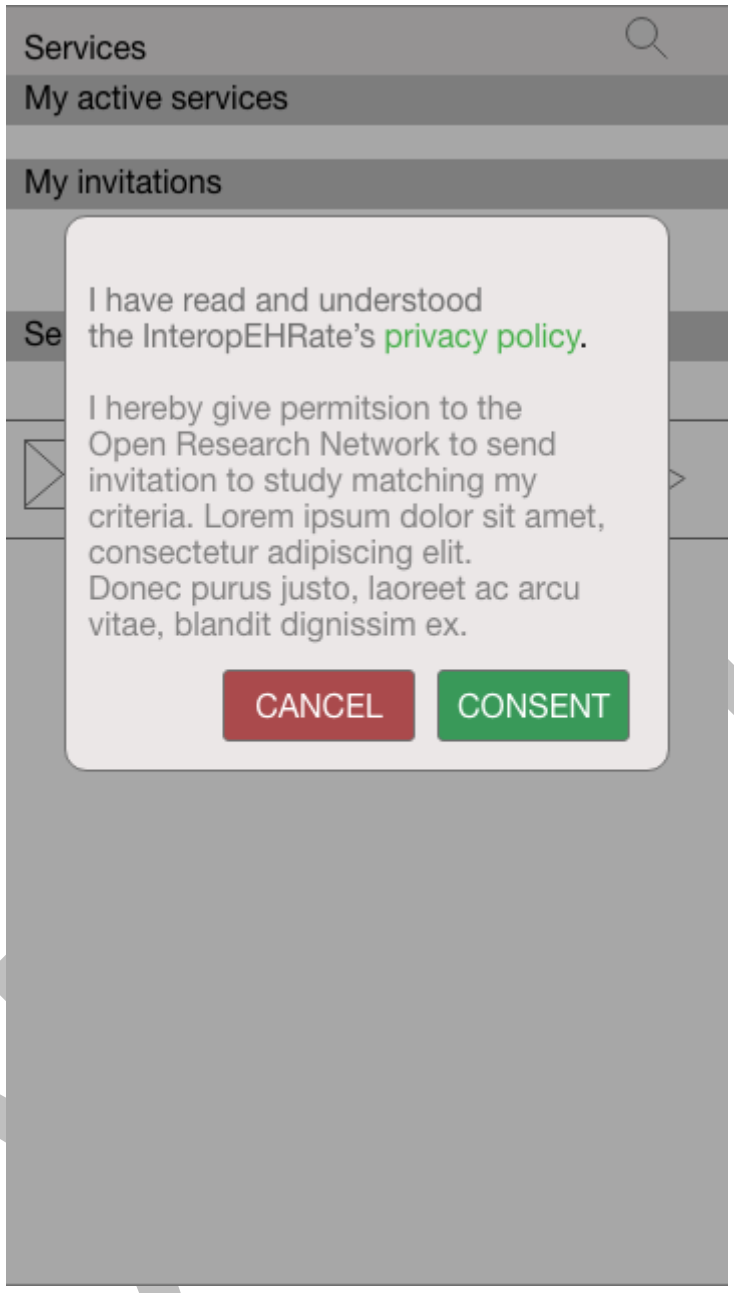

Figure 26 - Mockup: Citizen's consent to be part of InteropEHRate Open Research Network

6.1.4.2. *Citizen's withdrawal from research network*

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

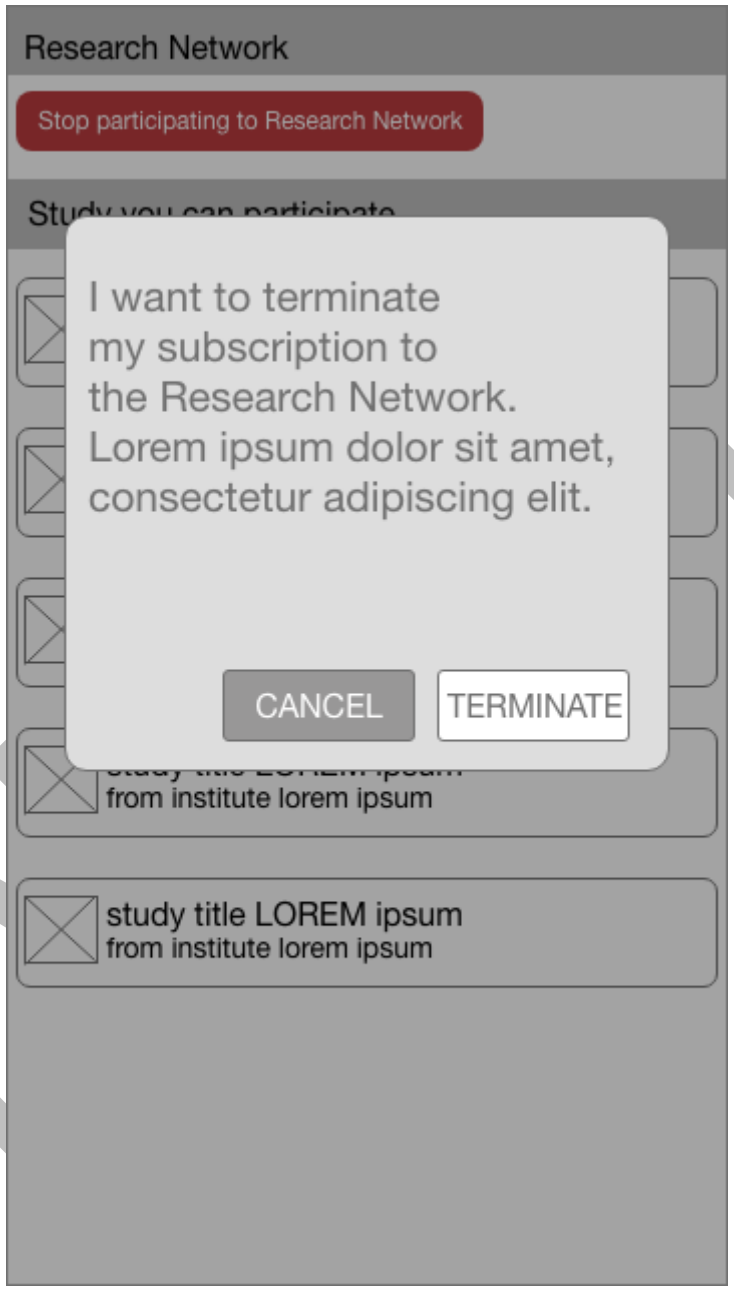

Figure 27 - Mockup: Citizen's withdrawal from research network

6.1.4.3. *Invitation of candidate citizens to participate in a research study*

The citizen can consult the studies in which they can participate, new studies that have not yet been seen by the citizen will be highlighted.

The citizen will receive a notification when one or more new studies are available. This notification will redirect them directly to this screen.

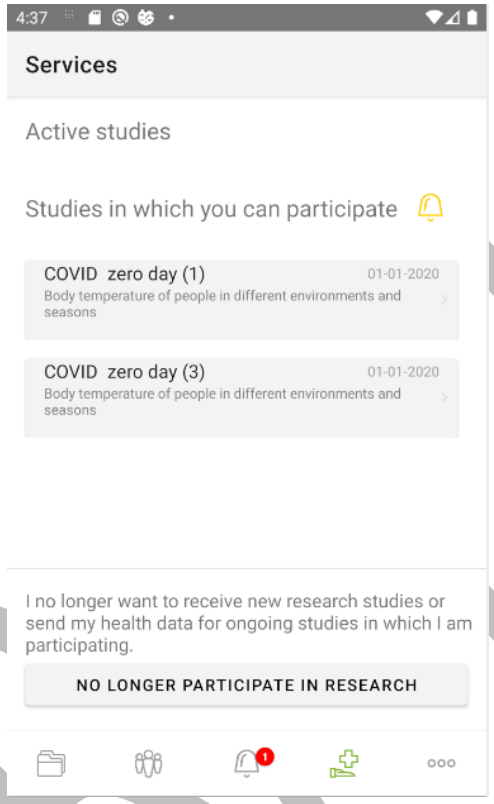

Figure 28 - Mockup: studies list

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

If the citizen wishes to participate in a study, it will be presented in a more detailed view, including a description of the study and the type of data that will be collected. The citizen will have to choose the reference centre that will collect their data.

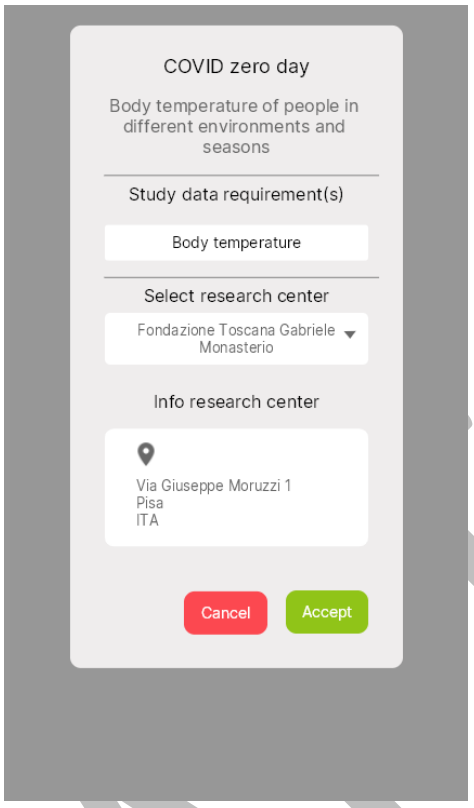

Figure 29 - GUI: Citizen's consent to share health data for a research study

7. CONCLUSIONS AND NEXT STEPS

The current deliverable presented the new functionalities and features of the reference implementation of a S-EHR in the context of the InteropEHRate project. 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. The updated version of software requirements specification of S-EHR App is the result of both technical improvements and software development and the continuous collaboration with the final users (co-design / co-creation sessions).

Taking into consideration the particular requirements of Task 6.1, the deliverable encompasses the updated UI design of the S-EHR application.

This deliverable is the third and final version of the three deliverables of Task 6.1 dedicated to software requirements specification and design of S-EHR and was the updated version of the previous deliverable [D6.2].

REFERENCES

- **[D2.3]** InteropEHRate consortium. *D2.3: User Requirements for cross-border HR integration - V3*, 2021. www.interopehrate.eu/resources/#dels
- **[D2.6]** InteropEHRate consortium. *D2.6 InteropEHRate Architecture - V3*, 2021. www.interopehrate.eu/resources/#dels
- **[D3.2]** InteropEHRate consortium. *D3.2: Specification of S-EHR mobile privacy and security conformance levels - V2*. Note that D3.2, final version of *privacy and security conformance levels*, is due at M36, December 2021. The previous version, *D3.1-Specification of S-EHR mobile privacy and security conformance levels - V2*, 2020, can be found at www.interopehrate.eu/resources/#dels
- **[D3.3]** InteropEHRate consortium. *D3.3 – Specification of remote and D2D IDM mechanisms for HRs Interoperability,* 2020. www.interopehrate.eu/resources/#dels
- **[D3.6]** InteropEHRate consortium. *D3.6: Specification of data encryption mechanisms for mobile and web applications - V2,* 2021. www.interopehrate.eu/resources/#dels
- **[D4.3]** InteropEHRate consortium. *D4.3: Specification of remote and D2D protocol and APIs for HR exchange - V3,* 2021. www.interopehrate.eu/resources/#dels
- **[D4.9]** InteropEHRate consortium. *D4.9: Specification of protocol and APIs for research health data sharing - V9*, 2021. www.interopehrate.eu/resources/#dels
- **[D6.1]** InteropEHRate consortium. *D6.1: Software requirements and architecture specification of a S-EHR - V1*, 2019. https://www.interopehrate.eu/resources/#dels
- **[D6.2]** InteropEHRate consortium. *D6.2: Software requirements and architecture specification of a S-EHR - V2*, 2020. https://www.interopehrate.eu/resources/#dels