pHealth 2022
B. Blobel et al. (Eds.)

doi:10.3233/SHTI220973

Electronic Health Records at People's Hands Across Europe: The InteropEHRate Protocols

Athanasios KIOURTIS[a,1], Argyro MAVROGIORGOU[a], Konstantinos MAVROGIORGOS[a], Dimosthenis KYRIAZIS[a], Alessio GRAZIANI[b], Chrysostomos SYMVOULIDIS[a,c], Gabor BELLA[d], Simone BOCCA[d], Francesco TORELLI[b]
[a] *Department of Digital Systems, University of Piraeus, Piraeus, Greece*
[b] *Engineering Ingegneria Informatica, SpA - R&D laboratory, Rome, Italy*
[c] *BYTE S.A., Athens, Greece*
[d] *University of Trento, Trento, Italy*

Abstract. Sharing of personal health data could facilitate and enhance the quality of care and the conduction of further research studies. However, these data are still underutilized due to legal, technical, and interoperability challenges, whereas the data subjects are not able to manage, interact, and decide on what to share, with whom, and for what purposes. This barrier obstacles continuity of care across in the European Union (EU), and neither healthcare providers nor data researchers nor the citizens are benefiting through efficient healthcare treatment and research. Despite several national-level EU studies and research activities, cross-border health data exchange and sharing is still a challenging task, which is addressed only under specific cases and scenarios. This manuscript presents the InteropEHRate research project along with its key innovations, aiming to offer Electronic Health Records (EHRs) at peoples' hands across the EU, via the exploitation of three (3) different protocol families, namely the Device-to-Device (D2D), Remote-to-Device (R2D), and Research Data Sharing (RDS) protocols. These protocols facilitate efficient, secure, privacy preserving, and General Data Protection Regulation (GDPR) compliant health data sharing across the EU, covering different real-world use cases.

Keywords. Health Information Exchange, Research Data Sharing, D2D protocol, R2D protocol, RDS protocol, InteropEHRate

1. Introduction

Personal health data are not currently utilized at their widest potential, for research and healthcare in the European Union (EU). There exist several challenges, such as legal or technical, with the major ones dealing with the way that these data could be unleashed [1]. Despite the evolution of research technologies, EU citizens still have limitations in accessing and controlling the health data they are producing, especially in cases when they must travel in different EU countries. Citizens' right to obtain an electronic copy of their data, established by Art. 15 of the General Data Protection Regulation (GDPR) [2], is not always implemented. Healthcare digitization in EU is progressing rapidly, however,

[1] Corresponding Author, Athanasios Kiourtis, 80, M. Karaoli & A. Dimitriou St., 18534 Piraeus, Greece; E-mail: kiourtis@unipi.gr.

personal health data can be found split across different healthcare providers and siloed in different data environments, shrinking their overall ability to lead healthcare research and innovation activities. There also exist barriers related with the different semantics. Hence, it is not always feasible for EU citizens to understand, access and share their clinical history, ensuring efficient healthcare treatment.

Some initiatives in national levels are targeting towards increasing citizens' access and control over their own data, to facilitate health data sharing and exchange. These include the example of MyData [3] that aims to accelerate transformation for ethical and human-centric data sharing and use, as well as Carequality [4] that provides a national-level interoperability framework to enable data exchange among health data sharing networks. With Cloud fax services [5] digital documents and reports can be efficiently routed into folders and organized in a larger document solution, while KONFIDO [6] aims towards secure cross-border health data exchange. However, these solutions are tailored to work under specific national-level cases, supporting a short list of real-world use cases. At the EU level, the paradigm of Health Information Exchange (HIE) follows an approach being healthcare centered. In detail, for national-level health data exchange, patients' health data are maintained and controlled by healthcare providers through the Electronic Health Records (EHRs) paradigm. The latter are centrally connected to EHRs being regional or national, providing the ability to citizens themselves, as well as to external research centers and healthcare organizations to access these data. To achieve this, the HIE is controlled through connected entities' networks or central EHRs. On the other hand, for achieving health data exchange in the cross-border context in the EU, this is enabled by the MyHealth@EU [7] services, for exchanging ePrescriptions and Patient Summaries utilizing the analogous services, via eHealth National Contact Points (NCPs).

However, these solutions have limitations into data sharing with citizens. Specific rules are missing in the form of protocols as data sharing means, compliant with data governance and protection regulations, to provide the citizens the ability to receive a copy of their own data and control them. In this manuscript, the InteropEHRate [8] project and its main results are presented, for releasing locally siloed health data and providing citizens' control into managing their personal health data among multiple countries and healthcare providers, through mature data exchange protocols.

The remaining paper has the following structure. Section 2 provides the different InteropEHRate protocols that have been specified for health data exchange and sharing. Section 3 includes a description of the evaluation scenarios on top of which these protocols are exploited, while Section 4 includes a discussion of the security and privacy challenges, as well as the overall stakeholders and offerings, concluding to our next steps.

2. InteropEHRate Protocols & Methods

The solutions of the InteropEHRate protocols adopt a citizen-centric approach, complementary to the healthcare-centered one, giving the ability to citizens to use, share, and manage their health data, utilizing their mobile devices. This is facilitated through the Smart Electronic Health Records (S-EHR) mobile application, which gives the capability to its users to locally manage and store health data in smartphones. Hence, citizens can control and share their data with stakeholders (i.e., research centers, healthcare providers), fully compliant with their own requirements and the GDPR.

InteropEHRate specifies five (5) different open protocols (Figure 1) that give the ability to S-EHR application owners to securely share health data, controlling what to share, when to share, as well as with whom to share. The protocols are organized in three (3) families called *Device-to-Device (D2D)*, *Remote-to-Device (R2D)* and *Research Data Sharing (RDS)* protocols, being structured upon the Health Level 7 (HL7) Fast Healthcare Interoperability (FHIR) standard [9], utilizing the electronic Identification, Authentication and Trust Services (eIDAS) [10] network for authentication purposes. Each protocol can be used alone or in synergy with the others, therefore the developers of S-EHR applications can choose what to offer to the users and the users are free to choose which ones to use. All the protocols exploit specific HL7 FHIR interoperability profiles to structure the managed data, and use local-language and terminology translation services, for a common health data interpretation. All the protocols, except for the R2D Emergency (part of R2D family), are peer-to-peer, offering data exchange between the citizen and another party, without intermediatory parties.

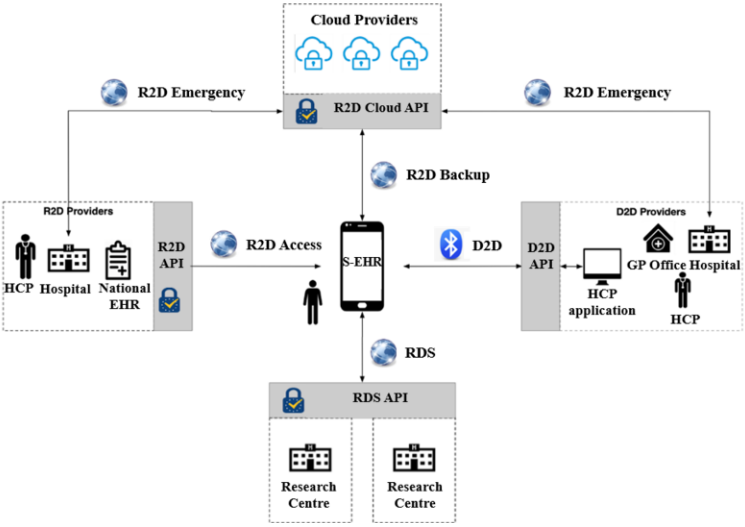

Figure 1. The InteropEHRate protocols.

2.1. Device-to-Device (D2D) Protocol

The D2D Protocol [11] specifies the means, the messages, and the health-related data to be exchanged between two devices in a close-range distance, avoiding the usage of internet connection. Data transfer takes places through the Bluetooth v4.0 short range distance communication protocol, where the citizens owning a S-EHR application can communicate and exchange data with Healthcare Practitioners (HCP) owning an HCP application (i.e., a secure for the HCPs, for instance an EHR frontend, also supporting the D2D protocol). Exchanged data may include both unstructured and structured data that can be transferred through Bluetooth, extending it for supporting HL7 FHIR data. The D2D protocol has high genericity, specified as a non-vendor specific solution.

2.2. Remote-to-Device (R2D) Protocols

The R2D Protocols is a family of three (3) communication protocols, exploiting the Hyper Text Transfer Protocol (HTTP) and the HL7 FHIR standard for health data exchange across interacting parties from different EU locations. These protocols are the:

- *R2D Access Protocol* [11]: It specifies the way for EU citizens to securely download health data from a remote repository of health data to their S-EHR application. It specifies a set of standardized rules for importing health data from any supporting provider, such as a clinical care provider (e.g., general practitioner, hospital) or a regional/national health system. It uses eIDAS so that citizens use the same credentials to download the data from any provider.
- *R2D Backup Protocol* [12]: It specifies the way for EU citizens to automatically backup and manually synchronize their HL7 FHIR encrypted health data that are already stored in their S-EHR application through the R2D Access Protocol, to any cloud storage service [13] and retrieve them on demand. The encryption key is not shared with the Cloud provider, for data subject privacy.
- *R2D Emergency Protocol* [12]: It specifies the way for authorized health providers to retrieve health information from a citizen's cloud storage service and enhance the health data of the patient at the case of an emergency scenario. The citizen can enable access to the health data that is stored (i.e., backed up through the R2D Backup Protocol) on the chosen cloud storage service, and data access can be provided to a qualified HCP with an HCP application, having a special Quick Read (QR) code provided by the data subject.

2.3. Research Data Sharing (RDS) Protocol

The RDS protocol [14] provides the way to citizens to share their health data for research purposes. Citizens are fully controlling and deciding how, when, and for what research studies their HL7 FHIR structured data will be utilized. Data are anonymised on the mobile device of the citizen before sharing them with the specific research study. The RDS protocol also provides the ability to citizens to remotely participate in research studies being prospective, giving the needed data via their S-EHR applications. The RDS protocol can address interoperability, privacy, and security gaps of citizen-driven data sharing, thanks to cross-border data integration and market-ready security paradigms.

3. Planning for Real-World Evaluation

As it has been stated, the current research is part of InteropEHRate, aiming to support patient-centered exchange of health records. The planning is to validate the protocols in countries hospitals' belonging to the project's consortium (e.g., University Hospital Center of Liege, Gabriele Monasterio Tuscany Foundation), providing a proof-of-concept of the protocols, via a specific validation plan [14] regarding the below scenarios.

3.1. Healthcare Visit Abroad Scenario

This scenario exploits the D2D protocol facilitating the case where a patient, while abroad, refers to a local physician, for a visit related to his/her health situation. The patient is admitted to the healthcare facility and communicates with the HCP exploiting the D2D protocol. The patient authorizes the HCP to access, through the HCP application, elements of his/her health data which have been already downloaded locally to the S-EHR application exploiting the R2D Access protocol or previous D2D protocol usages.

3.2. Emergency Access Scenario

This scenario exploits the R2D Backup and R2D Emergency protocols when a patient is abroad and has an emergency. The patient is driven to a hospital's emergency department for treatment. The patient had already backed up his/her data in the preferred cloud storage exploiting the R2D Backup protocol. Following, the R2D Emergency protocol is exploited by an HCP via the HCP application. The HCP verifies the patient's identity and gives access to the cloud storage where the emergency data are stored which may be downloaded to the HCP application. At patient's discharge, a Discharge Report is generated on the HCP application and uploaded to the citizen's cloud. The S-EHR application synchronizes with the cloud, to store this health data on the patient's device.

3.3. Research Data Sharing Scenario

This scenario exploits the RDS protocol to allow patients to share health data to support health research. A research center is conducting a research study for a medical condition's risk factors. It is required the prospective collection of health data for a specific period after a citizen's study enrolment, and the retrospective evaluation of the patient's data for a different (extended) period. Thanks to the RDS protocol, the S-EHR application automatically verifies if the citizen satisfies the enrolment criteria of available research studies, and the citizen may explore more details regarding this research and the types of requested data. The citizen can approve the research study invitation, signing through his/her smartphone a specific consent, authorising the S-EHR application to automatically provide the requested data in an anonymised format.

4. Discussion & Conclusions

With EHRs evolution, it is urgent to deploy techniques enabling health data encryption and access control in mobile applications towards protecting the security and privacy of clinical information. All InteropEHRate protocols are equipped with security mechanisms for achieving data integrity and confidentiality, as well as privacy preservation. These schemes follow the standards defined by ENISA's Minimum Security Measures for Operators of Essentials Services [14] and the healthcare domain needs, while credential management is based upon the use of Public Key Infrastructures (PKIs) [14]. All the protocols are exploiting the concept of standardized infrastructures deriving from a Certificate Authority (CA) [14] or from eIDAS regulations, including other EU services like the CEF eID [14]. Data integrity and confidentiality is achieved via encryption mechanisms based on trending solutions and Key Derivation Functions (KDFs) [15]. To satisfy data security as defined under Art. 32 of the GDPR [16], it is considered the use of advanced encryption, pseudonymization, and identity management. For privacy preservation, there are utilized variants exploiting cryptographic primitives, being aligned with the adopted techniques currently utilized by the final users. For GDPR compliance, the included legal perspective and privacy-by-default approach facilitates personal data treatment. Consent is required at several stages of use, and more specifically when (i) the applications are being installed, (ii) data are being exchanged, (iii) data are being stored in the cloud storage, and (iv) users are taking part in sharing of research data. Such actions provide the end user with control over data processing, ensuring adherence to the GDPR principles of transparency, fairness, and lawfulness.

InteropEHRate unlocks siloed health data and provides the citizens with the ability to manage their health data across different countries and health providers, boosting the efficiency and concept of health. The beneficiaries can be the: (i) Citizens taking advantage of better health services, (ii) Healthcare providers accessing health profiles and determinants from broader citizens, (iii) Health researchers accessing additional data and performing participatory clinical trials, (iv) Supply/demand side stakeholders being facilitated with advanced data protection, portability, and health data access, (v) Healthcare organizations and authorities enhancing care continuity, and (vi) Digital health start-ups, mobile health developers, and EHR vendors, offering features for interoperability and added value. The principles of InteropEHRate are user experience, security, privacy, and standardization, based on CAs and EU regulations. Semantic and technical interoperability is achieved via HL7 FHIR profiles, knowledge management tools and implementation guides. Next steps include the protocols' validation within real-world scenarios, user-experience enhancements, and comparisons with patient-centric commercial services (e.g., digi.me), and products (e.g., HealthVault, Google Health).

Acknowledgment

The research leading to the results presented in this paper has received funding from the EU funded Project InteropEHRate (GA no 826106).

References

[1] Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021;22(2):177-183.

[2] Art. 15 GDPR: Right of access by the data subject, [Online] Available: https://gdpr-info.eu/art-15-gdpr/

[3] MyData, [Online] Available: https://www.mydata.org/

[4] Carequality, [Online] Available: https://www.himss.org/resource-environmental-scan/carequality

[5] Kiourtis A, Mavrogiorgou A, Kyriazis D. A Comparative Study of Bluetooth SPP, PAN and GOEP for Efficient Exchange of Healthcare Data. Emerging Science Journal. 2021;5(3):279-293.

[6] Staffa M, et al. KONFIDO: An OpenNCP-based secure eHealth data exchange system. International ISCIS Security Workshop; 2018. Springer; pp. 11-27.

[7] Bonacina S, et al. Can the European EHR Exchange Format Support Shared Decision Making and Citizen-Driven Health Science? Public Health and Informatics; 2021. IOS Press; pp. 1056-1060.

[8] De Raeve P, et al. Leveraging the trust of nurses to advance a digital agenda in Europe: a critical review of health policy literature. Open Research Europe. 2021;1:26.

[9] Kiourtis A, Mavrogiorgou A, Nifakos S, Kyriazis D. A string similarity evaluation for healthcare ontologies alignment to HL7 FHIR resources. Intelligent Computing-Proceedings of the Computing Conference; 2019. Springer; pp. 956-970.

[10] Cuijpers C. M. K. C, Schroers J. eIDAS as guideline for the development of a pan European eID framework in FutureID. 2014.

[11] Kiourtis A, et al. Improving Health Information Exchange through Wireless Communication Protocols. 16th Int. Conf. on Wireless and Mobile Computing, Networking & Communications; 2020. pp. 32-39.

[12] Symvoulidis C, et al. Facilitating Health Information Exchange in Medical Emergencies. International Conference on e-Health and Bioengineering; 2021. pp. 1-4.

[13] Symvoulidis C, et al. HealthFetch: An Influence-Based, Context-Aware Prefetch Scheme in Citizen-Centered Health Storage Clouds. Future Internet. 2022;14(4):112.

[14] Unleashing personal health data for care and research: [Online] Available: https://www.interopehrate.eu/wp-content/uploads/2021/08/InteropEHRate-White-Paper.pdf

[15] Koh W. W, Chuah C. W. Robust security framework with bit ‐ flipping attack and timing attack for key derivation functions. IET Information Security. 2020;14(5):562-571.

[16] Art. 32 GDPR: Security of processing, [Online] Available: https://gdpr-info.eu/art-32-gdpr/