D2.4

InteropEHRate Architecture - V1

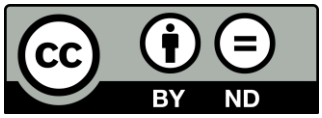
ABSTRACT

This report describes a novel architecture for citizen centred EHR interoperability and the structure of its reference implementation.
The InteropEHRate architecture specifies how different actors using applications offered by different vendors will be able to interoperate thanks to open (vendor independent) protocols and APIs.
This document also provides an introduction to the reference implementation, i.e. to the set of software components developed by the project to provide a concrete example of implementation of the open protocols and to support their usage.
A more detailed description of each specific protocol and software component will be described in referred forthcoming deliverables.

Delivery Date	3rd July 2019
Work Package	WP2
Task	T2.2
Dissemination Level	Public
Type of Deliverable	Report
Lead partner	ENG

InteropEHRate project is co-funded by the European Union (EU) Horizon 2020 program under Grant number 826106.

This document has been produced in the context of the InteropEHRate Project which is co-funded by the European Commission (grant agreement n° 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	Julien Henrard, Lucie Keunen	A7
	Debora Desideri, Alessio Graziani, Francesco Torelli	ENG
	Thanos Kiourtis, Argyro Mavrogiorgou	UPRC
	Sofianna Menesidou	UBIT
	Gabor Bella, Simone Bocca	UNITN
	Chrysostomos Symvoulidis	Singular Logic
Reviewers	Stefano Dalmiani, Paolo Marcheschi	FTGM
Reviewers	Simone Bocca	UNITN

LOGTABLE

Version	Date	Change	Author	Partner
0.1	2019-05-07	Creation of TOC	Debora Desideri	ENG
0.2	2019-05-14	Update of TOC	Debora Desideri, Francesco Torelli	ENG
0.3	2019-05-27	First version of component diagrams and description of standard and reference implementation architecture	Debora Desideri, Francesco Torelli	ENG
0.4	2019-05-27	Contributions on S-EHR Mobile App.	Julien Henrard	A7
0.5	2019-05-28	Description of R2D and D2D protocols	Thanos Kiourtis, Argyro Mavrogiorgou	UPRC
0.6	2019-05-29	Description of security protocol	Sofianna Menesidou	UBIT
0.7	2019-05-31	Document restructuring, Overview and relation to other reports, updates of section of	Debora Desideri, Francesco Torelli	ENG

		standard architecture, component view and deployment view of InteropEHRate framework.		
0.8	2019-06-02	Update of security protocols	Sofianna Menesidou	UBIT
0.9	2019-06-05	Updates to subsections of standard architecture, to UML image of InteropEHRate framework and to related scriptions	Debora Desideri, Francesco Torelli	ENG
0.10	2019-06-06	Description of R2D protocol	Alessio Graziani	ENG
0.11	2019-06-07	InteropEHRate Health Services	Gabor Bella, Simone Bocca	UNITN
0.12	2019-06-07	Updates of S-EHR Mobile App.	Julien Henrard	A7
0.13	2019-06-10	Interactions, updates of InteropEHRate Health Services	Gabor Bella, Simone Bocca	UNITN
0.14	2019-06-11	Description of S-EHR Cloud	Chrysostomos Symvoulidis	Singular Logic
0.15	2019-06-11	Updates of InteropEHRate Health Services and Interactions	Simone Bocca	UNITN
0.16	2019-06-12	Document restructuring and updates to InteropEHRate framework.	Francesco Torelli	ENG
0.17	2019-06-14	Description of HCP App	Nicu Jalba	SIVECO
0.18	2019-06-14	Updated description of HCP App	Julien Henrard	A7
0.19	2019-06-14	Updated description of S-EHR Cloud	Chrysostomos Symvoulidis	Singular Logic
0.20	2019-06-17	Alignment of content of last contributions. Glossary.	Francesco Torelli	ENG
1.0	2019-06-25	Internal review	Simone Bocca	UNITN

1.1	2019-06-25	Internal review	Stefano Dalmiani, Paolo Marcheshi	FTGM
1.2	2019-06-28	Changes based on reviewers' comments	Debora Desideri, Francesco Torelli	ENG
1.3	2019-07-02	Completed quality check	Argyro Mavrogiorgou	UPRC
Vfinal	2019-07-03	Final check and version for submission	Laura Pucci	ENG

ACRONYMS

Acronym	Description
CTMS	Clinical Trial Management System
D2D	Device to Device Protocol
EHR	Electronic Health Record System
HCP	HealthCare Professional
HCP App	HealthCare Professional Application
IHS	InteropEHRate Health Services
IHT	InteropEHRate Health Tools
IRS	InteropEHRate Research Services
MD2DI	Mobile Device to Device Interface
R2D	Research to Device protocol
R2DI	Remote to Device Interface
RSI	Research Interface
S-EHR	Smart HER
S-EHR App	Smart EHR Application
S-EHR mobile App	Smart EHR mobile Application
S-EHR-C	S-EHR Cloud
TD2DI	Terminal Device to Device Interface

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. Scope of the document

The main goal of the present document is to describe the *InteropEHRate standard architecture,* an open specification of an integrated set of interoperability protocols, that any vendor of software applications for health may implement. First of all the document identifies individual actors and organizations that (especially in the EU context) need to exchange health data in a secure and interoperable way. Afterwards it describes how new applications and protocols envisioned by the InteropEHRate project will support such an exchange by means of the citizens' mediation. A complementary goal of this document is to describe the architecture of the *InteropEHRate Framework*, that offers a reference implementation of the standard architecture and includes additional components to support the interoperability. These two architectures summarize the technical results expected from the project.

1.2. Intended audience

The document is intended to policy makers, architects and developers (1) interested to have an overview of how the InteropEHRate protocols and applications support the exchange of health data among EU parties in a secure and trustable way, (2) interested to understand which other reports provides additional details, and to identify software result they can reuse.

1.3. Structure of the document

Section 1 (this section) explains the goal and structure of the document and its relation to other reports. The section "2. Standard InteropEHRate Architecture" goes into the details of the standard architecture. Section "3. Architecture of the InteropEHRate Framework" presents the extended architecture of the reference implementation.

1.4. Updates with respect to previous version (if any)

This deliverable contains the first version of the InteropEHRate architecture.

1.5. Relation to other project results

The InteropEHRate project have the goal of complement the current European approaches for EHR interoperability, mainly based on the usage of central services for access to citizen health data, with a more decentralized model, based on "citizen mediation".

The main result of InteropEHRate will be an **open specification**, describing new kinds of applications and new open interoperability protocols, allowing the citizens to interact with healthcare organizations and research institutions.

The open specification is composed by the following elements, each one described by a separate document:

- **FHIR profile for EHR interoperability** (described in the upcoming report [D2.7]): the common data model, based on the FHIR standard, shared by all the InteropEHRate protocols.

- **S-EHR conformance levels** (described in the upcoming report [D3.1]): the constraints and guidelines that a S-EHR mobile app or a cloud storage service for health data has to fulfil to be considered secure, reliable and compliant to InteropEHRate.
- **Remote protocol for EHR interoperability** (described in the upcoming report [D4.1]): the secure communication protocol (and APIs), using the internet, for cross-border exchange of health data among Healthcare Organization Information Systems and S-EHR mobile app or S-EHR Cloud .
- **D2D protocol for EHR interoperability** (also described in the upcoming report [D4.1]): the secure communication protocol (and API) for exchange of health data among two near devices (not using the internet), one running a S-EHR mobile app used by the Citizen and the other running some application of the Healthcare Organization Information System used by the HCP.
- **Protocol for research health data sharing** (described in report [D4.8]): the secure communication protocol (and API) for exchange of health data, over the internet, between the S-EHR mobile app and any Research Centre.

The main purpose of the present document is to describe the first draft of the **InteropEHRate standard architecture**. The InteropEHRate standard architecture is a high level view of the open specification, correlating and constraining the other specific reports.

Each one of the specified protocols and applications may have different implementations, possibly provided by different competing vendors. The InteropEHRate project will also provide a **reference implementation**, called **InteropEHRate Framework**, composed of different software components, each one implementing a different part of the specification and reusable one independently from the others. The InteropEHRate framework will also contain a set of complementary tools, supporting the usage of the interoperability protocols.

The present document also defines the architecture of the InteropEHRate framework, correlating all the software results of InteropEHRate.

Both the standard architecture and the InteropEHRate framework are intended to realize the scenarios and to satisfy the requirements specified in the report [D2.1]. While the report [D2.1] adopts a point of view more oriented to the final users, this report is more intended to developers and therefore adopts a more technical language. Where possible anyway the two documents adopt a common terminology.

The following section will describe the current standard architecture, while the successive one will describe the current architecture of the InteropEHRate framework.

2. STANDARD INTEROPEHRATE ARCHITECTURE

The purpose of this section is to describe the standard InteropEHRate architecture for EHR interoperability, in particular it provides an overview of the involved actors and organizations, standard software services and applications and standard interaction protocols.

2.1. Actors

The InteropEHRate architecture is intended to allow different kind of users to exchange in a secure way a set of trusted health data. The following table describes the different kind of (individual) final users (called "actors", following the UML terminology). The same actors are defined in [D2.1] (replied here for simplifying the reading of the document).

Actors	Description
Citizen	A person of a specific country whose health data are managed by an application included in the InteropEHRate architecture
HCP	A health care professional that produces and/or access to health data of a Citizen
Researcher	A person that desires to exploit the citizens' health data for research purposes

Table 1- Actors

2.2. Organizations

Here after a description of the standard types of organizations that may interact by using the InteropEHRate protocols. As some interaction may be performed by different types of organizations belonging to a more general type, the types of organizations are hereby reported in a hierarchy of concrete and more abstract types of organizations. The following set of terms includes and extends the one adopted in deliverable [D2.1].

Type of organization	Description	More abstract type of organization
Health Data Provider	An organization maintaining health data and capable to provide them to authorized consumers.	
Healthcare Organization	An organization that provides healthcare services to citizens.	Health Data Provider
Healthcare Provider	A private or public local organization providing healthcare services (e.g. a Hospital, a General Practitioner).	Healthcare organization
National Healthcare System	An institution providing or managing at central level the public healthcare services of a country.	Healthcare organization
Research Centre	An institution exploiting the personal health data of citizens for research purposes.	
S-EHR Cloud Provider	A public or private organization that offers a cloud service to individual citizens for the storage of personal health data.	Health Data Provider

S-EHR Provider	A provider (for free or for sale) of a S-EHR mobile app.	
National Identity Provider	Public administrations or private sector organisations "issuing the electronic identification means and the party operating the authentication procedure". They provide their user base with a secure online identity which is used with a national eID scheme/s The identity provider is a national entity and provides electronic identifications that are accepted at national level[1].	
Member state	A state of EU community providing an eIDAS node[2].	
Healthcare Solution Provider	A provider (for free or for sale) of software products used by Healthcare organizations.	

Table 2 - Organizations

2.3. Overview of applications and services

The following figure shows in an informal way a typical set of actors, software services and applications exploiting the new application and protocols specified by InteropEHRate. The picture is intended just as an introduction to the main elements of the architecture and is informal both because it does not use a standard specification language and because the depicted components and interactions are not exhaustive, but represent just common examples. A more formal description using UML notation is provided in the

[1] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=71776009
[2] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

following sections.

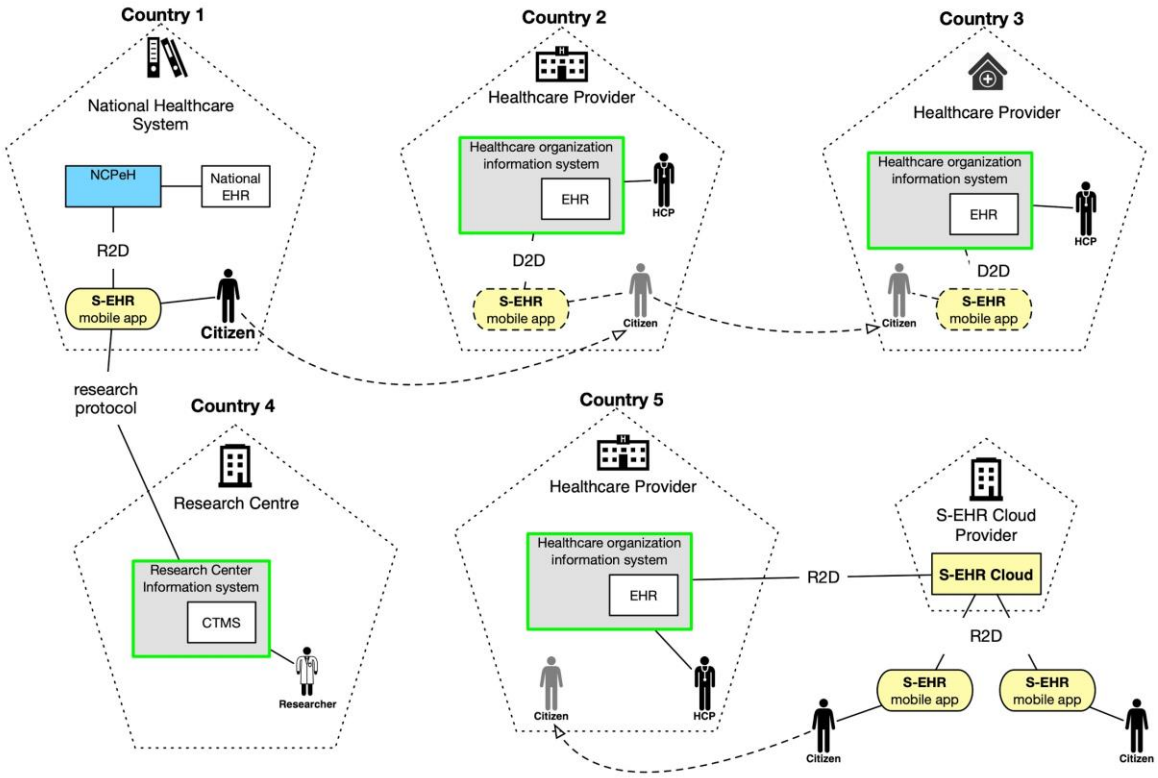


Figure 1 - Examples of health data exchange using the S-EHR mobile app and the S-EHR Cloud

The main objectives of InteropEHRate is to make easier the exchange of health information between citizen, healthcare organizations and research centres. The InteropEHRate architecture assumes that in the near future the EU citizens will own standard mobile applications called Smart EHRs (S-EHRs). To emphasize the fact that it is a user application, throughout all this specification, the S-EHR is also called S-EHR mobile app or S-EHR App. A S-EHR is able to store in a secure (encrypted) way on a mobile device any health data related to the history of the person that owns the device.
By mobile device we mean mainly modern smartphones or tablets, but it could include in future also other types of mobile devices with advanced computational capabilities, like smartwatches or smart bracelets and other kinds of smart devices that may move with the citizen. The stored health data may be produced by healthcare professionals, by sensors or by any citizen in the role of a patient.

A S-EHR is able to receive health data from any healthcare organization that adopts the standard protocols specified by the InteropEHRate project. These protocols guarantee the integrity of exchanged data, the traceability of their provenance and their trustability.

More specifically the S-EHR uses the so called Remote to Device (R2D) protocol to exchange health data at distance (on 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 usage of internet, but adopting short range communication technologies like bluetooth). Any portion of the information system of the healthcare organization used by HCPs to interact with the S-EHR is called HCP App.

The above picture shows an example of a citizen using the S-EHR for importing his health data from a national EHR provided by the National Healthcare System of his country and for exchanging the same data and new health data with the EHR system of a hospital located in a different country.

In particular, the R2D protocol is intended not only for the exchange of data directly with data producers, like Hospitals and Clinical laboratories, but also for importing health data from existing repositories such as cloud based Personal Health Records and national EHRs already provided to the citizens of EU countries.

In order to allow the exchange of health data with S-EHRs, the health data providers will need to extend their information systems (e.g. internal general purpose EHRs or more specific health applications) to provide the services, called InteropEHRate Health Services (IHS), required by the InteropEHRate protocols.

In the case of the R2D protocol, the person that is the subject of the data (the Citizen in the picture) exchanges health data using his/her S-EHR that interacts directly with the IHS, while in the case of the D2D protocol the health data is exchanged between the S-EHR and a terminal (e.g. a desktop computer or a tablet) where the application used by the Healthcare operator (HCP) runs. This application used by the HCP may be a legacy application already used by the healthcare organization and extended to support the D2D protocol or may be a completely new application.

In the InteropEHRate vision, different vendors may offer different kind of S-EHRs to the final users and each user may choose the preferred one, according to his/her needs and to the added-value functionalities offered by the specific S-EHR. Regardless of the differences, all kind of S-EHRs have to satisfy a set of standard rules and requirements aimed to guarantee strong levels of security and trustability (to be specified in upcoming report [D3.1]) to citizens and organizations that interact with them.

A S-EHR is different from many mobile applications and SaaS (Software as a Service) currently available on the market because it adopts open exchange protocols that are vendor independent (so avoiding the lock of citizen's data in proprietary data silos) and also because the user moves among countries (see dotted arrows in the picture) bringing the health data with her/him, stored on the mobile device. The user does not need to access any cloud service to consult the health data and does not need to allow a service provider to store and control all the collected personal health data. The health data of the user are always available on the mobile device and are fully controlled by the user. This approach allows to access the stored data also in situations where, for whatever reason, internet is not available. Also data exchange may be supported without sending the data on the internet, so reducing the risk of interception and corruption of the data. The distributed nature of the storage model (i.e. data of different citizens are stored on different devices) avoids the security risks of models where data of many citizens and coming from different data sources (e.g. different hospitals) are stored in the same central repository accessible from the internet and where a single hacker's attack put at risk the data of all users.

With InteropEHRate, users may still choose to maintain a backup copy of their personal health data on a cloud service, but this is an optional choice and any user may chose a different cloud storage service called S-EHR Cloud (see section S-EHR Cloud), possibly offered by a vendor distinct from the one that offers the S-EHR mobile application. Moreover, the data is sent to the cloud service in an encrypted format not intelligible to the service provider, therefore the risk of unauthorized usage of the data from malicious service providers or hackers is sensibly reduced. As shown in the figure, the communication between a S-

EHR mobile application and a S-EHR cloud is also specified by the R2D protocol (that is actually a set of different APIs and rules covering different scenarios for exchange of health data at distance).

The S-EHR may also support the Research Protocol, an electronic communication protocol that allows any person to send personal health data at distance (on the internet) in a secure way to Research Centre, to be exploited for research purposes. The research protocol allows scientists to engage voluntary citizens at cross-national levels in new research trials or retrospective studies, and allows the citizens to easily and securely send (in particular, donate) health data, including both certified (i.e. clinical) and wellness data, in pseudonymized or anonymized form. The protocol specifies both how the data must be sent and how the research centre may communicate, to the person, which are the aims of the research, and how the research centre may ask the needed consent for specific usage of the data.

Each one of the InteropEHRate protocols is composed by a security protocol, aimed to guarantee the cross border identification of the citizens and the privacy, integrity, and trustability of data exchange, and by a set of functional APIs for performing specific health data exchange operations.

The security protocols (see sections R2D security protocol and D2D security protocol) involve several organizations and services not shown in the simplified figure above. More in general, the InteropEHRate protocols are intended to complement the existing infrastructures and standards adopted by the EU for health data exchange. In particular they leverage existing standards established by the EPSOS project and related infrastructure eHDSI, and regulations like EIDAS and related EU services like CEF eID.

Traditional models for exchange of health data among different health care providers adopts central services for health data access. Typical examples are national EHRs, accessible from healthcare providers of the same country or region. Other examples are national contact points (like in the eHDSI infrastructure for EHR interoperability) that a country offers to national contact point of other countries to allow the authorized health care providers of these other countries to access to citizen's health data. Such models are "top down" in the sense that the access to data provided by different healthcare providers is coordinated from central services that are "on the top" of these organizations and of the citizens that receives the services. InteropEHRate is intended to integrate this "top down" model of interoperability with a "bottom up" approach where single vendors and healthcare providers may choose to implement and adopt the InteropEHRate protocols from the bottom, i.e. without the need of a central service above them. In this more decentralized model the exchange of health data is not mediated by institutions providing central services, but is mediated directly by the citizens that allow to access to their health data stored on their personal S-EHRs.

The traditional model and the InteropEHRate one are intended to coexist and complement each other in order to cover more usage scenarios.

InteropEHRate is aimed to promote the growth of a new market based on the offer of S-EHR Apps and related services. It is also aimed to empower the citizens, giving them more immediate access to their data, more control over their usage and more possibilities of exploitations health data both for improving personal health and for contributing to the increment of medical knowledge at the disposal of all EU citizens.

2.4.Standard applications and interfaces

This section and its sub-sections describe in a more formal way, using UML notation and textual descriptions, the standard applications and interfaces required by InteropEHRate, to support the communication between Citizens, Healthcare Organizations and Research Centres, in a cross-border context (i.e. for exchange of health data from within different countries) .

The main software systems and interfaces are shown on the following UML component diagram. Each software system is represented as a component offering and requiring different interfaces. For better clarity, different colours are adopted:

- grey, for legacy systems,
- blue, for standard legacy interfaces and systems,
- yellow, for (new) systems specified by InteropEHRate,
- green, for (new) interfaces specified by InteropEHRate.

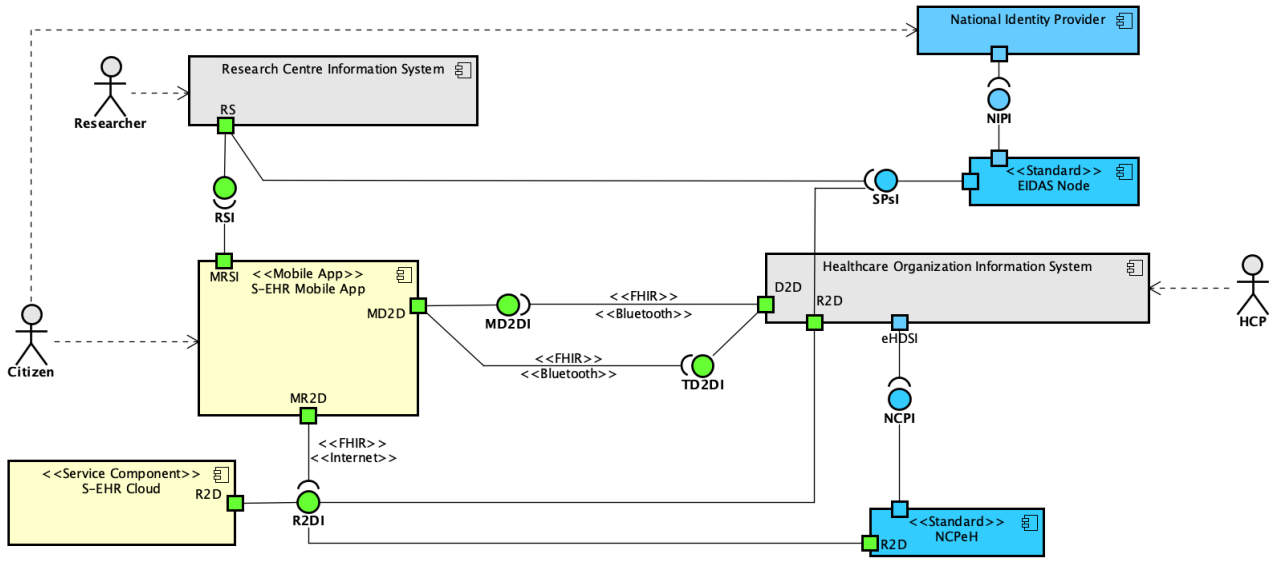


Figure 2 - InteropEHRate standard architecture

The InteropEHRate protocols constraint the interactions among three kinds of software systems:

1. S-EHR mobile app (at Citizen side): the mobile application, used by the Citizen, to store and exchange personal health data using the InteropEHRate protocols.

2. Healthcare organization information system (at Healthcare Organization side): the collection of all software applications used by the Healthcare Operators (HCPs) within a Healthcare Organization, extended to support the InteropEHRate protocols for health data exchange with S-EHR.

3. Research Center Information system (at Research centre side): collection of all software used by any Researcher (i.e. scientist), to produce and access to Citizens' health data.

Moreover the InteropEHRate protocols involve the following standard legacy systems:

4. eIDAS (electronic IDentification Authentication and Signature) Node, to support services capable of identifying citizens and businesses from other Member States. The eIDAS Regulation ensures that

people and businesses can use their own national eIDs to access online public services in other EU countries, where eIDs are available. The eIDAS Network consists of a series of eIDAS-Nodes implemented at the Member State level. National Identity Providers Interface (NIPI) is used to connect the eIDAS-Node in the user's Member State to their National Identity Provider. The procedure of user authentication takes place between the user and the National Identity Provider, it is outside both the eIDAS Network and InteropEHRate system.

5. eHealth Digital Service Infrastructure (eHDSI) National Contact Point for eHealth (NCPeH) for supporting existing initiative for cross-border health data exchange under the Connecting Europe Facility (CEF). National Contact Point Interface (NCPI) is used to exchange Patient Summary and ePrescription among healthcare organizations of cross-border countries. The InteropEHRate architecture also propose an extension of eHDSI in order to allow the Citizens to import on their S-EHR mobile app their documents available on the NCPeH.

Finally the protocols may also involve the following optional system:

6. S-EHR Cloud (offered by a specific vendor, to support the remote storage/backup of personal health data)

The new (open standard) interfaces introduced by InteropEHRate for the interactions among the different subsystems are listed in the following tables. Such interfaces are part of the interoperability protocols which first version is described in the reports [D3.3] and [D4.4]. The first versions of the protocols covers just a portion of functionalities of the architecture, while a full coverage will be provided with the final version. The data model adopted by the protocols and interfaces will be defined as a set of constraints and extensions on top of the standard [HL7 FHIR] and will be specified in [D2.7].

InteropEHRate standard interfaces	
RSI	Research Interface: offered by the Research Centre to support the research protocol, i.e. to engage citizens and to receive their health data and consent to usage.
R2DI	Remote to device interface: offered by the HealthCare Organization to support the R2D protocol, i.e. to exchange health data with citizen's S-EHRs by means of internet.
MD2DI	Mobile Device to Device Interface: offered by the S-EHR to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at short distance, without using internet.
TD2DI	Terminal Device to Device Interface: offered any application used by HCPs to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at short distance, without using internet.

Table 3 - InteropEHRate standard interfaces

The following sections provide a description of the main functionalities provided and required from each subsystem.

2.4.1. S-EHR Mobile App

A S-EHR is any application installed on a personal mobile device, that is able to store the personal health data of a user in a secure (encrypted) way according to the constraints specified by the "Specification of S-EHR mobile privacy and security conformance levels" [D3.1] and that supports the InteropEHRate protocols [D4.1][D4.8]. Different vendors may develop different S-EHRs.

A S-EHR contains health data of the user, produced and signed (for traceability and trustability) by the healthcare organization that produces them, but can also contain data directly stored and produced by citizens or by sensors. The provenance and author of each health data is unambiguously persisted on the S-EHR and the principles of integrity and non-repudiation are guaranteed.

The S-EHR supports the storage and exchange of three kinds of health data:

- Unstructured health data (txt, pdf, images, videos, signals).
- Structured health data compliant to the standard [HL7 FHIR].
- Structured health data compliant to the "InteropEHRate profile" [D2.7].

A S-EHR supports the natural language of the user and all structured health data that are compliant to the InteropEHRate profile are presented in the user's natural language.

Text content of the health data is always stored and presented in the form (and natural language) produced by the author, but may be annotated with translated versions of the text (obtained by manual or automatic translation) that are also presented to the user.

Structured data annotated with semantic codes conformant to the "InteropEHRate profile" and obtained by converting (in a manual or automatic way) local semantic codes (i.e. codes specific of a particular organization), always contains also the original local semantic codes.

A S-EHR allows the user to access his/her personal health data independently from the availability of internet and does not mandate the support of any cloud service for the storage of health data. In other terms, the user does not need to access any cloud service to consult the health data and does not need to allow a service provider to store and control the personal health data.

Which data are stored on the mobile application and which actor may access to them by using the InteropEHRate protocol is fully under the control of the user.

The main functionalities offered from a standard S-EHR mobile app are:

- To show to the authorized user all stored health data.
- To import/share health data from/with a Healthcare.
- Organization Information System by means of the D2D (device to device) communication protocol (short-range and wireless). These functionalities are supportive of use cases in which patients and HCPs wants to exchange health data during a face to face encounter and the use of "servers on the internet" is not possible (e.g. because the internet is not available) or desirable (for security reasons). To this end the S-EHR implements the interface MD2D and uses the interface TD2DI

offered by the computer terminal (part of the Healthcare Organization Information System) of the HCP.

- To import/share health data from/with an EHR using the remote R2D protocol. These functionalities are used when citizens and health data are in different places. Some example can be:
  - to import data from national electronic health record,
  - to send health data (e.g. produced abroad) to a national health organization,
  - to allow the citizen to receive from a healthcare organization a report produced after an encounter.

  To this end the S-EHR uses the interface R2D offered by the Healthcare Organization Information System.

- To receive and show a "health research protocol"[3] that the citizen is invited to participate by sending his/her personal health data. A health research protocol describes purposes and methodology to collect and process a specific dataset of health and/or social data, to learn more about human health and treatments (to be approved by an Ethical Committee).

- To send (in particular, donate) consent and health data in aggregated or anonymized or pseudonymized form to a research centre for a specific trial. To this end the S-EHR uses the interface RSI offered by the Research Centre Information System.

- To import/store data on an S-EHR Cloud service. This is useful to securely backup or move their data on another device. This operation is performed by using the interface R2DI offered by the S-EHR Cloud selected by the user.

- To authorise or de-authorise a specific health care organization to access, using the R2D or D2D protocol, to specific health data stored on S-EHR. This operation does not use external interfaces, but is completely performed on the S-EHR mobile app.

- To authorise or de-authorise any health care organization to access during an emergency, using the R2D protocol, to a specific set of health data stored on the S-EHR Cloud. This operation uses the interface R2DI offered by the S-EHR Cloud to set communicate the consents to the S-EHR Cloud.

- To trace any access to the user's health data. This operation does not use external interfaces, but is completely performed on the S-EHR mobile app.

2.4.2. S-EHR Cloud

A S-EHR Cloud is any service for secure storage on the cloud of user's health data, that support the InteropEHRate R2D protocol [D4.1] and fulfils the "S-EHR conformance levels" [D3.1].

A S-EHR Cloud may be offered by a vendor different from the one providing the S-EHR mobile app.

[3] Note that "Health Research Protocol" is different from "Research Protocol". The first one is a description of the rationale, objectives, and methodology of a clinical research trial. The second one is the set of rules specified by the InteropEHRate project that a S-EHR has to follow to exchange health data with the information system of a Research Centre.

The health data are exchanged with the S-EHR Cloud and stored on it in an encrypted format that cannot be decrypted by the S-EHR Cloud or its vendor.

A citizen may choose to use a S-EHR mobile app without using any S-EHR Cloud.

A user may use a S-EHR Cloud only for the backup of health data (and moving of data to other devices) or the user may authorize health organizations to access and decrypt a specific subset of the health data stored on the S-EHR Cloud in emergency situations.

A S-EHR Cloud implements the R2DI interface:

1. To allow the user of any authorized S-EHR to upload and store encrypted health data.
2. To allow the user of any authorized S-EHR to download encrypted health data previously stored by the same user.
3. To provide access to an HCP of a healthcare organization to predefined health dataset of a citizen in "emergency mode". The S-EHR Cloud trace in a persistent way any access to healthcare data in emergency mode, including all data needed to identify the person that requested to access the data.

2.4.3. Healthcare Organization Information System

A *Healthcare Organization Information System* is the software information system of any healthcare organization that manage citizen's health data and exchange them with authorize citizens using the InteropEHRate R2D or the D2D protocol.

Examples of a Healthcare Organization Information System are a Hospital EHR, a National EHR or an eHDSI National Contact Point that has been extended to allow the Citizens of a nation to import at distance in their S-EHR, using the R2D protocol, any personal health data collected from their National Healthcare System.

More in general, a *Healthcare Organization Information System* provides one or more of the following functionalities:

1. Allows authorized citizens to import their health data using the R2D protocol. To this end the Healthcare Organization Information System implements the interface R2DI used by the S-EHR of the citizen.
2. Is able to import during a face to face encounter health data, shared by a citizen. To this end the Healthcare Organization Information System uses the interface MD2DI exposed by the S-EHR of the citizen.
3. Is able access at distance to emergency health dataset of the citizen (also when a citizen is not connected with the S-EHR). To this end the Healthcare Organization Information System uses the interface R2DI exposed by the S-EHR Cloud of the citizen.

4. Is able access at distance to emergency health dataset of the citizen (also when a citizen is not connected with the S-EHR). To this end the Healthcare Organization Information System uses the interface R2DI exposed by the S-EHR Cloud of the citizen.

In order to implement the security protocols, that are part of the R2D and D2D protocols, a *Healthcare Organization Information System* uses the Service Providers interface (SPsI) exposed by the EIDAS node (for cross border identification of the citizens). Through this interface, the Healthcare Organization Information System sends authentication requests to the eIDAS-Node and receives the authentication responses. The procedure of user authentication takes place between the user and the Identity Provider, thus it is outside both eIDAS Network and InteropEHRate system.

2.4.4. Research Centre Information System

A *Research Centre Information System* is the software information system of any research centre able to receive health data from citizens using the InteropEHRate Research protocol.

A *Research Centre Information System* provides one or more of the following functionalities:

- It allows the citizen to obtain information on trials, such as:
  - The specific health data that are required for the trial,
  - if the data has to be provided in anonymized or aggregated form,
  - the kind of usage of these data that the citizen will have to consent to,
  - the purpose of the trial,
  - Involved research organizations.

  To this end, the *Research Centre Information System* implements the interface RSI used by the S-EHR to retrieve the description of the trials.

- It allows a citizen to send a consent for a specific usage of a specific set of his/her health data.

  To this end, the *Research Centre Information System* implements the interface RSI used by the S-EHR to send the consent.

- It is able to receive anonymized data from S-EHR mobile app shared by the citizen.

  The S-EHR uses the interface RSI implemented by the *Research Centre Information System* also to send the consent.

The Research Centre Information System uses the Service Providers Interface (SPsI) offered by the EIDAS node, to check the identity of the user that is providing the health data. Through this interface, the Research Centre Information System sends authentication requests to the eIDAS-Node and receives the authentication responses. The procedure of user authentication takes place between the user and the Identity Provider, thus it is outside both eIDAS Network and InteropEHRate system.

2.5. Interoperability protocols

The following section introduces the different kinds of interaction protocols.

2.5.1. R2D Security Protocol

The purpose of the R2D security protocol is to provide security in the R2D protocol. More precisely, by security we mean to fulfil all the identified security requirements in the context of deliverable D2.1, including Identity Management, Consent Management, Authorization Management and Encrypted storage and communication. The R2D security protocol utilizes the interface R2DI, that in the reference implementation (see section "Architecture of the InteropEHRate framework") is offered by specific components (Mobile R2D Security Management, Terminal R2D Security Management and Server R2D Security Management, Mobile Encrypted Storage, Mobile Encrypted Communication, Server Encrypted Communication).

The R2D security protocol leverage existing infrastructure provided by the epSOS project and its successor eHealth Digital Service Infrastructure (eHDSI) as well as the electronic Identification, Authentication and trust Services (eIDAS) regulation and EU services like CEF eID. Identity Management in R2D protocol is an eIDAS-based solution, for both reasons a) to provide the ability to support cross-border identification/authentication and b) to be compatible with existing solutions.

Authorization and Consent Management, is decentralized due to the nature of the architecture, based on Attribute Based Access Control (ABAC) approach, while citizen's consent is managed as an attribute. In addition, encryption mechanics for both health data storage (on mobile devices and cloud services) and health data exchange among S-EHR/EHR/EMR/ and Cloud services will be provided.

The first of the R2D security protocol covers the identity management, authorization and consent management, while the next versions will focus on encrypted storage and communication aspects.

More details of the R2D security protocol design and specifications are available in the report [D3.3], where information regarding the used technologies, sequence of exchanged messages and the involved actors, and involved components are mentioned and thoroughly discussed.

2.5.2. D2D Security Protocol

The purpose of the D2D security protocol is to provide security in the D2D protocol. More precisely, by security we mean to fulfil all the identified security requirements in the context of deliverable D2.1, including Identity Management, Consent Management, Authorization Management and Encrypted storage and communication. The D2D security protocol utilize the interfaces TD2DI and MD2DI, that in the reference implementation (see section "Architecture of the InteropEHRate framework") are offered by other specific components (Mobile D2D Security Management, Terminal D2D Security Management, Mobile Encrypted Storage, Mobile Encrypted Communication and Terminal Encrypted Communication).

Identity Management in D2D has two variants: a) In the first variant, the identification is done with the ID-Card of the citizen and a QR code generated by the hospital. This variant is more feasible, to be used immediately after the end of the project; b) In the second variant, the identification will be used in the future, when smart phone technology will be mature, that will use Qualified certificates of the citizens and qualified certificates of the hospitals. This variant will be also used for experimentation reasons, during the duration of the project. Authorization and Consent Management, is based on Attribute Based Access Control (ABAC) approach, while consent is managed as an attribute. In addition, encryption mechanics for both health data storage and health data exchange between S-EHR mobile app and HCP terminal will be provided. As in the R2D security management protocol, in the first year (version 1) of the D2D security protocol, we cover the identity management, authorization and consent management, while in the next versions we will focus on encrypted storage and communication aspects.

More details of the D2D security protocol design and specifications are available in the deliverables of WP3,

where information regarding the used technologies, sequence of exchanged messages and the involved actors, and involved components are mentioned and thoroughly discussed.

2.5.3. R2D protocol

The R2D protocol, defines the set of operations and structure of data used for enabling (in a standard way) the exchange of health data between any EHR or S-EHR Cloud and the S-EHR mobile app, with the usage of the internet (complementary to the D2D that is the protocol to exchange health data without the usage of internet).

The most characteristic aspect of InteropEHRate project is the fact that the EHR resides on a citizen's smartphone. Citizen's (health) data transfer is realized by using two protocols: D2D for short range transmission, R2D for remote transmission over the internet. The first draft of the R2D protocol defines how the S-EHR mobile app acquires medical data from an eHDSI (*eHealth Digital Service Infrastructure*) National Contact Point (NCP). The process of copying an EHR from a NCP to a citizen's smartphone is important to allow the Citizens to easily acquire their data already offered by the NCP.

The eHDSI project (under the CEF Programme) is providing initial deployment and operation of services for cross-border health data exchange among EU countries. Currently eHDSI supports just Patient Summary and ePrescription data, but according to *EU Commission Recommendation of the sixth of February 2019 on a European Electronic Health Record exchange format*, the baseline for the exchange contains the following health data:

- Patient Summary;
- ePrescription / eDispensation;
- Laboratory results;
- Medical imaging and reports;
- Hospital discharge reports.

R2D main purpose is to define a standard API for interacting with a source of medical data, providing a common data model and a common data representation. In this sense, R2D objectives are similar to eHDSI objectives, but with two main differences:

- eHDSI is a system available only to HCOs and HCP, it has not been designed considering the citizen as a primary actor. Primary actors are only HCPs of the involved countries. Differently, in InteropEHRate the citizen is the actor at the centre of the platform, he periodically downloads his data from the National EHR to his smartphone, and he handles directly his data when in front of an HCP.
- eHDSI uses a standard representation of data (HL7 CDA Rel. 2), but it does not adopt any of the pre-existing eHealth standard API: eHDSI defined a new API based on SOAP that should become a standard. Differently, R2D will be based upon a reduced version of the standard protocol defined by HL7 named *Fast Healthcare Interoperability Resources* (known as HL7 FHIR or simply FHIR). R2D will fully support FHIR API language and FHIR data model and data representation.

However despite these differences, the future evolution eHDSI is expected to be based also on FHIR[4]. The R2D protocol is intended to propose such an evolution of eHDSI. Thanks to this evolution, clients using R2D protocol will also be able to interact with eHDSI and consequently with all European National EHRs (adhering to eHDSI) in a standard way, overcoming the current technological impediments.

More specifically the R2D protocol includes two variants. One variant adopt the current API of eHDSI, extended with a security protocol to allow also the S-EHR mobile app to access to the existing API. The second variant is fully based on the FHIR standard, allowing to potentially exchange any kind of data supported by FHIR.

More details of the R2D protocol design and specifications are available in the report [D4.1], where information regarding the used technologies, sequence of exchanged messages and the involved actors, and involved components are fully described.

2.5.4. D2D protocol

The D2D protocol defines a set of patterns for exchanging messages and healthcare related data between the Healthcare Organization Information System used by HCPs and the S-EHR Apps used by citizen, to be adopted at EU level, without the usage of internet connection. This protocol is based on short-range wireless technologies and in particular Bluetooth.

Bluetooth technology is most commonly associated with exchanging data between two bluetooth enabled devices in short distance (±10 meters), through which a bluetooth enabled device as soon as it listens to the initialization advertisement message of a different bluetooth enabled device, it connects to it, being thus able to exchange and display information between them, without needing any other technologies or types of connection (e.g. internet connection). Adopting bluetooth, the proposed D2D protocol will facilitate the information exchange between patients (i.e. through smartphones) and healthcare practitioners (i.e. through a desktop computer including a bluetooth adapter), without the usage of central cloud services or any other parties.

The D2D protocol defines bluetooth services (represented by the interface TD2DI) to be offered by healthcare organizations to share health data contained in their EHR with the S-EHR mobile app, as well as bluetooth services (represented by the interface MD2DI) to be offered by the S-EHR mobile app for receiving requests from the Healthcare Organization Information System. The D2D protocol will also exploit D2D Security protocol (which interfaces are part of the R2DI and MD2DI) to perform Identity Management, Consent Management, and Authorization Management.

More details of the D2D protocol design and specifications are available in the report D4.1, where information regarding the used technologies, sequence of exchanged messages and the involved actors, and involved components are mentioned and thoroughly discussed..

2.5.5. Research protocol

The role of the Research Protocol is to support health data exchange among the S-EHRs of citizen and Research Centres. Using the service components released by the project or any other implementation compliant to the specification of the InteropEHRate protocols, scientists are able to provide detailed

[4] Section *3 "Future Work"* of **[EU CB ANNEX]** (ANNEX to the Commission Recommendation on a European Electronic Health Record exchange format) states: "*The refinement of the exchange format should consider the possibility offered by resource driven information models (such as Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR©)*"

information to the citizens about a research initiative, obtain their consent, and actually query the subset of patient data required for research.

The Research Protocol defines the interactions between the following actors:

- the Research Centre Information System;
- the researchers
- the patient's S-EHR Mobile App;
- the patient him/herself.

The protocol covers the following interactions in the order specified:

1. The Research Centre Information System publishes, using the RSI interface, a (already approved) Health Research Protocol. The description of Health Research Protocol is prepared by the researchers and contains a machine interpretable description of requested health data to be downloaded from S-EHR Apps of patients satisfying specific inclusion parameters, and a textual description of the motivations, involved research organizations and the data requested. The machine interpretable description of requested health data corresponds to a formal set of FHIR attributes and resources, and constraints to be queried in the form of an FHIR query.
2. The mobile app evaluates if the request can be satisfied, usually based on automatic evaluation of the patient's data against research protocol inclusion criteria and data request. If the evaluation is positive, then the patient is requested by the S-EHR App for his/her consent of the data collection, providing him/her details on the data collection and the motivations.
3. Upon positive consent, the S-EHR App executes an initial set of privacy-preserving operations on the requested data , such as de-identification.
4. The S-EHR App transmits the requested data in a privacy-aware and secure manner.
5. Upon reception, the Research Centre Information System may perform further privacy-preserving operations on the data collected, such as further de-identification and aggregation across the entire cohort.

Communication between the Researchers and the Research Centre Information System i.e., for the initial research description, its approval, and for the final transmission of de-identified and aggregated research data to the researchers, is not covered by the Research Protocol.
The Research Protocol will be specified in detail by report [D4.8].

3. ARCHITECTURE OF THE INTEROPEHRATE FRAMEWORK

This section describes the architecture of the InteropEHRate framework. The InteropEHRate framework offers a reference implementation of the standard InteropEHRate architecture. Moreover, the InteropEHRate framework extends the standard architecture with additional functionalities and components to support the exchange of health data. The following picture shows in informal way the components offered by the InteropEHRate Framework. Note that different colours are used, with respect to the informal picture shown in section 2, also for components that were already shown there (S-EHR mobile app, S-EHR Cloud). This is to stress that the InteropEHRate Framework offers specific implementations of the components specified by the standard architecture. For simplicity, the information systems of the healthcare organization and the research centre are not shown, but just the components running within them are shown (IHT, IHS, HCP app and EHR are part of the healthcare organization information system, IRS and CMTS are part of the research centre information system depicted in Figure 1).

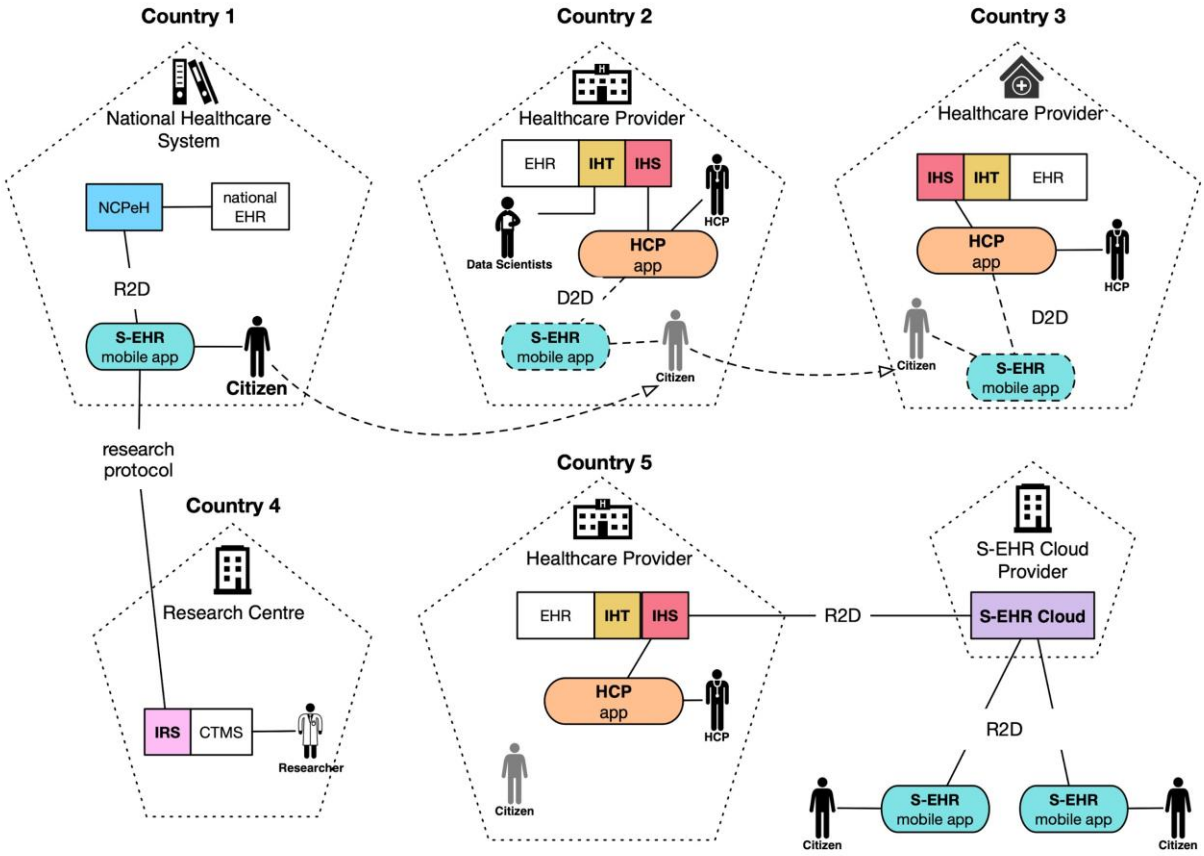


Figure 3 - Examples of health data exchange using the components offered by the InteropEHRate Framework

In the following it is described what are the specific technologies chosen for the components of the framework, where they can be deployed and how they depend each one from the others and what are the reports that further describes these components.

3.1. Additional actors

Other than the actors described in section 3.1 Actors, the InteropEHRate framework adds a further actor, involved in the usage of the additional tools provided by the framework.

Actor	Description
Data Scientist	A person able to understand specific kind of health data and to express them according to specific standards adopted in the health domain. In [D2.1] scenarios it is also called "domain expert".

Table 4 - Additional actors

3.2. Component view

The following picture shows the high level architecture of the InteropEHRate framework.

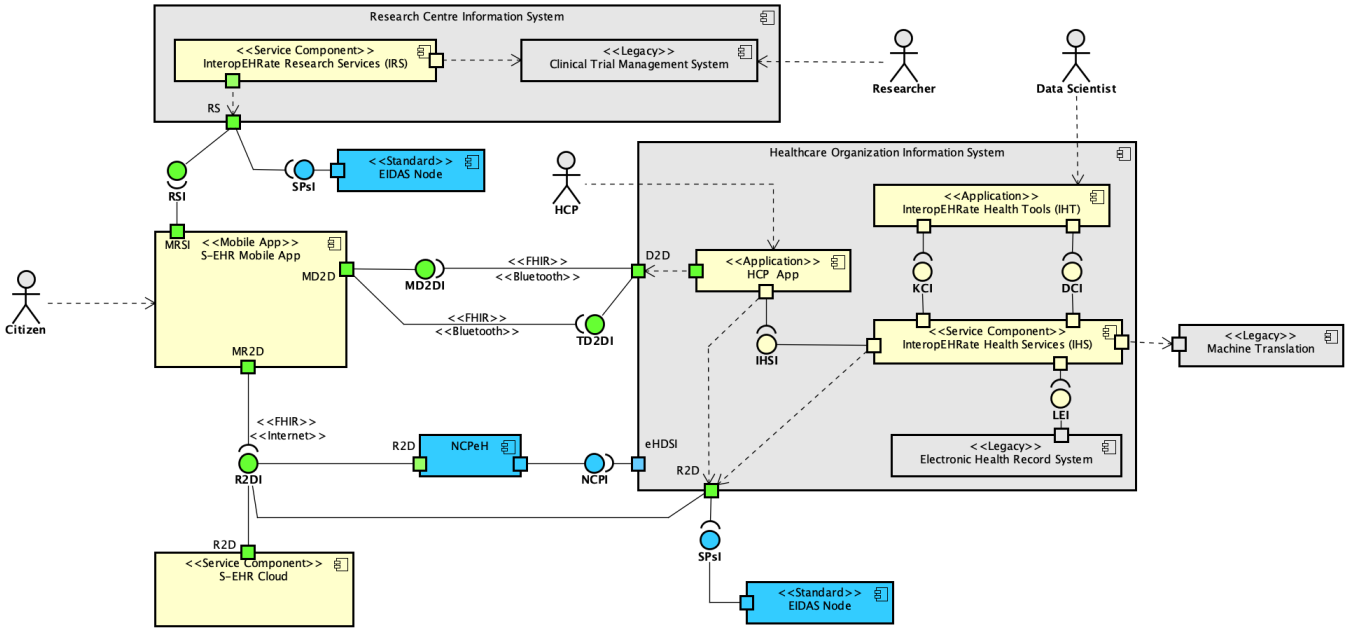


Figure 4 - Architecture of the InteropEHRate framework

The "InteropEHRate Framework", is composed of different systems, one usable independently from the others. These systems are in turn composed of reusable libraries, each one representing a reference implementation of a different portion of the InteropEHRate protocols.

Reference implementation of the standard InteropEHRate architecture

- ***Reference implementation libraries***: see section 3.4
- **S-EHR Mobile App RI**: reference implementation of S-EHR Mobile App, able to import/share data from/with EHR and with research centres, using short-range wireless D2D (device to device) communication or remote communication protocols. See section 3.5.
- **S-EHR Cloud RI**: reference implementation of S-EHR Cloud, able to store on the cloud the data collected by S-EHRs, adopting the standard protocols defined by the project. See section 3.6.

Additional systems reusable by the Healthcare Organization

Other than the reference implementation libraries, the InteropEHRate framework provides the following three components to help to integrate the InteropEHRate standard within the information systems of the healthcare organization:

- **HCP App**: an example of software application for HCPs that supports the InteropEHRate protocols. The objective of this prototype is to demonstrate concretely how the HCP can use InteropEHRate protocols and how can exploit the IHS (see below).
- **InteropEHRate Health Services (IHS)**: this component offers runtime functions for data conversions and translation and it exposes the interfaces for R2D protocol to interact with the S-EHR cloud. It interacts with existing legacy EHR systems through the LEI interface, that allows the import of health data from the legacy systems. The IHS can convert structured data from legacy to S-EHR and vice versa and uses an external service to translate free text to the local language and/or to the citizen language.
- **InteropEHRate Health Tools (IHT):** prototype of tools for
    - managing healthcare knowledge (lexical units, schemas, ontologies and encoding standards used by member countries). It interacts with IHS through the KCI interface
    - defining mapping rules for health record data, usable both locally to serve the data integration needs of local services (such as a hospital) and Europe-wide for cross-jurisdictional data exchange. It interacts with IHS though the DCI interface

Additional system reusable by the Research Centre

- **InteropEHRate Research Services (IRS)**: a prototype of a Research Interoperability Service. It is a component that interoperates with any S-EHR using the protocol for research health data sharing (through the RSI interface), allowing the scientists to engage voluntary citizens at cross-national level in new research trials and retrospective studies and to receive health data from them. It produces data that may be exploited by the applications (e.g. in a Clinical Trial Management System) of a research centre.

3.3.Deployment view

The following UML deployment diagram, summarize where the different components of the InteropEHRate framework are expected to be deployed. Deployment nodes offered by the same organization are grouped in the same rectangle.

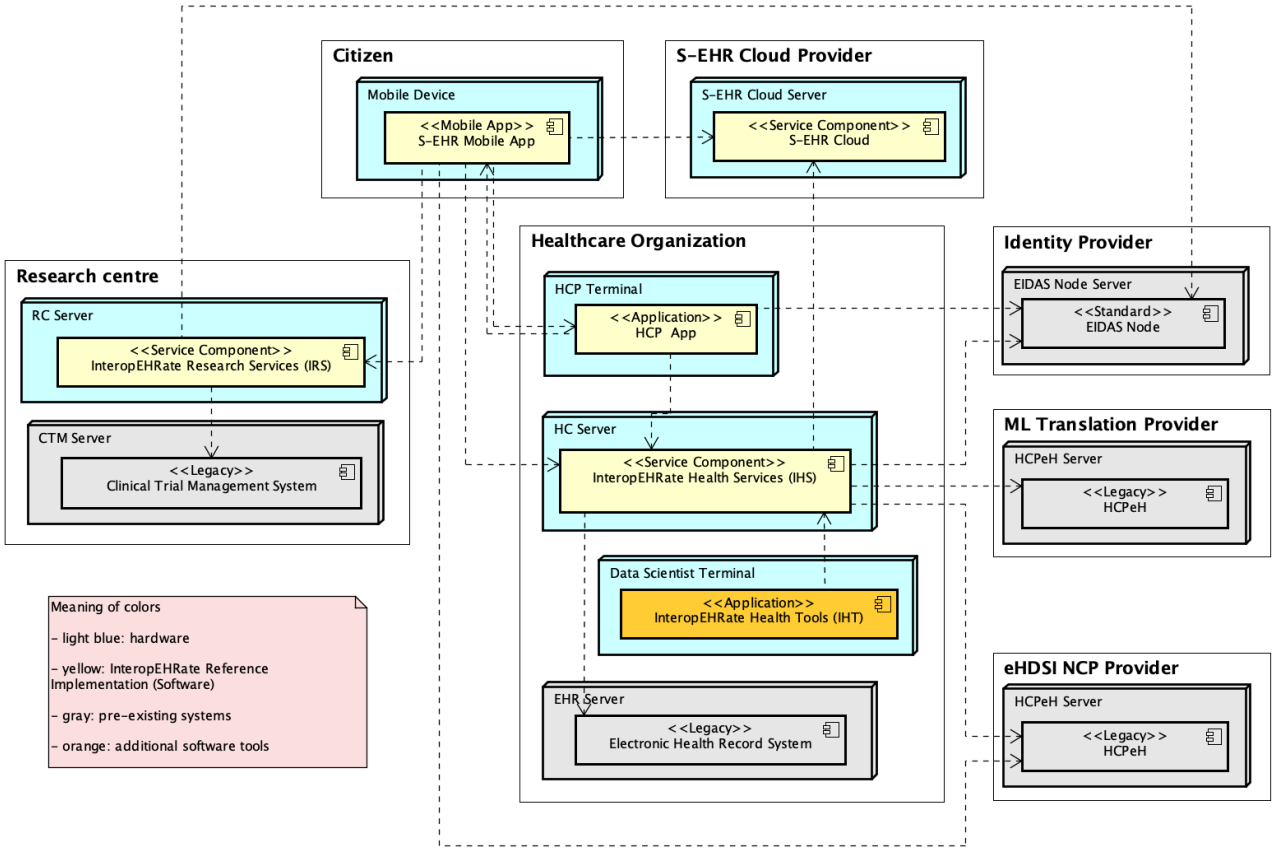


Figure 5 - Deployment view of the InteropEHRate framework

Each Citizen controls the personal mobile device where his/her S-EHR Mobile App is installed.
Each S-EHR Mobile App may interact with a S-EHR Cloud that is deployed on a different node (S-EHR Cloud Server) potentially offered by a different service provider (S-EHR Cloud Provider).
The S-EHR Mobile App may interact (using the D2D protocol) with the HCP App installed on the computer of any HCP (HCP Terminal) and with the IHS installed typically on a different server (HC Server) of any healthcare organization. If a healthcare organization outsources its IT service to another provider, then the IHS could also be hosted on the servers of the same provider.
Within the healthcare organizations is also used the IHT, usually installed on the computer (Data Scientist Terminal) of one or more Data Scientists. The IHS may interact with the legacy EHRs of the same healthcare organization, typically also running on a different server.
The S-EHR App may interact with the IRS installed on the machines (RC Server) of Research Centres. The IRS may interact with the legacy Clinical Trial Management System of the same Research Centre, installed on a different server (CTM Server).
For completeness also the deployment nodes of the EIDAS node, eHDSI National Contact Point (NCPeH) and the provider of external services for machine translation are depicted.

The following sections describes the single components of the InteropEHRate framework.

3.4.Reference Implementation libraries

The framework will provide a reference implementation of the InteropEHRate protocols as a set of reusable libraries, each one implementing a portion of one of the protocols. Each library may be reusable independently from the others.

Security libraries:

- **Mobile R2D Security Management**, **Terminal R2D Security Management**, **Server R2D Security Management**: These three libraries implement the main security functionalities (Identity Management, Consent Management, Authorization Management) required by the R2D protocol. They are usable respectively for mobile applications (e.g. the S-EHR of the Citizen), for desktop applications (e.g. the HCP App) and for server side services (e.g. for IHS and IRS).
- **Mobile D2D Security Management**, **Terminal D2D Security Management**: Similarly to the previous libraries, these two libraries implement the main security functionalities required by the D2D protocol.
- **Mobile Encrypted Storage**: this library implements the functionality to securely store encrypted health data on a mobile device in the respect of the "S-EHR mobile privacy and security conformance levels" [D3.1].
- **Mobile Encrypted Communication**, **Terminal Encrypted Communication**, **Server Encrypted Communication**: this library offers useful functionalities for encrypted exchange of health data to be exploited respectively for the implementation of mobile applications, desktop applications and server sides services.

Details on the design of security libraries may be found in upcoming report [D3.9].

Libraries for D2D and R2D protocols:

- **Mobile R2D HR Exchange**, **Terminal R2D HR Exchange**, **Server R2D HR Exchange**: These three libraries extends the R2D security libraries to offer an implementation of the R2D protocol for the exchange of health data on the internet [D4.1]. They are usable respectively for mobile applications, desktop applications and server-side services.
- **Mobile D2D HR Exchange**, **Terminal D2D HR Exchange**: These two libraries extends the D2D security libraries to offer an implementation of the D2D protocol for the exchange of health data on bluetooth [D4.1]. They are usable respectively for mobile applications and desktop applications.

Details on the design of libraries for D2D and R2D protocol may be found in upcoming report [D4.4].

Libraries for research protocol:

- **Mobile Research Data Sharing**, **Server Research Data Sharing**: These two libraries extends the R2D security libraries to offer an implementation of the research protocol for allowing the citizen to share health data for research purposes [D4.8]. They are usable respectively for the implementation of mobile applications and server-side services.

Details on the design of libraries for research protocol may be found in upcoming report [D4.10].

3.5.S-EHR Mobile App RI

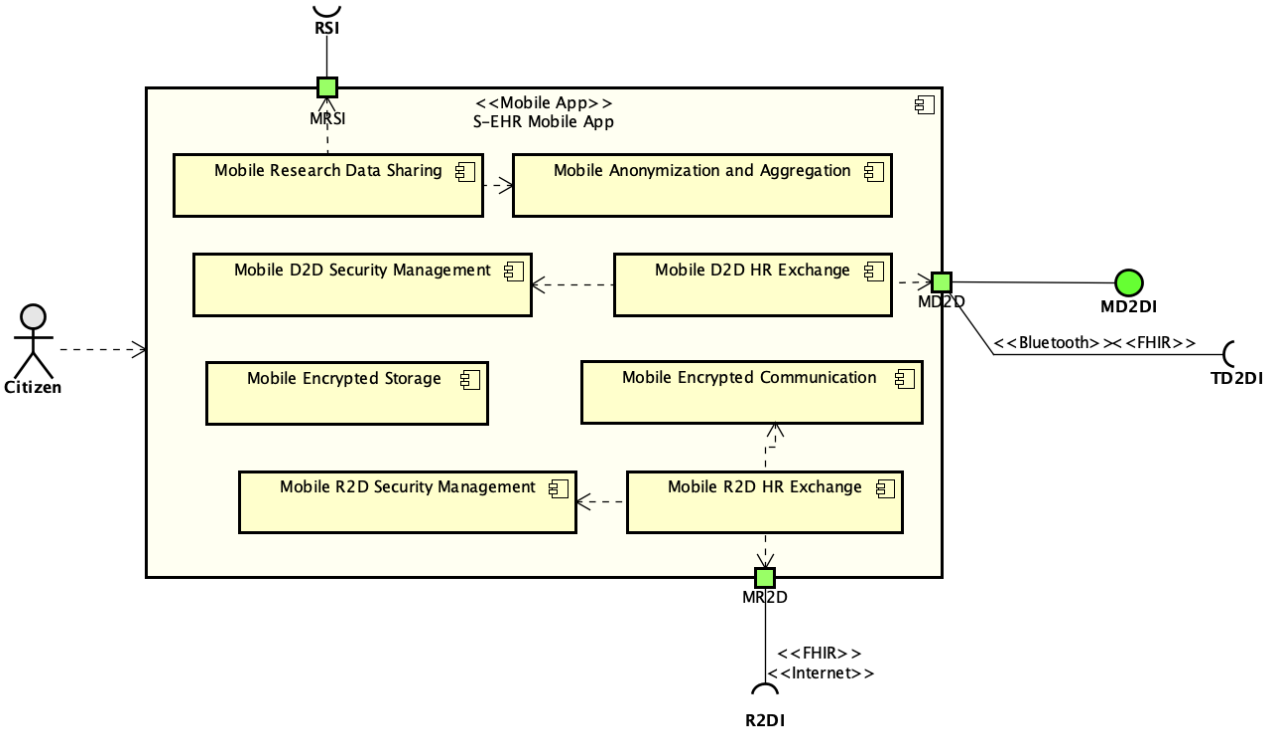


Figure 6 - S-EHR mobile app internal view

The S-EHR Mobile App RI is the reference implementation of a S-EHR satisfying the privacy and security conformance levels defined by the standard architecture [D3.1]. It provides a solution that is cantered on the citizen, to collect all health data of a citizen on a mobile device. Acting like a hub of his own data, it offers the possibility to exchange his data with other actors or organizations, such as hospitals, research centres, etc.

The S-EHR Mobile App RI is an Android application that, as shown in the figure above, integrate some of the reusable libraries described in previous section (3.4). It uses an encrypted data storage for all collected health data thanks to the library “Mobile Encrypted Storage”. Moreover, it integrates other libraries offered by the InteropEHRate framework implementing the client side of the three protocols defined by InteropEHRate:

- “Mobile Research Data Sharing” to share health data with Research Centres. Before sharing health data with a research centre, they are anonymized and aggregated, using the library “Mobile Anonymization and Aggregation”.
- “Mobile D2D HR Exchange” for the exchange of health data offline, through bluetooth.
- “Mobile R2D HR Exchange” for the exchange of health data online, remotely.

All these libraries in turn use the libraries “Mobile Encrypted Communication” to assure that any remote communication is encrypted, and use the libraries for identification and authorization (“Mobile D2D Security Management” and “Mobile R2D Security Management”).

The first version of the S-EHR Mobile App RI be able in particular to:

- trigger the bluetooth connection through QRCode;
- collect and transmit patient's consent (connection bluetooth, access and share of data, ...);

The S-EHR Mobile App RI will be available on the Android store for free.

3.6.S-EHR Cloud RI

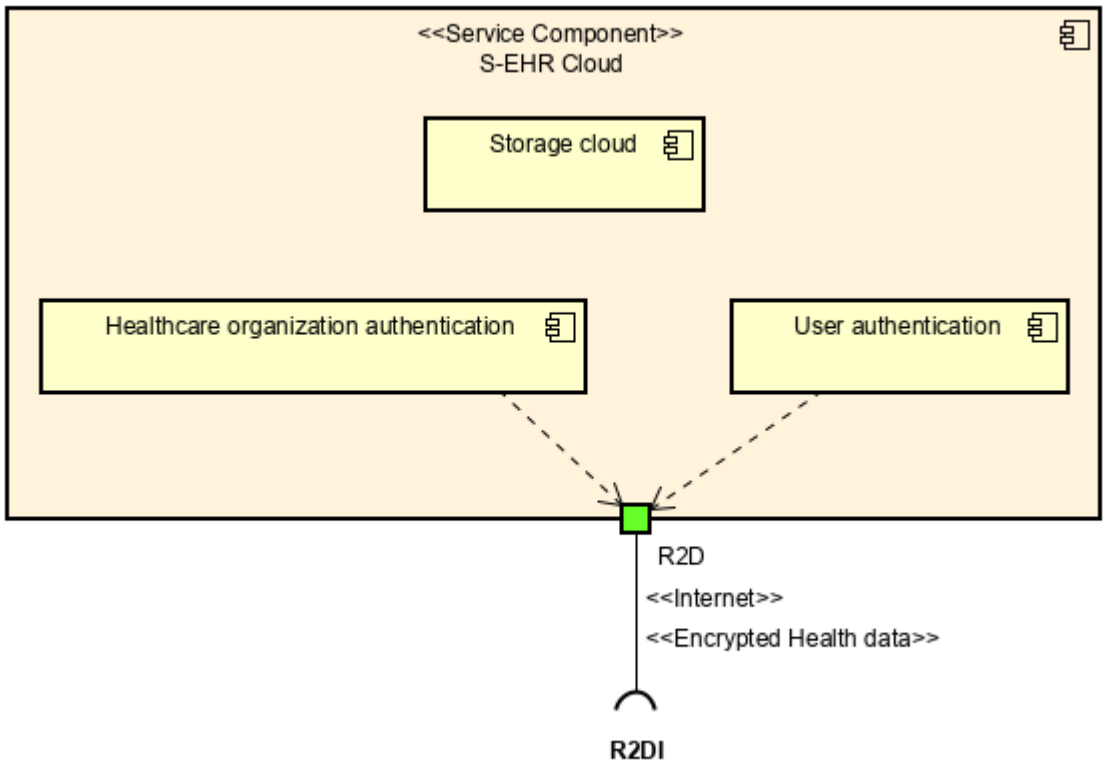


Figure 7 - S-EHR cloud internal view

The S-EHR Cloud regards an optional service in charge of the secure storage of the user's data in the cloud. Its design will fulfil the conformance levels as described in the [D3.1]. Using the S-EHR Cloud the user will have the ability to choose whether they want to store their encrypted health data in the cloud or prefer to be stored locally only in their smartphone.

The connection with the S-EHR Cloud service will be established through the R2D protocol and will allow only authorized users to (i) store their data in order to be accessible only by them, and (ii) download data. In addition, only authorized HCPs will also have the ability to access a set of predefined data in an emergency mode scenario.

The libraries that will be used for the secure transfer and storage of the data are the ones described in section 3.4.

The architecture of the S-EHR Cloud service is going to be provided later in the project in the corresponding deliverable [D6.7].

3.7.Example of HCP App

The InteropEHRate Framework includes a simple example of HCP App. It is a software application designed to provide medical staff with the ability to access and operate patients' data from S-EHR Mobile App, S-EHR Cloud and EHR of the Healthcare Organization. In other words, the HCP App is an application used by the HCPs to securely exchange health data of their EHRs with any S-EHR Mobile App and to read health data stored in S-EHR Cloud using the InteropEHRate protocols .

The HCPs of a Healthcare organization are not required to use a new application to exploit the InteropEHRate protocols. Indeed it is possible to extend the already used application to support the InteropEHRate protocols (one of the demonstrators developed by the project will indeed follow this approach). On the other hand, the HCP App is a new application built from scratch. It has the purpose to show to applications developers how the reusable libraries (see section 3.4) can be exploited to support the InteropEHRate protocols and how it is possible to exploit the IHS to interact with the content of an existing EHR. The HCP App is also intended to produce a demonstrator that can be easily distributed to show to the final users how HCPs can take advantage of the InteropEHRate protocols. In this respect this HCP App implementation will have functionalities for:

- Import data from S-EHR and export them back using the D2D protocol (TD2DI);
- Import data by the remote protocol (R2DI) with the S-EHR cloud;
- Import health data from current systems (EHRs) within healthcare organization.

Considering the overall architecture, user requirements specified in [D2.1] and technical solutions available at the moment, the HCP App will developed using web technologies. According to [D4.1] the D2D protocol will be implemented using Bluetooth, this will require to install the HCP app as a desktop application on health care professional's workstation (terminal)[5].

The HCP App will be developed using java technologies, thus ensuring Operating System independence and will have direct communications with S-EHR Mobile App and IHS as is illustrated in the following figure. Healthcare organizations may use the HCP App or may choose to evolve the GUIs of their legacy systems to add the same functionality provided by HCP App. The figure also shows which reusable libraries of the InteropEHRate framework will exploited for exchanging information with S-EHR Mobile App and S-HER Cloud. As said, looking at the code of the HCP App, the developers will more easily understand how to integrate the existing libraries also in their legacy systems, in order to offer functionalities similar to the ones of the HCP App. A description of the libraries integrated in HCP App can be found in chapter 3.4 – Reusable libraries.

[5] It would be advantageous to adopt a SaaS (Software as a Service) model of deployment, but this cannot be done yet in a reliable and secure way. The future standard to allow a (SaaS) Web Application to access the bluetooth connection of the user terminal will be the so called "Web Bluetooth API" **[WBA]**. Because Web Bluetooth API specification is not finalized and well implemented by the main web browsers, it will not be used for establishing the communication between HCP App and S-EHR Mobile App, at least for the moment. Considering this limitation, the HCP App can not be deployed as a centralized application even if it is developed as a web application.

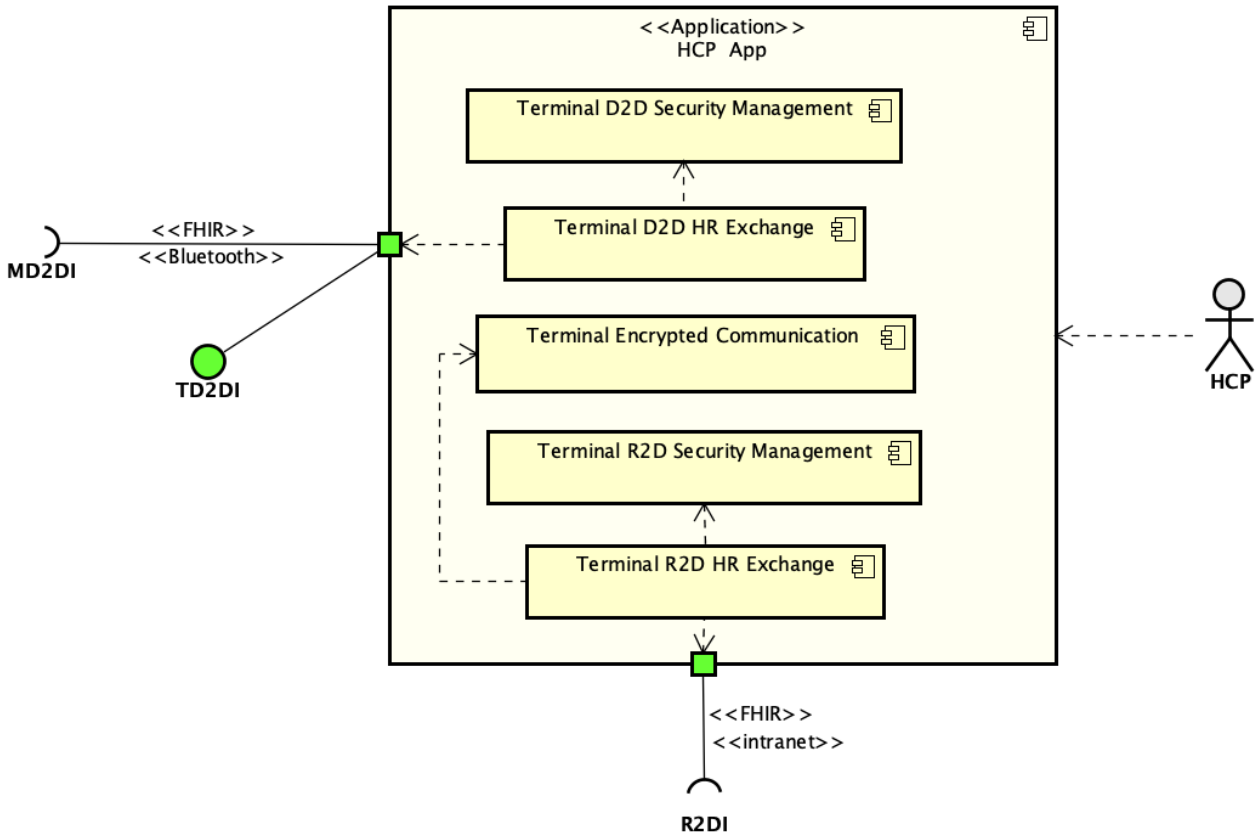


Figure 8 - HCP app internal view

HCP App will be distributed as a microservice with all components included and the installation on the health care professional's terminal consisting of copying a single file.

3.8.InteropEHRate Health Services (IHS)

InteropEHRate Health Services is a high-level component in charge of the conversion of local EHR formats to the interoperable S-EHR representation and of their translation into multiple European languages. In order to do so, the IHS exposes a set of high-level and low-level *S-EHR conversion and translation services:*

- Converting an entire legacy health record (EHR) into the common S-EHR representation, including the FHIR format and the use of interoperable medical coding systems;
- translating the contents of an entire S-EHR from one language to another;
- mapping individual coded values between local and international standards;
- providing the natural-language descriptions of such coded values in multiple European languages;
- providing translations of natural-language text contained within EHRs.

The IHS component supports three different levels of interoperability, each deployment site (e.g., hospital) being able to choose the level of support they are able to provide according to their technical and infrastructural capabilities:

1. Secure: beyond assuring the security of the EHR content, no conversion or translation is applied;
2. syntactic: in addition to the previous level, the S-EHR uses standard FHIR profile(s) as defined in Deliverable 2.7; however, data values remain in their original representations, with the possibility of free-text translation being applied to them;
3. semantic: in addition to the previous level, data values in the S-EHR undergo meaning-level conversions, such as the mapping of medical codes or the extraction of medical terms from natural-language text.

The following picture shows the main components of the IHS. It exploits the two reusable libraries "R2D Security Management" and "R2D HR Exchange" (see section 7.4), moreover it offers additional components further described in the next subsections.

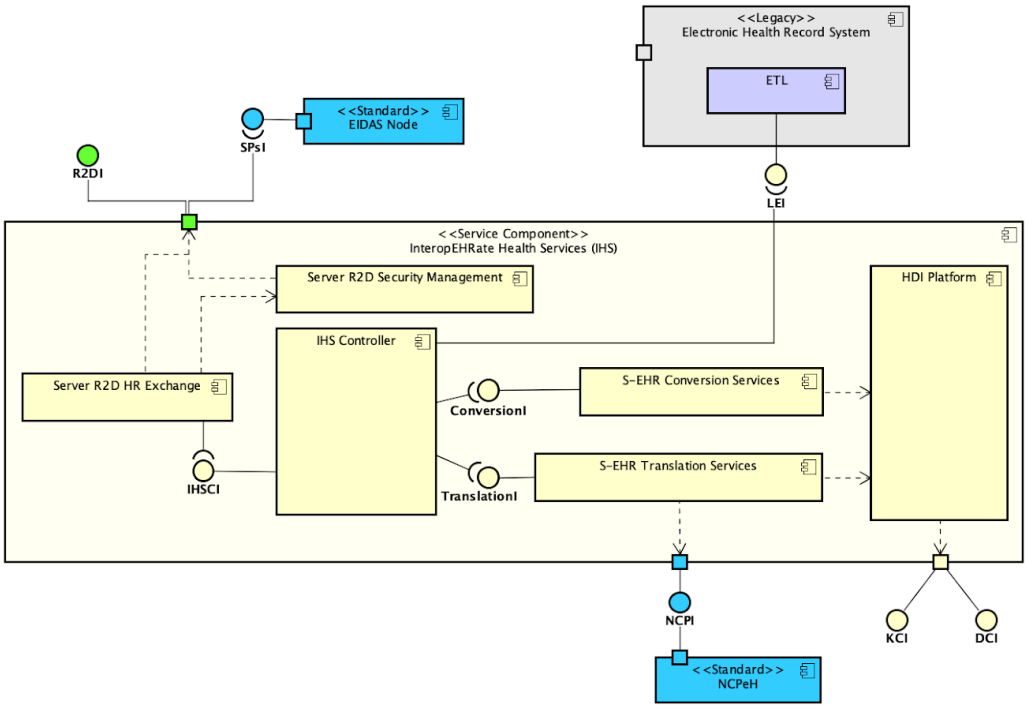


Figure 9 - IHS internal view

3.8.1. S- EHR Conversion and Translation Services

The EHR interoperability services offered by IHS are divided into two main categories, as realised by the components in the figure above:

- *conversion services:* these are implemented by the *S-EHR Conversion Services* component;
- *translation services:* these are implemented by the *S-EHR Translation Services* component.

The table below provides the main functionalities provided by these two components for each interoperability level:

Level	Conversion Services	Translation Services
Secure	None	none
Syntactic	• Conversion of EHR data structures to FHIR.	• Free-text translation for an entire S-EHR; • free-text translation for individual labels.
Semantic	• Conversion of EHR data structures to FHIR; • mapping of coded values to interoperability standards; • extraction of medical terms from natural-language text and linking them to non-ambiguous meanings.	• Free-text translation for an entire S-EHR; • free-text translation for individual labels; • translation of attribute names; • providing human-readable definitions for coded values in multiple languages.

Table 5 - Conversion and Translation service functionalities

The S-EHR Translation Service uses an external, third-party machine translation (MT) component for providing free-text translation. For all other conversion and translation services, the two components use the *HDI Platform*.

3.8.2. HDI Platform

These conversion and translation functionalities rely on an innovative knowledge-based data integration platform, shown as *Health Data Integration (HDI) Platform* in the figure above. The platform provides the following lower-level functionalities to the conversion and translation services:

- Multilingual natural language processing (NLP) for the health domain;
- cross-lingual knowledge management for the mapping and translation of medical terminology and coding standards;
- conversion of data structures from legacy to FHIR-based.

The HDI Platform is knowledge-based in the sense that data structures, terminology, labels in multiple languages, as well as locally specific NLP functions are all represented internally as adaptable and extensible knowledge. The initial bootstrapping and subsequent adaptation of knowledge is performed partly programmatically by a local software developer and partly interactively by a local *data scientist*, using graphical knowledge management tools that connect to the HDI Platform through the interfaces *Knowledge Configuration Interface* and *Data Integration Configuration Interface*. The knowledge management tools are presented below under the section *Interoperate Health Tools*.

3.8.3. IHS Controller

The role of the *IHS Controller* component is to provide high-level external interfaces for the IHS services and to adapt the (a priori generic) health services to the precise needs of the local environment. These involve:

- connecting to the legacy EHR system through a *Legacy EHR Interface (LEI)*, implemented by the local institution, for the reading and writing of legacy EHRs to/from local databases; in particular,

legacy EHRs are provided by the local systems to IHS in an agreed meta-format to be defined in D5.7;

- connecting to the *HCP App* through the *IHS Interface (IHSI)* that provides high-level services such as "localize a S-EHR to the local environment", into lower-level conversion and translation operations;
- serving requests, via the internal *HR Exchange* component and the R2D protocol, to remote devices requesting patient data over the Internet;
- defining the level of interoperability supported and using conversion and translation services accordingly.

3.8.4. R2D Security Management

This library (see section 7.4) provides an implementation for the R2D Security Protocol (see section 6.2.1), including identity management, authorization and consent management, as well as encrypted storage and communication, to be used over the R2D protocol when S-EHRs are transmitted through the Internet, as in the InteropEHRate emergency scenario.

3.8.5. R2D HR Exchange

The *HR Exchange* library (see section 7.4) receives and serves S-EHR requests from the Internet through the R2D protocol (see section 6.2.3). It delegates requests to the IHS components in charge of EHR processing, and uses the *Server R2D Security Management* component to assure the security of remote communication.

3.9. InteropEHRate Research Services (IRS)

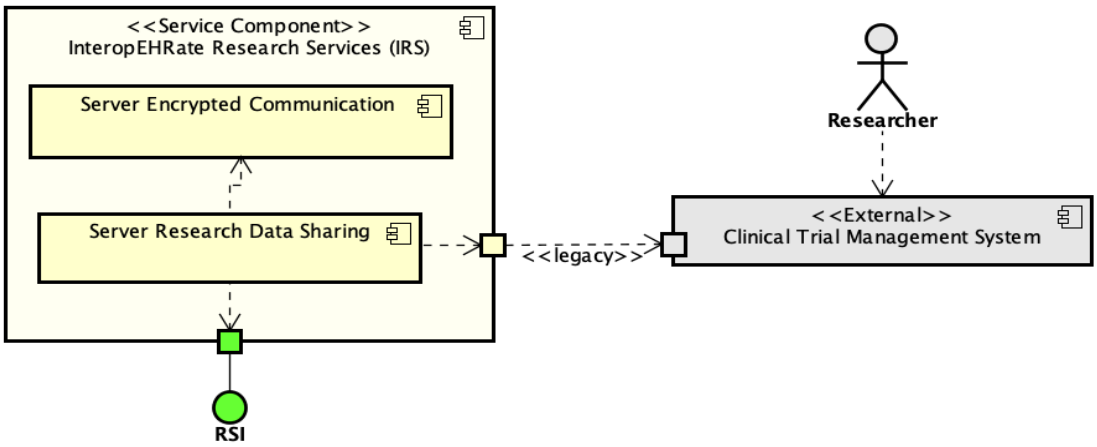


Figure 10 - IRS internal view

The *InteropEHRate Research Services (IRS)* implement functionalities that orchestrate data collection from the S-EHRs of patients in possession of the S-EHR Mobile App. As such, it is a software component that acts as a bridge between medical researchers (and their own IT infrastructure) and patients (and their S-EHR-enabled mobile devices). The role of IRS involves:

1. Receiving a formally defined experiment request from a Research Centre (through their *Clinical Trial Management System*);
2. evaluating, typically through human expert involvement, the acceptability and feasibility of the experiment request from multiple points of view (technical, legal, ethical, etc.), and approving or refusing it;
3. sending a data collection request to the S-EHR Apps of a predefined set of patients, including the data attributes queried and corresponding constraints (e.g., *age >= 18 years*);
4. receiving and handling consent or refusal from individual patients;
5. receiving data collected from patients, which has already undergone an initial level of de-identification;
6. further de-identifying collected patient data, and aggregating such data across patients;
7. providing aggregated and anonymous patient data to the requestor Research Centre.

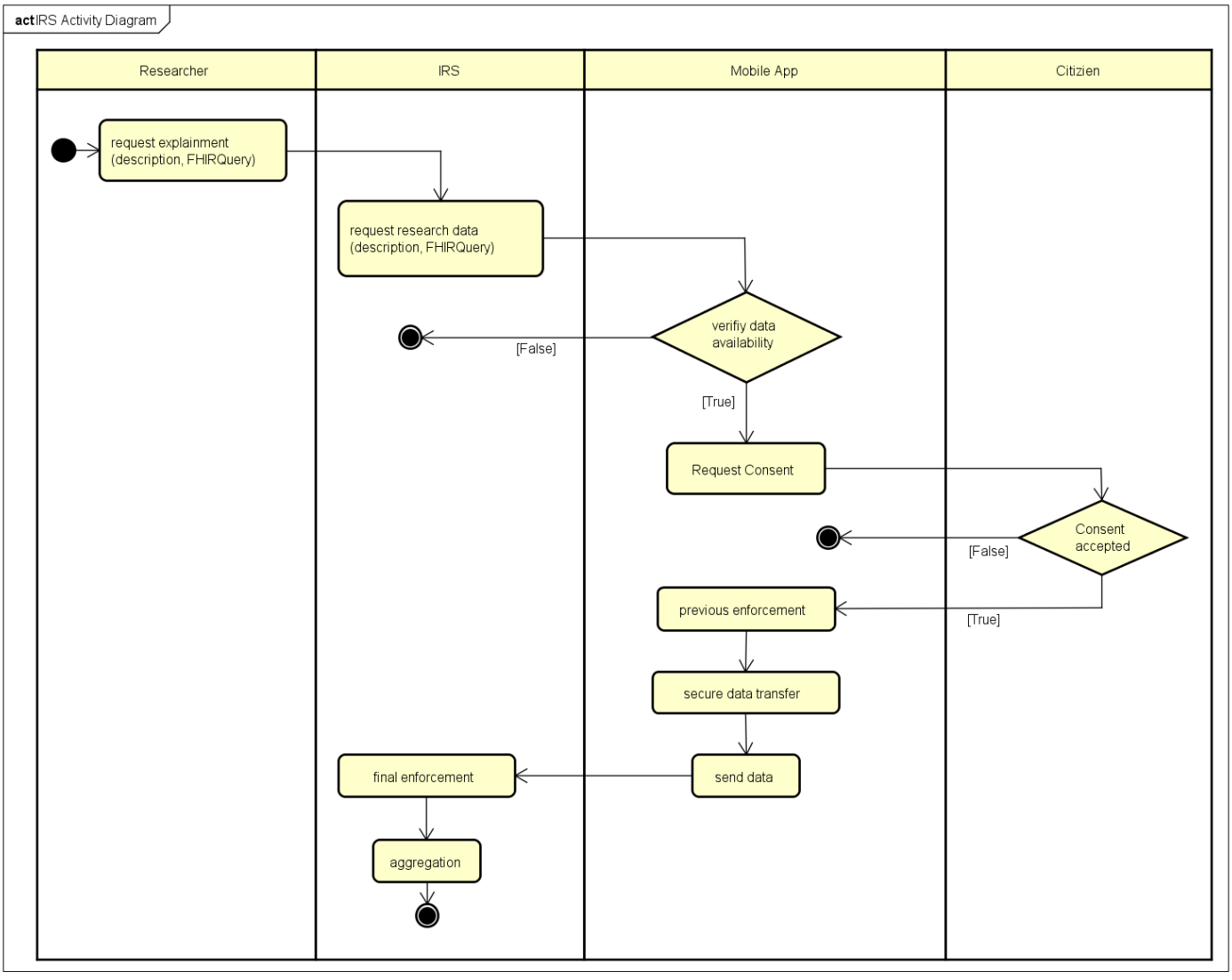


Figure 11 - IRS activity diagram

3.10. InteropEHRate Health Tools (IHT)

As part of the InteropEHRate framework, the *InteropEHRate Health Tools* are interactive tools that serve the purpose of configuring and adapting the *HDI Platform*, and as such the entire IHS, to the specific needs of the local institution (e.g., hospital). Configuration and adaptation involve supporting:

- Local language;
- local medical terminology;
- locally used medical coding systems and their mapping to international ones;
- local data structures and their mapping to FHIR.

Note that local terminologies, codings, and data structures evolve over time: thus, their maintenance and adaptation is not a one-shot effort but rather a continuous process. Still, the bulk of the configuration effort is foreseen as part of the initial deployment phase of the IHS.

All of the configuration aspects above are represented in the HDI Platform as formal *knowledge*. This formalisation effort, that encodes local formats, standards, and semi-formal or informal practices as knowledge, is executed by a local *data scientist* using the interactive IHT tools. In case some of the effort needs to be automated through scripting (e.g., uploading the definitions of thousands of terms), the data scientist can be assisted by a *software developer* in charge of programmatically automating some of the processes instead of using the IHT.

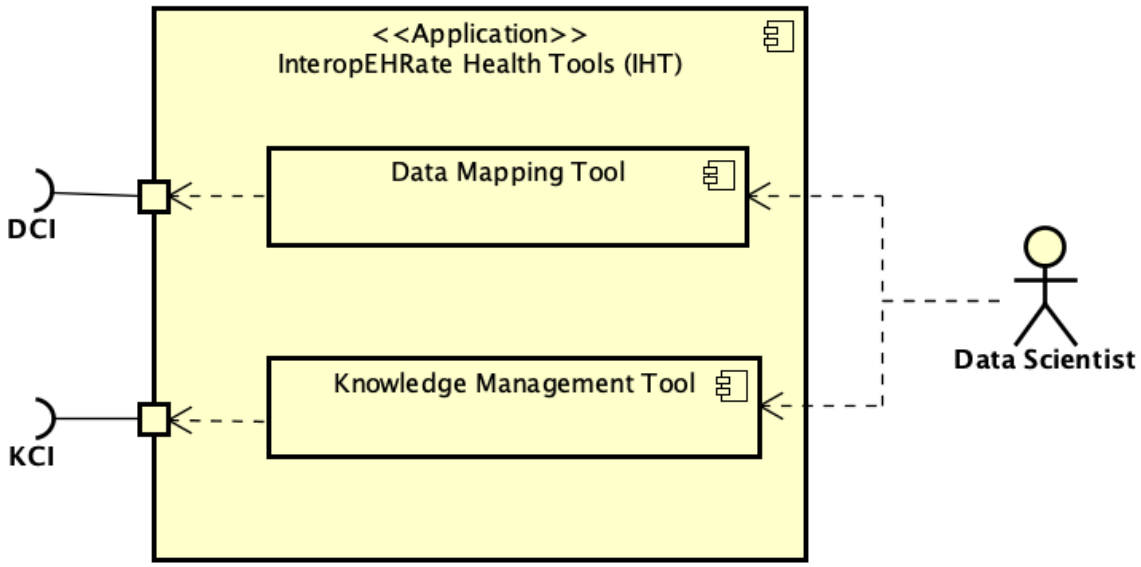


Figure 12 - IHT internal view

As depicted above, IHT is composed of two principal tools:

- a *Data Mapping Tool* with which the data scientist defines how to convert data from the legacy EHR structure to the FHIR-based structure;

- a *Knowledge Management Tool* which is used to define and describe the lexicon, medical terminology, medical encodings, and their mappings.

The tools are typically used in the following order and manner:

1. Knowledge that defines and describes interoperability standards (e.g., FHIR or international encodings) is *a priori* built into the HDI Platform, all the while remaining adaptable and extensible.
2. The Knowledge Management Tool is used:
    a. To define locally relevant concepts and their relatedness (underlying the meanings of terms, data attributes, coded values, etc., that are used by the local institution or on regional or national levels);
    b. to define natural-language labels associated to the concepts above (how the meanings above are expressed inside local datasets);
    c. to adapt and extend, if necessary, the FHIR reference schemas to which local EHRs or third-party S-EHRs are converted;
    d. to define mappings, wherever applicable, between locally relevant and international concepts.
3. The Data Mapper Tool is used interactively to define the mappings of local EHR data attributes to FHIR attributes, as well as corresponding data conversion methods. The result is a data mapping "recipe" that the HDI Platform is able to execute automatically on EHRs.
4. The results of steps 2-3 are tested through the automated execution of the conversion and translation of a test set of EHRs. In case of problems encountered, steps 2-4 are repeated to fix the knowledge and/or the mappings and re-test the results.

3.11. Interactions between HCP App, IHS and legacy systems

3.11.1. Extract S-EHR content from source hospital

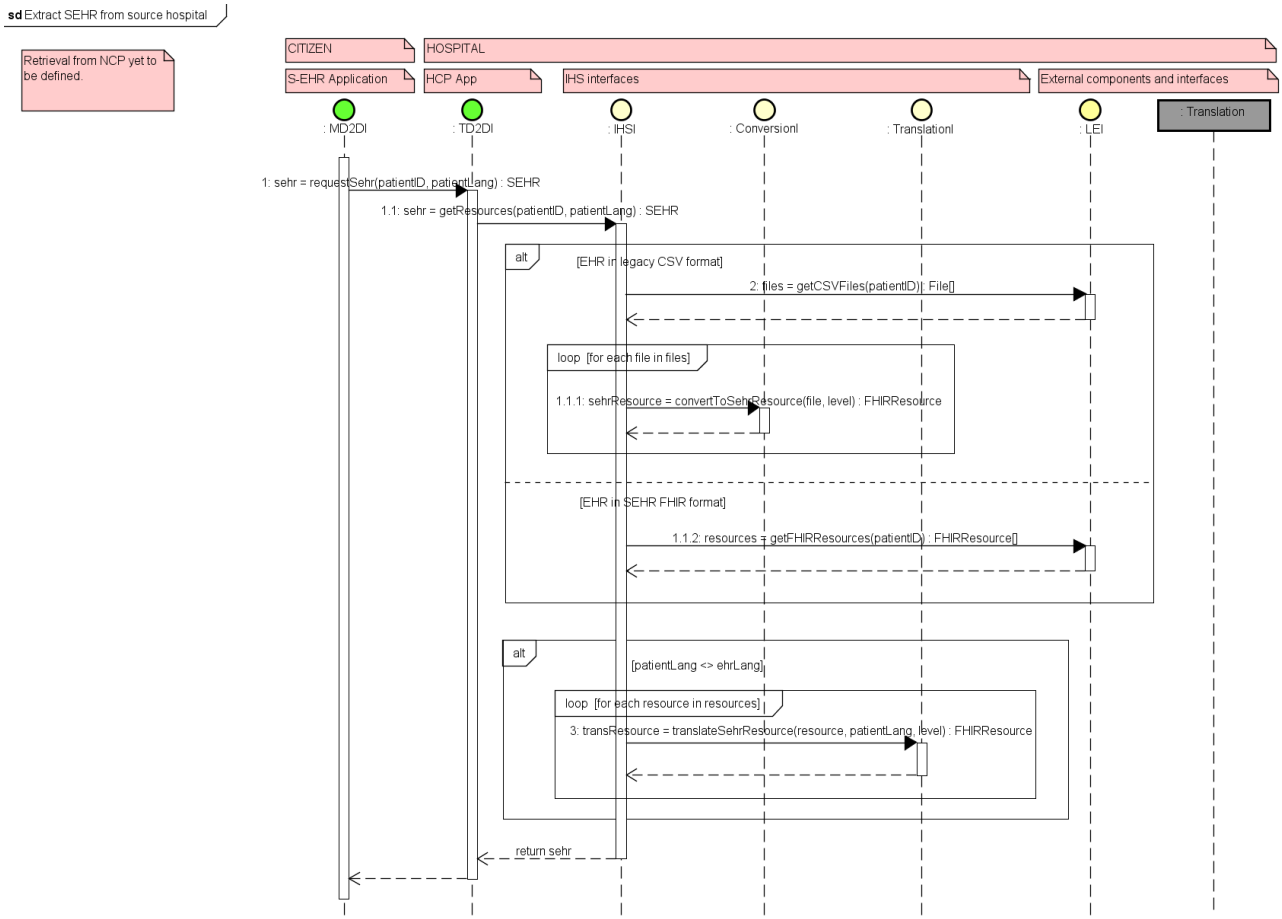


Figure 13 - Sequence diagram: extract S-EHR content from source hospital

The sequence diagram above describe a situation in which a patient wants to get his/her own health data from a hospital. The first actor in the diagram is the citizen, represented by a S-EHR App, and the second one is the hospital that is composed by:

- HCP App: the component that communicates with the citizen.
- IHS Interfaces: the component that offers the usage of S-EHR conversion and translation components described in section 7.4.5
- external components and interfaces: elements such as interfaces with legacy EHR (LEI) and external tool of machine translation.

The first method is called from the citizen interface to the HCP App interface, to request the "SEHR" object that contains the citizen health data, in this call are specified the patientID and the wanted language for the result data. After that the HCP App invokes a request of resources, identified by the patientID, to the IHS interface (IHSI). The IHSI have to check if the corresponding EHR is present only in legacy CSV format, or the EHR already exists in S-EHR FHIR format:

- In the first case, IHSI calls a method to retrieve the CSV files requested, and then, for each file, invokes the *convertToSehrResource* method of the conversion component that returns a FHIR version of the file.
- In the second case, IHSI have to retrieve, through LEI, the resources in FHIR format calling the method *getFHIRResources* that search them by patientID.

In the end, if the patient's own defined language (in the first method call) is different from EHR language retrieved, IHSI, for each resource obtained in the previous phase, calls the *translateSehrResource* method of the translation component that returns the FHIR resources translated in the language specified by patientLang parameter. Finally the S-EHR data are returned to the HCP App and then to the citizen.

3.11.2. Download and use S-EHR content at target hospital

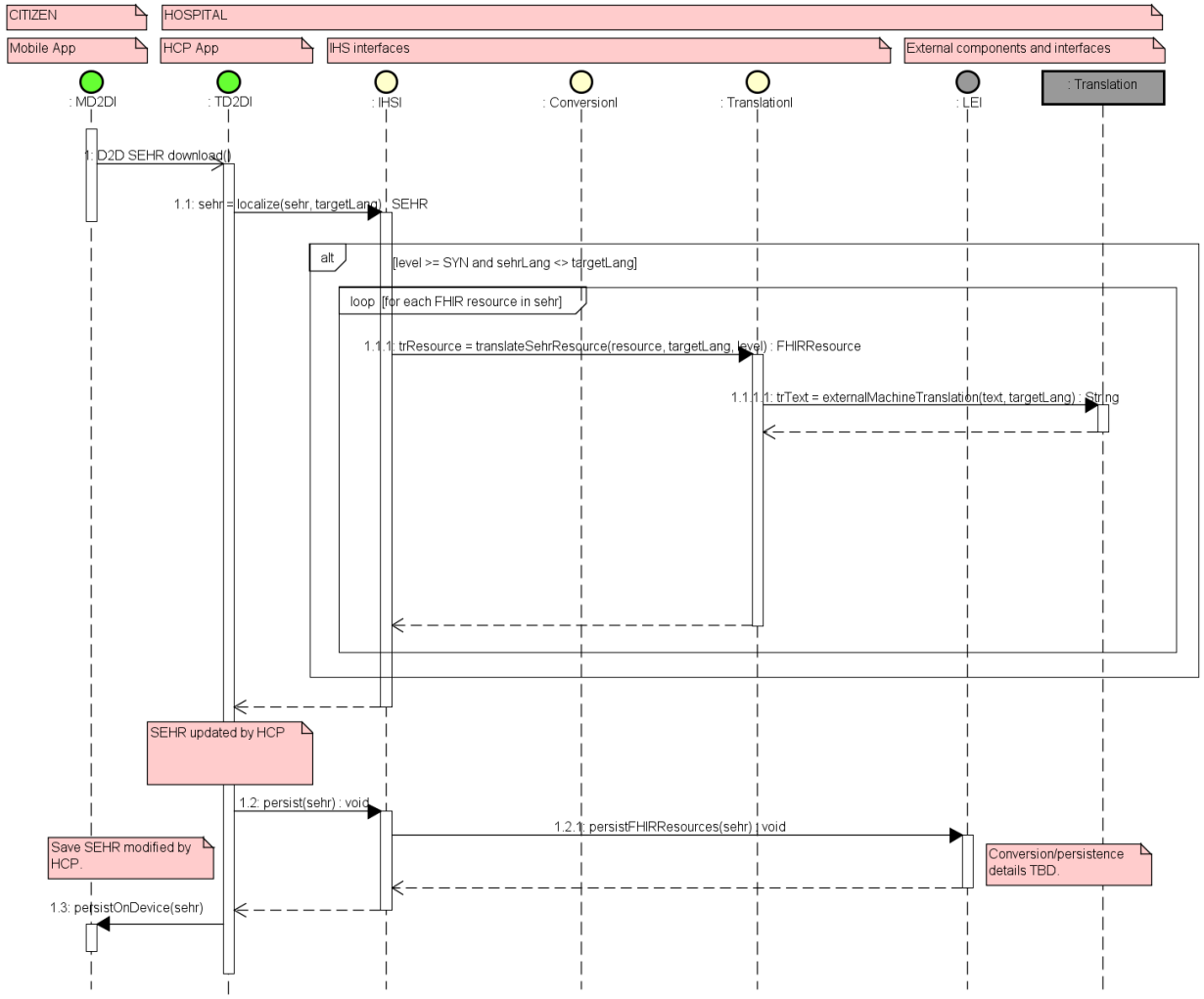


Figure 14 - Sequence diagram: download and use S-EHR content at target hospital

The sequence diagram above describes a situation in which a hospital wants to download the citizen's health data from the mobile app, to update/modify these data. The actors and the components of this diagram are represented exactly in the same way as the previous one.

At the start the mobile app of the citizen calls a method to download the health data to the HCP App , then the HCP App invokes a method of IHSI to specifying as parameters, the S-EHR object and the language in which the hospital wants to read/manage the data (targetLang parameter). After that, the IHSI checks if the language of the sher object is different from the language specified by the targetLang parameter, and, in this case, for each FHIR resource in S-EHR object, calls the *translationSehrResource* method of the translation component. The text of each resource is translated using an external component for machine translation. After that the FHIR resources are returned to IHSI and then to the HCP App that can update/modify them.

The final phase of the diagram describes the methods for update the database with the new data and the update of these modification also on the mobile app of the citizen.

4. CONCLUSIONS AND NEXT STEPS

This report described a first draft of the InteropEHRate standard architecture and of its reference implementation, the InteropEHRate framework. Similarly to other reports of the InteropEHRate project, this document presents just a first draft of the intended content, reflecting the current understanding by the project consortium. Other two updated versions of this report are planned, one on March 2020 and another one on March 2021.

The following versions could introduce other elements to the architecture, and will likely change some of the ones currently specified. The changes will be based on the new knowledge acquired from the experience of development during the first year, from external feedback (e.g. from focus groups) and from the detailed design of components and interfaces that are planned for next year.

Major changes are expected in particular with respect to the relation among components related to R2D and research protocols that are involved in usage scenarios [D2.1] not yet analysed in detail.

GLOSSARY

Term	Definition
Clinical Trial Management System	It is a software system used by biotechnology and pharmaceutical industries to manage clinical trials in clinical research.
Device to Device Protocol	Secure communication protocol (and API) for exchange of health data among two near devices (not using the internet), one running the S-EHR mobile app and the other running an HCP (desktop, web or mobile) application (e.g. a GUI of an EMR).
Electronic Health Record System	according to the definition of [ISO/TR 20514]: "A system for recording, retrieving and handling information in electronic health records".
HealthCare Professional	Every health care professional that produces and/or access to health data of a Citizen. It is a member of a multidisciplinary team composed by several healthcare professions working together to execute healthcare processes (e.g. Medical Doctors, Nurses, Midwives, physiotherapists, …)
HealthCare Professional Application	Any software application used by HCPs to securely exchange health data with any S-EHR using the communication protocols defined by InteropEHRate. An HCP App may be an advanced front end an EHR, may be a distinct application integrated with an EHR, or it may be a completely independent application. It is part of the "Healthcare Organization Information System".
InteropEHRate Health Services	It is a set of reusable components offered by the InteropEHRate Framework, deployed within healthcare organizations, implementing the D2D and the R2D protocols to share health data contained in their EHR with the S-EHR.
InteropEHRate Health Tools	Tools, offered by the InteropEHRate Framework, used by the Domain Experts for configuring the conversion of health data from a local format to the InteropEHRate FHIR profile and to the language of the user.
InteropEHRate Research Services	it is a set of reusable components offered by the InteropEHRate Framework that interoperates with any S-EHR using the protocol for research health data sharing, allowing the scientists to engage voluntary citizens at cross-national level in new research trials and retrospective studies and to receive health data from them.
MD2DI	Interface offered by the S-EHR to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at short distance, without using internet.
R2D	Secure communication protocol (and API), using internet, for cross-border exchange of health data among S-EHR, HCP applications, EMR, EHR and cloud storage systems. The protocol will cover two kind of data exchange: (1) peer-to-peer exchange of

	health data among two specific nodes (e.g. among a specific S-EHR and a specific EMR); (2) federation of health data, to access all health data of a citizen from any federated EHRs/EMRs.
R2DI	Interface offered by the HealthCare Organization to support the R2D protocol, i.e. to exchange health data with citizen's S-EHRs by means of internet.
RSI	Interface offered by the Research Centre to support the research protocol, i.e. to engage citizens and to receive their health data and consent to usage.
S-EHR	Model of secure mobile applications for the storage, control, anonymization and exchange of health data on smart devices (e.g. smartphones or tablets), without the obligation to store data in the cloud. A S-EHR is able to import/share data from/with EHR/EMRs and with research centres, using short-range wireless D2D (device to device) communication or remote communication protocols. The S-EHR allows to store on a smart device the health data about a single citizen and produced by the citizen itself or by HCPs.
S-EHR App	Synonymous of S-EHR
S-EHR mobile App	Synonymous of S-EHR
S-EHR-C	Secure cloud service, fulfilling the S-EHR conformance levels, able to store on the cloud the data collected by S-EHRs, adopting the standard protocols defined by the project. A citizen may choose to use a S-EHR mobile app without using any S-EHR cloud. In this case, his/her health data will be accessible to health professionals by using the short-range D2D protocol or the EHR federation.
TD2DI	Interface offered any application used by HCPs to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at short distance, without using internet.

REFERENCES

- **[D2.1]** InteropEHRate Consortium. *D2.1 : User Requirements for cross-border HR integration - V1*. InteropEHRate project, June 2019. www.interopehrate.eu/resources
- **[D2.7]** InteropEHRate Consortium. *D2.7 : FHIR profile for EHR interoperability - V1*. InteropEHRate project, Due on September 2019. www.interopehrate.eu/resources
- **[D3.1]** InteropEHRate Consortium. *D3.1 : Specification of S-EHR mobile privacy and security conformance levels*, Due on March 2020. www.interopehrate.eu/resources
- **[D3.9]** InteropEHRate Consortium. *D3.9: Design of libraries for HR security and privacy services - V1*, Due on September 2020. www.interopehrate.eu/resources
- **[D4.1]** InteropEHRate Consortium. *D4.1: Specification of remote and D2D protocol and APIs for HR exchange - V1,* June 2019. www.interopehrate.eu/resources
- **[D4.4]** InteropEHRate Consortium. *D4.4: Design of libraries for remote and D2D HR exchange - V1*, Due on September 2019. www.interopehrate.eu/resources
- **[D4.8]** InteropEHRate Consortium. *D4.8 : Specification of protocol and APIs for research health data sharing - V1*, Due on March 2020. www.interopehrate.eu/resources
- **[D6.7]** InteropEHRate consortium. *D6.7 : Design of a service for cloud storage of S-EHR content (S-EHR Cloud) - V1,* Due on April 2021. www.interopehrate.eu/resources
- **[HL7 FHIR]** HL7 Fast Healthcare Interoperability Resources Specification. http://hl7.org/fhir/
- **[EU CB ANNEX]** ANNEX to the Commission Recommendation of 6.2.2019 on a European Electronic Health Record exchange format
- **[WBA]** Web Bluetooth Draft Community Group Report, 14 June 2019. https://webbluetoothcg.github.io/web-bluetooth/
- **[ISO/TR 20514]** ISO, TR. "20514: 2005 Health Informatics-Electronic Health Record Definition, Scope and Context Standard." International Organization for Standardization (ISO), Geneva, Switzerland (2005).