Identification of Barriers and Facilitators for eHealth Acceptance: The KONFIDO Study

P. Natsiavas[1], C. Kakalou[1], K. Votis[2], D. Tzovaras[2], N. Maglaveras[3], I. Komnios[4] and V. Koutkias[1]

[1]Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Greece
[2]Information Technologies Institute, Centre for Research & Technology Hellas, Thermi, Greece
[3]Department of Electrical Engineering & Computer Science, McCormick School of Engineering & Applied Sciences, Northwestern University, Evanston, IL, USA
[4]Exus Software Ltd, London, UK

Abstract—**In this paper, we present one of the key KONFIDO project's activities, the identification of key barriers and facilitators regarding eHealth solutions acceptance, focusing on security and interoperability. The methodology presented includes an end-user survey and an end-user workshop, engaging various stakeholders from Europe, in order to gain value out of their experience and insight in real-world healthcare settings. The analysis of the results provides a list of explicitly identified barriers and facilitators of adopting eHealth solutions in a Europe-wide scale, useful in the context of KONFIDO and beyond.**

Keywords—**eHealth acceptance, barriers, facilitators, cross-border health data exchange, security of eHealth systems.**

I. Introduction

Recent advances in health IT intend to transform the healthcare delivery, especially via the increase of use of telemonitoring solutions, mHealth applications and genomic data. However, the constantly increasing digitalization and use of sensitive data come along with the cost of proliferation of cyber-crime. For example, 2015 has been an all-time record year for security breaches in healthcare with over 100 million health records accessed by hackers globally [1]. Despite the benefits of technological advances, security is considered as one of the most important barriers for the large-scale adoption of new eHealth services. Lack of security results to patients and healthcare personnel unwillingness to share health data and adopt eHealth solutions, as well as of investors (both private and public) to fund such activities. In addition, during the last decade, we witness a considerable increase of citizen's mobility in Europe for education, training, work and tourism. Nevertheless, people suffering from chronic diseases are facing obstacles in travelling either within or outside their country of residence, due to the lack of an established, systematic and secure framework for data exchange among healthcare organizations across EU.

The KONFIDO project (http://konfido-project.eu/) aims to leverage proven tools and procedures as well as novel approaches and cutting-edge technology, such as homomorphic encryption and blockchains, to create a holistic paradigm for secure cross-border exchange, storage and overall handling of healthcare data. KONFIDO aspires to fulfil the prerequisites for cross-border patient mobility, in the interest of EU citizens, allowing secure cross-border exchange of personal health data. KONFIDO is organised in four complementary phases, namely, 'User requirements'; 'Design'; 'Technology development'; and 'Integration, testing and validation'. As part of the 'User requirements' phase, KONFIDO reviews and maps applicable legal frameworks, ethical and social norms at EU level and in the project's pilot-site countries (i.e. Denmark, Italy and Spain), defining operational constraints and requirements. This process includes surveying all relevant stakeholders in participating countries (and other European countries too) to identify key factors and weak-signals that may considerably affect (at present and in the future) user acceptance, go-to-market strategies and overall operational sustainability of eHealth.

The current paper presents the methods employed to identify barriers and facilitators of eHealth acceptance linked with security and interoperability and the obtained results.

II. Methods

The two pillars employed to identify key barriers and facilitators to adopt eHealth solutions linked with security and interoperability were (a) an End-user survey, and (b) an End-user Workshop. The scope of these pillars as well as their organization details are presented in the following.

A. End-user Survey

The End-user survey focused on identifying the facilitators and barriers of applying security practices in real-world healthcare delivery settings. Thus, its main goal was to identify the currently applied practices regarding security and interoperability on existing e-health infrastructures, for organizations of varying size and nature (e.g. private and public), also focusing on specific stakeholder categories, namely managers, healthcare professionals (HCPs) and health IT stuff working in hospitals.

The survey has been implemented as an online survey, enabling sophisticated features like: (a) conditional workflow of questions based on answers submitted on earlier questions, so that only relevant questions appear for the user; (b) validation of input to avoid erroneous or malicious input; (c) export of the collected responses in a format convenient for further analysis, and (d) creation of personalized invitations and automatic reminders for the involved participants. The design of the survey is based on the guidelines presented in [2].

While making the survey public and using widely accepted forums, email lists, social media etc. would certainly increase the obtained responses, it would inevitably increase the risk of receiving answers of questionable value. Therefore, we decided to avoid a totally open invitation policy for survey submissions and invited specific individuals (experts) expecting high-value responses. The target audience has been carefully selected among stakeholders working on hospitals or health administrative regional units across Europe, able to provide the anticipated insights. A time window of one week has been given to the participants to submit their responses, while further extensions of this deadline have also been given. While the responses of the participants have been treated as anonymous, each invitation has been related with an automatically produced token to allow trace-back of the submitted responses for quality control reasons.

The survey questions have been structured in 6 sections:

- *Organization profile section*: refers to the organization's size and structure (e.g. employees number, activities' domain etc.) to provide a context for the responses.
- *Security facts section*: focuses on security incidents happened in the organization. This section targets technical staff (engineers and IT security staff) and managers.
- *Security policy section*: refers to policies applied in the organization (e.g. existence of security and risk management policies, use of encryption etc.).
- *Security incident management section*: targets on the handling of security breaches in a technical level. This section targets mostly technical staff (engineers and IT security staff) and managers as medical staff could not practically provide details on such issues.
- *Barriers and facilitators section*: aims on identifying key issues that facilitate or discourage the adoption of security oriented best practices.
- *Personal view section*: focuses on awareness (e.g. use of publicly available cloud storage services, importance of security in everyday work etc.) and satisfaction regarding current security status.

B. End-user Workshop

The End-user Workshop has attracted more than 30 key stakeholders from the eHealth and healthcare across Europe. It has been organized to encourage open discussion, exploring the open issues in the domain of cross-border health data exchange through eHealth solutions. Personal invitations were sent to candidate participants from diverse organizations (healthcare, standards developing organizations, health IT associations, regional healthcare authorities, privacy authorities, research/academia, etc.), to obtain input from the widest possible spectrum of stakeholders composing the eHealth ecosystem. In each of the Workshop sessions, short presentations concerning key aspects of the project were provided, while sufficient time was assigned for discussion among participants. Discussions were recorded, to allow transcription and elaboration upon the discussed issues.

III. Results

A. End-user Survey

a) Organization profile section

The end-user survey has been completed by 39 selected stakeholders across Europe. More than 50% of the participants refer to organizations with more than 1,000 employees and 80% of the submissions refer to organizations having more than one facility location. This is important as large organizations might tend to handle infrastructure issues in a more systematic way than small ones and this would probably lead in a more systematic approach on IT security issues, policies, etc., given that smaller organizations (e.g. peripheral hospitals) probably lack resources, expertise, etc. Furthermore, it should be also noted that participants' distribution among occupations was rather well distributed, keeping a balance among participants with a technical background (engineers and IT security staff), HCPs, and management stuff. A high number of participants is also leaning towards research (about 34%). Finally, the collected responses refer to a wide distribution of IT system types, with Electronic Health Records (EHR), Digital Prescription Records (DPR) and Laboratory Information Systems (LIS) being the most frequent.

b) Security policy:

The submitted responses clearly identify that security policies are widely applied. However, the lack of an overall security mentality is also identified. A clear majority of the survey participants (over 80%) answered that a specific IT security policy in their organization exists, while more than 40% identify standards or legislation on which their organization's policy refers to. 14.29% answered that there is no responsible person for IT security and more than 75% declared that encryption is used, at least to some extent. Personal data (clinical, demographic and personnel data) were recognized as more important than other operational data (ERP, CRM, email). However, only 14.29% of the survey participants declared that there is an incentive to discover and report security breaches, 27.59% knew of a specific information classification scheme used in their organization and 40% declared that there is no budget regarding IT security or it is lower than 1%, while 20% declared ignorance. Furthermore, none of the participants declared that there is breach insurance available (60% declared that there is no breach insurance and 40% declared ignorance). These findings clearly depict a lack of an everyday security-oriented mentality.

Regarding inter-organizations' data exchange, 68.57% explicitly declared that they regularly exchange data with other organizations and 40% exchange data with foreign organizations. Almost 80% act upon agreements with third-party organizations (e.g. other hospitals), to securely exchange sensitive data, while 35.71% declared that their state cross-border data exchange agreements are GDRP [3] compliant.

Technically, only 51.43% declared that there is a central antivirus management in their organizations, while 37.4% declared that there is a central IT resources access mechanism (Active Directory or LDAP). It should be noted that engineers, managers and HCPs have unlimited access to highly sensitive data, once they log in, in percentages reaching 40%.

These findings depict that KONFIDO should focus on raising awareness on real-world security policy issues.

c) Security incident management:

Regarding the main cause of security breaches, "External attacks" is identified as leading cause and "Employee negligence" follows, while "Employee negligence" was characterized as the "most undetected" by 70% of the participants. Furthermore, organizations are ready to conduct risk assessment, but do not take actual measures to enforce security like breach monitoring and mitigation. The most frequently used security tool identified is VPN (70%), while there is little usage of advanced tools like Intrusion Detection Systems or Intrusion Prevention Systems (10% and 15%, respectively).

The above findings clearly depict that KONFIDO should also focus on raising awareness regarding more advanced security tools that are currently available. KONFIDO is expected to provide a Security Event Information Management (SIEM) system, that would also improve the respective organizations' incident management capabilities.

d) Barriers and facilitators:

Many survey participants referred to security measures as an obstacle for usability (34.29%). 75% declared that sometimes they skip a security rule and that their colleagues also try to skip security rules, either regularly or occasionally, implying a direct link between usability and security measures. Furthermore, almost 70% identified that lack of budget is a clear obstacle towards a more secure IT infrastructure, while almost 60% identifies the shortage of IT staff as barrier as well. Regarding the evolution of security measures and their efficiency, 57.14% feels that the overall security has improved, mostly due to the commitment of the management towards applying security practices. Only 5.71% declared that the situation has worsened, mostly due to the lack of management commitment. Conclusively, management commitment, budget increase and definition of a specific policy are the main issues expected to facilitate the adoption of security-oriented best practices.

e) Personal view:

Network intrusions, malicious insider attacks, phishing and loosing storage devices were identified as the most important threats, according to the participants. 42.86% consider public cloud storage services unsafe to use and another 20% is not allowed to use them. Loss of productivity, fear for assets and organization's image are considered the most affected factors by a security incidence. More than 50% considers IT security as top priority, while only 30% appears to be satisfied with the level of IT security of their organization.

B. End-user Workshop

The major outcomes of the End-user Workshop concerning barriers and facilitators include:

a1) Information flow barriers:

- Cross-border health data exchange is typically manual and document-driven. The capability to "translate" the content is crucial and could be a major burden.
- Terminology issues can cause ambiguities.
- The diversity of the internal workflows applied in healthcare organizations. Applying IT-oriented approaches could lead to new information workflows that HCPs are reluctant to accept.
- Lack of trust among organizations (partially due to different information handling workflows), discourages (if not prohibits) data sharing.

a2) Information flow facilitators:

- Using widely accepted, standardized encodings, thesauri, ontologies, etc. could facilitate interoperability and reduce ambiguities among different organizations due to the use of different languages and terminologies.
- Workflow heterogeneity among the healthcare organizations could be overcome through the definition of a simple common/baseline workflow (it could include only medical data sharing with no administrative data), acting as a proxy among the various local workflows.

b1) Legislation barriers:

- National and European legislation formulates a complex grid of unaligned laws, hard to be interpreted and applied
- Liability issues are not yet sufficiently clarified regarding data sharing scenarios.
- Ambiguities regarding data ownership.
- As technology evolves, new scenarios of data usage and transfer are emerging, causing legal gaps, as legislation cannot keep pace with fast evolving IT.Giving consent

for health data handling is very important and could be proven as a major problem.

b2) Legislation facilitators:

- GDRP and the 95/46/EC directive [4] provide a robust basis on which the EU Member States build agreements. Having a clear legal point of reference can significantly facilitate data process agreements among organizations.
- Several EU initiatives work on the alignment of legislation among EU Member States. Working groups, forums, etc. are constantly being formulated to facilitate interstate agreements and the application of EU directives in a uniform way across.
- A legal process that could facilitate data exchange and minimize legal problems is patient's explicit consent. Patient's consent could overcome the need of cross-institutional or international agreements. As patients tend to care most for their treatment than for their privacy, the process of consent must be carefully designed and consider proper information providing, opt-out or regret capabilities and delegation processes, e.g. for cases of patients being unconscious.

c1) Technical barriers:

- Lack of a clearly established technical infrastructure for health data sharing.
- Usability shall be a top priority.
- Network availability has risen as a consideration in cases where high mobility is required.
- While standards exist for almost any procedure of data sharing, their application is a barrier itself.

c2) Technical facilitators:

- Advanced technologies could be used to extract structure out of unstructured free-text data (e.g. Natural Language Processing) and encode the outcomes using widely-accepted, standardized coding schemes.
- Provenance information could be proven as a key facilitator for data validity. Through provenance, errors could be identified and possibly corrected.
- To overcome usability issues, the paradigm of a summary report document could be useful as a paradigm that they the various stakeholders are familiar with.
- Several technologies and standards in the context of secure and interoperable cross-border health data exchange already exist, providing valuable tools and experience for the construction of real-world infrastructure.

IV. Conclusions

The main outcome of the End-user survey is that currently applied security practices are far from ideal due to several reasons, including lack of management commitment, lack of security culture in every-day activities but also shortage of available funding. Furthermore, in real-world settings, interoperability (cross-border or in-border) practices are not widely applied through standardized procedures, while the use of central, security-oriented tools (Active Directory, LDAP, Intrusion Detection Systems, etc.) is severely lacking. Moreover, management commitment to ensure the adoption of efficient security best practices must go further than just defining a policy and must practically enhance procedures through budget and specialized IT personnel. In the scope of the End-user Workshop, we identified many technical, organizational and legal barriers targeting cross-border health data exchange scenarios. Despite all the available technological achievements and the already evolving legal initiatives within EU, a lot of effort must be invested in aligning the legislations and the workflow of actions among EU Member States to provide the context of an IT solution facilitating cross-border secure data exchange and processing.

Acknowledgment

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 promoting the survey and for participating at the End-user Workshop.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

1. HIT Consultants: http://hitconsultant.net/2016/01/05/healthcare-cyber-attacks-in-2015-infographic, last access October 6, 2017.
2. Shaughnessy J. et al. (2011). Research methods in psychology (9th ed.). New York, NY: McGraw Hill. pp. 161–175.
3. General Data Protection Regulation Portal: http://www.eugdpr.org/, last access October 6, 2017.
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

Author: Pantelis Natsiavas
Institute: Institute of Applied Biosciences, Centre for Research & Technology Hellas
Street: 6th Km. Charilaou-Thermi Rd, P.O.BOX 60361, 57001
City: Thermi
Country: Greece
Email: pnatsiavas@certh.gr