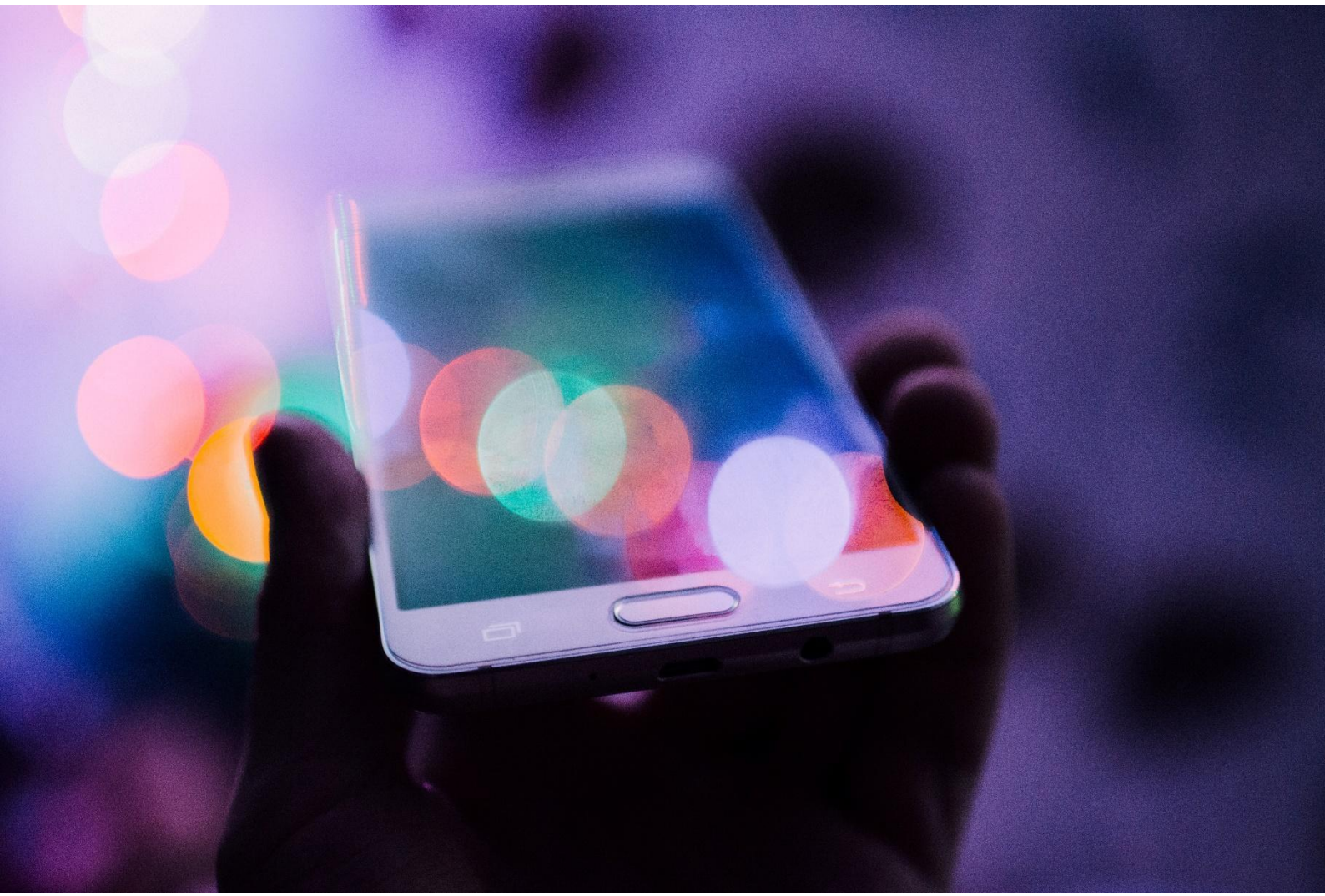
InteropEHRate
EHR in people's hands across Europe

Unleashing personal health data for care and research:

The InteropEHRate approach



White Paper

August 2021

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

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

Version 25 August 2021

Cover photo by Rodion Kutsaev

Table of Contents

Abbreviations

API	Application Programming Interface
CA	Certificate Authority
CCMM	Continuity of Care Maturity Model
CEF	Connecting Europe Facility
D2D	Device-to-device
EHR	Electronic Health Record
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
EMR	Electronic Medical Record
EMRAM	Electronic Medical Record Adoption Model
EU	European Union
GDPR	General Data Protection Regulation
HCP App	Healthcare provider application
HL7 FHIR	Health Level Seven Fast Healthcare Interoperability Resources
IPS	International Patient Summary
IT	Information technology
KDF	Key Derivation Function
PKI	Public Key Infrastructure
QR	Quick Response
R2D	Remote-to-Device
RDS	Research Data Sharing
S-EHR	Smart Electronic Health Record
SME	Small and medium-sized enterprise

1. Why do citizens need to be empowered to use their health data?

Personal health data is still not used as widely as it could be for care and research in Europe. The challenge is how to unleash that data.

Today, citizens have limited access to, and lack control of, their own health data, especially when they move around Europe. While the digitisation of healthcare in the European Member States is making rapid progress, patient health data is spread across health providers and locked in different data silos, hampering its potential use for health innovation and research.

Barriers are frequent. There are legal and technological constraints to data sharing, but also semantic barriers, such as the different languages and terminologies adopted by countries. Consequently, citizens cannot easily make sure that their complete health data is available to different health care providers so as to ensure their safe and efficient treatment (even less so across borders) and cannot access their full clinical history and share it for research.

At present, health data exchange follows predominantly a *healthcare-centred approach*. Healthcare providers maintain and control patients' health data through Electronic Health Records (EHRs). Generally, these EHRs are connected centrally to national or regional EHRs, allowing other healthcare organisations, authorised research centres, and citizens themselves to access the health data. In this approach, the exchange of health data is mediated by the central EHRs or by networks of connected entities.

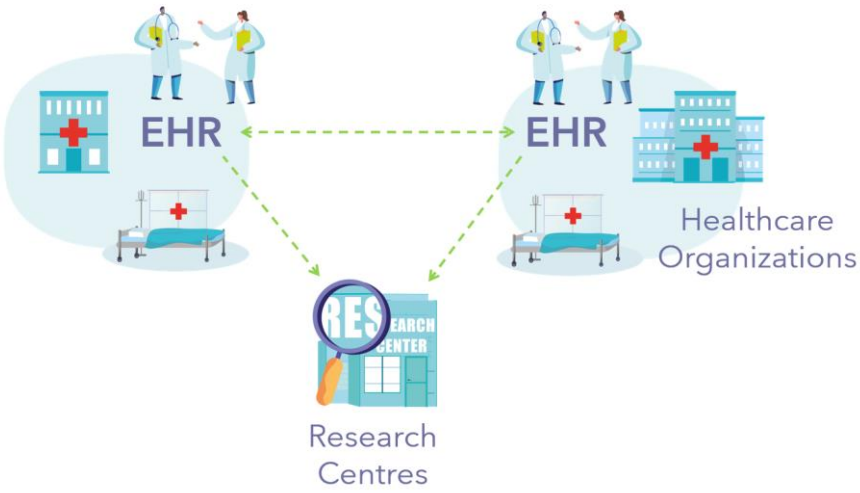


Figure 1. Healthcare-centred approach to health data exchange

Cross-border health data exchange in Europe is, however, making progress enabled by MyHealth@EU[1] which exchanges Patient Summaries and ePrescription services through the Member States' National Contact Points for eHealth.

Citizens' access to personal health data supports patient empowerment and self-care and can contribute significantly to medical research. This benefits continuity of care between healthcare providers at national level and across borders.

Yet today's predominantly healthcare-centred approach limits data sharing with citizens, and thus fails to offer opportunities for better care and research. Data sharing tools that are

[1] MyHealth@EU: https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en

compliant with approved data protection and data governance are needed to give citizens control over their own health and care data.

InteropEHRate aims to unleash health data from local silos and offer more power to citizens in managing their own health data across different health providers and countries, thereby improving care and accelerating health research.

2. How does InteropEHRate enable a citizen-centric approach?

InteropEHRate solutions draw on a citizen-centric approach complementary to the existing healthcare-centred model and permit the use of personal health data by citizens for both care and research.

2.1 Access to personal health data in Europe for care

Through their mobile devices, citizens are in control of their personal health data which they are able to share with healthcare professionals and research centres in compliance with the General Data Protection Regulation (GDPR) and their own preferences.

Smart Electronic Health Records (S-EHRs) are a key vehicle for the citizen-centric model. S-EHRs are mobile applications that store health data in smartphones, independent from cloud storage. InteropEHRate open protocols enable S-EHRs to exchange health data securely under the citizens' control of what to share, with whom, and when.

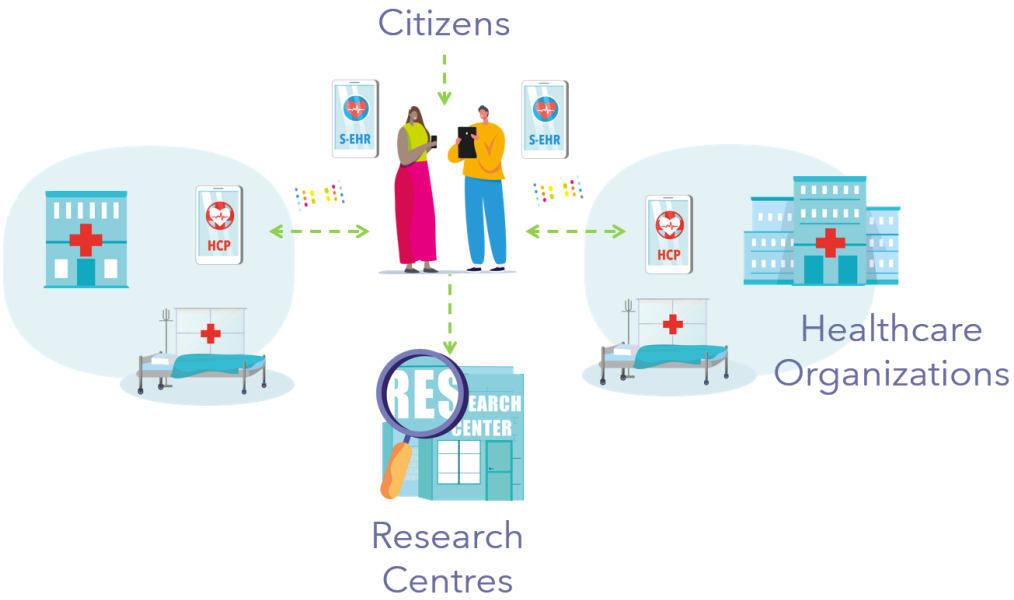


Figure 2. Citizen-centred approach to health data exchange

Two use cases illustrate the applications of InteropEHRate solutions in two different healthcare scenarios: the healthcare visit abroad (Box 1), and the emergency access (Box 2).

Box 1. Healthcare visit abroad scenario

A Belgian male patient has chronic ischemic heart failure and atrial fibrillation. The patient is regularly followed up at the outpatient clinic of a tertiary centre where he undergoes twice a year electrocardiogram and blood tests, and yearly echocardiogram, cardiopulmonary exercise testing, device control and 24-hour Holter monitoring, together with cardiological consultation.

The patient moves to Greece for a two-year stay, during which he complains progressively of mild lower limbs oedema, dyspnoea, and a reduction in his tolerance for exercise.

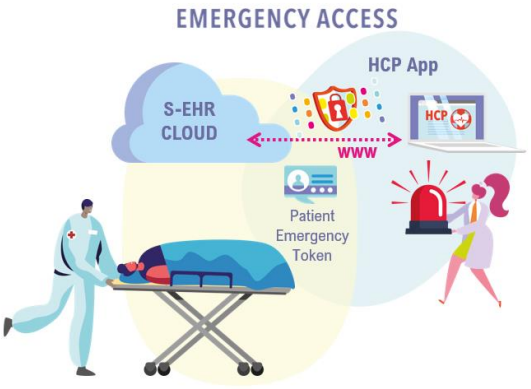
The patient's demographic data, consent, and his previous clinical history were already loaded on the S-EHR App before he left for Greece. During his stay in Greece, the patient seeks medical care. At the healthcare visit and using the S-EHR App, the patient authorises the healthcare professional in Greece to access elements of his health data, such as his allergies and adverse drug reactions. The clinician accesses this shared data from an HCP App which can make use of a Device-to-Device (D2D) protocol. Patient treatment is established on these grounds, and any prescription is transferred to the S-EHR on the patient's mobile phone.

Once the patient has left the hospital, the doctor has no further access to additional information from the S-EHR. On his return to Belgium, the patient will similarly be able to exchange the newly collected health data with other health professionals using the D2D protocol.

Box 2. Emergency access scenario

A 56-year-old female patient is abroad. She complains of nausea, vomiting, and mild abdominal pain. She is transferred by ambulance to a local hospital emergency department. Her condition deteriorates, she is in shock and requires prompt treatment.

The patient previously enabled the S-EHR Cloud. While travelling abroad, she has also brought with her a personal identity token for use in emergency settings.



Emergency care professionals use a healthcare provider application (HCP App) that supports the Remote-to-Device (R2D) protocol for healthcare. Following the protocol, the application verifies their identity and professional role using the national identity provider. Using the patient emergency token and, thanks to their authenticated identity and role, the healthcare professionals are granted access to the emergency dataset stored in the patient's S-EHR Cloud. The access is traced using "emergency mode" and records the credentials of the treating healthcare professionals. The patient's health data are retrieved from the S-EHR Cloud, translated into the local language, and medical terminology so as to support a risk-free diagnosis and treatment of the patient.

When the patient is discharged from the hospital, the S-EHR Cloud is updated by the healthcare professionals. Her Discharge Summary contains the cause of her admission to hospital, discharge diagnostic assessment, information about any other visits, recommendations, therapy, and prescriptions. Thanks to the R2D protocol for citizens, this latest health data will be available on the S-EHR App.

2.2 Health data sharing for research

Health data remain locked in data silos. This hampers the potential for data to be used positively to improve health innovation and research. The efforts and costs involved in health data collection, and the lack of a common regulation to empower European Union (EU)-level protocols, currently limit clinical research.

The main obstacles to health data sharing are the lack of access to health data, identity and consent management, and the inability to donate data for research purposes. In recent years, global movements and national initiatives (e.g., MyData[2]) have pledged to increase citizens' control over their personal data so as to ensure that all citizens can share their health data in order to further the common good of health research.

In 2020, a European large-scale citizen survey found that people had a consistent willingness to share data with health researchers when their data privacy is protected, and the data are not used commercially.[3]

Figure 3. Citizen survey on attitudes on the use of data for research (DigitalHealthEurope 2020)

Addressing overcoming challenges to data altruism is, however, not enough to unlock the use of real-world data for research. Standard methodology of clinical research, based on trials to develop new medicines and devices, are facing similar obstacles.

Three noticeable challenges to conducting sound clinical trials are patient recruitment, prevention of patient dropout, and data collection. This is where decentralised models of clinical trials come into play in response. Decentralised Clinical Trials can improve patient involvement in trials, increase the participation of diverse populations, and enhance data collection. They also enable more real-time collection of data[4], and the data collected is much richer: in addition to the medical data previously available, nutrition, activity, sleep data, and all kinds of real-world data and social determinants of health, can be added to the collection.

InteropEHRate can enable data collection in diverse and innovative areas such as digital therapeutics, rare diseases, orphan drugs trials, and treatments or studies based on patient reported outcome measures.

---

[2] MyData: https://mydata.org/

[3] DigitalHealthEurope. Citizen-controlled health data sharing governance. October 2020. https://digitalhealtheurope.eu/wp-content/uploads/2020/11/Consultation-Paper-Citizen-controlled-health-data-sharing-governance.pdf

[4] Data are sent from home by patients via anonymised questionnaires and do not require a visit to the doctor's office every time they are completed.

Box 3. Research data sharing scenario

The research centre of a Regional University Hospital is conducting a research study about the incidence and risk factors among the general community for a specific medical condition. The research protocol requires two sets of data to be collected: the prospective collection of anonymised health data for two years after patient enrolment in the study, and a five-year retrospective evaluation of the patient's data.

Eve, a patient with chronic hypertension, learns through her S-EHR App (or via a discussion with her doctor) that the Regional University Hospital is conducting a study called "Side effects from hypertensive medication study". It uses the InteropEHRate format.

Using the S-EHR App, Eve explores more information about the research and, in particular, the kind of data requested for the research. As someone who is generally altruistic, Eve accepts the invitation to participate in the study and she signs the consent form on her smartphone.

The research protocol requires sharing the health data of her previous five years and for the next two years, restricting their use only to that specific research protocol. Eve is asked to fill out a questionnaire on self-reported side effects from antihypertensive medications.

A few months later, Eve complains of nausea probably related to the intake of the antihypertensive medications. Eva opens her S-EHR App and accesses the questionnaire of the research protocol, filling the questionnaire with the symptom. The questionnaire is sent to the university hospital conducting the research.

Eve can withdraw her participation in the research at any time. In the case of withdrawing, the event is anonymously notified to the Research Centre of the University Hospital.

Last but not least, the COVID-19 pandemic in 2020-21 has often required innovative solutions to be developed through the conduct of rapid clinical trials and has led to the promotion of decentralised clinical trials and data donation initiatives.

The InteropEHRate vision for collecting data for research is to enable citizens to share health data with research centres without cloud storage.

In a nutshell, InteropEHRate has several key features that benefit citizens, healthcare professionals, and researchers.

Key features of the citizen-centric approach of InteropEHRate

For citizens:

- Online and offline access to health data.
- High degree of privacy and control.
- Higher health awareness.

For healthcare professionals:

- Online and offline access to health data.
- Broader health profile of patients.
- Access to real-world data.
- Access to real-time data.

For researchers:

- Access to more data more easily.
- Combination of research data and real-world data.
- Access to real-time data.

3. What technical solutions is InteropEHRate developing?

In support of secure cross-border exchange of health data, InteropEHRate is developing three technical solutions: open-source communication protocols and application programming interfaces (APIs), a set of constraints for mobile applications and cloud services, and a reference implementation (i.e., proof-of-concept software).

Device-to-Device (D2D), Remote-to-Device (R2D) and Research Data Sharing (RDS) open protocols structure data according to specific profiles, ensuring a common interpretation of health data and a trustful translation into different languages. These protocols are based on the HL7 FHIR[5] standard and exploit the electronic Identification, Authentication and trust Services (eIDAS) network[6] for the cross-border digital authentication of European citizens. Common FHIR profiles support reliable translation into different natural languages.

Table 1. InteropEHRate open protocols

Open protocols	Description
Device-to-Device (D2D)	Secure information technology (IT) communication protocol and remote APIs for exchanging health data between two nearby devices without an internet connection. One runs a S-EHR App and the other operates an HCP App.
Remote-to-Device (R2D)	A family of technical protocols.
R2D Access	Secure IT communication protocol and remote API used by a S-EHR App for receiving health data from a healthcare organisation via the internet.
R2D Backup	Secure IT communication protocol and remote API for the backup of health data from a S-EHR App on a S-EHR Cloud.
R2D Emergency	Secure IT communication protocol and remote API for the exchange of health data between an HCP App and a S-EHR Cloud during emergency care e.g., in a hospital.
Research Data Sharing (RDS)	Secure IT communication protocol and APIs for publishing and retrieving machine-processable descriptions of research studies and for sending a citizen's consent(s) and health data from S-EHR Apps to a research centre, without any cloud storage of health data.

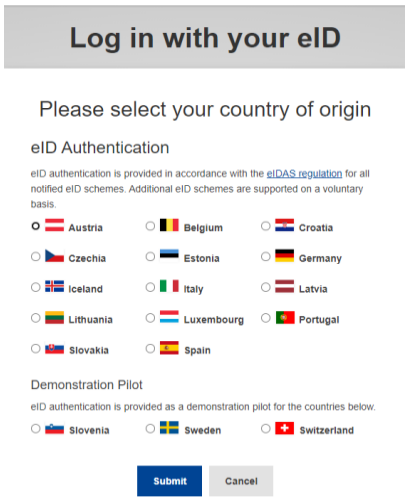
InteropEHRate open specifications offer specific advantages. Citizens and health organisations avoid vendor lock-in and data provenance is digitally traced. Many EU citizens already possess a legally valid electronic identity (eID) issued by national identity providers

[5] HL7 FHIR: https://www.hl7.org/fhir/

[6] eIDAS: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

that conforms to the eIDAS regulation (e.g., itsme in Belgium, SPID in Italy)[7]. Healthcare organisations that comply with InteropEHRate will recognise eIDAS eIDs.

Thanks to these kinds of specifications, EU patients will be able to download their health data from different European healthcare organisations (e.g., hospitals, general practices, laboratories) located in different countries, without the need to manage different accounts or use a variety of apps.



In practice, when citizens ask to download their health data from a healthcare organisation, they will be directed by the S-EHR App to input their strong credentials (eIDAS user and password, 2-factor authentication, smart ID card readers, etc.). Doing this will confirm the patient's identity to the healthcare organisation, which will then authorise the download of the health data. With InteropEHRate, in face-to-face encounters, citizens will be able to exchange their health data with personnel in a healthcare organisation without using the internet. (In this case, citizens may also be identified by using traditional identification systems such as an ID card.)

Besides open protocols, InteropEHRate defines **S-EHR conformance levels**, a set of constraints for mobile applications and facultative cloud services called S-EHR Cloud. It also develops the **InteropEHRate Framework**, a reference implementation of the open specifications that will be piloted with patients in four hospitals.

In some of the use cases that InteropEHRate is developing health data can be exchanged without the internet and without cloud storage. When required, this exchange can be done by 'hiding' a patient's personal health information from the cloud providers.

To support different use scenarios, these technical protocols can be exploited either independently or together. Software providers may deploy different implementations of the protocols, applications, and services defined by the InteropEHRate open specifications. Conformance to the open specifications guarantee interoperability among protocols' implementations of different vendors.

4. What is InteropEHRate leaving for the market to develop?

InteropEHRate offers essential building blocks for a wide range of eHealth market players working with EHRs. It will not, however, deliver a complete solution for a citizen-centric data sharing approach.

InteropEHRate is of interest to both the demand side and the supply of the eHealth market. On the demand side, the InteropEHRate solutions can serve a range of organisations, including national, regional, and local health authorities, healthcare organisations, and healthcare providers. On the supply side, they will bring value to major EHR vendors, mobile health developers, and digital health start-ups.

[7] For a full list of trust service providers visit https://webgate.ec.europa.eu/tl-browser/#/

The interoperability and the complementarity of these solutions can secure InteropEHRate adoption either in new eHealth systems or integration in existing infrastructures. On the one hand, countries that have not yet decided on a specific EHR format, could adopt InteropEHRate FHIR profiles and thereby ensure that their citizens benefit from data protection and portability. On the other hand, Member States which have an EHR format in place can extend its functionalities with minimum effort or expenditure.

Healthcare organisations can benefit from InteropEHRate results in two ways: by complementing their national offerings, and through leapfrogging.

InteropEHRate may offer data sharing features that are not provided to the healthcare organisations by the national/regional central systems (this may be especially the case when the national direction is unclear, or the national infrastructure is either non-exclusive or not yet completely deployed). Through the InteropEHRate Framework, the healthcare organisations can integrate InteropEHRate solutions into their existing health information systems.

Healthcare organisations with less advanced Electronic Medical Records (EMRs) and less health information exchange among providers may benefit even more from InteropEHRate. Hospitals with EMRs that are classified as being up to EMRAM[8] stage 4 could leapfrog ahead by adopting InteropEHRate FHIR profiles. Continuity of care across types, settings, and populations, up to CCMM[9] stage 4, could be expanded nationally and cross-borders through InteropEHRate Health Services and Tools.

On the supply side, EHR vendors have strong incentives to adopt InteropEHRate results in both the short and long run. Early adopters of InteropEHRate solutions could win a competitive advantage. In a highly fragmented EHR market characterised by lack of interoperability, these vendors would in fact offer higher interoperability. In the long term, InteropEHRate results adoption would enable EHR vendors to focus on adding value to their solutions for healthcare providers and citizens through offering them new features and functionalities.

App developers can gain a significant advantage by highlighting data access and data sharing features to their end-users. A well-designed, fully featured mobile health application is the vehicle for end-users like citizens to benefit from the functionalities provided by InteropEHRate.

Start-ups and small and medium-sized enterprises (SMEs) could also benefit from the InteropEHRate Framework in two ways, as a risk mitigation factor and as a catalyst to shortening time-to-market – a key metric for their sustainability.

[8] EMRAM – Electronic Medical Record Adoption Model. https://www.himssanalytics.org/emram

[9] CCMM – Continuity of Care Maturity Model. https://www.himssanalytics.org/ccmm

5. How are security, privacy, user experiences, and standardisation addressed?

InteropEHRate focuses on five areas of importance: security, privacy, user experience, standardisation, and semantic interoperability. Each is explored systemically here. The quality of its data conversion techniques especially has been recognised publicly by the European Commission.

5.1 Security

Insecure communication and data storage are among the ten major risks faced by mobile apps users globally.[10] With the rapid increase in the number of EHRs, the need for access control and health data encryption in mobile applications has become more prevalent in order to protect sensitive clinical information.

InteropEHRate's security approach tackles security protocols, data confidentiality and data integrity, and two variants of privacy preservation.

In this data encryption context, InteropEHRate security protocols specify security schemes exploited by all InteropEHRate protocols. These schemes are intended to satisfy the security goals and the technical measures needed for enhanced security-by-design and privacy-by-default. They follow the current standards defined by ENISA's Minimum Security Measures for Operators of Essentials Services[11] and the requirements of the healthcare domain.[12]

The data security and user privacy protocols leveraged by InteropEHRate are based on the use of Public Key Infrastructures (PKIs) for credential management and privacy-friendly authentication services. The common denominator in these kinds of architectures is the existence of trusted (centralised) infrastructure entities for the support of services, such as authenticated registration, pseudonym provision, and revocation, for either the system users or the S-EHR App. InteropEHRate security protocols are coupled with the use of standardised infrastructures that come from a Certificate Authority (CA) or have emerged from eIDAS regulation, and other EU services like the Connecting Europe Facility (CEF) eID.[13,14]

---

[10] Basatwar G. OWASP Mobile Top 10: A Comprehensive Guide For Mobile Developers To Counter Risks. Appsealing News. 23 January 2020. https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/

[11] ENISA. Minimum Security Measures for Operators of Essentials Services. 2020. https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

[12] InteropEHRate Consortium. D2.2. User Requirements for cross-border HR integration – V2. April 2020. https://www.interopehrate.eu/wp-content/uploads/2020/10/InteropEHRate-D2.2-User-Requirements-for-cross-border-HR-integration-v2.pdf

[13] European Commission. Person Identification and Authentication – Key to eHealth and eGovernment Service. 16 November 2019. https://ec.europa.eu/digital-single-market/en/news/person-identification-and-authentication-%E2%80%93-key-ehealth-and-egovernment-services

[14] European Commission. Trust Services and eID (eIDAS regulation). 2017. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Data confidentiality and integrity – both for data storage and health data exchange – are provided through advanced encryption mechanisms based on the use of well-established and state-of-the-art solutions and Key Derivation Functions (KDFs).

5.2 Privacy and data protection

Given the sensitive nature of health data, the processing of such data poses a risk to the rights and freedoms of users. Ensuring the security of data processing is therefore a crucial concern and an important legal requirement under Article 32 of the GDPR. To achieve security of data processing, InteropEHRate implements a robust security protocol that incorporates the use of pseudonymisation, identity management, advanced encryption, and other mechanisms that ensure security and privacy-by-design.

In terms of privacy preservation, two variants are used. One variant is standardised with state-of-the-art cryptographic primitives for enriching privacy; the other variant aligns with the currently adopted mechanisms used by the end-users. This approach has two benefits: it enhances the applicability of the InteropEHRate Framework, while it also enables the project to perform a detailed investigation of new privacy-preserving enablers that can extend the state-of-the-art and potentially be considered as a new standard.

To ensure GDPR compliance, InteropEHRate protocols include a legal perspective and adopt a privacy-by-default approach in the technological design process, incorporating data protection principles through the treatment of personal data and security processing.

InteropEHRate adopts a user-centric consent management strategy to ensure GDPR compliance. When interacting with InteropEHRate applications, users are asked at different stages to provide their consent to the processing of their data. Consent is required at least at four stages of use of InteropeEHRate, including when installing the applications, exchanging data, storing data in the cloud, and participating in research data sharing. In each instance, the user will be asked to consent actively by ticking a box and will be given the opportunity to refuse or withdraw his or her consent at any time. This gives the user control over data processing and thus ensure that InteropEHRate adheres to the GDPR principles of lawfulness, fairness, and transparency.[15]

In order to fulfil the obligation to inform the user at the highest attainable standard and with transparency, InteropEHRate provides a comprehensive privacy policy to the data subject in the sense of the term used in the GDPR. This legal statement specifies what a controller does with personal data collected from users, along with how the data is processed and for what purposes. Since it is important that every InteropEHRate user fully understands the processing of his/her data, InteropEHRate's privacy policy can be accessed by a user at any time; it is also layered and uses clear and plain language.

5.3 User experience

Good user experiences of the use of InteropEHRate solutions are vital. Citizens and healthcare professionals are the end-users of data sharing applications enabled by InteropEHRate solutions. A positive user experience, when using all the different functionalities of S-EHR and

[15] Outlined in GDPR, Art. 5(1)(a)

HCP Apps, is crucial for users' adoption of the InteropEHRate solutions, considering elements of privacy, identification, consent management, and translation services.

Citizens value a clear identification of the healthcare actors involved in the InteropEHRate communication process. They are also concerned by the privacy and security related to the use of quick response (QR) codes.

A co-design process with end-users, based on real use cases illustrating the data exchange procedure, ensures usability aspects like transparency, clarity, and security that can influence positively the trust of patients. Easy logging, data labelling, screen titling and explanatory notes are used to facilitate citizens' use and understanding. Data traceability options are taken over by health data management features. Balancing simplified and easy-to-use interfaces that offer multiple choice options is a challenge addressed in InteropEHRate's co-design process. An example is how to describe the type of personal data that will be shared or automatically exchanged and saved in the S-EHR.

Likewise, healthcare professionals need to trust that data sharing is exchanged securely and no interception or corruption of data can occur during any device-to-device connection. They may also be concerned about the accuracy and quality of information displayed on screen during the transmission, how easy it is to spot the latest data incorporated, and the identification of data sources.

5.4 Standardisation

Data exchange between different health information systems requires both technical and semantic interoperability. To enable cross-border data sharing among health providers, patients, and researchers, InteropEHRate defines interoperability profiles and protocols that are subject to international standards to improve interoperability of different applications for specific use cases. InteropEHRate engages with the most important and suitable European and international standardisation organisations: HL7 Europe[16], HL7 International[17], and IHE Europe[18].

Interoperability Profiles are used with the InteropEHRate communication protocols to share standardised information between the different actors, thereby ensuring both syntactic and semantic interoperability. They adopt existing domain-agnostic data models and HL7 FHIR profiles for a flexible support of health data exchange of different domains, and they define a set of core data and profiles that enable communication and transactions. Existing HL7 FHIR-based Implementation Guides like the International Patient Summary (IPS)[19] cover identified and derived data requirements. The profiles defined in these Implementation Guides are used and adapted to project specific requirements.

Data requirements that cannot be met by existing implementation guides are included in new guides developed by InteropEHRate itself. For instance, data exchanged through the RDS protocol include aspects such as an unstructured and human readable definition of the clinical

[16] HL7 Europe: http://www.hl7.eu/

[17] HL7 International: https://www.hl7.org/

[18] IHE Europe: https://www.ihe-europe.net/

[19] International Patient Summary: https://international-patient-summary.net/

research protocol, and structured and machine-processable definitions of the research protocol, data security and access control, and data set results of any research data query.

InteropEHRate has focused on the most efficient options for standardising a subset of the project results with the specified resources. As a result, InteropEHRate has developed an objective assessment strategy complete with defined and weighted decision criteria such as the results' uniqueness, exploitability, and maturity level.

Two benefits result. According to the assessment results, the standardisation of the D2D protocol through the specification of an IHE Profile for the D2D exchange of medical data is the most beneficial contribution option. For the research scenario, the specification of a new HL7 FHIR Implementation Guide is a second beneficial contribution option.

The use of international standards is a necessary, but not a sufficient, condition for efficient long-term interoperability. At least two more actions are needed to guarantee interoperability. A scalable adaptation to the heterogeneous and constantly evolving environment of the European healthcare ecosystem requires agile data modelling and data transformation practices. Furthermore, a large proportion of health data is expressed in unstructured form, such as shorter or longer pieces of text, which escape standardisation attempts and needs to be transformed into structured formats to ensure its interoperable processing.

5.5 Semantic interoperability

Semantic interoperability includes any conversion, translation, or other transformation of data that is made for the purpose of preserving the meaning underlying data. Changing data formats such as language, coding systems, or data structures is a major scientific and technological challenge that has not yet been entirely solved in practice. To address semantic interoperability, InteropEHRate provides a pragmatic solution that is composed of multiple technological and process innovations.

The need for semantic data interoperability underlies all the InteropEHRate scenarios. For example, in a practical use scenario, when a patient transfers his/her health record from one country to another, it is assumed that the clinicians and the IT systems in the hospital(s) in the target country will be able to understand the data and work with it. Likewise, in the research scenario, it is assumed that structured health data can be automatically queried and retrieved from citizens' mobile devices. This querying and retrieval is independent of the variety of data representations originally used to produce the data in the hospitals, regions, and countries participating in any given research study.

InteropEHRate combines innovative multilingual knowledge extraction methods with an agile and interactive methodology for defining the rules that govern data transformations. While the processes can be automated, they are also fully supervised by human experts who have a complete understanding of the data transformations taking place and who can intervene quickly to improve the system or cause it to evolve.

InteropEHRate's automated data conversion and translation operations are traced by the system, which can tell practitioners explicitly if a translation or conversion has been undertaken

on a given data value. The interactive data transformation tools proposed by InteropEHRate were highlighted in 2020 by the Innovation Radar of the European Commission.[20]

6. What are InteropEHRate's main outcomes?

The two chief outcomes of InteropEHRate are open specifications that classify new kinds of applications and define new open interoperability protocols, and the overall InteropEHRate framework.

6.1 InteropEHRate open specifications

InteropEHRate's open specifications include four protocols and profiles: D2D Protocol, R2D Protocols, RDS Protocol, and FHIR profiles for EHR interoperability.

6.1.1 D2D Protocol

The Device-to-Device (D2D) Protocol is a secure communication protocol for exchanging messages and healthcare-related data between two nearby devices, without using an internet connection, therefore, no Internet Protocol (IP)[21]. Transmission occurs by adopting short range communication, in particular Bluetooth v4.0 technology.

InteropEHRate S-EHR App users (i.e., citizens) and HCP App users (i.e., healthcare professionals practicing in healthcare organisations or other institutions) exchange healthcare-related data.

The data exchanged in the InteropEHRate applications refers both to structured and unstructured data and can be directly transmitted on top of Bluetooth, extending its usage for the permission of the exchange of HL7 FHIR structured data. The D2D protocol is generalisable and can be used with most of the main operating systems (e.g., Windows, MacOS, Linux, Android, iOS). It is specified and implemented as a non-vendor specific solution.

All citizens owning a smart device can benefit from the D2D protocol to connect with healthcare providers. A specific S-EHR App and HCP App must be installed on the devices of each party. There are, however, two distinct needs. Citizens must have a smart device with either an Android or iOS operating system supporting Bluetooth v4.0 technology. The healthcare provider must have a desktop or a smart device with a Windows or a Mac operating system, also supporting Bluetooth v4.0 technology.

[20] European Commission. Horizon 2020 Innovation Radar. Knowledge Management Tools and Data Mapping Tool enabling healthcare providers legacy systems to securely exchange health data with secure patients EHR. 2020. https://www.innoradar.eu/innovation/37052

[21] Protocols used by the Internet Protocol such as the transmission control protocol (TCP) and the user datagram protocol (UDP).

6.1.2 R2D Protocols

Remote-to-Device (R2D) Protocols are a family of communication protocols that exploit the HTTP and HL7 FHIR standards for the exchange of health data, in addition when the communicating parties are located in different EU countries.

The R2D family is composed of three protocols:

- R2D Access: used by citizens to import health data securely from a remote health data repository to the citizen's smartphone.
- R2D Backup: used by citizens to do an automatic backup of the health data available in the citizen's smartphone on the citizen's preferred S-EHR cloud service and restore the data when needed.
- R2D Emergency: used by healthcare providers to download data from a S-EHR Cloud and enrich a patient's health data during an emergency.

The **R2D Access protocol** defines a web API and a set of rules based on well-established standards for downloading health data from any health data provider to a S-EHR App controlled by an EU citizen. The health data provider may be either a specific clinical care provider (e.g., a hospital or a general practitioner) or a national or regional healthcare system. R2D Access is intended to standardise the citizen's access to very varied sources of personal health data which are located even in different EU countries.

The R2D Access protocol enables:

- European citizens to download their health data from different European health data providers by using just a single eIDAS-based digital identity and their preferred S-EHR App. Citizens can do this without being locked into a single app provider, and they can download entire documents or just portions of them.
- Healthcare providers to adopt a common protocol to give their patients access to the health data produced in their facilities.
- Software companies to develop competitive mHealth apps based on a common protocol for communication with various health data providers.

From a technical point of view, the R2D Access protocol is a read-only protocol based on HL7 FHIR, that uses the eIDAS network as the identity provider for the citizens. The data model used by the protocol is based on a set of FHIR Implementation Guides defined by the InteropEHRate consortium. Operations of the protocol are based on FHIR RESTful APIs[22] with the addition of appropriate restrictions and constraints.

[22] FHIR RESTful API: https://www.hl7.org/fhir/http.html

InteropEHRate's next version of R2D Access will comply with the IHE MHD[23] profile for access to clinical documents and will support the DICOM WADO-RS API[24] for access to medical images.

The **R2D Backup protocol** defines the set of operations used for enabling a standard backup of encrypted health data between a mobile application (S-EHR App) acting on behalf of a patient and a storage cloud (S-EHR Cloud). In more detail, via the R2D Backup protocol, citizens may upload their encrypted health data to their preferred S-EHR Cloud provider for backup purposes. Citizens may also download this data on their S-EHR App.

The R2D-Backup protocol enables:

- European citizens to back up their health data in any supporting S-EHR Cloud in a secure way from several different European health data providers through their preferred S-EHR App.
- Software companies to develop S-EHR Apps based on a common protocol enabling communication with a variety of storage cloud providers.
- Software companies to develop health-related storage clouds based on a common protocol enabling the communication with a variety of S-EHR App providers.

The **R2D Emergency protocol** defines the set of operations used for enabling in a standard way two actions in emergency situations for a citizen to (i) offer access to the healthcare information that is backed up on his/her preferred S-EHR Cloud service, and (ii) access of encrypted health data stored in a given S-EHR Cloud service to an HCP App (i.e., a healthcare institution's system) operated by a healthcare professional.

In more detail, for emergency purposes via the R2D Emergency protocol, an authenticated healthcare provider may access a citizen's encrypted health data stored on the citizen's preferred S-EHR Cloud provider. In addition, the healthcare provider may also upload new content on this S-EHR Cloud. With the citizen's approval, the uploaded content will be added to the already backed-up healthcare information.

The R2D-Emergency protocol enables:

- European citizens to grant access to health data to authorised healthcare professionals in emergency situations.
- European healthcare professionals to access the health record(s) of a citizen in need through their HCP Apps.
- Software companies to develop HCP Apps based on a common protocol enabling the communication with a variety of cloud storage providers.
- Software companies to develop health-related cloud storage based on a common protocol enabling the communication with a diversity of HCP Apps.

[23] IHE MHD profile: https://wiki.ihe.net/index.php/Mobile_access_to_Health_Documents_(MHD)

[24] DICOM WADO-RS API: https://www.dicomstandard.org/dicomweb/retrieve-wado-rs-and-wado-uri

6.1.3 RDS Protocol

The Research Data Sharing (RDS) Protocol introduces three novel mechanisms.

The first novel mechanism is collecting personal health data for the purposes of medical research. By collecting health data directly from citizens' personal mobile devices, InteropEHRate puts citizens in full control over when, how, and for which research studies their data will be used. Informed consent, and the strict authorisation of the use of donated data for the selected research, is capable of informing citizens about the nature of the data to be shared down to the level of individual data elements.

A second innovation of the protocol is that it allows citizens to participate remotely in prospective research studies, providing information through their mobile devices. Thus, the citizens are not required to pay regular visits to a research centre.

Thirdly, the protocol innovates through its reliance on the cross-border research infrastructure developed by InteropEHRate: this allows health records produced in any European country to be interoperable for the purposes of research, and thus shareable cross-border.

The RDS Protocol is able to tackle the serious security, privacy, and interoperability challenges related to citizen-driven data sharing thanks to its reliance on three mechanisms: market-ready security; pseudo-anonymisation; and cross-border data integration.

Adopters of the protocol – such as public or private IT solution providers for medical research – should be ready to employ such mechanisms, either by exploiting reference implementations and demonstrators provided by the InteropEHRate project or by taking inspiration from them.

6.1.4 FHIR profiles for EHR interoperability

The HL7 FHIR profiles for EHR interoperability are used with the newly specified communication protocols to share and exchange information between the different actors in a standardised way, thus ensuring syntactic and semantic interoperability of information. These profiles adopt existing domain-agnostic data models and HL7 FHIR profiles for a flexible support of Health Information Exchange of different domains and define profiles that enable the communication and transactions among software systems as defined by the protocols.

The total number of all the FHIR profiles for EHR interoperability constitute the data model of a generic S-EHR. FHIR profiles and resources defined in existing Implementation Guides (e.g., the International Patient Summary) are used and adapted to project-specific requirements, where necessary.

Data requirements that cannot be met by existing Implementation Guides are specified as new HL7 FHIR resources, profiles (e.g., Research Definition Document) or project-specific implementation guides. To this end, the FHIR profiles for EHR interoperability follow a specific standardisation strategy: the strategy is aligned with HL7 FHIR profiles or HL7 FHIR Implementation Guides because InteropEHRate personnel contribute to existing working groups or write a new implementation guide.

For all these protocols, a reference implementation is provided. In the case of the S-EHR App, the Andaman7 publicly accessible PHR can be downloaded from either the Apple or Google stores. It demonstrates the use of InteropEHRate protocols in a real-life, industry-accepted system. On the healthcare provider side, a reference HCP App can also be made available by the consortium.

6.2 InteropEHRate Framework

The InteropEHRate project provides its users with a set of services and applications that can be used to take advantage of the InteropEHRate protocols. The integration of these services and applications form the InteropEHRate Framework. All five of them are described in the following table.

Table 2. InteropEHRate Framework

Services and applications	Description
InteropEHRate Health Services (IHS)	Set of libraries and services that can be exploited by any healthcare organisation. The IHS includes the implementation of the protocols defined by the InteropEHRate project and allows any HCP App to exchange health data safely between citizens and healthcare providers.
InteropEHRate Research Services (IRS)	Set of libraries and services that can be exploited by any certified research centre. Through the IRS, research centres may request citizens for their health data for research purposes, and if necessary, reach them back for further information.
S-EHR Mobile Application	It can be used to visualise and store safely health data that are either created by citizens or provided by healthcare providers. A S-EHR Mobile Application works as a hub that can be also used for the exchange of healthcare information in a variety of ways. Examples include between the citizen and a healthcare provider by exploiting the D2D protocol or the R2D Emergency protocol or with a researcher using the RDS protocol. A citizen can even back up their health data on their preferred S-EHR Cloud provider through the R2D Backup protocol.
S-EHR Cloud	Service architecture that gives the citizen the ability to store their personal health data that are collected through the S-EHR App on the cloud for back-up purposes. A S-EHR Cloud service is managed by the citizen himself or herself. As a result, the S-EHR Cloud provider cannot have access to the data stored in the citizen's back-up. The citizen may, however, grant access to the S-EHR Cloud to authorised healthcare providers in emergency situations.
HCP Web Application	Application used by healthcare providers to access, visualise, and write notes on the health data of their patients. To collect this data, the HCP Web Application uses the IHS (libraries and services) to transfer data from S-EHR Mobile Applications or S-EHR Clouds.

7. Key messages

A citizen-centric approach to data sharing that is **complementary to the current healthcare-centred model** is already possible today. As a result, it can enhance both healthcare and research. Citizen control and empowerment requires advanced digital health literacy. Citizen-mediated health data exchange requires innovative solutions to increase access and control of health data and overcome existing technical barriers. This is InteropEHRate's main purpose.

InteropEHRate aims to unleash health data from local silos and offer more power to citizens in managing their own health data across different health providers and countries, facilitating care and accelerating health research as a result. Several different sets of players will benefit. InteropEHRate's solutions are based on a number of new technical developments.

Benefits for a range of different players:

- Citizens can benefit from better and innovative health services fuelled by health research.
- Healthcare professionals can benefit from InteropEHRate solutions to access broader patients' health profiles.
- Health researchers can access more data more easily and conduct decentralised clinical trials combining research and real-world data in cooperation with patients.
- Demand and supply side actors of the eHealth market can benefit from InteropEHRate essential building blocks to facilitate health data access, portability, and protection for citizens.
- On the demand side, health authorities and healthcare organisations can improve continuity of care integrating open protocols to existing infrastructures.
- On the supply side, EHR vendors, mobile health developers and digital health start-ups can win competitive advantage, offer higher interoperability, and add value to their solutions offering user new features and functionalities.

Technical developments

InteropEHRate is developing a number of **technical methods for enhancing citizen-centric approaches to data-sharing**: open-source communications protocols and APIs, S-EHR conformance levels, and a reference implementation for citizens' S-EHR Apps and healthcare providers applications. These solutions enable technically the citizen-centric approach in three different scenarios: healthcare visits abroad, emergencies, and research data sharing.

Key principles for these technical developments are **security, privacy, user experience and standardisation**. Security-by-design and privacy-by-default approaches are followed in all InteropEHRate protocols based on Certificate Authorities and European regulations – eIDAS and GDPR. A co-design process with citizens and health professionals ensures good user experiences of privacy, identification, consent management and translation services. Technical and semantic interoperability is reassured by the adoption of HL7 FHIR profiles and implementation guides, and knowledge management tools.

Ultimately, to develop citizen-oriented services, InteropEHRate relies on the generation of **secure health data spaces** that support the creation of health innovation and research ecosystems.

References

Basatwar G. OWASP Mobile Top 10: A Comprehensive Guide For Mobile Developers To Counter Risks. Appsealing News. 23 January 2020. https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/

DigitalHealthEurope. Citizen-controlled health data sharing governance. October 2020. https://digitalhealtheurope.eu/wp-content/uploads/2020/11/Consultation-Paper-Citizen-controlled-health-data-sharing-governance.pdf

ENISA. Minimum Security Measures for Operators of Essentials Services. 2020. https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

European Commission. Horizon 2020 Innovation Radar. Knowledge Management Tools and Data Mapping Tool enabling healthcare providers legacy systems to securely exchange health data with secure patients EHR. 2020. https://www.innoradar.eu/innovation/37052

European Commission. Person Identification and Authentication – Key to eHealth and eGovernment Service. 16 November 2019. https://ec.europa.eu/digital-single-market/en/news/person-identification-and-authentication-%E2%80%93-key-ehealth-and-egovernment-services

European Commission. Trust Services and eID (eIDAS regulation). 2017. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

InteropEHRate Consortium. D2.2. User Requirements for cross-border HR integration – V2. April 2020. https://www.interopehrate.eu/wp-content/uploads/2020/10/InteropEHRate-D2.2-User-Requirements-for-cross-border-HR-integration-v2.pdf

Basatwar G. OWASP Mobile Top 10: A Comprehensive Guide For Mobile Developers To Counter Risks. Appsealing News. 23 January 2020. https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/

Web: www.interopEHRate.eu

Email: info@interopehrate.eu