ALFRED

Personal Interactive Assistant for Independent Living and Active Ageing

WP9 – Impact

D9.6.2 Standardization, Policy and Ethical issues

Deliverable Lead: IESE

Contributing Partners: ATOS, TUDA, ASC

Delivery Date: 09/2015

Dissemination Level: Public

Version 1.0

This second version of the Standardization, Policy and Ethical issues builds on previous D9.6.1. This document summarizes the standards, ethical and policy issues that are relevant to ALFRED's implementation.

SEVENTH FRAMEWORK PROGRAMME

Document Status	
Deliverable Lead	Esther Vizcaino, Marta Ribeiro, Cesar Mediavilla, Michael Krummen, Tim Dutz
Internal Reviewer 1	Florian Feldwieser, CHA
Internal Reviewer 2	Jorge Doménech, AITEX
Type	Deliverable
Work Package	WP9: Impact
ID	D9.6.2 Standardization, Policy and Ethical issues
Due Date	30.09.2015
Delivery Date	30.09.2015
Status	For Approval

Note

This deliverable is subject to final acceptance by the European Commission.

Disclaimer

The views represented in this document only reflect the views of the authors and not the views of the European Union. The European Union is not liable for any use that may be made of the information contained in this document.

Furthermore, the information is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user of the information uses it at its sole risk and liability.

Project Partners

Ascora GmbH, Germany	Atos Spain sau, Spain
Worldline, Spain	Charité - Universitätsmedizin Berlin - Department of Geriatrics, Germany
Asociacion de Investigacion de la Industria Textil, Spain	Technische Universität Darmstadt, Germany
National Foundation for the Elderly, The Netherlands	Talkamatic AB, Sweden
E-Seniors, France	TIE Nederland N.V., The Netherlands
IESE Business School, Spain	

Executive Summary

This document is the second report of the three due as part of task 9.6, Standardization, Policy and Ethical issues. The report summarizes the standards, ethical and policy issues relevant to ALFRED's deployment that are and/or will be implemented.

The ALFRED solution will provide a mobile virtual butler to enhance autonomy, social activity and health status of older persons. ALFRED is highly interdisciplinary in character and functions (medical, technological, social and business-related functions) and therefore requires a high level of standardisation for the integration and interoperability of its four pillars.

The enforcement of standards in the design of the ALFRED solution is essential to enable interoperability among system components and potentially with other systems within an eHealth based integrated healthcare sector. This document describes the standards used within the ALFRED project to become an interoperable solution.

In addition, a review of the European Regulatory Context in the field of mobile health was conducted. After the review, we can conclude that there is an urgent need of developing a comprehensive regulatory framework on mHealth to exploit its full potential, especially regarding data protection issues.

Finally, this document highlights the main ethical issues arising during ALFRED deployment, particularly on user involvement. ALFRED will require access to the user's personal and health related information. Hence, recommendations to ensure data protection and privacy are provided.

This report constitutes a roadmap for the development of ALFRED solution and we will update it throughout the whole duration of the project. This will allow us to adapt ALFRED to the technical evolution and to reflect changes in the regulatory and market environment. Future updates will be provided in the subsequent deliverable of 9.6 at the end of the project.

Table of Contents

List of Tables

1 Introduction

ALFRED – Personal Interactive Assistant for Independent Living and Active Ageing – is a project funded by the Seventh Framework Programme of the European Commission under Grant Agreement No. 611218. It will allow older people to live longer at their own homes with the possibility to act independently and to actively participate in society by providing the technological foundation for an ecosystem consisting of four pillars:

- **User-Driven Interaction Assistant** to allow older people to talk to ALFRED and to ask questions or define commands in order to solve day-to-day problems.
- **Personalized Social Inclusion** by suggesting social events to older people, taking into account their interests and their social environment.
- A more **Effective & Personalized Care** by allowing medical staff and caretakers to access the vital signs of older people monitored by (wearable) sensors.
- **Physical & Cognitive Impairments Prevention** by way of serious games that help the users to maintain and possibly even improve their physical and cognitive capabilities.

1.1 ALFRED Project Overview

One of the main problems of western societies is the increasing isolation of older people, who do not actively participate in society either because of missing social interactions or because of age-related impairments (physical or cognitive). The outcomes of the ALFRED project will help to overcome this problem with an interactive virtual butler (a smartphone application also called ALFRED) for older people, which is fully voice controlled.

The ALFRED project is wrapped around the following main objectives:

- To empower older people to live independently for longer by delivering a virtual butler with seamless support for tasks in and outside the home. This virtual butler (the ALFRED app) aims for a very high end-user acceptance by using a fully voice controlled and non-technical user interface.
- To prevent age-related physical and cognitive impairments with the help of personalized serious games.
- To foster active participation in society for the ageing population by suggesting and managing events and social contacts.
- And finally, to improve caring by offering direct access to vital signs for carers and other medical staff as well as alerting in case of emergencies. The data is collected by unobtrusive wearable sensors monitoring the vital signs of ALFRED's users.

To achieve its goals, the project ALFRED conducts original research from a user centred perspective and applies technologies from the fields of Ubiquitous Computing, Big Data, Serious Gaming, the Semantic Web, Cyber Physical Systems, the Internet of Things, the Internet of Services, and Human-Computer Interaction. For more information, please refer to the project website at http://www.alfred.eu.

1.2 Deliverable Purpose, Scope and Context

ALFRED, like other AAL applications, is highly interdisciplinary in character and functions (medical, technological, social and business-related functions). It requires a high level of security for the management of personal data and standardisation for the integration and interoperability of its different pillars. It is important to define technical specifications to ensure interoperability and security in the very early phases of development.

The purpose of this deliverable is to describe the standards that are used or will be used in ALFRED and the current regulatory framework that applies to ALFRED exploitation. The deliverable also draws attention to the ethical issues related with the management of end users' data when using ALFRED. The European Commission puts a strong emphasis on ethical issues related to projects and products that involve end-users and personal data. The collection, storage and use of personal and medical data including details of the patient's vital signs, data about social contacts, domestic activities and sickness data implies to implement specific processes to ensure data protection and privacy. As such, ALFRED will dedicate time towards safeguarding the ethical issues (guidelines, informed consent, etc.) during the project.

1.3 Document Status and Target Audience

This document is listed in the Description-of-Work (DoW) as "public", as it provides general information about the goals and scope of the ALFRED project and can therefore be used by external parties in order to get according insight into the project activities.

While the document mainly aims at the project's contributing partners, this public deliverable can also be useful for the wider scientific and industrial community. This includes other publicly funded research and development projects, which may be interested in collaboration activities.

1.4 Abbreviations and Glossary

A definition of common terms and roles related to the realization of the ALFRED project as well as a list of abbreviations is available in the supplementary document “Supplement: Abbreviations and Glossary”, which is provided in addition to this deliverable. Further information can be found at http://www.alfred.eu.

1.5 Document Structure

This deliverable is broken down into the following sections:

- Chapter 1 provides an introduction for this deliverable including a general overview of the project, and outlines the purpose, scope, context, status, and target audience of this deliverable.
- Chapter 2 describes the standards that are used or will be used in the ALFRED project. It also describes some recommendations for the ALFRED implementation phase
- Chapter 3 focuses on the current European policy framework that will have influence on the exploitation of ALFRED products. In particular, on data protection issues.
- Chapter 4 reviews the ethical issues that apply to ALFRED. Due to ALFRED access to its user’s personal and health related information, special consideration needs to be given to protect user’s personal and medical information and privacy.

2 Standards, Interoperability and Certification Schemes

The medical app market is evolving rapidly; there are thousands of apps available from a range of app stores[1]. It is essential to establish some quality criteria to help healthcare services, payers and end users to make a choice. Due to the nature of ALFRED, a significant amount of data will be exchanged between systems and components. Since the final goal is that third parties develop apps for ALFRED platform, interoperability is a key requirement for the success and long term sustainability of ALFRED. Standardised interfaces between systems and (current and future) components are therefore mandatory.A review on standards relevant for ALFRED was performed in D9.6.1. Based on this review and in partners experience and aims, the current report collects the standards, guidelines or initiatives identified by the partner and that are (or will be) use in ALFRED components.

2.1 Standardization within ALFRED

Following previous work of D9.6.1, the aim of this subsection is to define standards that are used or will be used and addressed in the ALFRED project. The standards have been grouped by domains: usability, accessibility, connectivity, safety and trust and privacy; although in some cases one standard could apply to more than one of the domains.

2.1.1 Usability

Usability is a quality attribute that assesses how easy user interfaces are to use. The word "usability" also refers to methods for improving ease-of-use during the design process. Usability is defined by 5 quality components:

- Learnability: How easy is it for users to accomplish basic tasks the first time they encounter the design?
- Efficiency: Once users have learned the design, how quickly can they perform tasks?
- Memorability: When users return to the design after a period of not using it, how easily can they reestablish proficiency?
- Errors: How many errors do users make, how severe are these errors, and how easily can they recover from the errors?
- Satisfaction: How pleasant is it to use the design?

The consortium has implemented a methodology during the development phase – which includes the involvement of the end-users - to ensure the final usability and usefulness of the technology.

Wizard of Oz: more than a standard, it's a well-established method for gathering end user feedback, frequently used for prototyping and data collection. In ALFRED, end-users have been involved at the early stage of the project, in the definition of the requirements. In addition, there is a pilot only focused on the Usability (led by the National Foundation for the Elderly in the Netherlands). The initial usability study has been performed from M1 and it will be performed iteratively in parallel with the technological development on the user driven interaction assistant and personalized social inclusion, guaranteeing a continuous

[1] See for example "Consumer Health Apps For Apple's iPhone report" Mobil Health News Report (2011)

user involvement in the project. The pilot study will use the different prototypes (low, mid and high fidelity prototypes) to test with approximately 5-10 older adults. Usability (as well as accessibility) will be also checked in the other two pilots. D8.1 and D8.1.2 gave specific details on how this methodology has been used.

2.1.2 Accessibility

Taking into account ALFRED objectives, accessibility is a key issue for the consortium. Therefore, the project should adhere to most important standards and guidelines on accessibility, including the related to a wide range of disabilities, including visual, speech, language learning, cognitive.

WCAG: Web Content Accessibility Guidelines (WCAG) 2.0, make content more usable by older individuals with changing abilities due to ageing and improve usability for users in general.

2.1.3 Connectivity

The following standards concern mainly the interoperability with other products or between back-end components and their clients in the ALFRED system. These standards enhance the interoperability between components, making easy to add or remove components in a plug and play approach.

IEEE 802.15.1: this standard dealt with Bluetooth connectivity with fixed, portable and moving devices

BT-LE: Bluetooth Low Energy intendeds to provide considerably reduced power consumption and cost while maintaining a similar communication range.

REST: Representational State Transfer: also known as REST (Fielding, 2002), is an architectural style. It prescribes rules that describe an abstract model of web-architecture. This architectural style is significantly based on the Hypertext Transfer Protocol (HTTP) and, in fact, it is characterized by the very same principles. In a very simplistic definition, REST is a structured way of using HTTP. The principles of the architecture design are the following:

- The system must be Client-Server (Layered System). In this way, based on the separation-of-concerns, client is not concerned with specific details of the server. The layers implemented on the services side are not visible to the client. In this sense, the client cannot distinguish the end server from possible intermediary services contacted along the way.
- It must be Stateless. No state is kept between client and server. This is a strong requirement which is eventually relaxed in many real implementations where authentication and sessions are required.
- It must be Cacheable. In the system clients can cache responses which when correctly implemented and managed reduces client-server interactions.
- The availability of a Uniform Interface between client and server makes it possible for both sides to evolve independently so far the interface is followed. The Uniform Interface is also significantly based on the HTTP protocol. In fact, it is characterized by the use of URIs and data format like HTML, XML or JSON.

REST applications stick to all aforementioned principles.

WSDL: Web Services Description Language: also known as WSDL (WSDL, 2007), is an XML format that is used to describe several services characteristics. The main properties that can be described are the location of the service, which identifies where the application can be found; the operations that the service is able to perform and the corresponding messages, protocols used and so on. Since is written in XML, this description can be processed at runtime and accordingly, dynamic requests for the specific operations can be requested.

WADL: Web Application Description Language, also known as WADL, is an XML format that is used to describe services. The main properties that can be described are the location of the service, which identifies where the application can be found; the operations that the service is able to perform and the corresponding messages, protocols used and so on. Since is written in XML, this description can be processed at runtime and accordingly, dynamic requests for the specific operations can be requested. WADL is fully REST compliant.

JSON: JavaScript Object Notation (JSON) is a lightweight format to exchange data, based on the ECMA 404 standard. This is a programming language independent format that is used to exchange data. It is built on collection of name-value pairs and ordered list of values. With this representation, all available data-structures can be easily described. It is also protocol independent and can be used as payload to represent data in all communication technologies. It is fast to process and easy to manipulate. The Personalization Manager's services will exchange data with clients using JSON format.

2.1.4 Safety and Trust

Developed and implemented technologies should comply with the requested directives and recommendations regarding Safety, Trust and Quality. Further on, other quality control standards and production management systems may be used by manufactures at their sites.

Radio Equipment Directive (RED) 2014/53/EU: new products placed on the market must be compliant with this Directive after June 2016.

Restriction of the use of certain hazardous substances (RoHS) Directive 2011/65/EU: related to the restriction of the use of certain hazardous substances in electrical and electronic equipment.

2.1.5 Data Protection and Security (Privacy)

During the project, different standards and recommendations for the protection of individuals with regard to the processing of personal data and on the free movement of such data will be implemented.

AES: Advanced Encryption Standard is a symmetric block cipher used to protect information and is implemented in software and hardware to encrypt sensitive data.

RFC-2617: protocol for digest access authentication. This can be used to confirm the identity of a user before sending sensitive information.

2.1.6 Other Technical Standards for Development

Standards, norms and recommendations used during the entire development phase with different aims (facility the collaboration, as a basis for other standards/recommendations, etc.).

XML: Extensible Markup Language format for dialogue-enabled app development. XML is an established file format understood by most developers and supported by most editors.

JSON: JavaScript Object Notation is a lightweight format to exchange data, based on the ECMA 404 standard.

WSDL: Web Services Description Language (WSDL, 2007), endorsed by W3C, is a XML-based interface definition language that is used for describing the functionality offered by a web service.

2.2 ALFRED Contribution to European Standardization

The ALFRED project aims to contribute to European standardization efforts by establishing the foundation for a metadata description format for digital serious games.

As described in D7.1.1, serious games are games that have a purpose beyond mere entertainment. Within the ALFRED project, for example, such games are utilized to increase the user's motivation to be physically and/or mentally active – an important part in preventing physical and mental decline. In ALFRED, only five of such games will be developed and as such, the selection of a game that fits a specific user's interests and abilities is not a significant challenge. However, when third party developers will eventually start developing additional (serious) games for the ALFRED open platform, this limited number of games may rapidly grow and as such, it will become increasingly difficult for an end-user to pick the "right game" from the set of all available games.

In response to this problem, the ALFRED consortium has started working on a metadata description format for serious games, as described in the deliverables D7.1.1 and D7.1.2. This effort is motivated by the vision of establishing a uniform machine-readable formalism that allows domain experts to describe the characteristics of a given serious game, such as the physical and/or cognitive requirements for playing this game, the expected benefits for the user's health and wellbeing, the number of supported players, etc. Based on this formalism, an automatic selection mechanism will then choose those games from the list of all available games that match the user's wants and needs. In order for this selection mechanism to function as intended, there needs to be one metadata file for every game available and additionally, there also needs to be a similar profile for the user that captures her abilities and interests.

Technically, the metadata description files are markup language text files, such as HTML or XML files, but more closely related to HTML than XML, as they make use of a set of predefined tags. It is the standardization of these tags on a European level that the ALFRED consortium aims for. Only through this standardization, game search engines would be able to reliably browse various game databases located around the globe and to automatically select those games that are suited best to the user.

As of October 2015, the metadata description format is still being refined and as such, no actual standardization efforts have yet been made. However, once the conceptualization

of the formalism is completed and successfully evaluated within ALFRED (being the basis for the Game Manager's game suggestion mechanism), the ALFRED consortium plans to publish the format and to actively promote its standardization.

2.3 Requirements and Recommendations for ALFRED

ALFRED is an API solution, making some components available to third parties. It will be very important that apps included in the ALFRED solution are accurate and reliable. Currently there are no clear recommendations or certifications (from any official EU body) to ensure that apps provide credible content and contain safeguard for user data. There is a lack of solutions providing a comprehensive evaluation of the quality and effectiveness of mobile health apps, and translating this information to healthcare providers and end users in a simple and transparent way. Despite this lack of official regulations, there are several on-going proposals for developing health app certification programmes, which begin to highlight the need of quality guidelines and recommendations on mobile health apps. They are described in the following paragraphs.

The UK National Health Service (NHS) has launched the Health App Library2, a library of apps that has been endorsed by the NHS for patients which can be prescribed by doctors. All submitted apps meet three minimum requirements:

- Apps are relevant to people living in England
- Apps comply with data protection laws
- Apps comply with trusted sources of information

The US Food and Drug Administration (FDA) regulates some specific apps. They released the Mobile Medical Applications Guidance for Industry and Food and Drug Administration on 2013 [FDA13].The guide explains the agency vision of mobile medical apps as devices.

myhealthapps©[3] assesses apps from user's perspective. The apps featured on the site have been approved and reviewed by independent healthcare communities, including individual patients, patient groups and not-for-profit organisations at both local and international level.

Recently, the Royal College of Physicians (RCP) in UK published a factsheet [RCP15] on the use of medical apps, to help doctors protect patients. Although they have no plans to endorse particular medical apps they are involved with other organisations in establishing quality criteria for apps.

Mobile health Global[4] hosts a catalogue of health apps that includes more than 250 apps for managing health, classified by clinical area and area of interest. All of them have been recommended, certified or created by medical institutions and organizations, which guarantees their quality and reliability.

The Health Quality Agency of Andalusia has developed a guide of recommendations[5], in Spanish, for the design, use and evaluation of mobile health applications. The recommendations focus on the following areas:

[2] http://apps.nhs.uk
[3] http://myhealthapps.net
[4] http://www.mobilehealthglobal.com/showroom/catalogue/ca_apps
[5] http://www.calidadappsalud.com

- Design and usability
- Content and functionality
- Confidentiality and data privacy
- Technological requirements

Some of the most relevant recommendations that might also apply to ALFRED are summarized in Table 1.

Table 1: Recommendations developed by Health Quality Agency of Andalusia for the design, use and evaluation of mHealth apps [ACSA12]

Group	Criteria	Standard
Design and Pertinence	Pertinence	1. The health app clearly defines its functional scope and the purpose for which it was developed, identifying the groups to which it is addressed and the objectives pursued with respect to these groups.
	Accessibility	2. The health app follows the principles of universal design, as well as standards and references from accessibility recommendations.
	Design	3. The health app complies with the design standards and recommendations set out in the official guidelines provided by the different markets.
	Usability	4. The health app has been tested with potential users prior to its availability to the public.
Information Quality and Safety	Adaptation to the audience	5. The health app is adapted to the type of targeted audience.
	Transparency	6. The health app provides transparent information on the identity and location of their owners.
		7. The health app provides information on sources of funding, promotion and sponsorship, as well as potential conflicts of interest.
	Authorship	8. The health app identifies the authors / responsible parties for its content, as well as their professional qualifications.
	Information Update/Reviews	9. The health app contains the last review date for the published material.
		10. The health app notifies the users of updates that affect or modify content or functionality about health or any other sensitive data.
	Contents and sources of information	11. The health app is based on one or more reliable sources of information and takes into consideration the available scientific evidence.
		12. The health app provides concise information about

		the process used to select its contents.
		13. The health app is based on ethical principles and values.
	Risk management	14. The health app identifies possible risks on patient safety
		15. Appropriate actions are taken on possible known risks and adverse events
Service Provision	Technical Support / Help	16. The health app has a help section.
		17. The health app provides technical support, ensuring a certain response time for the user.
	eCommerce	18. The health app describes the terms and conditions regarding the marketing of their products and services.
	Bandwidth	19. The health app makes efficient use of communication bandwidth
	Advertising	20. The health app notifies of the use of advertising and how to disable or skip it
Privacy and Confidentiality	Data protection	21. Prior to its download and installation, the app declares what user data is collected and for what purpose, its policies on data access and processing, as well as possible trade agreements with third parties.
		22. The health app describes which personal information is recorded, in a clear and understandable terms and conditions.
		23. The health app preserves the privacy of the information recorded, contains explicit consent of the user and warns about the risks of using mobile health applications through public networks
		24. If the app collects health or health information exchanges or any other particularly sensitive data on its users, it ensures the appropriate security measures.
		25. The health app informs users when accessing any device resources, user accounts or social networking profiles.
		26. The health app ensures at anytime the right of access to recorded information, as well as to any update or change in its privacy policy.
		27. The health app implements measures to protect children in accordance with current legislation.
	Security	28. The health app does not contain any known

		vulnerability or any type of malicious code.
		29. The health app describes its security procedures to prevent unauthorised access to personal information collected, as well as access restriction to protected data by third parties.
		30. The health app offers data encryption mechanisms for information storage and exchange, and password management mechanisms.
		31. The health app states the terms and conditions of cloud services used, including the security measures for this purpose

Further work is needed to develop some specific guidelines for ALFRED that app developers (or all involved stakeholders) would need to comply. This could be an initial step towards an “ALFRED certification”. Unfortunately, a certification programme

is very resource intense and ALFRED Consortium lacks the funds to implement it. Instead, when ALFRED will enter the market, some specific ALFRED guidelines could be provided for a first self-assessment phase performed by the mobile application owners, followed by an evaluation process carried out by the ALFRED team.

3 Regulatory Framework that Apply to ALFRED

mHealth is a rapidly evolving sector, very promising for the healthcare in the EU. It can play a key role in addressing major health challenges in the EU and contribute to active and healthy ageing, prevention, diagnosis and management of chronic conditions and sustainability of healthcare systems. It is essential to clarify the regulatory framework which applies to mHealth since this may be one of the most important barriers to ALFRED deployment. The following section identifies the current regulatory framework applicable to ALFRED and different initiatives implemented in Europe to foster mHealth.

3.1 The eHealth Action Plan 2012-2020 and the eHealth Task Force Report

Two publications formally addressed the lack of regulations and policies in eHealth and mHealth: The eHealth Task force report and the eHealth Action plan.

The eHealth Task Force report [EC12-1] highlights the lack of quality criteria for the thousands of health apps available on the market. It also states that there are no standards for data management and consumer information. After the eHealth Task Force report, the European Commission recognised the importance of tackling clarity on legal and other issues surrounding mobile health applications. In 2012, following the eHealth Task Force report, the commission launched the eHealth Action Plan 2012-2020 with the aim of addressing persistent barriers hampering the deployment of eHealth services [EC12-2]. The European Commission's eHealth Action Plan 2012-2020 provides a roadmap to empower patients and healthcare workers, to link up devices and technologies, and to invest in research towards the personalised medicine of the future.

3.2 The eHealth Network

The eHealth network[6] was set up under Article 14 of Directive 2011/24 on the application of patient's rights in cross-border healthcare [EC11]. The network brings together the national authorities responsible for eHealth from all the Member States on a voluntary basis to work on common orientations for eHealth. The aim is to ensure EU wide interoperability of electronic health systems and to ensure safety and continuity of cross-border healthcare. The network is in charge of producing EU guidelines on eHealth. It plays a strategic role in the governance of interoperable cross-border eHealth services and infrastructure. The network will be consulted and fully involved in the activities foreseen in the eHealth Action Plan. However, to our knowledge, there is no a subgroup working directly on a mHealth strategy.

3.3 The Green Paper on mhealth: the Public Consultation

In 2014 the EC released the green paper on mHealth and wellbeing applications in response to the recommendations of the eHealth Task Force [ECGP14]. The Green Paper requested stakeholders' views on 11 identified issues related to the uptake of mHealth in

[6] http://ec.europa.eu/health/ehealth/policy/network/index_en.htm

the EU. The commission received 211 responses in the context of this consultation [ECGP15]. The results argued the following topics:

- Security, Big Data and Privacy. Data safety and privacy is essential to win the patient's trust**. It would be beneficial to draw-up a code of conduct or guidelines covering issues such as privacy, security and user safety**. Encryption and authentication mechanisms were also demanded. Also, app developers should only collect, process and store the personal data that is absolutely necessary.
- Interoperability: The need for European standards. There is a consensus that mHealth solutions should be integrated with electronic medical records
- Patient safety and legal framework. Respondents considered lifestyle and wellbeing mobile apps not regulated enough in legal terms.
- Clinical evidence needed. The difficulty of establishing the efficacy of mHealth solutions is highlighted in the report.
- The role of mHealth in healthcare systems. **The evidence of economic benefits of mHealth is limited** due to the lack of large-scale deployments.
- Reimbursement models. mHealth services are not reimbursed in almost any of the European countries.

Following the mHealth Green Paper, the European Commission has started paving the way for an industry-led Code of Conduct for mobile health apps. This initiative was presented during the mHealth stakeholder meeting at eHealth Week 2015[7]. Three topics were discussed:

- **Privacy and security.** The EC presented a new initiative on preparing an industry-led ***Code of Conduct*** on mobile health apps.
- **Safety and transparency**. It was agreed that ***guidelines*** *or* ***standards*** for quality criteria of lifestyle and wellbeing apps were needed.
- **Web entrepreneurs' access to the market.** The unclear and fragmented legal framework, the lack of interoperability and open platforms were defined as clear barriers for the deployment of mHealth.

3.4 Data Protection Policies

Previous D9.6.1 reviewed the current regulatory framework of personal data protection. Briefly, privacy and protection of personal data are fundamental rights under Article 7 and 8 of the EU Charter of fundamental rights [EC50]. The Data Protection Directive 95/46/EC [EC95] and the ePrivacy directive [EC00] define some restrictions for the processing of personal information at European level.

Because the rapid advances in technology and changes to the ways in which individuals and organisations communicate and share information, the EU legislative bodies are preparing, in a slow and controversial way, an updated and more harmonized data protection law to replace the current regulatory framework: the proposed General Data Protection Regulation “GDPR” [EC12-3]. The GDPR will introduce substantial changes concerning data protection and will provide new guidelines applicable in the context of

[7] http://ec.europa.eu/digital-agenda/en/news/mhealth-green-paper-next-steps

mHealth. The GDPR remains under negotiation in a draft form. It has been anticipated that the text of the regulation will be finalized in the first half of 2016. ALFRED will be following the GDPR progress to be updated accordingly.

3.4.1 mHealth - Reconciling Technical Innovation with Data Protection

The European Data Protection Supervisor ("EDPS") published an opinion on Mobile Health ("mHealth") [EC2015].This opinion admits several concerns in relation to individuals' rights to privacy and protection of their personal data. It highlights some aspects of data protection that might be overlooked (or underestimated) by developers and suppliers of lifestyle and well-being mobile apps. The opinion also provides a number of recommendations for the integration of data protection requirements in the design of mHealth apps: to encourage privacy by design and allocate responsibility for data protection among mHealth stakeholders. Some of the key discussed issues are pointed here:

Data protection implications of mHealth

To determine whether data protection compliance issues exist, it is necessary to establish if the data processed includes any personal data. Data processed in the context of mHealth is likely to be personal data as it relates to identifiable individuals. Additionally, pseudonymous data might be also personal data since a particular individual can be re-identified by the data controller or by third parties (through a combination of that data with external information from other sources). After this premise, it is essential to consider whether data processed should be treated as health data, falling under the stricter data protection regime and applicable to sensitive personal data.

On this sense, the EDPS suggests that lifestyle and well-being data can be considered health data when:

- It is processed in a medical context,
- The information regarding the individual's health may be inferred from the data (in itself, or combined with other information), especially when the purpose of the application is to monitor the health or well-being of the individual.

The new GDPR will give more granularity than previous directive 95/46/EC on what constitutes health data for data protection purposes, but in the absence of a clear definition in the meantime, the notion of what constitutes health data should be interpreted broadly.

Key recommendations

The EDPS also identifies some measures that would bring substantial benefits in the field of data protection in mHealth:

- The EU legislator should foster accountability and allocation of responsibility of those involved in the design, supply and functioning of apps. This should include designers and device manufacturers. The EDPS also considers that a code of conduct elaborated by mHealth stakeholders with the contribution of data protection agencies might also help encourage a coherent application of existing data protection rules in relation to mHealth;

- App designers and publishers should design devices and apps to increase transparency and the level of information provided to individuals in relation to processing their personal data, and avoid collecting more data than is required in order to perform the expected function. App designers and publishers should embed privacy and data protection settings in the design of these apps, applying the same level of creativity and dynamicity they usually display in introducing attractive devices and apps to also provide individuals with effective and user-friendly privacy notices and setting options;
- Industry should use Big Data in mHealth for purposes that are beneficial to individuals, such as medical research, and avoid using them for practices that could cause them harm, such as discriminatory profiling for employment or insurance purposes
- The EU legislator should enhance data security and encourage the application of privacy by design and by default through privacy engineering and the development of appropriate building blocks and tools.

3.4.2 Article 29 Data Protection Working Party

The working party was set up under Article 29 if Directive 95/46/EC. It is an independent advisory body on data protection and privacy[8]. It is entitled to examine questions such as:

- To uniform application of the national measures adopted,
- To provide the Commission opinions on the level of protection in the Community and in third countries,
- To advise the Commission on possible legislation amendments, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms (article 30).

3.4.2.1 Opinion 02/2013 on Apps on Smart Devices

In this opinion [WP13] the working party clarifies the legal framework applicable to the processing of personal data in the development, distribution and usage of apps on smart devices. It analyses the key data protection risks, provides a description of different parties involved and highlights their legal responsibilities. The opinion notes that whilst app developers wish to provide new and innovative services, the apps may have significant risks to the private life and reputation of users of smart devices if they do not comply with EU data protection law. In addition, apps must provide sufficient information about what data they are processing before it takes place in order to obtain meaningful consent and the opinion further notes that poor security is another risk which could lead to unauthorised processing of personal data which increases the possibility of a data breach.

Opinion 02/2013 provides some recommendations for parties involved in the development, distribution and technical capabilities of apps:

[8] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

Recommendations for App Developers

- App developers must be aware of and comply with their obligations as data controllers when they process data from and about users.
- App developers must ask for consent before the app starts to retrieve or place information on the device i.e. before installation of the app.
- App developers must allow users to revoke their consent and uninstall the app and delete data where appropriate.
- It is recommended that app developers inform users about their proportionality considerations for the types of data collected or accessed on the device, the retention periods of the data and the applied security measures.

Recommendations for App Stores

- App stores must be aware of and comply with their obligations as data controllers and enforce the information obligation of the app developer.
- App stores must give special attention to apps directed at children to protect against unlawful processing of their data.
- It is recommended that app stores subject all apps to a public reputation mechanism and provide feedback channels to users to report privacy and/or security problems.

Recommendations for OS and Device Manufacturers

- Both parties must enable users to uninstall apps and provide a signal to the app developer to enable deletion of the relevant data user.
- Both parties must develop clear audit trails into the devices such that end users can clearly see which apps have been accessing data on their devices and the amounts of ongoing traffic per app, in relation to user-initiated traffic.

Third Parties must

- Be aware of and comply with their obligations as data controllers when they process personal data about users.
- Comply with the consent requirement under Article 5(3) of the ePrivacy Directive [EC00] and not circumvent any mechanism to avoid tracking.
- Develop and implement simple but secure online access tools for users without collecting additional excessive personal data and only collect and process data that are consistent with the context where the user provides the data

3.5 Policy Recommendations

It has already been stated several times along the document that the lack of regulation is one of the major barriers for mHealth deployment. Releasing the potential of mHealth requires pushing forward the current regulation framework. Some recommendations for policy makers already rose from ALRED research are presented below:

- Policy makers need to establish urgently a **comprehensive regulatory framework** to govern the mHealth arena; clear guidelines on data protection, standardisation and safety are required. It is important to find the right balance to avoid over-regulation and consequently limit mHealth deployment.
- EU bodies must implement **Digital Literacy Policies,** especially among older users. By developing and enhancing digital skills of older users, they will have more opportunities for learning and being confident in the use of digital tools, while they will be more aware of the emerging risks of the use of new technologies.
- To ensure the quality of products providing formal **guidelines** for **best practices** and public **certification programmes** of mHealth initiatives. This is fundamental for consolidating the mHealth market.
- mHealth solutions need to be integrated into healthcare systems to unleash its potential. New strategies on pricing and reimbursement are needed. To allocate specific budget for mHealth in the member states would help.
- mHealth should have a recurrent presence in the production of the forthcoming research programmes (H2020, etc). Further research is needed dealing with the adoption of mHealth initiatives in the healthcare services and patient's needs
- Policy makers need to consider responsibilities of those involved in the **design** and the **supply** in the mHealth ecosystem. Embedding privacy and data protection settings in the design and making them applicable by default.
- Apps designers must increase **transparency** and the level of information provided to users in relation to processing of their data. They need to avoid collecting more data than is needed to perform the expected function.
- ALFRED would recommend the creation of a **European Network of mHealth**. The Network would foster mHealth in Europe, increasing the visibility of mHealth initiatives with the subsequent impact on the EU health agenda. It would act as a platform for exchanging experience and expertise on mHealth, fostering co-operation and facilitating liaison between organizations and individuals active in mHealth across Europe and internationally. The network would aim at being complementary to other networks (or even nested) such as the EU (eHhealth network[9]) and would work closely with them on issues of common interest.

[9] http://ec.europa.eu/health/ehealth/policy/network/index_en.htm

4 Ethical Analysis

This section describes those aspects of the project that are associated with ethical concerns. The API architecture (the open Marketplace) proposed by ALFRED might imply some privacy risks such as user profiling, abuse and traceability of movements and activities. While previous version of this deliverable (D9.6.1) was mainly focused in the project development; this new version is intended to identify potential ethical risks during the ALFRED deployment phase, it also describes solutions that we suggest to mitigate the potential risks.

4.1 Ethical Aspects of ALFRED

There are some ethical aspects concerning the use of ALFRED, mainly related to the collection, use and storage of both personal and biometric information that are relevant of consideration. Specially, because nowadays in terms of mHealth, legislation does not exist or remain ambiguous and insufficient. Here we present some ethical aspects that concern ALFRED and its application.

4.1.1 Privacy

Privacy and principles of basic privacy protection are universal. Collecting, processing, storing and disclosing personally identifiable information bring forth concerns of information privacy. ALFRED users will have the right to control the use and dissemination of their personal information and to decide which information they want to provide and store.

In ALFRED three systems are in place to allow the user the total control of data. Firstly, a permission-based system allows controlling what ALFRED Apps can have access to what ALFRED services. This is the same approach, which is utilized in Android. To track Apps and “not let them to bully”, permissions are given (or revoked) during the installation process and at a later stage. This allows ALFRED users to install an App and later revoke the permission to user’s data. We also plan to develop strict policies for third party developers to access to the ALFREDO marketplace. These policies will contain first of a strict “graceful degradation” instead of “hard failure” principle. These policies will enforce that an App that does not have a particular permission has to recover from this in the best possible manner, instead of just stop working. In the case of an App that shows live vital data as well as legacy vital data, the App should still visualise the live vital data even when the permission “access legacy data” is revoked. More importantly, policies will contain clear restrictions of what an App may not do. This will be especially relevant for any sort of data transfer or storing data outside of the ALFRED system, ensuring that the ALFRED platform will have total control of the user’s data and in so doing the user.

Secondly, a fine granular system is set in place allowing the user to provide or revoke permission to access (CRUD – Create, Read, Update, Delete) each data set individually. This complete control allows scenarios where a user shares for example his heart-rate with an informal carer but not his blood pressure. All the information can be controlled in this way, allowing different users to access different data (or none) of every user. Obviously, this implies important efforts of setting up the system, but it is envisioned to overcome this usability challenge with different short-cut profiles.

Thirdly, an audit system is in place in two locations: In the Knowledge and Information Storage (KIS – to speak the central database) and in the Authentication and Authorisation Mediator (AAM). The audit contains of a log of every action in these two components. In the final setup this data will be fed in an encrypted database. Access to the database would be only provided under the four-eye-principle in case of a suspected misuse of information. The two combined log would allow to reconstruct and thereby to provide evidence for every internally misuse of data linked to specific users (including Apps) of the system.

4.1.2 Security

Security refers to the safeguards, techniques, and tools used to protect against the inappropriate access or disclosure of information. Research suggests that legitimate users of a system often may be the likely cause of impaired security when they overlook rules, because they underestimate or fail to understand the costs of their actions [BA04]. While outsiders may intentionally attempt to access information or try to figure out someone's identity or location from intercepting communications, such efforts will account for a minority of security threats. Many breaches are preventable through having a high-quality security plan that pays special attention to the most common and simplest reasons for data losses. The overall goal of effective security protocols is to protect participant identity and secure data in such a way that if unauthorized individuals were to gain access, they would be unable to link the data with a particular person or with other data being sent. This is especially true because while no single source of data may be identifiable, the combination of multiple sources of data may make identifiable linkages possible [AY14].

In ALFRED State-of-the-Art security is used. The communication channel TLS will be always used. The advanced standard AES-256 is used for data encryption. The Knowledge and Information Storage (KIS – so to speak the central database) will use for the final setup different keys abbreviated from the user credentials for the encryption of every Data Bucket. In addition, different IV (initialisation vectors) will be used for every Data Bucket of the same user or for different database used for the Data Bucket. The combination of the strong encryption with the different keys and IV's will render both brute-force attacks as well as rainbow-table attacks futile. The Authentication and Authorisation Mediator (AAM) will be used for the authentication of all users (all ALFRED components, all ALFRED end users and all ALFRED Apps). The AAM allows the authentication of every user when an ACCEPT Service is called. The utilisation of temporary and component tokens allows a single sign own solution, which is both usable and secure. The AAM implies that authorisation will not be handled centrally; the components can register again the AAM to allow the redirection of the authorisation. The bundles for the installation for ALFRED Apps, including the driver for additional sensor will make use of signatures using RSA 4096 in the final version of the marketplace, closing an additional attack vector.

4.1.3 Confidentiality

Any personal information about ALFRED users must not be disclosed in any situation without the user's permission. Personal identifiable information should always be protected, and both technological and personal safeguards are needed for ensuring it. Secure encrypted systems are essential for promoting confidentiality (see previous section).

4.1.4 Consent

The ALFRED project has implemented informed consent for all participants of ALFRED pilots. Specifications were detailed in the previous version of this deliverable. We plan to follow the same principles for the ALFRED solution once in the market. It is crucial that ALFRED users have access to all relevant information before signing the informed consent. The reason for using ALFRED, the pros and cos and possible consequences of it use, should be thoroughly explained in order to maximize transparency.

4.1.5 Trust

A key issue in mHealth is the need for transparency in order to engender trust. Enhanced transparency increases end-user trust for organisations offering mHealth services. ALFRED will make sure that its end-users fully understand the implications of using ALFRED. ALFRED will also be completely open regarding data collection and how it is processed. This openness will also include third-parties when involved. ALFRED will make publicly available clear explanations in an understandable language of their policies, procedures, and practices regarding the collection, storage, and use of personally identifiable health information.

4.1.6 Autonomy

The use of ALFRED can give a peace of mind to the caregivers of the patient, but the patient who is monitored can feel that his/hers autonomy and independence are threatened by the use of technology. It is important that the opinion of the older users is taken into account when planning the introduction of ALFRED and that there is an appropriate balance between needs and autonomy. User's autonomy should always be respected; their independence and self-determination should be promoted by minimizing the restrictions of their own decision-making concerning risks they want to take.

4.2 Identification of Potential Ethical Risks using ALFRED

4.2.1 Data Privacy Risks

Data collection, storage and processing might create a risk of confidential information being accessed without the knowledge or consent of the users. Some technical aspects are key in terms of security and privacy requirements. Previous sections described the technical specifications of the ALFRED system for guaranteeing the security and privacy related requirements. As an introduction, to identify privacy risks, it is very useful to describe how data will be collected, processed and stored within ALFRED and the security and control methods that ALFRED uses to safeguard user's data privacy.

4.2.1.1 Description of Data Flow

ALFRED might store huge amounts of different data and information about its user. For this reason, the software architecture for the ALFRED system foresees a sophisticated privacy and security setup allowing full control of the end user over data and providing a secure environment.

The most critical data are the sensor data. The raw sensor data will never leave the phone and will not be stored at all. The pre-processed sensor data will be cached in the Health Monitor Client (HMC). The user may allow third party applications access to these data

and the HMC to forward it to the Health Monitor Server (HMS) for further analysis and usage in the ALFRED system. The HMS will post-process the data further. The data will be used for anomaly detection and may be also stored (depending on the settings of the user) to have access to historical data. The anomaly detection is also planned as plug-in system in the final version of the HMS, were each plugin needs the access rights for any given attribute of the Health Profile by the end user.

The same approach is used for the user profile information. No attribute of ALFRED user profile will be accessible without the user specifically granting the access. The Personalisation Manager (PM) will retrieve all new event data from the Event Manager (EM) to find event recommendations for the end user without her data leaving the PM.

4.2.1.2 Security and Control Mechanisms

The security and privacy requirements in terms of technical specifications are the following:

- *Privacy settings in the end user front-end.* Controlled by the Personal Assistant (PA) and managed by the Personal Manager (PM)
- *Access control within components.* All components will use the Knowledge and Information (KIS) to store data securely. This will ensure that personal data will not leak to other ALFRED components or to third parties, unless that explicitly configured to allow this access.
- *Security in web based inter-component communication.* The communication between client and server side could be done across an untrusted network and the data could be leaked. In order to avoid this situation, the communication will be secured adopting the Transfer Layer Protocol (TLS)which ensures an encrypted communication between authenticated communication partners. This security method is also known as HTTPS.
- *Authentication and Authorization.* Once the communication is secure, the user of a web service has to be authenticated. For this the central Authentication and Authorisation Mediator (AAM) is in place. Every user (which are in the context of the AAM all users of the system from human to machine) have to first authenticate on this central component providing a Single Sign On (SSO) solution where authentication credentials will be stored and temporary access token provided. All credentials will be stored hashed (scrypt) with unique salts. The Authorisation on the other hand will be forwarded to each component.

4.2.1.3 Risk Mitigation Associated to Data privacy

It is the right of individuals to determine for themselves when, how, and to what extent personal information is communicated to others. The consent gives users appropriate knowledge of what data are being collected, how they are stored and used, what rights they have to the data, and what the potential risks of disclosure could be. Unfortunately, low technological literacy among older adults might limit ALFRED user to understand the true risks and benefits of mobile technologies.

Because changes in technological literacy might take time to implement among older users, we have implemented security systems to protect user's privacy and we will provide clear information in a comprehensible language before starting using ALFRED. The majority of security breaches in mHealth are due to unauthorized access to a device or

from mishandling or misusing data. Thus, when it comes to securing data, ALFRED users should try to prevent the most likely breaches, such as leaving mobile devices unsecured, sharing passwords or leaving them written on notes, accessing sensitive information in public areas using open-WiFi networks, or even losing a mobile device [BB10].

Here some of the specific solutions that are being or will be implemented to mitigate data privacy and security risk:

- ALFRED will be very explicit about the data is collected. It will be transparent and it will communicate in a very plain language.
- ALFRED users will choose which data to share, whether before data collection or after data have been sampled. A simple electronic or paper checklist of possible data points administered before data collection will allow ALFRED users to exercise their rights to control and access their data. This has the added benefit of helping ALFRED users to learn about their privacy options which at the same time, should enhance technological literacy
- ALFRED components and third party developers will be thoughtful about what data they will collect
- ALFRED will collect the minimum amount and detail of data needed to reduce the risk of identification.
- Third data developers will get clear instructions to understand the privacy and confidentiality policies of ALFRED, especially when the data target the sensitive subject
- Minimise access to identifiable data
- Delete identifiable data when no longer necessary
- Disclose only anonymized data
- Monitor who access to user's data-third party developers
- Publish a code of practice to manage the use of Data for third party developers

4.2.2 Other Potential risks

There are other common issues around the constraints of technology itself, for example problematic device and telecommunication technologies, battery failures or unreliable internet connection. Additionally, there is always the possibility of theft, loss, or malfunction of the mobile device that could have serious consequences when important data are not stored in a second location. All these possible deficiencies, failure in electronic equipment, internet connection, etc, will be described to the ALFRED users to avoid false security. Clear information will be provided in order to manage their expectations.

4.3 Ethical code for ALFRED

During the mHealth stakeholder meeting at eHealth Week 2015**,** the EC presented a new initiative on preparing ***Code of Conduct*** on mobile health apps leaded by industry. Legal basis are grounded on article 27 of the data protection directive 95/46/EC. An industry code of conduct working group was set up in March 2015 with the EC as facilitator. It is intended to be signed by the main parties involved in the processing of data in the apps

environment and possibly, to be approved by the Article 29 Working Party. The first meeting of the stakeholder group was held in April 2105. Among the drafting team there were companies like Apple, Google, Intel, Microsoft, Samsung or the App Association. This still a draft in a working phase. We will be following the process to be updated.

Another international initiative is the “eHealth code of ethics [RR00]. The goal of the "e-Health Code of Ethics" is to ensure that all people worldwide can confidently, and without risk, realize the full benefits of the Internet to improve their health. The following code of ethics was prepared as a result of the "eHealth Ethics Summit," which convened in Washington DC on 31 January 2000 - 2 February 2000, organized by the Internet Healthcare Coalition and hosted by the World Health Organisation/Pan-American Health Organisation (WHO/PAHO), and attended by a panel of about 50 invited experts from all over the world. It sets guiding principles under five main headings: candor and trustworthiness; quality; informed consent, privacy and confidentiality; best commercial practices; and best practices for provision of health care on the Internet by health care professionals. Table 2 presents the guiding principles and their definitions. These Guiding principles are a very good starting point and it might serve to ALFRED to elaborate their own code or ethics in future work.

Table 2: Guiding Principles of the eHealth Code of Ethics

Candor Disclose information that would likely affect their understanding or use of the site, or purchase or use of a product or service	Disclose vested financial interests Disclose key information for consumer decisions
Honesty Be Truthful and not deceptive	Present information truthfully No misleading claims
Quality Provide health information that is accurate, easy to understand and up to date. Provide information that users need to make their own judgments about the health information, products or services provided by the site	Information must be: Accurate, clear, current and evidence-based Readable, culturally competent, accessible Citations, links, editorial board and policies must be provided
Informed Consent Respect user's right to determine whether or how their personal data may be collected, used or shared	It needs to be clearly stated: Privacy policy and risks Data collection and sharing Consequences of refusal to consent
Privacy Respect the obligation to protect user's privacy	Prevent unauthorized access or personal identification of aggregate data Let users review and update personal data
Professionalism Respect fundamental ethical obligations to patients and clients. Inform and educate patients and clients about the limitations of online healthcare	Stand for professional codes of ethics Disclose potential conflicts of interest Obey applicable laws and regulations Point out limits of online practice
Responsible partnering Ensure organizations and sites with which they affiliate are trustworthy	Choose trustworthy partners, affiliates, and links Maintain editorial independence from sponsors Tell users when they are leaving the site
Accountability Provide meaningful opportunity for users to give feedback to the site	Provide management contact info Encourage user feedback Respond promptly and fairly to complaints

Since ALFRED will develop and adopt its own code, it is important to promote it to end users and third parties. This can be a competitive advantage and can show end users how to find reliable mHealth services through other sources.

Meeting the mHealth challenges ahead calls for innovative management and new focus on ethical issues. ALFRED will ensure that technology is used according to the highest possible ethical standards.

5 References

[FDA03] Guidance for Industry and Food and Drug Administration Staff - Non binding recommendations, FDA, Sept. 25, 2003. Available: http://www..gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf [Accessed: Sep. 23, 2015].

[RCP15] Using apps in clinical practice guidance. RCP. April 2015. Available: https://www.rcplondon.ac.uk/sites/default/files/apps_guidance_factsheet.pdf [Accessed: July. 23, 2015].

[ACSA12] Estrategia de calidad y seguridad en aplicaciones móviles de salud. Available: http://www.calidadappsalud.com/

[EC12-1] The e-Health Task Force report. Redesigning Health in Europe. Available: http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/redesigning_health-eu-for2020-ehtf-report2012_01.pdf [Accessed: May. 29, 2015].

[EC12-2] The e-health action plan 2012-2020. Available: http://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century [Accessed: May. 29, 2015].

[EC11] *Directive 2011/24*/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45) Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2011:088:TOC [Accessed: Sep. 29, 2015].

[ECGP14] European Commission, “Green Paper on mobile Health (“mHealth”),” European Commission, Brussels: COM(2014) 219 final, Apr. 10, 2014. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5147 [Accessed: Sep. 29, 2014].

[ECGP15] Summary report on the public consultation on the green paper on mobile health. Available: https://ec.europa.eu/digital-agenda/en/news/summary-report-public-consultation-green-paper-mobile-health [Accessed: July, 2015].

[EC50] European Convention for the Protection of on Human Rights and Fundamental Freedoms, European Court of Human Rights, Rome, Nov. 4, 1950. Available: http://www.echr.coe.int/documents/convention_eng.pdf [Accessed: Sep. 29, 2014].

[EC95] European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [EU Data Protection Directive], Official Journal, L 281 of 23.11.1995, Nov. 23, 1995. Available: http://eur-lex.europa.eu/legal-content/en/ALL/;ELX_SESSIONID=wdHZJphYcVbyvG5h1fbyhM21Spsrt1ZT19V53HTTnJxQX4hvLHsq!-1058168386?uri=CELEX:31995L0046 [Accessed: Sep. 29, 2015].

[EC50] European Convention for the Protection of on Human Rights and Fundamental Freedoms, European Court of Human Rights, Rome, Nov. 4, 1950. Available: http://www.echr.coe.int/documents/convention_eng.pdf [Accessed: Sep. 29, 2014].

[EC00] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the

electronic communications sector (Directive on privacy and electronic communications) (L201, 2002-07-31, pp. 37 – 47) Available: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML[Accessed: Sep. 23, 2015].

[EC12-3] Proposal for the EU General Data Protection Regulation. European Commission. 25 January 2012. Available: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Accessed: Sep. 28, 2014]

[EC15] Opinion 1/2015 "Mobile Health – reconciling technological innovation with data protection. European Commission. 21 May 2015. Available: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf [Accessed: May. 27, 2014]

[WP13] Opinion 02/2013 on apps on smart devices. Article 29 Data Protection Working Party. 27 February 2013 Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf [Accessed: May. 28, 2014]

[BA04] Besnard D & Arief B *(*2004*).* Computer security impaired by legitimate users. Computers & Security, 23(3):253–264.

[AY14] Arora S, Yttri J, Nilse W. (2014). Privacy and Security in Mobile Health (mHealth) Research. Alcohol Research. 36(1):143-51.

[BB10] Bennett, K.; Bennett, A.J.; and Griffiths, K.M (2010). Security considerations for e-mental health interventions. Journal of Medical Internet Research 12(5):e61

[RR00] Rippen H, Risk A. (2000). e-Health Ethics Draft Code. Journal of Medical Internet Research. 2(1):e2