MEDINFO 2019: Health and Wellbeing e-Networks for All
L. Ohno-Machado and B. Séroussi (Eds.)

doi:10.3233/SHTI190317

Citizen Perspectives on Cross-Border eHealth Data Exchange: A European Survey

Pantelis Natsiavas[a], Christine Kakalou[a], Kostas Votis[b], Dimitrios Tzovaras[b], Vassilis Koutkias[a]

[a] *Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Thessaloniki, Greece*
[b] *Information Technologies Institute, Centre for Research & Technology Hellas, Thermi, Thessaloniki, Greece*

Abstract

Efficient and secure cross-border eHealth data exchange has been recently identified by the European Commission as one of the top-three priorities for the digital transformation of health and care in the European Union. To this end, various organizational, legal, ethical, and technical challenges, related to citizens' privacy and health data security arise. This paper discusses an online survey that was conducted with the participation of European citizens, aiming to identify how they feel about exchanging their health data with healthcare professionals or eHealth service providers and to what extent they are aware of the privacy, legal, security, and technology acceptance issues (e.g. use of biometrics, mobile apps, etc.). The survey rationale, structure, and results are presented, while potential barriers and facilitators regarding cross-border health data exchange and the adoption of eHealth solutions at large are discussed.

Keywords:

Health Information Exchange, Privacy, Computer Security, Surveys and Questionnaires

Introduction

Recent advances in digital health technologies outline a paradigm shift for healthcare delivery [1, 2]. While technologies such as the Internet of Things (IoT), big data analytics, Artificial Intelligence (AI), robotics, the Future Internet offer new opportunities for more effective and personalised healthcare delivery, they also introduce significant challenges that have to be addressed [3]. In particular, due to the increased connectivity and the underlying technical complexity of these novel technological artifacts, complex cybersecurity risks have to be tackled. To this end, cybersecurity threats could prove a significant barrier for their adoption in the healthcare sector. These concerns are further reinforced by various alarming reports purporting approximately 90% of healthcare institutions as victims of security breaches and cyberattacks [4]. Since 2010, cyberattacks have increased up to 125% and have been the main culprit of health data security breaches. As a result, patients/citizens, healthcare providers (HCPs) as well as policy makers tend to be reluctant about digital health services [5]. Investors also express scepticism to fund such activities, thus significantly affecting the acceptance of these new technologies as a part of the provided healthcare services.

As the number of travellers for work, education, and tourism constantly increases in the European Union (EU), cross-border health data exchange becomes a natural need to support proper healthcare services and continuity of care. However, people, especially those suffering from chronic diseases, are facing obstacles in travelling outside their country of residence, due to the lack of an established framework for health data exchange among healthcare organizations across the EU. To this end, one of the top three priorities of the European Commission regarding the digital transformation of health and care in the Digital Single Market constitutes citizens' secure access to their health data, including across borders of the EU [6].

To-date, the core effort in the EU for enabling cross-border health data exchange has been focusing on interoperability aspects, with projects such as epSOS (European Partners – Smart Open Services) [7], OpenNCP (Open-source and reference version of the NCP software [8] - the software implementation of epSOS), and lately the Trillium project, which focuses on EU-US cooperation and particularly on exchanging patient summary data. However, limited focus has been given to the cybersecurity aspects that are entailed in cross-border health data exchange.

Aiming to address this challenge, the EU-funded H2020 KONFIDO (Secure and Trusted Paradigm for Interoperable eHealth Services) project [9] that develops a toolset to facilitate secure cross-border exchange, storage, and overall handling of health data [10]. The toolset leverages various novel technologies, such as homomorphic encryption [11], photonic Physical Unclonable Functions (p-PUF) [12], a Security Information and Event Management (SIEM) system, [13] and blockchain-based auditing [14]. In addition, it builds upon existing frameworks, mainly OpenNCP and eIDAS (electronic IDentification, Authentication, and trust Services) [15]. OpenNCP offers a set of interoperability services to enable national and regional eHealth platforms to conduct cross-border health data exchange, while eIDAS implements the EU regulation regarding electronic identification and trust services for electronic transactions in the internal market, which includes eHealth applications among others.

As part of the KONFIDO user requirements engineering phase [16], we conducted an online survey to gain useful insights for the technical development of the envisaged toolset. The main goal of the survey was to identify how patients/citizens feel about exchanging their health data with healthcare professionals or eHealth service providers, as well as to what extent patients/citizens are aware of the entailed privacy and security issues. The survey also aimed to investigate technology acceptance issues, like the use of mobile health apps and the potential use of biometrics based on input collected from citizens across Europe.

In this paper, we present the overall survey methodology and the results, and conclude by consolidating these outcomes in terms of key barriers and facilitators regarding the acceptance and ultimately the adoption of digital health technologies focusing on cybersecurity and interoperability issues.

Methods

The survey was designed and implemented upon key principles of human psychology [17]. The main steps involved in this methodology are:

1. Deciding what information should be collected
2. Deciding how to conduct the survey
3. Constructing a draft of the respective questionnaire
4. Revising the draft questionnaire
5. Pre-testing the questionnaire
6. Revising the questionnaire and its use procedures

Several online sources were investigated prior to the questionnaire design. These included relevant surveys conducted by other organizations, reports, and scientific papers. In addition, the survey was designed and deployed, incorporating sophisticated features, such as:

- conditional workflow of questions based on the answers submitted on earlier questions, so that only questions relevant to the responder appear;
- input validation to avoid erroneous data entries;
- use of control questions (or "trap questions") to verify response quality; and
- export of the collected responses in a format that facilitates further data analysis

The respective questionnaire was built in an iterative fashion to validate its alignment with the survey scope and comprehension. The final version of the questionnaire was published in seven European languages, namely, Danish, Dutch, English, French, Greek, Italian, and Spanish.

The questions (35 in total) were organized in six sections:

7. *Awareness regarding Information Technology (IT) risks*: Focused on identifying the responder's awareness level regarding the risks entailed (both explicitly and implicitly) in using digital health tools
8. *Legislation*: Aimed at identifying the responder's familiarity with relevant legislation artifacts
9. *Cross-border medical treatment*: Aimed to provide insights on whether the responder was medically treated or hospitalized abroad, detailing the circumstances under this event
10. *Cross-border health data exchange*: Concerned with the responder's opinion regarding the need of cross-border health data exchange
11. *Barriers and facilitators*: Aimed at identifying key issues that facilitate or discourage cross-border health data exchange from a patient's/citizen's viewpoint
12. *Demographics*: Aimed to identify some key information about the responder, in order to facilitate the statistical analysis of the obtained data

The online survey was disseminated publicly via relevant forums,, mailing lists, and social media (i.e. KONFIDO project Twitter and Facebook accounts), targeting citizen groups that could be related with the subject of cross-border health data exchange (for example, chronic patient associations, immigrant groups, medical tourism groups) and also the general public. No exclusion criteria were applied aiming to increase participation of people who were not necessarily aware of the recent advances in the eHealth domain and its security aspects..

Before conducting the survey, it was approved by the Bioethics Committee of the Centre of Research and Technology Hellas (CERTH), as CERTH was responsible for the data collection and control of the study. The survey did not require the disclosure of the responder's identity.

Results

The survey was available online for three weeks and collected a total of 437 responses, out of which about 30% of responders contributed to the online questionnaire but did not complete it (124 incomplete responses out of 437 in total). This is a typical behavior in online surveys, as the responder might quit the process for any reason, therefore, the incompletely taken surveys were still taken into account. More specifically, regarding the demographics of the responders, their average age was 43.96 years, their gender distribution was 38.54% females and 57.96% males, and they were distributed in 14 European countries (most of the responders declared that they were from Greece, Germany, or Denmark). Since the survey distribution was conducted via public Internet communication channels, we cannot confirm the number of people reached through the online invitation campaign and, therefore, the response ratio cannot be calculated. We summarize the main findings in the following section.

Awareness regarding IT risks

The key results from this questionnaire section can be summarized as follows:

a) 11.96% did not thought about possible health data risks.

b) Only 36.41% felt informed about these risks.

c) 66.21% of the responders did not read the respective applications' "Terms and Conditions", with more than 30% declaring that they did not feel it is worthy, given the time required to read them and 19.79% declaring indifference towards them (Figure 1).

Figure 1 - Answers to Question "Why haven't you read the terms and conditions?" (Only Responders Who Answered the Previous Question that They Did Not Read the "Terms and Conditions" Were Asked)

Furthermore, the responders expressed confusion and lack of confidence on the subject. Only 26.09% of the responders felt confident regarding their electronic health data privacy, 38.04% felt concerned but helpless about, and 16.3% stated that they avoid using eHealth services due to the lack of confidence regarding their data handling.

An interesting remark is that the responders clearly preferred to entrust their health data to national and state organizations than to private ones, despite the rather high-rate (35.33%) declared in using applications exploiting personal health data.

These applications are typically provided and operated by private companies, mostly belonging to the category of life-style/wellbeing monitoring.

It should also be noted that only 20% of the responders felt that their privacy was fully covered in the "Term and Conditions" of the applications. The findings regarding the reasons that led responders to not read the "Terms and Conditions" were directly linked to legislation complexity, legislation misalignment between countries and the need for usability – most of the responders felt that too much time is required to read them, and 12.50% declared that they do not understand them.

Legislation

The need for raising awareness was also evident from the findings of this section (Figure 2 and Figure 3). While almost 80% of the responders declared being familiar with the EU General Data Protection Regulation (GDPR) [18], more than 50% declared that they were familiar with legislation items that do not really exist (as captured by a control question). In particular, about 27.37% declared being aware of data concepts/initiatives that do not really exist. The need for raising awareness was also supported by the fact that 24.93% of the responders expressed no opinion on whether the current legislation effectively protects them.

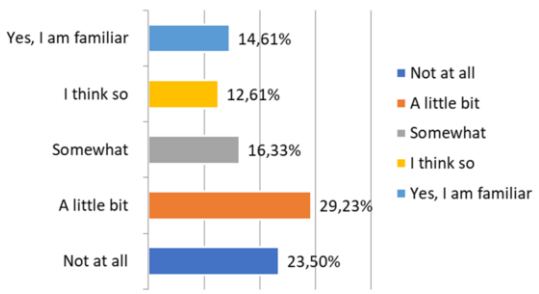

Figure 2 – Answers to the Question "Are you familiar with legislation that concerns the use of health data?"

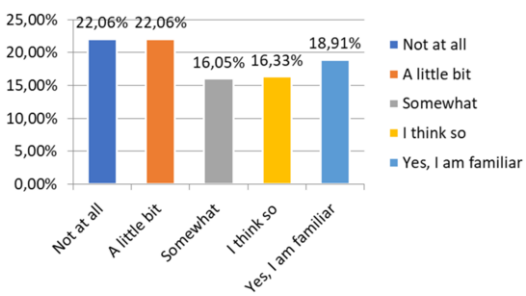

Figure 3 – Answers to the Question "Are you familiar with the data ownership concept?"

Regarding the effectiveness of the current legislation, only 27.79% of the responders felt protected, while 37.54% felt either defenceless, or insufficiently protected (Figure 4). As shown in Figure 5, citizens argued that legislation alignment among EU countries is a necessity. Furthermore, dissemination regarding legal issues and the level of legal protection provided were also identified as important items.

Cross-border Medical Treatment

28.16% of the responders were medically treated abroad. The reasons for their hospitalization or medical treatment abroad

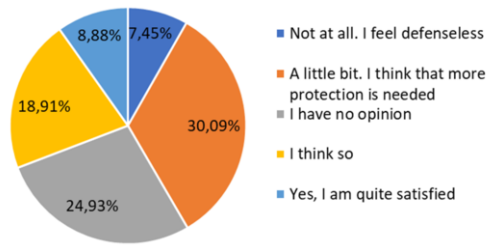

Figure 4 – Answers to question "Are you satisfied with the level of protection provided by current legislation?".

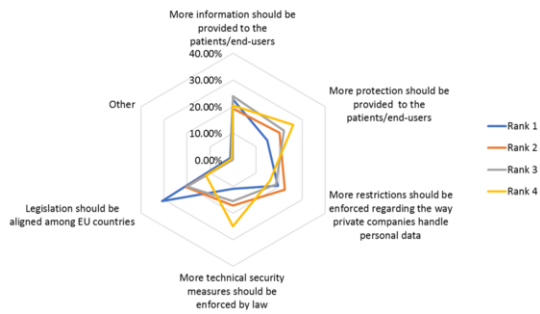

Figure 5 – Ranking of reasons for question "Regarding legislation, please rank the most important things to be improved regarding cross-border health data exchange".

were clearly depicted: 44.90% of the responders reported a sudden incident while travelling (e.g. a car accident), 37.76% were immigrants, and 16.33% referred to other reasons (e.g. studying abroad).

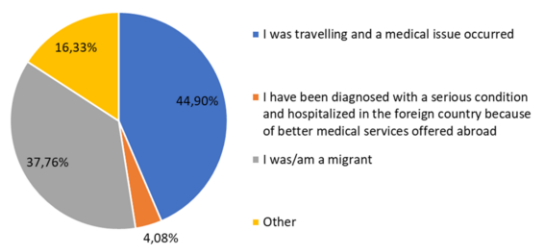

Figure 6 – Answers to the Question "In what circumstances have you used medical services abroad?"

These findings clearly highlighted that unscheduled access to healthcare services abroad, such as accidents/incidents while travelling, were critical for European citizens.

Cross-border Medical Data Exchange

The responders were highly in favor of cross-border data exchange, since only 9.28% expressed a negative opinion (Figure 7). Among the responders who viewed this issue as a critical one, the main concern involved technical issues and, particularly, information security aspects. Furthermore, a high percentage of responders (71.56%), would consent in sharing medical data with foreign medical personnel in case of an emergency, with the rest of them mostly worrying about the technical issues.

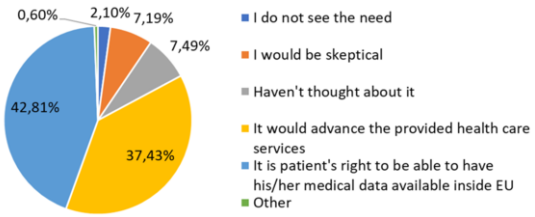

Figure 7 – Answers to the Question "How do you feel about medical data shared with foreign healthcare professionals /institutions to facilitate treatment while being abroad?"

It is also clear that the responders would prefer to use a European authentication card, rather than using biometric characteristics to authenticate themselves for cross-border eHealth data exchange. In addition, the need for a detailed description of the underlying context for using health data was evident, given that 53.29% of the responders wanted to be thoroughly informed before consenting to their health data usage.

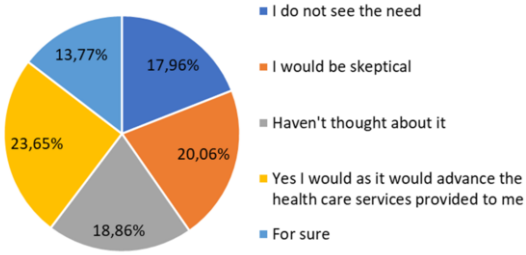

Figure 8 – Answers to the Question "Would you prefer using a biometric characteristic (e.g. fingerprints) instead of an ID card to facilitate cross-border medical data exchange?"

An interesting remark is that the vast majority of the responders (72.46%) declared that they were in favor of sharing personal data for research purposes, at least under the terms of anonymization. Finally, it should be noted that the responders who were sceptical towards cross-border health data exchange did not focus on the cross-border data exchange, but rather on the security challenges that have to do with data sharing, regardless of whether this sharing had to do with foreigners or not.

Barriers and Facilitators

The responders identified the following key factors for the acceptance of cross-border health data exchange:

1. A common legislation among EU Member States
2. Better control of data management practices applied by companies
3. More information on the processing of citizen health data

These key points clearly support the application of new European regulation, GDPR. Providing consent is one key aspect of the overall data sharing process: it could, on one hand, facilitate the process and, on the other hand, act as a barrier. The results clearly indicate the need for a flexible consent process, as 73.44% of the responders supported that "*Patient consent should be actively enforced. However, in some special cases (e.g. when the patient is unconscious), it could be skipped in favour of the provided medical services*" (Figure 9).

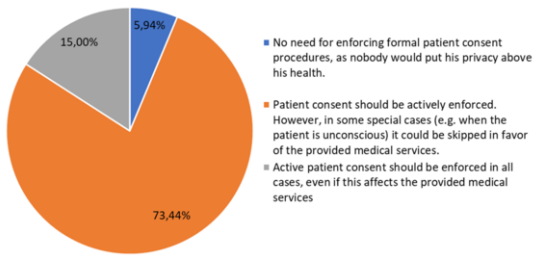

Figure 9 – Answers to the question "Please select in your opinion the level of required patient consent, in cases of cross-border data exchange"

Finally, the most important barriers regarding the acceptance of cross-border health data exchange are:

1 Lack of trust regarding the intentions of data collection

2. Lack of suitable legislation

3. The risks of interlinking these data with other personal information already available and traceable in the Internet (e.g. posts in social media platforms)

Consolidated Outcomes

The main outcomes of the survey focusing on how these could contribute to the development of cybersecurity solutions for health data exchange at large, and in cross-border scenarios in particular, are as follows:

- Raise awareness among patients/citizens and other stakeholders. More specifically, awareness should be raised regarding: (a) the risks of using IT for health data management (b) citizens' confidence with respect to their personal data handling (c) the need to simplify the "Terms and Conditions" for using eHealth services/applications (d) the need for a flexible and comprehensive consent process, and (e) the need for a clear and aligned legislation across EU Member States.
- Incidents during travel seem to be of high value. However, other use cases (such as immigrants living temporarily abroad) should be considered.
- The main control of cross-border health data exchange should be built upon national infrastructures (such as the national Electronic Health Record), as the patients/citizens tend to trust them more.
- Technical solutions should focus on using a Europe-wide authentication method such as one based on eIDAS and avoid the use of biometric characteristics.
- Provide a simple and comprehensible consent process, while being flexible in cases where the patient is unconscious (emergency scenarios).

Discussion and Conclusion

Citizens are a key stakeholder in eHealth data management, as cross-border health data exchange becomes a necessity across the EU. Recent regulation and legislation activities such as the GDPR set a framework for legal, ethical, and practical issues related to health data management and personal data protection. The KONFIDO project develops a technology toolset,

aiming to enhance information security for cross-border health data exchange, building upon emerging European frameworks such as OpenNCP and eIDAS.

To this end, the project relied on an intensive end-user engagement strategy [16], aiming to obtain feedback related to the current landscape and the practical issues that health data exchange entails through digital health solutions. Various activities were conducted, including a survey with health IT professionals, eHealth companies, and health policy makers [19], to identify digital health acceptance barriers and facilitators, using the survey presented in the current paper.

We presented the main results of the survey focusing on European citizens. A list of key issues was identified and a number of challenges were consolidated. These results could be used as a beacon for the development of new technical solutions in the context of health data exchange and health data management at large, including cross-border health data exchange. We thus argue that our findings provide useful insights for stakeholders of the European eHealth ecosystem, encouraging them to adapt their services and reinforce the acceptance and consequently the adoption of their solutions by the targeted end-users.

The main limitations of the current study relate to the risk of bias due to the following reasons: (a) the specific questions could be considered as "leading" responders to specific answers based on the reader's subjective judgement, and (b) the non-uniform distribution of the responders across European countries. The lack of detailed responders' demographic information is because of the fact that all the questions were optional and as the demographics section was put last, only a small portion of the responders answered them. As part of the presented methodological approach, all project partners revised the questionnaire to avoid responder "guidance" and also tried to disseminate the survey as widely as possible. Despite these limitations, we consider the results valuable and be able to provide useful insights. In order to reduce the effect of bias and further explore the collected data, the collected responses will be analyzed in combination and in comparison with the relevant studies and surveys conducted by other organizations such as the Healthcare Information and Management Systems Society (HIMMS).

Acknowledgements

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 727528 (KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services). This paper reflects only the authors' views and the Commission is not liable for any use that may be made of the information contained therein.

The authors would like to thank the KONFIDO partners for their help on the survey dissemination and the questionnaire translation to the supported European languages.

References

[1] M. Herrmann, P. Boehme, T. Mondritzki, J.P. Ehlers, S. Kavadias, and H. Truebel, Digital Transformation and Disruption of the Health Care Sector: Internet-Based Observational Study, *J Med Internet Res.* **20** (2018) e104.

[2] B. Meskó, et al., Digital health is a cultural transformation of traditional healthcare, *MHealth*. **3** (2017) 38.

[3] A. Sharma, et al., Using Digital Health Technology to Better Generate Evidence and Deliver Evidence-Based Care, *J Am Coll Cardiol.* **71** (2018) 2680–90.

[4] Cyber Attacks and Negligence Lead to Rise in Medical Data Breaches, (n.d.). https://www.nbcnews.com/tech/tech-news/cyber-attacks-negligence-lead-rise-medical-data-breaches-n575471 (accessed November 25, 2018).

[5] M.P. Jarrett, Cybersecurity - A Serious Patient Care Concern, *JAMA*. **318** (2017) 1319.

[6] European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, Brussels, 25.4.2018 COM(2018) 233 final, Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51628.

[7] epSOS project web site, (n.d.). http://www.epsos.eu/ (accessed November 16, 2018).

[8] M. Fonseca, K. Karkaletsis, I.A. Cruz, A. Berler, and I.C. Oliveira, OpenNCP: a novel framework to foster cross-border e-Health services., *Stud Health Technol Inform*. **210** (2015) 617–21.

[9] KONFIDO project website, (n.d.). http://www.konfido-project.eu/konfido/ (accessed Nov. 15, 2018).

[10] M. Staffa, et al., An OpenNCP-based Solution for Secure eHealth Data Exchange, *J Netw Comput Appl.* **116** (2018) 65–85.

[11] X. Yi, R. Paulet, and E. Bertino, Homomorphic Encryption, in: *Homomorphic Encryption Appl.*, Springer, Cham, 2014: pp. 27–46.

[12] C. Mesaritakis, et al., Physical Unclonable Function based on a Multi-Mode Optical Waveguide, *Sci Rep.* **8** (2018) 9653.

[13] S. Bhatt, P.K. Manadhata, and L. Zomlot, The Operational Role of Security Information and Event Management Systems, *IEEE Secur Priv.* **12** (2014) 35–41.

[14] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing, in: 2018 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng., IEEE, 2018: pp. 1374–1379.

[15] eIDAS web site, (n.d.). https://www.eid.as/home/ (accessed November 16, 2018).

[16] P. Natsiavas, et al., Comprehensive user requirements engineering methodology for secure and interoperable health data exchange, *BMC Med Inform Decis Mak.* **18** (2018) 85.

[17] J.J. Shaughnessy, et al., Research methods in psychology, n.d., 10th Edition, McGraw-Hill, 2014

[18] EU General Data Protection Regulation (GDPR), (n.d.). https://eugdpr.org/ (accessed November 25, 2018).

[19] P. Natsiavas, C. Kakalou, K. Votis, D. Tzovaras, N. Maglaveras, I. Komnios, and V. Koutkias, Identification of Barriers and Facilitators for eHealth Acceptance: The KONFIDO Study, in: Springer, Singapore, 2018: pp. 81–85.

Address for correspondence

Dr Vassilis Koutkias, Institute of Applied Biosciences, Centre for Research & Technology Hellas, 6th Km. Charilaou-Thermi Road, P.O. BOX 60361 GR – 57001, Thermi, Thessaloniki, Greece.

Email: vkoutkias@certh.gr.