Ref. Ares(2017)3294073 - 30/06/2017

European Security in Health Data Exchange

Deliverable D2.2

SHiELD Requirements Analysis

Editor(s):	James Smedley, Antony Shimmin
Responsible Partner:	AIMES
Status-Version:	Draft
Date:	28-Jun-2017
Distribution level (CO, PU):	CO

Project Number:	GA 727301
Project Title:	SHIELD

Title of Deliverable:	SHiELD Requirements Analysis
Due Date of Delivery to the EC:	30-Jun-2017

Work Package responsible for the Deliverable:	AIMES
Editor(s):	AIMES
Contributor(s):	TECNALIA, Osakidetza, FSCR, LANCS, Stelar, Ibermatica
Reviewer(s):	Xabier Larrucea Uriarte (Tecnalia)
Approved by:	Tecnalia
Recommended/mandatory readers:	All WP's

Abstract:	The objective of this deliverable is to describe the SHiELD use case scenarios, the derived functional and non-functional requirements and finally the technical requirements that SHiELD tools shall comply with. These requirements will serve as input for the development of the WP4 and WP5 tools.
Keyword List:	Use case scenario, functional and non-functional requirements, technical requirements
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	1/05/2017	working draft version	James Smedley, Antony Shimmin (AIMES)
V1.0	30/06/2017	Final document	James Smedley, Antony Shimmin, Eunate, Eleonora, Xabier Larrucea, Jason Mansell

Table of Contents

Table of Contents 4
List of Figures 7
List of Tables 7
Terms and abbreviations 8
Executive Summary 9
1 Introduction 10
1.1 (O1) Systematic protection of health data against threats and cyber-attacks. 10
1.1.1 (KR01): Knowledge base of generic security issues that may affect a system. 11
1.1.2 (KR02): Tool that provides an automated analysis of data structures in order to identify sensitive elements that may be vulnerable to specific threats. 11
1.1.3 (KR03): Security requirements identification tool: 11
1.2 (O2) Definition of a common architecture for secure exchange of health data across European borders 11
1.2.1 (KR04): SHiELD open architecture and open secure interoperability API: 12
1.2.2 (KR05): SHiELD (Sec)DevOps tool: 12
1.3 (O3) Assurance of the protection and privacy of the health data exchange. 12
1.3.1 (KR06): Data protection mechanisms: 12
1.3.2 (KR07): Privacy protection mechanisms: 13
1.4 (O4) To understand the legal/regulatory requirements 13
1.4.1 (KR08): Legal recommendations Report. 13
1.5 (O5) Validation of SHiELD in different pilots across three Member States: 14
1.5.1 (KR09): Pilots: 14
1.5.2 (KR10): Best practices: 14
2 Context for analyzing SHiELD requirements 14
3 Summary actors' descriptions 17
3.1 Human actors (individuals) 17
3.1.1 Patient 17
3.1.2 Health Care Professional (HCP) 17
3.1.3 Application Developers 17
3.2 Institutional actors 17
3.2.1 Health Care Service Providers Organization 17
3.2.2 Health Authorities Institutions 17
3.3 System actors 17
3.3.1 National Contact Point or NCP 17
4 Innovation upon existing epSOS Use Case Descriptions 18
4.1 M13-M24 – Phase 1 18

4.2 M19-M30 – Phase 2 18
4.2.1 Italy – Spain: 18
4.2.2 UK: 19
4.2.2.1 KR 4 and Lancashire Care 19
4.2.2.2 KR 5 and Lancashire Care 19
4.2.3 Osakidetza (Basque Use Case) 19
4.2.3.1 KR05 Shield (Sec)DEVOPS tools 19
4.2.3.2 KR06 Data protection mechanism 19
4.2.3.3 KR07 Privacy Tool 20
4.3 M25-M36 – Phase 3 (KR 9) 20
5 Functional and Non-Functional Requirements 20
5.1 Functional Requirements 20
5.1.1 FR01: Compliance Checklist 21
5.1.2 FR02: HIE Compliant API 21
5.1.3 FR03: DEVOPS community interface 21
5.1.4 FR04: Detection of threats 21
5.2 Non-functional Requirements 22
5.2.1 NFR01: Trust between countries 22
5.2.2 NFR02: Response time 22
5.2.3 NFR03: Availability 22
5.2.4 NFR04: Maintainability 23
5.2.5 NFR05: Portability 23
6 Relationship between use cases and requirements 23
7 Example storyboards 24
7.1 In country data exchange health care-to-health care provider 24
7.1.1 Storyboard number 1 24
7.2 Data exchange between UK health care system and ‘wearable device’ 24
7.2.1 Storyboard number 4 24
7.2.2 Storyboard number 5 25
7.3 Data exchange between Italy and Spain health care systems 25
7.3.1 Storyboard number 6 25
7.4 Tri-jurisdictional data exchange 25
7.4.1 Storyboard number 7 26
8 Legislative National and Pan European Requirements 26
9 Conclusions 28
10 References 29

List of Figures

FIGURE 1 SHIELD GENERAL SCENARIOS 15
FIGURE 2: RELATIONS BETWEEN TDPS AND WORK PACKAGES 15
FIGURE 3 TRADITIONAL DEVELOPMENT PHASES AND THE SHIELD'S RESULTING TOOLS. 16
FIGURE 4 SHIELD GENERAL SCENARIOS, SHIELD ARCHITECTURE AND THE IDENTIFIED TOOLS 16
FIGURE 5 STORYBOARD 6 USE CASE DIAGRAM 25
FIGURE 6 STORYBOARD 7 USE CASE DIAGRAM 26

List of Tables

TABLE 1 TRACEABILITY MATRIX OF KR'S TO BE ADDRESSED 24

Terms and abbreviations

AA	Auditing & Accounting
AC	Access Control
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CENELEC	Comité Européen de Normalisation Electrotechnique
EHR	Electronic Health Record
ETSI	European Telecommunications Standards Institute
EPSOS	European Patients Smart Open Services
GDPR	General Data Protection Regulation
HCP	Health Care Professional
HCPO	Health Care Professional Organisation
IoT	Internet of Things
KR	Key Result
LOPD	Statute Law on Data Protection (LOPD in its Spanish acronym)
LPRES	Lancashire Person Record Exchange Service
N3	NHS National Network
NCP	National Contact Point
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 describe the SHiELD use case scenarios, the derived functional and non-functional requirements and finally the technical requirements that SHiELD tools shall comply with. This document is the result of the first months of SHiELD and its dedline is on month 6 (End Of June 2017), and it has a stong link with the SHiELD architecture (D2.3) and the scenarios descriptions (D6.1) which deadlines are on month 12 (December 2017). Therefore this document reflects a first step towardsthe generic use case descriptions, functional, non-functional and technical requirements of SHiELD's SecDevOps and supporting tools to be developed in the context of WP4 and WP5.

In order to analyse properly the SHiELD requirements and the scenarios at the same time we have analysed how the general scenarios description, the SHiELD work packages and the resulting tools are linked. Readers will find a specific section detailing this process. This section provides a context for analyzing SHiELD requirements.

This document represents the basic requirements at month 6 of the project. These requirements will be refined in D6.1 due in M12.

1 Introduction

SHiELD is a digital security project within an e-health context and will unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges preventing this data being exchanged with those who need it.[1]

Whilst the exchange of health data is already possible, it rarely happens in practice because of the complex informatics and information governance rules making it difficult to ensure the security of the 'end-to-end' process and compliance with data protection laws across different jurisdictions.

SHiELD will generate case studies to address a number of cross-border scenarios, which will include:

- A resident of one EU Member state, visits another EU Member state and requires urgent health care. In order for the health care professional to treat them correctly they will require access to the electronic health record in a 'break-glass' emergency scenario.
- A resident of one EU Member state who has to manage a long term medical condition, recording data via a wearable, requires access to their electronic helath record and wearable database.

These case studies will help to address opportunities for using health data through the development of products, services and guidance on best practice to achieve end-to-end security and data protection compliance in health and health related applications.

The aim of this document is to produce storyboards for each scenario and detail the use cases from a system and security perspective. The detailed use-cases and storyboards will be used to elicit the functional, non-functional and technical requirements.

The general objective of the project is broken down into objectives with key results identified as follows:

1.1 (O1) Systematic protection of health data against threats and cyber-attacks.

Health data can be very sensitive and must be protected to maintain the patient's right of privacy. SHiELD will focus on providing a better protection for health data storage and exchange across borders. The first objective will be to implement a 'security by design' approach to ensure that systems producing, exchanging and using health data are protected 'end-to-end'. SHiELD shall provide support to designers for analysing the possible threats to and vulnerabilities of the data, and support the design of valid measures to protect the data which are compatible with different architectures and with the regulatory requirements in the different jurisdictions in which the (cross-border) end-to-end system is operating. This objective will be implemented mainly in WP4, led by IT Innovation using their experience of semantic modelling and machine reasoning for automated threat identification and compliance verification.
Key Results:

1.1.1 (KR01): Knowledge base of generic security issues that may affect a system.

This knowledge base will capture threats that should be managed by the architecture (supporting objective O2) and regulatory data protection requirements (supporting objective O4). In the context of this objective, it will allow automatic identification of threats and compliance issues in specific end-to-end applications and scenarios using KR03 (see below). The main goal is to ensure that the knowledge base covers all the main types of (malicious and accidental) threats through which health data may be compromised and regulatory compliance requirements for multiple member states.
Success criteria: knowledge base covers general cyber security threats based on a suitable standard threat taxonomy such as RFC4949, plus specific threats arising in health data exchange such as de-anonymisation attacks using weaknesses in data exchange schema, and regulatory compliance requirements for the three member states involved in validation pilots.

1.1.2 (KR02): Tool that provides an automated analysis of data structures in order to identify sensitive elements that may be vulnerable to specific threats.

Having as input the knowledge base developed previously, this tool will analyse the flaws and weaknesses of data structures used for the storage and exchange of especially clinical data, so as to identify sensitive elements that may be exposed to threats.
Success criteria: The analysis will be used during the design phase for the exchange infrastructure and used for the SHiELD pilots to ensure identification of sensitive data. Data identified as sensitive will be traced during the pilots to ensure its privacy and access rights requirements are kept.

1.1.3 (KR03): Security requirements identification tool:

This tool will allow models of end-to-end applications to be created, and security threats and compliance issues affecting that application to be automatically identified. This will be achieved through the application of machine reasoning techniques, which will enable to map security knowledge from KR01 and K02 to specific systems, applications and situations, in order to identify the potential threats that can occur. The tool will then support a process for addressing these in a systematic way by specifying security countermeasures to be used in the deployed application components. This will normally be done in the early stages according to 'security by design' principles, but the tool will also allow modelling of existing systems to support the retrofitting of security measures in legacy systems.
Success criteria: modelling tool allows threats and compliance requirements to be identified, and security measures to address them specified at least an order of magnitude faster than by using conventional methods. The analysis should also be easy to repeat should new threats emerge or regulations change.

1.2 (O2) Definition of a common architecture for secure exchange of health data across European borders.

European patients shall improve their access to their health data and health assistance across Europe. Data exchange shall be available in a securitized way, starting by a secure cloud storage ensuring the other patients' privacy remains untouched as well as the data remains correct. SHiELD shall provide support for a faster and more reliable identification of end-to-end security and data protection requirements along with the means to address them. SHiELD shall address the understanding and demonstration of how new and emerging data protection mechanisms can be used alongside existing mechanisms to protect patient data in

heterogeneous, cross-border systems. This objective will be implemented mostly in WP2, led by Tecnalia based on their expertise in secure cloud and IoT architectures.

1.2.1 (KR04): SHiELD open architecture and open secure interoperability API:

SHiELD architecture will extend previous works carried out by epSOS project and the OpenNCP community. It will include an open specification, enabling other implementers to replicate the SHiELD approach. This open architecture will be accompanied by an open secure interoperability API, which shall be a set of specifications for deriving requirements which will include the security features and will provide data as services to be adapted to citizens´ and health care providers' expectations. Security requirements will take into consideration areas such as consent, data protection, device security and system security. The open specification will allow any member state to adopt the approach and to offer their citizens and health care providers the possibility for accessing their health data from other countries

Success criteria: SHiELD architecture will be implemented and used for the SHiELD pilots to facilitate the exchange of the patients' data. The use of this open specification, extending OpenNCP modules, will provide a common method for different states to access to the previous connected states improving this way the Europeans health assistance while moving through the borders.

1.2.2 (KR05): SHiELD (Sec)DevOps tool:

This result includes on one hand, at development time, a set of architectural patterns to implementing data protection security mechanisms and on the other hand, at run time it will provide security monitoring tools that will alert the operator of the system that a threat is likely to occur, alongside with the patterns that can be applied to solve that threat, which may be dynamically triggered. The SecDevOps approach (which promotes the close collaboration between software development and operation teams) enables to deploy features into production quickly and to detect and correct problems when they occur, without disrupting other services, thanks to its continuous integration, continuous testing and continuous deployment philosophy and accompanying tools. Furthermore, this KR will integrate KR01, KR02, KR03, KR07, and KR09.

Success criteria: Speeding up the process of achieving compliance with data protection regulations in health care, as well as, decreasing the development and operation time of secure-aware systems.

1.3 (O3) Assurance of the protection and privacy of the health data exchange.

While data is exchanged among the different Member States, it is needed to ensure that appropriate measures are taken before, during and after data is exchanged to make sure the data is protected, secured and adheres to privacy regulation. This objective will be addressed mostly in WP5, led by IBM based on their expertise in novel data security mechanisms in PRISMACLOUD.

1.3.1 (KR06): Data protection mechanisms:

A suite of security mechanisms to address data protection threats and regulatory compliance issues in end-to-end heterogeneous systems. This includes (but not limited to) tamper detection for mobile devices, data protection mechanisms, and consent-based access control mechanisms.

Success criteria: Ability to detect tamper in a mobile at a level sufficient to meet ISO/TS 22600*.*

1.3.2 (KR07): Privacy protection mechanisms:

These privacy mechanisms will address different aspects of privacy protection and regulation, both when the data is exchanged and when the data is stored. These include methods to identifying where private and sensitive information is located, as well as anomalies when the data is being exchanged. SHiELD will use and develop methods to mask private sensitive information dynamically on the fly as well as methods able to anonymize data while enabling analysis on the data. This analysis will consider compliance requirements in different jurisdictions such that a superset is identified and that subsets which are required for individual jurisdictions are deliverable. The result will be a privacy protection mechanisms for cross border access monitoring which supports the principles of data ownership and data stewardship.
Success criteria: Incorporating privacy protection mechanisms within the SHiELD architecture to achieve improved protection of personal information as well as compliance with data protection regulations in health care.

1.4 (O4) To understand the legal/regulatory requirements

In each member state, which are only partly aligned by previous EU directives and regulations and provide recommendations to regulators for the development of new/improved regulations. SHiELD aims to highlight the technical and economic barriers which arise when we need to comply with the different states regulations especially across borders. This objective will be implemented in WP3. The work will build on objective O1, using the knowledge base from KR01 in which compliance requirements in different jurisdictions are formally represented to identify equivalences and extract common subsets and a superset covering multiple jurisdictions. This objective will be implemented mostly in WP3, led by Stelar exploiting their involvement in key EU initiatives including CEN/CLC JWG 8 on Privacy Management in Products and Services, CEN/TC 251 Health Informatics – Security and Privacy and ETSI TC CYBER as well as its equivalent body in Germany.

1.4.1 (KR08): Legal recommendations Report.

Set of recommendations that need to be implemented by regulators to create a common regulatory framework where the legal requirements regarding security among the state members are aligned. Recommendations will be based on the actual security requirements of the different legislation and propose a common view with a clear security goal and proposals for compliance. The aim is that the recommendations make a clear state of the goals pursuit making possible that implementations and technologies could evolve but compliance means will remain. The recommendations will take into account the process supported by the threat modeller tool (KR03) as risk-related information and complete the SHiELD (Sec)DevOps toolset of secure architectural design patterns at development time (KR05) as well as the SHiELD masking and anonymisation mechanisms (KR07).
Success criteria: This report covers the legal EU data protection principles such as data minimisation, plus technical privacy measures such as pseudonymisation in response to the specific privacy impact caused by automatic health data exchange. It will specify the obligation of "data protection by design and by default" according to Article 23 of the General Data Protection Regulation (as agreed in 12/2015) for health data exchange, using documents of the Article 29 Working Party on Data Protection (e.g., on EHR) and European technical standardisation of "privacy by design" carried out by CEN and Cenelec (Joint Working Group 8) on the Request M/530 of the European Commission.

1.5 (O5) Validation of SHiELD in different pilots across three Member States:

SHiELD Key Results will be tested and piloted in a series of use cases demonstrating the secure storage of data, secure data exchange across borders or between health care and commercial (e.g. lifestyle) services, and management of potential threats that can occur in both cases. This objective will be implemented in WP6, led by FCSR and driven by all the health care partners.

1.5.1 (KR09): Pilots:

Test implementations deployed in three EU Member States, supporting validation scenarios.
Success criteria: Between the different pilots the project shall address the full coverage of at least 70% of features developed in the project.

1.5.2 (KR10): Best practices:

A report describing lessons learned and best practices for protecting health data based on experiences from the validation tests conducted using pilot systems.
Success criteria: This report will offer eHealth providers a management system covering the security elements of the knowledge base and threat modelling tools (O1), interoperability API and tool (O2), security controls and privacy mechanisms (O3), and legal data protection guidance (O4). The management system will explain the European eHealth providers how to implement the security elements in a systematic way, in order to give them a competitive edge in the market environment.

2 Context for analyzing SHiELD requirements

In order to analyse SHiELD requirements we need to set up a general overview of the project. In this sense we need to identify the links among all work packages, resulting tools and the general scenarios description.

The first step is to figure out how the scenarios are working, and the relationships among the main stakeholders. All use cases are deriving from this figure and the cornerstone is the OpenNCP architecture. Basically, medical doctors are granted to access our SHIELD architecture, and the scenarios are based on the interchange of information among these three OpenNCP instances which are following the European laws (represented by “Authorities” in the Figure 1).

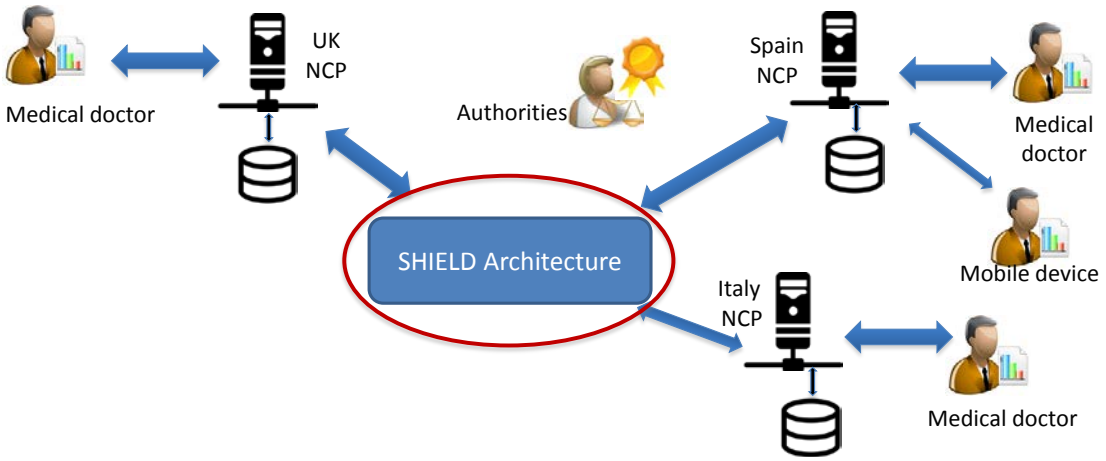

Figure 1 SHiELD general scenarios

The second step is to identify work packages and its relationship with traditional development phases (TDP): Analysis, Design, Deploy and Runtime. Requirements are analysed in this document. So we are not including this phase on this figure because we are analysing the context of the SHiELD project as a whole.

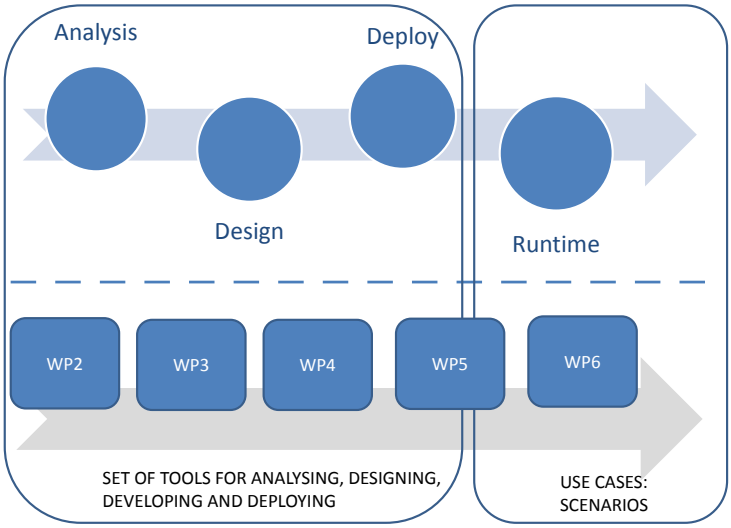

Figure 2: Relations between TDPs and work packages

Most of the results of this project are focused on the analysis, design and deployment of the resulting SHIELD architecture. This architecture is enhanced with security mechanisms at the design time and at the runtime. In fact, the SHiELD phases are:

- Design time: This phase includes the following sub-phases:
  - Analysis
  - Design
  - Deployment
- Runtime: This phase is related with the execution of the scenarios described in D6.1

For each phase there are some resulting tools which are:

- SHIEL architecture
- Legal requirements
- Security Modelling Tool

- Security knowledge base
- Security design patterns
- Data sensitivity
- Consent Manager
- Seure Monitoring

All these tools are described on the work packages descriptions, but our motivation si to show how they are related with the scenarios and what are the expected contributions. This is shown in Figure 3.

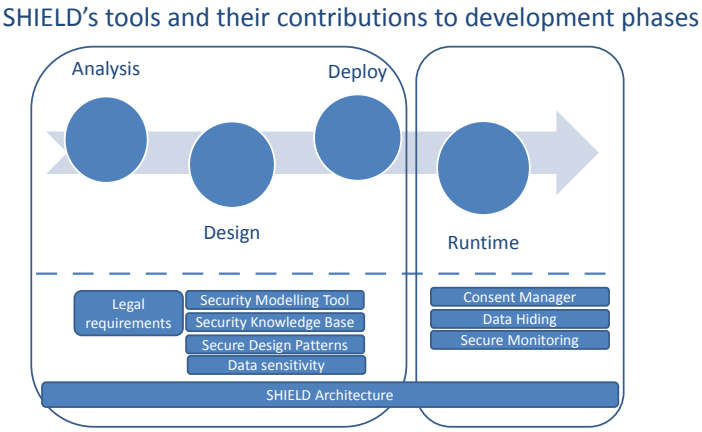

Figure 3 Traditional development phases and the SHiELD's resulting tools.

The third step is to relate the main Figure 1 and Figure 3. Figure 4 summarises the relationships among the main components of the SHiELD architecture, the scenarios (the main interactions and roles involved in scenarios), and the resulting SHIELD tools. In fact, there is not a single tool, nor a single tool chain that is going to be delivered. There is a set of several tools which are focused on different development phases (design time and runtime). Each tool deals with a specific SHiELD contribution.

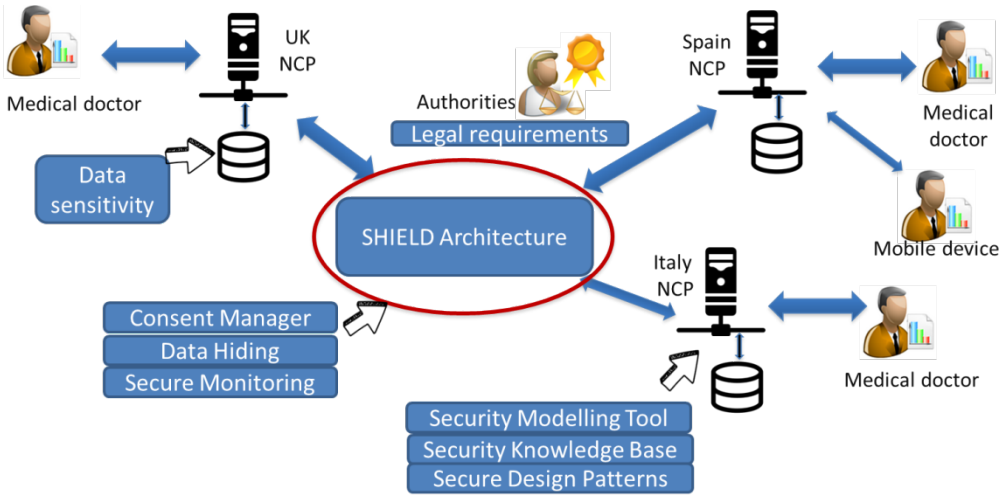

Figure 4 SHiELD general scenarios, SHIELD architecture and the identified tools

3 Summary actors' descriptions

The following actor description are building upon those in section 5.1 Summary actors' description of the the epSOS requirements document [2] [1] and details the actors involved in the Patient Summary service. Given the nature of the proposed SHiELD architecture, using this methodology to detail the requirements is a sensible approach to allow us to detail the initial requirements of the SHiELD use cases.

3.1 Human actors (individuals)

3.1.1 Patient

An individual from country A requesting Health Care in countries A, B or C. This person could need emergency or regular treatment as part of manging a long-term condition.

3.1.2 Health Care Professional (HCP)

It is the HCP who will provide the Health Care. They must be registered with at least one HCPO or to a Health Authority belonging to either country A, B or C that can provide an identification and verification service for him or her. Each country must have a system to validate the access rights of the HCP who requests the healt care record on behalf of the patient.

3.1.3 Application Developers

We anticipate Application Developers to be end users directly of the SHiELD toolset, so that they can create epSOS compliant secure eHealth applications.

3.2 Institutional actors

3.2.1 Health Care Service Providers Organization

These are the organisations to which the HCP is registered with and provide the HCPs a status, identification, an authentication, from which the HCP trust is derived.

3.2.2 Health Authorities Institutions

These are generally public institutions and provide the governance of health services within a given territory in country A, B and C. They assign and assure the status, the function and sometimes the authentication of HCP.

3.3 System actors

(information system or provider such as those used to convey information
across borders):

3.3.1 National Contact Point or NCP

The NCP takes care of external and internal national communication and the semantic mapping between information on either side. The NCPs will be furthermore responsible towards all EU member state partners and within SHiELD between the three partner countries for ensuring that the needed processes are properly implemented in their own networks which is typically where care is prvided. The NCP will deal with the identification of patients and identification and authentication of HCPs. The information is made exchangeable by means of the National Contact Points in the three countries.

4 Innovation upon existing epSOS Use Case Descriptions

We are proposing that SHiELD evaluates the exchange of data through the use of third party applications, but based around an epSOS compliant architecture. The use cases that were tested as part of epSOS were to facilitate the exchange of a patient summary and prescription data. The two main uses cases identified within epSOS were as follows:

-USE CASE 1: an occasional visitor in country B, for example someone on holiday or attending a business meeting. The distinguishing characteristic is that this type of visit is irregular, infrequent, and may not be repeated. This is a type of incidental encounter where the Health Care professional may have no previous record of the person seeking care.

-USE CASE 2: the person is a regular visitor to country B, for example someone who lives in one country but works in another country. The distinguishing characteristic is that this type of visit is regular, frequent, and the person seeking care may be accustomed to using services in the country where he or she works as a matter of personal convenience. This is a type of occasional situation where the Health Care professional may have some information available from previous encounters, therefore the patient could have a medical record locally stored in country B, and maybe a PS in country B plus in country A. If this is the case, both PSs should be available for the HCP to be consulted.

4.1 M13-M24 – Phase 1

For SHiELD Phase 1, all three EU member states will simulate a data exchange within their respective jurisdictions, involving two different hospital facilities. More in detail, staff from Hospital 1 needs to consult an Electronic Health Record of a specific patient, previously created at Hospital 2. The two Hospital Integrated Systems might be different, even if sharing a common storage resource (e.g. server or cloud).

Specifically in relation to Ospedale San Raffaele (OSR), as a practical use case, we will consider both facilities as parts of San Donato Group, the company that OSR belongs to. Details of data storage, management, compression, encryption and/or anonymization, access and sharing will be described in this specific configuration.

These are the Key Results involved and how they will be addressed:

- KR01/KR02: a deep analysis of specific cyber security threats, intentional or unintentional, affecting the scenario according to actual policies of clinical and sensitive data exchange is required
- KR03: we will perform a resilience and dynamic modelling of existing systems involving data storage, access and exchange within the specific use case, in order to identify characteristic threats and quickly apply compliant countermeasures (“at least an order of magnitude faster than by using conventional methods”)

4.2 M19-M30 – Phase 2

4.2.1 Italy – Spain:

In the second phase, both Italian (Lombard - Country A) and Spanish (Basque - Country B) Health Systems are involved. Although the use case is similar in Phase 1, in this scenario we must deal with the jurisdictions of two different countries (Country A & Country B), as well as heterogeneous models of EHRs access and policy of data management. The best outcome should be the achievement of the same (or better) health care service that the patient would

experience in their home country (Country A) whilst visiting another country (Country B) whilst adhering to specific security policies and liability regulation across the two jurisdictions.

These are the Key Results involved and how they will be addressed:

- KR04/KR05: we need to start from epSOS OpenNCP concepts and extend their functionalities through the integration of DevOps tool in order to ensure a security and privacy compliant sharing of health care data across European borders
- KR06/07/08: both data and privacy protection methods are needed to provide a safe, custom and reliable protection of sensitive data, according to liability requirements related to data ownership and stewardship involving different European Countries

4.2.2 UK:

In phase two we will look at how the respective SHiELD key results (as identified below) will aid the development of applications which integrate with the Lancashire Care affinity domain, Lancashire Person Record Exchange Service (LPRES).

Given the fact LPRES is based upon an epSOS architecture, the compatibility of the key results both cross border and otherwise will be tested as a result of this exercise.

4.2.2.1 KR 4 and Lancashire Care

Despite the UK not adopting Open NCP, the Lancashire Care use case utilises the Tiani Spirit [3] Platform (which is based upon epSOS) at the heart of LPRES [4]. Although this solution and methodology is widely adopted across Europe and even the USA, the UK has not historically adopted this, and the Tiani implementation within the Lancashire region has been a resounding and award winning success.

In order for additional services to be layered on this technology, the use of an Open API would allow for easy, scalable and secure access to be provided to LPRES.

4.2.2.2 KR 5 and Lancashire Care

The DevOps paradigm and integration with clinical systems has not been seamless. The use of clinical data within third party mobile applications or services has been a time consuming, laboured and expensive challenge. Even with these challenges, there are over 165,000 eHealth applications [5], and a more, faster, secure and scalable approach to building eHealth services would better enable services to be delivered to the Lancashire region. The ORCHA Initiative [6] demonstrates the size of this market place but given their work within the Lancashire Region is a vehicle for promotion of the SHiELD DevOps tool.

4.2.3 Osakidetza (Basque Use Case)

4.2.3.1 KR05 Shield (Sec)DEVOPS tools

All the tools that are necessary are usually allowed to be installed as long as it does not involve extracting data from servers outside the corporate network. The application can be free or paid if the license is available for use. All users within Osakidetza that have access to clinical data access using their National ID number and a password that has to be actualised every 3 months. SHiELD DEVOPS tools will be used to deploy our OpenNCP architecture.

4.2.3.2 KR06 Data protection mechanism

Osakidetza must comply with the current LOPD until it is updated (the new regulation will come into effect from May 2018) and the new European data protection regulations, GDPR.

Informed consent is necessary and with the new legislation, in the case of special data, informed consent is required.

4.2.3.3 KR07 Privacy Tool

Osakidetza has the highest level of protection and privacy from the outset and from here it will be possible to grant access only to authorized persons.

4.3 M25-M36 – Phase 3 (KR 9)

Phase 3 will provide the opportunity to validate the outputs of SHiELD, including security and data privacy tools, the DevOps community interface, API and knowledge of regulations. We will assemble these within a tri-jurisdictional use case; The three EU member states are Italian (Lombard - Country A), Spanish (Basque - Country B) and English (Lancashire Care – Country C).

The scenario is similar to those in the previous phases, with a HCP in Country A accessing patient summary data from Country B. However this will include an additional interaction for the HCP in Country A who will consult the patient's sensitive data collected by a commercial resource stored in Country C. The data will have originated from a smartphone or wearable based application developed using the SHiELD DevOps community interface, installed on a personal device with SHiELD privacy tools running. SHiELD monitoring tools will be utilised to ensure compliance with end-to-end regulations as the data transfers between the three EU member states.

This will demonstrate that the availability and access to quality data can assist the HCP in providing the patient with personalised medical advice and treatment thanks to the exploitation of non-conventional data sources and that cross-country access does not affect their personal privacy and security, adhering to the definition of standards of best practices. The goal is to guarantee security and user trust even when data are collected by commercial resources. Indeed, IoT based devices are passible of threats, as a result SHiELD privacy tools will be tested to demonstrate the privacy-by-design requirements.

The success of KR09 is expected by implementing this use case according to different configurations in terms of patient's condition (*e.g.,* with chronic illness or with recently surgery), specific jurisdiction constraints (*e.g.,* European GDPR restrictions) and/or functional requirements (*e.g.,* preventative measures for an Emergency Department).

5 Functional and Non-Functional Requirements

The individual elements of the SHiELD tool set will address specific needs which derive from the use case providers and scenarios of which they will test during the lifetime of the project which are highlighted in section 6. Although specific work packages will be designing the services to specification, it's important that the use case providers present views which can be taken on board during the design process.

The following is a high level breakdown and narrative describing specific elements of functionality which would be required by the use cases in order to meet their specific needs.

It is important that the use cases identify their requirements specifically in relation to the key results and provide some high level expectations as to what the key results should deliver at the end of the project. These will be embellished as part of the work in D6.1.

5.1 Functional Requirements

The following requirements are high level to identify needs of the respective use case partners in relation to the SHiELD outputs. We anticipate that in D6.1 which is due in M12 the

requirements will provide more detailed and thorough content. Within the respective technical work packages there will be discussions around specific requirements and information which they need to elicit from the use cases.

We have attempted to standardise this approach by presenting the limited elicited requirements in the form which has been presented in the epSOS project.

We are not differentiating between different use case partners at this stage, as the intention is that the outputs of the project and requirements address common challenges faced in delivering secure epSOS compliant services.

5.1.1 FR01: Compliance Checklist

Requirement FR01	***Compliance Checklist***
Description	Compliance Checklist for National and Pan EU regulations. The API should check for compliance at design and run time.
Associated goals	Design and Deployment of compliant eHealth Services
Actors	Application Developers, Patients, HCP

5.1.2 FR02: HIE Compliant API

Requirement FR02	***HIE Compliant API***
Description	API should be able to aid in the development of exchanging HL7 messages between an HIE compliant service and third party application.
Associated goals	Scalable and More efficient route to market
Actors	Application Developers, Health Informatics Staff

5.1.3 FR03: DEVOPS community interface

Requirement FR03	***DEVOPS community interface***
Description	DEVOPS Community Interface should allow for the ability for application developers to be able to choose individual SHiELD tools which are applicable to their service.
Associated goals	Faster development of compliant eHealth Apps
Actors	Application developers

5.1.4 FR04: Detection of threats

Requirement FR03	***Knowledge Base***
Description	At design time, threats which have not been addressed in the design of an end to end solution should be highlighted.
Associated goals	More secure eHealth services

Actors	Application developers

5.2 Non-functional Requirements

5.2.1 NFR01: Trust between countries

Requirement NFR01	Trust between countries
Description	For the effective exchange of medical information using the Secured Open-NCP of SHILED across borders it is key that the national authorities agree and trust that the usage of the information provided complies with all the regulations of the different countries.
Associated goals	Definition of a common architecture for secure exchange of health data across European borders.

5.2.2 NFR02: Response time

Requirement NFR01	Response time
Description	For the effective deployment of the SHIELD proposed solution, it is key that the response-time across borders, when a user needs to access the information of a patient from a different country is as quick as if it was located in the consulting country
Associated goals	Definition of a common architecture for secure exchange of health data across European borders.

5.2.3 NFR03: Availability

Requirement NFR01	Availability
Description	The ISO 25000 https://www.iso.org/standard/64764.html defines a productquality model defining availability as the degree to which a system, product or component is operational and accessible when required for use
Associated goals	The final OpenNCP architecture should be reliable

5.2.4 NFR04: Maintainability

Requirement NFR01	Maintainability
Description	The ISO 25000 https://www.iso.org/standard/64764.html defines a productquality model defining availability as degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers
Associated goals	More secure eHealth services

5.2.5 NFR05: Portability

Requirement NFR01	Portability
Description	The ISO 25000 https://www.iso.org/standard/64764.html defines a productquality model defining availability as degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another. This includes potentially other aspects such as adaptability and installability which are tightly related to DevOps
Associated goals	Faster development of compliant eHealth Apps

6 Relationship between use cases and requirements

This is a traceability matrix to define at this stage of the project what KRs will be validated within what use cases that we have described above.

Table 1 Traceability Matrix of KR's to be addressed

Key Results	Lancs	FCSR	OSA
KR01	x	x	x
KR02	x	x	x
KR03	x	x	x
KR04	x	x	x
KR05	x	x	x
KR06		x	x
KR07		x	x
KR08			
KR09	X	x	x

7 Example storyboards

This section will detail a list of storyboards. These have been designed to exploit the use cases and ensure validation of the key results and ensure that the objectives can be achieved for the project overall.

7.1 In country data exchange health care-to-health care provider

7.1.1 Storyboard number 1

JS a 27 year old man from Preston is visiting Blackpool to observe the illuminations with his family. During the trip he begins to feel unwell and becomes disorientated and has a fever. He visits the local A&E and during the triage assessment he makes the doctors aware that he is allergic to a certain medication but cannot recall the exact name.

SHIELD: by using the tools within SHIELD the A&E triage nurse could securely consult the patients' record at the GP surgery and retrieve the allergy details and allow the correct treatment to be given.

7.2 Data exchange between UK health care system and 'wearable device'

7.2.1 Storyboard number 4

AS a 26 year old man from Chorley is diagnosed with chronic obstructive pulmonary disease (COPD). The doctor prescribes an app that will allow the patient to self-manage the condition. Whilst using the app the data collected will be shared with the GP surgery and alerts will also be sent if the patient experiences a flare-up or the condition worsens as classified within the app.

SHIELD: by using the tools within SHIELD the patient will be able to self-manage the condition from within the app with the GP/doctor having full access to the entire data recorded within the device and also receiving alerts to any flare-ups encountered by the patient.

7.2.2 Storyboard number 5

EC is a 47 year old man from Lytham and has been diagnosed as obese and at risk of being diagnosed with diabetes. As a result the GP has recommended that the patient undertakes a significant lifestyle change, including increasing their daily step count. To track the patients progress they have prescribed an app to record the daily step count and heart rate monitoring.

SHIELD: by using the tools within SHIELD the patient will be able to record the amount of steps and their heart rate. The data will automatically be synced with the GP system to allow easy review during the next consultation.

7.3 Data exchange between Italy and Spain health care systems

Cross border data exchange involving a patient from Italy who needs treatment while traveling in Spain and vice-versa.

7.3.1 Storyboard number 6

XH is a 27 year old man from Italy is on holiday in the Basque country of Spain. During the trip he begins to feel unwell and suffers a sudden stroke. He visits the local A&E and during the triage assessment the HCP needs to consult the patients EHR to determine the correct pathway and medication for the patient.

SHIELD: by using the tools within SHIELD the A&E triage HCP could securely consult the patients' record at the Italian hospital and retrieve the patients history and allow the correct treatment to be given.

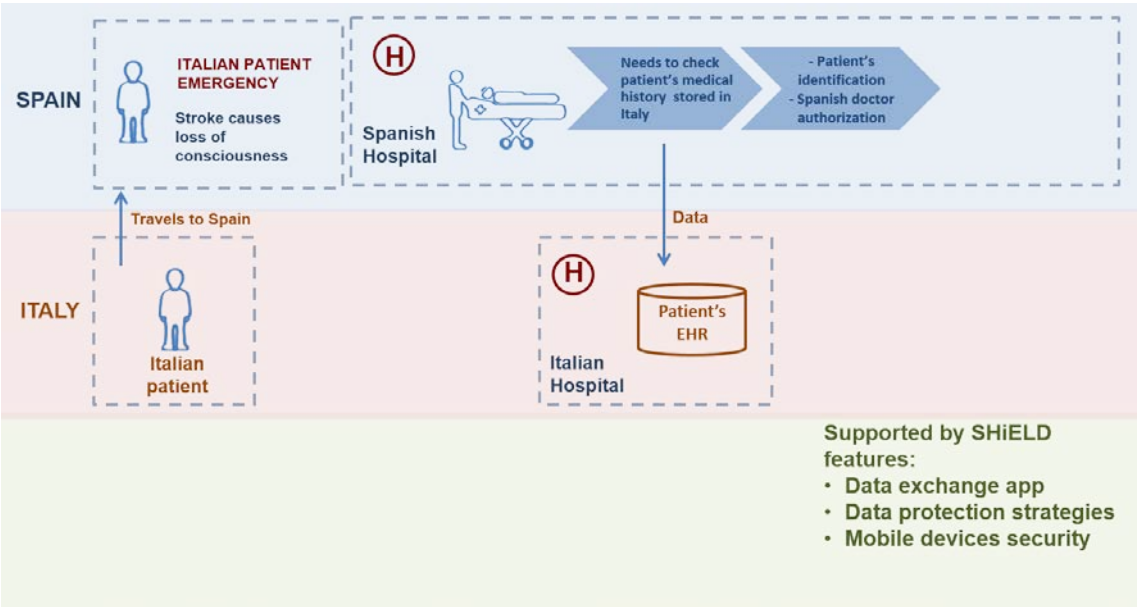

Figure 5 Storyboard 6 use case diagram

7.4 Tri-jurisdictional data exchange

A tri-jurisdictional scenario involving a patient from Spain using a wearable system from the UK who needs treatment while travelling in Italy. And all other clinical cases that need to consult

a clinical history data while the patients are travelling in three countries (Spain, Italy, UK). Emergency and non-emergency cases.

7.4.1 Storyboard number 7

GB is a 32 year old man from Italy and has been prescribed with a mobile smartphone/wearable device to collect vital signs and step counts. Whilst on a cycling trip to Spain, he begins to feel unwell and visits the local hospital. During this visit, the HCP needs to consult the patients EHR and wearable data to determine the correct pathway and medication for the patient.

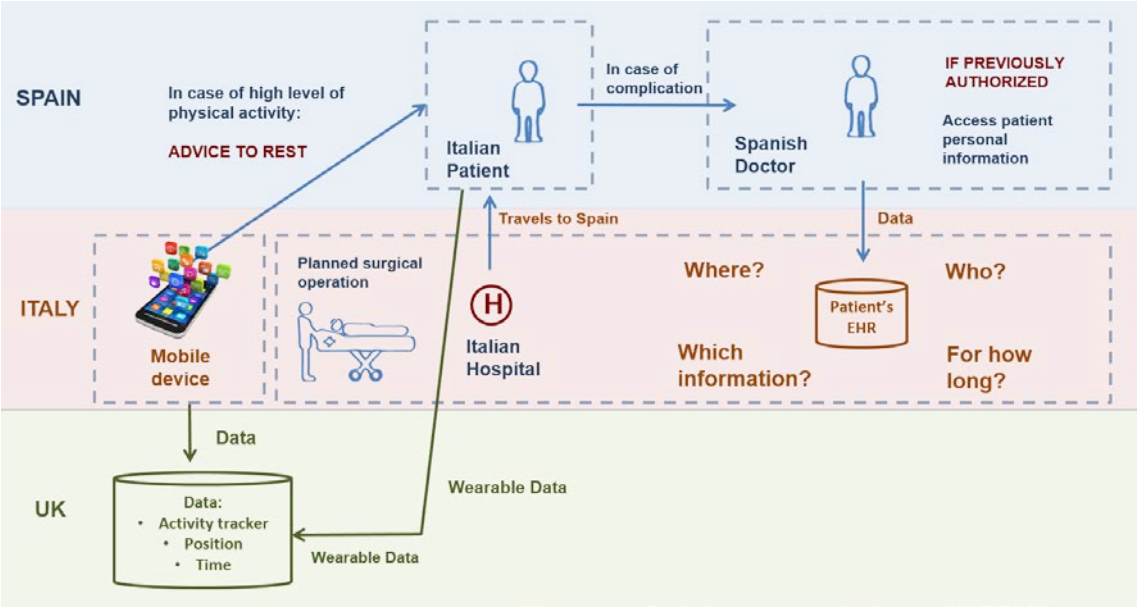

Figure 6 Storyboard 7 use case diagram

8 Legislative National and Pan European Requirements

The legal requirements with the highest priority in terms of privacy and data protection for SHiELD, are defined by the 2016 EU General Data Protection Regulation 2016/679/EU (GDPR). The GDPR does not only have a high impact on the market. It replaces different national laws by a single piece of EU legislation, introduces dissuasive sanctions in case of non-compliance and applies to organisations anywhere in the world as soon as they handle data about people within the EU terrority (see SHiELD deliverable D7.1 'Market analysis'). However the GDPR also includes legal requirements with an impact on the research and technical development of the SHiELD project. On one hand, it defines classic legal data-protection requirements that are also codified under the 1995 European Data Protection Directive 95/46/EC. On the other hand, the GDPR introduces new concepts for legal data-protection obligations.

The classic data-protection requirements consist in the principles of lawfulness, purpose limitation, data minimisation, data security, proportionality, existence of independent supersivory authorities, and so on. In SHiELD, the following classic requirements were identified as having an impact on the design of the technical concepts developed in the SHiELD project (see SHiELD deliverable D3.1 'Report on legal requirements'):

- Data processing must be based on law or consent (lawfulness)
- Data must be accurate and regularly updated (data accuracy)
- Automatic decisions must not be taken for granted without sufficient human verification (profiling prohibition)

- The free movement of personal data in the EU must not be restricted for reasons of data protection (data availability, free movement of data)
- Data must be processed only for specified and non-incompatible purposes (purpose limitation)
- Safeguards for special categories of information (purpose limitation: sensitive data)
- Data must be processed with a level of security appropriate to the risks for the data subjects (data security)
- Data must be processed in a transparent ("who processes what when") manner (data subject rights: transparency)
- Data subjects have the right to know, correct and delete their data (data subject rights: participation)
- The amount of data (data categories) must be reduced as much as possible given the specified purposes (data minimisation: data amount)
- Data must be deleted or data subjects must be (effectively) anonymised as soon as possible given the specified and non-incompatible purposes (data minimisation: retention period)
- Concerning the retention period only for non-incompatible purposes, an element of compliance may be the implementation of pseudonymisation in order to safeguard the rights and freedoms of data subjects (data minimisation: pseudonymisation)
- System user rights must be enforced per “controller” and “processor” (responsibility)
- Data must be processed fairly (fair decision-making)
- Indidviduals have the right to protection of their privacy and personal data (privacy and data protection)
- Data processing must be based on the consent of the person concerned or some other legitimate basis laid down by law (autonomy and lawfulness)
- Individuals must not be treated unequally (non-discrimination)
- Human dignity is inviolable and must be respected and protected (human dignity)
- Individuals have the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices (access to health care)
- A high level of human health protection must be ensured in the definition and implementation of all European Union policies and activities (public health)
- Any limitation on the exercise of the rights and freedoms of individuals must be proportionate (proportionality)
- Precautions must be taken against misuse of technology originally intended for a legitimate use (mission creep, function creep).

New concepts for data-protection obligations introduced by the GDPR comprise the risk-based approach, accountability, data protection by design and by default, certification, data protection impact assessment, right to data portability, right to be forgotten, and one-stop shop, among other things. In SHiELD, the following of those new legal obligations were identified as having the highest priority for 'privacy and data protection by design' in the research and technical development of the SHiELD project (see SHiELD deliverable D3.1 'Report on legal requirements'):

- Controllers must take into account the state of the art and the cost of implementation (risk-based approach: feasibility and reasonability)
- Controllers must take into account the nature, scope, context and purposes of processing (risk-based approach: quality of processing)

- Controllers must take into account the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (risk-based approach: rights and freedoms)
- Controllers must implement appropriate (risk-based approach) measures to be able to demonstrate compliance with the legal requirements (accountability)
- One element of demonstration of compliance may be the implementation of data protection by design
- Another element of demonstration of compliance may be the adherence to codes of conduct or certification schemes
- Measures for demonstration of compliance must be regularly reviewed and updated
- Controllers must implement appropriate (risk-based approach) measures during the time of the determination of the means for data processing (at design time), for meeting the legal requirements (data protection by design)
- An element of compliance may be the implementation of pseudonymisation designed to implement data-protection principles such as data minimisation
- Other elements of compliance may be:
    - Minimising the processing of personal data
    - Pseudonymising personal data as soon as possible
    - Transparency with regard to the functions and processing of personal data
    - Enabling the data subject to monitor the data processing
    - Enabling the controller to create and improve security features

When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations

- The principles of data protection by design and by default should also be taken into consideration in the context of public tenders
- Measures for 'data protection by design' must be regularly reviewed and updated
- Controllers must be able to demonstrate (assess or verify) the effectiveness of the implementation and integration of the measures for 'data protection by design'

9 Conclusions

This document provides an overview of the SHiELD project and how the expected results are connected with the general scenarios descriptions. This is a critical aspect for analysing which requirements are involved in SHiELD. In addition, we have identified that there is a real need for the KR's across the use cases, and we have detailed at a high level how the consortium intends to properly validated the results of the project. This will be achieved by creating a number of ficitiuous scenarios (3) over the lifetime of the project, with the final scenario addressing KR09.

The requirements of the use case providers will be further detailed in D6.1, and the respective technical work packages will work indepdently to gather defined specific requirements for their tools.

Input into this document from a requirements definition perspective has been provided mainly by the use case providers, and although technically minded the information provided

has only been given from one perspective. Therefore the technical work packages must focus their requirements elicitation excercises on who they perceive to be the end users of the SHiELD outputs, rather than the beneficieries of the outcomes.

10 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.