European Security in Health Data Exchange

Deliverable D2.1

eHealth security challenges

Editor(s):	Xabier Larrucea, Jason Mansell, Alberto Berreteaga
Responsible Partner:	TECNALIA
Status-Version:	Draft
Date:	31/03/2017
Distribution level (CO, PU):	CO

Project Number:	GA 727301
Project Title:	SHIELD

Title of Deliverable:	eHealth security challenges
Due Date of Delivery to the EC:	31/03/2017

Workpackage responsible for the Deliverable:	Tecnalia
Editor(s):	Tecnalia
Contributor(s):	Tecnalia, AIMES, Stelar, FCSR, IT Innovation, Osakidetza, Lancashare care NHS, Symphonic, IBM, Metrarc, Ibermatica
Reviewer(s):	Antony Shimmin, Ed Conley, Matthias Pocs, Micha Moffie, Muhammad Barham
Approved by:	Tecnalia
Recommended/mandatory readers:	All WP's

Abstract:	The objective of this deliverable is to identify eHealth security challenges to be tackled by the SHIELD project. A qualitative study and a quantitative study are carried out for this identification. A state of the art for the SHIELD context is provided, and a survey is defined and analysed for the identification of these challenges
Keyword List:	eHealth security challenges, interoperability, security
Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	09/02/2017	working draft version	Xabier Larrucea, Jason Mansell, Alberto Berreteaga (TECNALIA)
v0.2	23/03/2017	First draft version	Xabier Larrucea, Jason Mansell, Alberto Berreteaga (TECNALIA)
V0.3	29/03/2017	Contributions and revisions	Stefanie Cox (IT Innovation), Micha Moffie, Muhammad Barham (IBM); Matthias Pocs (Stelar), Antony Shimmin (AIMES)
V1.0	29/03/2017	Reshape document structure, survey data and conclusions	Xabier Larrucea, Jason Mansell, Alberto Berreteaga (TECNALIA)
V2.0	31/03/2017	Last review	Xabier Larrucea, Jason Mansell, Alberto Berreteaga (TECNALIA)

Table of Contents

List of Figures

List of Tables

Terms and abbreviations

AA	Auditing & Accounting
AC	Access Control
CEN	European Committee for Standardization (*Comité Européen de Normalisation)*
CENELEC	Comité Européen de Normalisation Electrotechnique
ETSI	European Telecommunications Standards Institute
EPSOS	European Patients Smart Open Services
KR	Key Result
N3	NHS National Network
NHS	National Health Service
OECD	Organisation for Economic Co-operation and Development
OpenNCP	Open National Contact Point
PKI	Public Key Infrastructure
RIPsec	Reputation-Based Internet Protocol Security

Executive Summary

The objective of this deliverable is to identify eHealth security challenges to be tackled by the SHIELD project. Some current tools, methods, solutions stemming from European projects related to data security and privacy in the eHealth domain are analysed. In this sense we identify current eHealth challenges stemmed from literature (qualitative study) and SHIELD stakeholders' experience based on a survey (quantitative study).

1 Introduction

Security challenges applied to eHealth is a complex field. Our aim is to narrow the focus of our efforts, and to select a set of challenges to be addressed by SHIELD which will overcome these security and compliance barriers by:

- providing models and analysis tools providing automated identification of end-to-end security risks and compliance issues and supporting privacy and compliance 'by design';
- using this to analyse compliance rules across borders with reference to the security risks they address, to identify how they could be improved and converged to address a common set of privacy risks, and feed this into the standards being developed by CEN, Cenelec and ETSI to meet the requirements identified by the forthcoming General Data Protection Regulation;
- defining an open and extensible data exchange architecture based on epSOS, supporting security measures that address these risks;
- developing security mechanisms to deal with new and emerging risks, such as inference attacks on sensitive data, and risks from relatively unprotected mobile edge devices;
- providing faster and more cost effective methods to verify and monitor compliance with multiple sets of applicable regulations;

One of the specific developments to be done in SHIELD is the end-to-end systemic analysis of potential risks to health data. This will be achieved by creating a knowledge base from potential threats including 'classical' cyber security threats (e.g. unauthorized remote access), emerging threats to personal data (e.g. inference attacks to disclose personal data without direct access, or attacks on encrypted data exploiting schematic vulnerabilities), and compliance threats (i.e. failure to use security or governance mechanisms required by regulations).
In this context and according to the OECD's Health Systems Characteristics Survey (http://qdd.oecd.org/subject.aspx?Subject=hsc) a large majority (>75%) of primary care physicians use a personal computer (93,33%) for their current activities such as making appointments, ordering laboratory tests, keeping records of consultation and so forth. This means that issues relating to the use of a hospital workstation and related security and privacy aspects represent some of the main eHealth challenges that must be addressed in order to preserve and enhance security and privacy of stakeholders. In addition, due to diversity of health care models in Europe, there is a wide variety of which has been implemented and most of them are distributed [1] which implies an increase of technological infrastructures and therefore more sensitive to security threats. This kind of implementation for eHealth systems, provide flexibility and immediate access to data, and to manage personal health information among others [2].
Due to this diversity of situations there are several eHealth security challenges stemming from use cases. For example, mHealth[3] as part of eHealth, are suffering from technology based threats. No matter which care model is implemented, we need to ensure *confidentiality, integrity and availability of the data* [4]. Such requirements are law in some EU member states.

Recently some research works apply traditional security services such as Public Key Infrastructure (PKI) for privacy/security regulations [5] in eHealth systems. These security services are analysed in order to identify which are the most appropriate for the SHIELD project.

Another relevant aspect pointed out in the SHIELD is that tools will be developed to automatically determine where and how all types of threats apply to a specific end-to-end system or application scenario, and how they can be countered using security mechanisms. These offline analysis tools will allow systematic analysis of health data security in end-to-end data exchange scenarios.

2 Current tools, methods and solutions from related projects

In this context there are too many general purpose tools and methods that can be used or are being used in different eHealth scenarios. Our aim is to describe those existing methods, tools and approaches related to SHIELD project which are used by the consortium in order to achieve the expected results. As reminder the main objective of the SHIELD project is *to create an open and extendable security architecture supported by security mechanisms and privacy by design modelling and analysis tools to provide systematic protection for the storage and exchange of health data across European borders, subject to control by the data subjects, compatible with existing regulatory frameworks, ensuring the privacy, availability and correctness of the data while improving trust of patients in the security of their data and its use to address their needs*.

There are several European and national projects dealing with the security and interoperability of eHealth data. These projects generate a set of tools or methods covering a wide set of security aspects, and some of them are related to SHIELD objectives. The following table 1 summarizes which projects set the basis for input to the SHIELD project.

Table 1. Research projects related to SHIELD

Project name	Description
OPTET	Threat identification and analysis tools from the OPTET project (http://www.it-innovation.soton.ac.uk/projects/optet), which provides open source tools. However it lacks of a knowledge base covering privacy and compliance issues. This tool can be used as a basis for building tools.
epSOS	epSOS project (www.epsos.eu) provides a set of open source tools for cross-border interoperability between electronic health record systems in Europe. One of its results is the OpenNCP architecture specification which will be the basis for our SHIELD approach. epSOS aimed to design, build and evaluate a service infrastructure that demonstrates crossborder interoperability between electronic health record systems in Europe. The epSOS services are focused on the sharing of patient summaries and electronic prescriptions. The intention of epSOS has been to deliver and test building blocks to implement cross-border eHealth services in the future. epSOS has achieved this in different ways: • by defining and setting up the necessary infrastructure based on National Contact Points (NCPs) which exchange patient information with other countries and • by defining, testing and evaluating the services from a user's – health professionals and patient's – perspective. SHiELD will base its secure data exchange architecture on epSOS, by introducing

Project name	Description
	secure design patterns and security mechanisms able to counteract threats to health data exchange, including data anonymization and other masking mechanisms depending on the sensitivity of specific data items. The SHiELD pilot sites will also use epSOS specifications when creating their data exchange gateways, including open source software from OpenNCP.
e-SENS	e-SENS (https://www.esens.eu/) focuses on cross-border interoperability in eHealth, eJustice and eProcurement, aiming to provide generic and re-usable software components for, inter alia, e-Delivery, e-Identity (eID) and e-Signature. SHiELD will be inspired by the improvements made by e-SENS in relation with e-Identity and e-Signature to be applied in patients and designed practitioners identification and for providing consent.
EXPAND	EXPAND Project (http://www.expandproject.eu/) focuses on supporting the expansion of pilots such as epSOS to large-scale deployment and to progress towards an environment of sustainable cross border eHealth services, established at EU level by the Connecting Europe Facility (CEF) and at national level, through the deployment of suitable national infrastructures and services.
OPERANDO	The OPERANDO project (http://www.operando.eu/servizi/notizie/notizie_homepage.aspx) provides comprehensive user privacy enforcement in the form of a dedicated online service, called "Privacy Authority" which is used by independent Privacy Service Providers (PSPs). SHiELD will extend this concept to systemically address end-to-end security between the systems in which health data is exchanged and used. DevOps approaches will be explored as well. OPERANDO project develops among other tools and approaches an anonymization component.
MUSA	MUSA project (www.musa-project.eu) provides a set of tools for facilitating security in multi-cloud systems. It provides a DevOps approach for multiclouds which can be reference in SHIELD project. The main goal of MUSA is to support the security-intelligent lifecycle management of distributed applications over heterogeneous Cloud resources via a security framework that includes: a) security-by-design mechanisms to allow application self-protection at runtime, and b) methods and tools for the integrated security assurance in both the engineering and operation of multi-Cloud applications.
eWALL	The eWALL project (http://ewallproject.eu/) aims to develop a sensor-based eHealth platform deployed at the elderlies' homes. As part of the research project, knowledge about a legal Privacy-by-Design method was generated. Whereas that method covers patient data (about physical activity and other lifestyle patterns) that is used locally where the patient resides between a few systems (local and cloud), SHiELD will extend this to specify privacy mechanisms for interoperability with numerous national eHealth systems.
WITDOM	WITDOM project (http://witdom.eu/) empoWering prIvacy and securiTy in non-trusteD envirOnMents. WITDOM project targets the development of malleable obfuscation technologies allowing the secure and privacy-preserving outsourcing of data and computations to untrusted domains. SHiELD can take advantage from the definition of Electronic Genomic Record given within WITDOM along with the privacy/security metrics identified in the project, and exploit the platform developed within WITDOM as one end involved in the communication of health data to another CDO.
PRISMACLOUD	PRISMACLOUD project (https://prismacloud.eu/) is focused on providing a set of PRIvacy & Security MAintaining Services in the CLOUD and a Health Data

Project name	Description
	Repository is provided. PRISMACLOUD aims at enabling and advancing the TRL of several already available technologies exploited in distributed systems for the secure and private sharing and storage of data. It also focuses on the modular combination of such components to provide secure and privacy-preserving usage of cloud services for data storage and processing. SHiELD can take advantage from the results of PRISMACLOUD building upon the results obtained in the project and incorporating solutions proven to be successful in its architecture.
ASSURED	The Innovate UK project ASSURED aims to develop a knowledge base corresponding to the current UK regulations defined by HSCIC for connection to the NHS National Network (N3), and to use this to speed up the process of applying for and approving connections, and to improve the implementation and monitoring of security measures. SHiELD will use results from ASSURED as a starting point, covering asset-centric network security but not new and emerging threats and countermeasures, or cross-border compliance issues. A Secure System Modeller tool facilitates the modelling part of ASSURED.
SUNFISH	SUNFISH project (http://www.sunfishproject.eu/) provides a SecUre iNFormatIon SHaring in federated heterogeneous private clouds.

In this diverse context for assuring cross border interoperability, security and privacy we need to use different technologies and standards. In fact the three European standards organisations (CEN, Cenelec and ETSI) were requested by the European Commission to provide data protection guidance for the security industry. This guidance will be used in SHIELD and incorporated into its design patterns and security knowledge base.

From the above table there are three aspects to be studied in detail:

- OpenNCP: one of the epSOS project's result is the OpenNCP architecture and implementation. The OpenNCP community has designed and developed a set of Open Source Components based on the services developed in epSOS that can be used by Participating Nations to build their local implementation of an NCP. Some of the countries involved in SHiELD use cases have previously piloted some of the services using OpenNCP implementations such as the patient summaries access (Spain and Italy) and electronic prescription (Spain). SHiELD plans to collaborate with the OpenNCP community, using its software and extending components such as the Security Manager, the Policy Manager and the Consent Manager Components in order to support new (and evolving) security requirements and legislations. FCSR will use OpenNCP software in SHiELD to provide an epSOS compliant data exchange gateway. Additionally the OpenNCP community will be a target for dissemination and exploitation.
- STORK 2.0 is a European project and it contributed to the realization of a single European electronic identification (e-ID) and authentication solution. It built on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities. SHIELD reuses STORK authentication mechanisms.
- E-SENS (https://www.esens.eu/) and OpenNCP will be integrated as it is described by its roadmap. SHIELD will also analyse its potential re-use.

Table 2. Projects and related tools and methods

Project name	TOOL/METHODS
OPTET	Current project website is not available, but the following link (https://tinyurl.com/jwcopal) provides some of the tools developed under this project. This tool is based on FIWARE (https://tinyurl.com/k82cvt9), and this approach can be helpful for reaching our objectives. Other approaches resulting from this project are related to trustworthiness [6] and [7].
epSOS	The main tools and method are described by the OpenNCP community (https://tinyurl.com/kgxknpq). Some interesting tools and approaches are described in [8], [9] and [10].
e-SENS	Among other tools they provide a standalone adapter in the e-ID area to bridge the gap between e-IDAS based German middelware and the Dutch PEPS based on STORK 2.0. In addition the e-SENS project developped an 'Evidence Emitter', a mechanism for achieving non-repudiation in cross-border communication though evidence generation and collection.(https://tinyurl.com/n72xgjc), and a reference architecture (https://tinyurl.com/l8dbugc)
EXPAND	Neither tools nor methods are identified in this project which can be used by SHIELD. However epSOS states on his website www.epsos.eu (last view March 21st 2017) that they had a collaboration with EXPAND.
OPERANDO	Several tools and methods are proposed in OPERANDO. For example, Business Driven Tools [11] and privacy enhanced tools [12] are provided.
MUSA	MUSA provides the following tools: • MUSA Dashboard which provides integration of different tools. • MUSA Modeller helps users to annotate security information with CAMEL language. • MUSA Decision Support Tool (DST) which helps stakeholders to define security requirements. • MUSA SLA Generator which is used to define service level agreements • MUSA Deployer used as a deployment tool. • MUSA Security Assurance Platform (SAP) controls security behaviour.
eWALL	The eWALL architecture is based on two main components: eWALL Sensing Environment and eWALL Cloud. An example of this kind of tools is described in [13]. An interesting approach for Cloud systems is described.
WITDOM	WITDOM provides a secure interface between IT departments and Cloud providers as described in [14].
PRISMACLOUD	There are some interesting tools developed by this project called PRISMACLOUD toolbox (https://prismacloud.eu/toolbox/): • Secure Object Storage Tool (SECOSTOR) is a security tool for supporting confidentiality and availability. • Flexible Authentication with Selective Disclosure (FLEXAUTH) is a tool allowing authentication of arbitrary messages (or documents) by means of digital signatures. • Verifiable Data Processing (VERIDAP) is used to verify correctness. • Topology Certification (TOPOCERT) is used to support graph signatures to certify and prove properties of topologies. • Data Privacy (DATPRIV) tool provides several capabilities including: (1)specialized data encryption such as Format Preserving Encryption and Order Preserving Encryption and (2) big data anonymization.
ASSURED	This project provides an approach to asset-centric network security including emerging threats and countermeasures. In SHIELD we address and extend it for cross-border compliance issues, because some regulations are not compliant if we connect to the N3 network from outside the UK

Project name	TOOL/METHODS
SUNFISH	It is still under development but there are interesting tool such as [15] where author explains how to integrate securely cloud services as well as privacy tools for masking and anonymization of data .

These results are going to be considered for the SHIELD requirements analysis (Deliverable D2.2 SHIELD Requirements Analysis). In addition some technical considerations should be considered while defining the final architecture and to the architectural decisions in the final solutions.

3 Identified Security Challenges

There are several challenges identified in eHealth domain which are reported by several authors [16], [17] from a diverse perspective. This comprehensive set of challenges depends, among other factors, on the care system model. Figure 1 aims to represent the global shift that is suffering care models. Therefore the umbrella of new challenges and opportunities is increasing, but at the same time new threats are appearing because security is a chain and it is as strong as its weakest link.

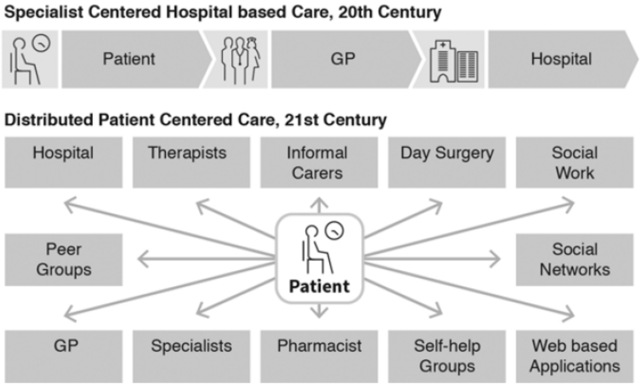

Figure 1: Global shift in care models [1]

There is a predominant set of challenges identified by several authors, and which should be tackled in most of the systems. One of these challenges reported is "privacy" which has been treated by several authors and situations including tele-monitoring [18]. Another cornerstone to be preserved is the eHealth related data, where its access [19] and storage are critical steps in this security chain. As users are being considered as the centre of eHealth systems, new ways of thinking should be considered in these environments as stated by [20] where a new digital signature scheme approach is defined.

In this myriad of technologies regulatory aspects are playing a key role. In fact it is a relevant aspect when we deal with cross border situations [21]. Several security services such as PKI [5] are dealing with regulations, and there are several experiences documented [22]. In addition, these aspects including ontologies [23] are also important aspects for interoperability among systems because formats, exchange mechanisms and protocols are required to set an interoperable system. As example, OpenEHR (http://www.openehr.org/) is a project focused on providing an open domain-driven platform for developing flexible e-health systems. Standards are enablers for reaching interoperability among systems. In this sense and according to ISO 27799:2008 (Health informatics — Information security management in health using ISO/IEC 27002), some of the key aspects in the eHealth domain are maintaining information confidentiality, availability, and integrity (including authenticity, accountability and auditability). These elements are considered the main goals of information security.

In addition, eHealth systems should provide a trusted environment [24] among others. Several approaches have been studied [25], and reputation-Based Internet Protocol Security frameworks such as (RIPsec) [26] or CORE [27] have been proposed. All of them are dealing with security and privacy aspects, and several research works are aligned to these aspects. For example the authors in [16] provide a quite long list of requirements. According to [28] three out of seven major threats that occur when sensitive information is: (1) sent via the Internet using insecure protocols; (2) stored on third party servers; (3) registered into un-secured system logs. These aspects are tightly related to the implemented platform or infrastructure. For example, Cloud environments provide several benefits, but some research works such as [29] reveal some security and privacy requirement for digital health.

The epSOS project has identified which security aspects should be taken into account [8]. They have identified the following elements:

- **Security Policies**
    - Object & principles
    - Security infrastructure
    - Risk management strategy
    - Security services and measures
    - Physical security
    - Personnel security
    - Security checking
- **Security services**
    - AC (Access Control)
    - AA (Auditing & Accounting)
    - Data-Exchange
    - Non Repudiation
    - Data-Confidentiality
    - Data-Integrity
    - PKI

The aforementioned security policies and security services are some aspects to be included in SHIELD results. According to a recent literature review [30] *the most common authentication mechanisms are digital signature schemes based on PKI (22%) and logins/passwords (26%).* PKI has been widely used [31] such as for granting trust [32] in several environments including Web [33]. However despite the current limitations of PKI [34], [35]or even in smartcards [36], its use is widespread across different domains. Therefore PKI is one of the infrastructures to be analysed.

Other studies provide a summary of opportunities and challenges in eHealth such as [37] where author identifies privacy and integrity as well as trust-based unified service delivery platforms and interoperability, as the main challenges.

3.1 Framing the study to SHIELD context

From the selected European projects (table 1) we have analysed them with respect to SHIELD key results (KR01 to KR12). Some of these key results are more focused on SHIELD general aspects such as KR09 Pilots, KR10 Best Practices, KR11 Publications and KR12 Take up opportunities. Others are more related to technical aspects such as:

- [KR04] SHiELD open architecture and open secure interoperability API
- [KR06] Data protection mechanisms
- [KR07] Privacy tool
- [KR08] Legal recommendations Report

Therefore we have compared each European project's results with each key result in order to identify to what extend each project can contribute to the achievement of each key result (table 3). One of the main conclusions is that there is no project covering all key results. However this table 3 provides an overview of what project can contribute to what key result.

Table 3. European projects results (methods&tools) and SHIELD key results

European projects\SHIELD key results	[KR04] SHiELD open architecture and open secure interoperability API	[KR06] Data protection mechanisms	[KR07] Privacy tool	[KR08] Legal recommendations Report
OPTET	✗	✗	✓ (partially)	✗
epSOS	✓ (partially)	✗	✗	✓ (partially)
e-SENS	✓ (partially)	✗	✗	✓ (partially)
EXPAND	✗	✗	✗	✗
OPERANDO	✗	✓ (partially)	✓	✗
MUSA	✓ (partially)	✗	✗	✗
eWALL	✓ (partially)	✓ (partially)	✗	✓ (partially)
WITDOM	✓ (partially)	✓ (partially)	✗	✗
PRISMACLOUD	✓	✓ (partially)	✓ (partially)	✗
ASSURED	✗	✗	✓ (partially)	✓ (partially)
SUNFISH	✓ (partially)	✗	✗	✗

From the study of these projects we have identified a set of challenges (table 4). They may vary along the project execution, but most of them are related to the existing SHIELD project objectives. Therefore for each challenge we relate it to one or several SHIELD key results as it is reflected in the following table 4. This relationship does not mean that solving a challenge the related key results will be automatically solved. This relationship means that these challenges will be treated when dealing with the related key results. This approach helps us to focus the efforts on specific aspects.

Table 4. Challenges and SHIELD key results

Challenge\SHIELD key results	[KR04] SHiELD open architecture and open secure interoperability API	[KR06] Data protection mechanisms	[KR07] Privacy tool	[KR08] Legal recommendations Report
interoperability	✓	✗	✗	✗
confidentiality	✗	✓	✗	✗
availability	✗	✗	✓	✗
integrity	✗	✓	✗	✗
Data-Integrity	✗	✗	✓	✗
privacy	✗	✓	✓	✓
regulations	✓	✓	✓	✓
eHealth related data	✗	✓	✗	✗
PKI	✓	✗	✗	✗

3.2 Results from the survey

According to an ENISA report[38] it is common to have incidents in eHealth systems. Several breaches have been reported in different States, and these kinds of systems are becoming more vulnerable due to various reasons: level of exposure, flexibility to access medical information across countries, and to manage information security. Different countries define different critical assets, and therefore there are different critical eHealth services. In order to prioritize which services and assets are going to be tackle by SHIELD project, we need to prioritize them.

In this sense we have carried out a survey among the SHIELD partners in order to identify security objectives and security challenges in their current eHealth systems. (survey: https://docs.google.com/forms/d/1f0D2PaOVKhVdPJOGLD33ml_RGR9IFNARzu8TNTkdk_Y/edit). These results represent a first iteration, and it will be enhanced with further questions and other respondents. This survey will be circulated periodically beyond the consortium in order to refine the results.

According to this survey the most important security challenges in eHealth infrastructures and systems are the following:

- System availability
- Lack of compliance and trust, data integrity, Access control and authentication
- lack of interoperability

With respect to which security objectives are the most important according to their priorities, respondents answered:

- Access control
- Network security
- Risk management

The following figures represent the four major priorities identified by this survey. Figure 2 represents health information system, and respondents agree that preserving security in this kind of systems is crucial. Figure 3 and Figure 4 are related to data repository. 56,5% of respondents consider of high priority clinical data repositories. Data access and storage are some of the SHIELD project and they are going to be treated during the project. This includes clinical data and patient health records. ePrescription service (Figure 5) is a relevant service and it is being considered in the OpenNCP architecture.

What also needs to be acknowledged when it comes to challenges is the cultural nuances when it comes to data belonging to a person. Processing, accessing or using one's personal data for whatever purpose that is often brings about apprehension.

The introduction of technologies to solve these challenges however can be frowned upon, so it is important that the challenges we solve are challenges, which want to be solved. In the first instance, focussing on three countries to demonstrate the advantages that can arise from the use of the SHiELD tools already demonstrates a commitment from 3 distinct and EU health authorities to explore how data can be used and secured.

The challenges faced in regards to eHealth are diverse and depending on who the stakeholders are they can be often contradictory. This document very much focusses on specific tools and services, but what also needs to be acknowledged is the stakeholder view of the challenges faced within this

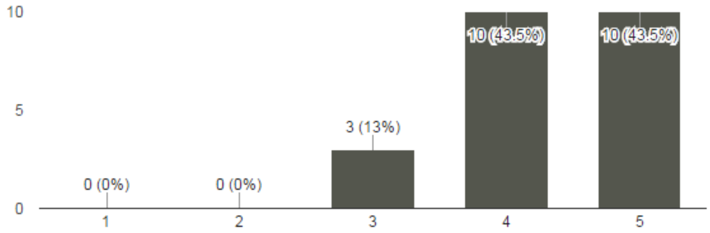

Figure 2: Health information system priority

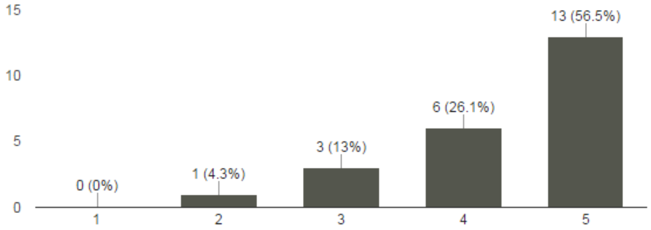

Figure 3: Clinical data repositories priority

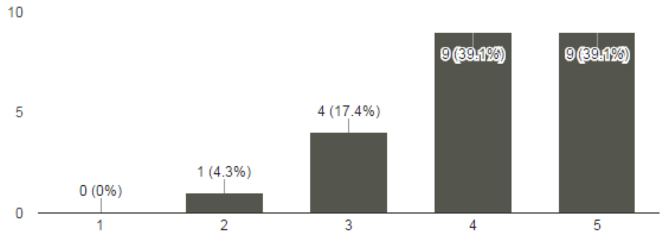

Figure 4: Patient Health Record service priority

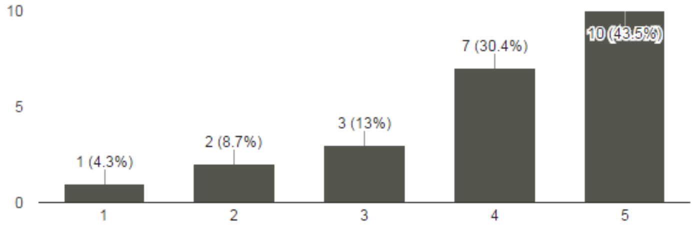

Figure 5: ePrescription service priority

4 Conclusions

This deliverable provides qualitative and quantitative studies for identifying the eHealth challenges for the SHIELD project. As result of the previous sections we can conclude some security challenges to be addressed by the SHIELD project for the eHealth domain. These challenges do not differ too much from traditional software security challenges, but In addition we are taken into account some of the latest European projects results. As summary these challenges are:

- Interoperability: there is still some interoperability issues when patients travel abroad and want to access to their prescriptions and clinical data. In particular, this is dealt with by CEN Technical Committee TC 251 'Health informatics' and ISO TC 215 'Health ICT' as well as the Interoperability Working Group of EHTEL, the association of European health telematics providers (e.g., concerning OpenNCP).
- Confidentiality: it is crucial to limit access to some medical data.
- Availability: patients and medical doctors should access to medical trials and results at any time
- Integrity: the system should be accurate and consistent all the time
- Data-Integrity: as a subset of the previous challenge, data should be accurate and consistent among systems and across countries.
- Privacy: which aspects should be handled in a way that promotes patients' privacy is still a pending task. In particular, CEN/TC 251/Working Group I started a standards project related to privacy by design in the development of eHealth products and services.
- Regulations: this is a domain highly regulated and countries have their own approaches and laws. However, the General Data Protection Regulation 2016/679 provides a single European piece of legislation for the protection of patients' data and their privacy as well as the free flow of data across national borders between healthcare providers.

- eHealth related data: it is relevant to identify which data is going to be treated. Not all data is relevant or is going to be managed within the SHIELD project. However it is important to identify them in order to set security measures.
- PKI: Public Key Infrastructure is a traditional approach and it is used in several countries and systems. We need to take into account this kind of infrastructure in order to identify gaps and potential improvements.

This document will be used as the base for both the in depth requirements analysis for SHIELD (D2.2 Shield Requirement Analysis) as well as setting the main pillars for the SHIELD architecture detail design (D2.3 SHIELD architecture).

5 References

[1] K. Bourquard, F. Le Gall, and P. Cousin, "Standards for Interoperability in Digital Health: Selection and Implementation in an eHealth Project," in *Requirements Engineering for Digital Health*, S. A. Fricker, C. Thümmler, and A. Gavras, Eds. Cham: Springer International Publishing, 2015, pp. 95–115.

[2] C. George, D. Whitehouse, and P. Duquenoy, "Assessing Legal, Ethical and Governance Challenges in eHealth," in *eHealth: Legal, Ethical and Governance Challenges*, C. George, D. Whitehouse, and P. Duquenoy, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 3–22.

[3] F. Rahman, I. D. Addo, S. I. Ahamed, J.-J. Yang, and Q. Wang, "Privacy Challenges and Goals in mHealth Systems," in *Advances in Computers*, vol. 102, Elsevier, 2016, pp. 47–62.

[4] R. Vargheese and P. Prabhudesai, "Securing B2B Pervasive Information Sharing between Healthcare Providers: Enabling the Foundation for Evidence based Medicine," *Procedia Comput. Sci.*, vol. 37, pp. 525–530, 2014.

[5] J. Hu, H.-H. Chen, and T.-W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Comput. Stand. Interfaces*, vol. 32, no. 5–6, pp. 274–280, Oct. 2010.

[6] N. Gol Mohammadi and M. Heisel, "Enhancing Business Process Models with Trustworthiness Requirements," in *Trust Management X*, vol. 473, S. M. Habib, J. Vassileva, S. Mauw, and M. Mühlhäuser, Eds. Cham: Springer International Publishing, 2016, pp. 33–51.

[7] F. Di Cerbo, N. Gol Mohammadi, and S. Paulus, "Evidence-Based Trustworthiness of Internet-Based Services Through Controlled Software Development," in *Cyber Security and Privacy*, vol. 530, F. Cleary and M. Felici, Eds. Cham: Springer International Publishing, 2015, pp. 91–102.

[8] Smart Open Services for European Patients, "D.3.7.2. FINAL SECURITY SERVICES SPECIFICATION DEFINITION - Congruity-Suitability_analysis," 2010.

[9] Smart Open Services for European Patients, "D.3.7.2. FINAL SECURITY SERVICES SPECIFICATION DEFINITION- Section II - Security Services," 2010.

[10] Smart Open Services for European Patients, "Report on Activities of Expert Groups – 2013 (Security, Clinical and Semantic)," 2013.

[11] OPERANDO-online privacyenforcement, rights assurance and optimization, "D6.9 – Final (MVP) Version of Business Driven Tools," 2016.

[12] OPERANDO-online privacyenforcement, rights assurance and optimization, "D6.2–Initial (Prototype)version of privacy enhanced tools," 2016.

[13] A. Mihovska, S. A. Kyriazakos, M. Mihaylov, and R. Prasad, "Standardization and Innovation for Smart e-Health Monitoring Devices:," 2015, pp. 283–290.

[14] Juan Ramón Troncoso-Pastoriza and Elsa Prieto Pérez, “WITDOM: Empowering Privacy and Security in Non-trusted Environments,” *ERCIM News*, vol. 2016, no. 104, 2016.

[15] B. Suzic, “Securing integration of cloud services in cross-domain distributed environments,” 2016, pp. 398–405.

[16] S. Adibi, Ed., *Mobile Health*, vol. 5. Cham: Springer International Publishing, 2015.

[17] P. Duquenoy, N. M. Mekawie, and M. Springett, “Patients, Trust and Ethics in Information Privacy in eHealth,” in *eHealth: Legal, Ethical and Governance Challenges*, C. George, D. Whitehouse, and P. Duquenoy, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 275–295.

[18] M. Layouni, K. Verslype, M. T. Sandıkkaya, B. De Decker, and H. Vangheluwe, “Privacy-Preserving Telemonitoring for eHealth,” in *Data and Applications Security XXIII*, vol. 5645, E. Gudes and J. Vaidya, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 95–110.

[19] M. Drozdowicz, M. Ganzha, and M. Paprzycki, “Semantically Enriched Data Access Policies in eHealth,” *J. Med. Syst.*, vol. 40, no. 11, Nov. 2016.

[20] F. C. Werlang, R. F. Custódio, and M. A. G. Vigil, “A User-Centric Digital Signature Scheme,” in *Public Key Infrastructures, Services and Applications*, vol. 8341, S. Katsikas and I. Agudo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 152–169.

[21] D. D. He, J. Yang, M. Compton, and K. Taylor, “Authorization in cross-border eHealth systems,” *Inf. Syst. Front.*, vol. 14, no. 1, pp. 43–55, Mar. 2012.

[22] M. Beštek and A. Brodnik, “Interoperability and mHealth – Precondition for Successful eCare,” in *Mobile Health*, vol. 5, S. Adibi, Ed. Cham: Springer International Publishing, 2015, pp. 345–374.

[23] D. Moodley, C. J. Seebregts, A. W. Pillay, and T. Meyer, “An Ontology for Regulating eHealth Interoperability in Developing African Countries,” in *Foundations of Health Information Engineering and Systems*, vol. 8315, J. Gibbons and W. MacCaull, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 107–124.

[24] D. W. Chadwick and A. Basden, “Evaluating Trust in a Public Key Certification Authority,” *Comput. Secur.*, vol. 20, no. 7, pp. 592–611, Oct. 2001.

[25] A. Avramidis, P. Kotzanikolaou, C. Douligeris, and M. Burmester, “Chord-PKI: A distributed trust infrastructure based on P2P networks,” *Comput. Netw.*, vol. 56, no. 1, pp. 378–398, Jan. 2012.

[26] T. H. Lacey, R. F. Mills, B. E. Mullins, R. A. Raines, M. E. Oxley, and S. K. Rogers, “RIPsec – Using reputation-based multilayer security to protect MANETs,” *Comput. Secur.*, vol. 31, no. 1, pp. 122–136, Feb. 2012.

[27] P. Michiardi and R. Molva, “Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” in *Advanced Communications and Multimedia Security*, B. Jerman-Blažič and T. Klobučar, Eds. Boston, MA: Springer US, 2002, pp. 107–121.

[28] S. S. Bhuyan *et al.*, “Privacy and security issues in mobile health: Current research and future directions,” *Health Policy Technol.*, Jan. 2017.

[29] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, “Security and privacy challenges in mobile cloud computing: Survey and way ahead,” *J. Netw. Comput. Appl.*, Feb. 2017.

[30] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, “Security and privacy in electronic health records: A systematic literature review,” *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, Jun. 2013.

[31] D. M. Evans and D. C. Yen, “Private key infrastructure: balancing computer transmission privacy with changing technology and security demands,” *Comput. Stand. Interfaces*, vol. 27, no. 4, pp. 423–437, Apr. 2005.

[32] D. W. Chadwick and A. Basden, “Evaluating Trust in a Public Key Certification Authority,” *Comput. Secur.*, vol. 20, no. 7, pp. 592–611, Oct. 2001.

[33] J. Braun, F. Volk, J. Buchmann, and M. Mühlhäuser, "Trust Views for the Web PKI," in *Public Key Infrastructures, Services and Applications*, vol. 8341, S. Katsikas and I. Agudo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 134–151.

[34] P. Nose, "Security weaknesses of a signature scheme and authenticated key agreement protocols," *Inf. Process. Lett.*, vol. 114, no. 3, pp. 107–115, Mar. 2014.

[35] A. Pasquinucci, "Defeating security with security," *Comput. Fraud Secur.*, vol. 2008, no. 2, pp. 6–9, Feb. 2008.

[36] A. Young, "A weakness in smart card PKI certification," 2003, pp. 30–34.

[37] S. Sabnis and D. Charles, "Opportunities and Challenges: Security in eHealth," *Bell Labs Tech. J.*, vol. 17, no. 3, pp. 105–111, Dec. 2012.

[38] Dimitra Liveri, Anna Sarri, and Christina Skouloudi, "Security and Resilience in eHealth Infrastructures and Services." European Union Agency for Network and Information Security, 18-Dec-2015.

6 Annex 1: Survey schema

Systematic protection of health data against threats and cyber-attacks

Which criteria is the most important to assess criticality of assets?

- Impact to society in case of breach (Likert scale 1 to 5)
- Sensitivity of data (oriented to privacy) (Likert scale 1 to 5)
- Services affected (oriented to security) (Likert scale 1 to 5)
- Financial impact(Likert scale 1 to 5)

eHealth assets

- Which of the following assets are the most important?
- Health Information systems, i.e. the information networks in the hospitals
- Clinical data repositories i.e. the databases in each hospital where information is stored locally
- Authentication server i.e. to perform access control and authentication of users
- Laboratory Information System
- Radiology Information Systems
- Picture Archiving and Communication Systems (PACS), i.e. transferring radiology results
- Electronic Health Record components
- Patient Health Record service
- ePrescription service

Security challenges in eHealth infrastructures and systems

Which do you believe are the most important security challenges in eHealth infrastructures and systems?(see https://tinyurl.com/jxcp3mu for description of each element)

- Systems availability
- Access control and Authentication
- Cross borders incidents

- Incidents management
- Lack of interoperability
- Data integrity
- Network security
- lack of security expertise
- data loss
- Lack of compliance and trust
- Lack of standardization

Which security objectives are the most important according to your priorities?

- Risk Management
- Awareness raising and training
- Business continuity and disaster recovery
- Supplier chain security
- Network security
- Human resource security
- Access control
- Incidents management
- Physical and environmental security
- Compliance with international standards
- Internal and external security audits on a regular basis,

Threats

Do you know any existing threat database?

If yes, which one(s)?

Which threats do you consider the most relevant?