WP 9 – Impact

D9.6.1 Standardization, Policy and Ethical Issues

Report

Deliverable Lead: IESE

Contributing Partners: All

Delivery Date: 09/2014

Dissemination Level: Public

Version 1.0

The main objective of this deliverable is to define the standard requirements for the ALFRED solution to comply with technical and ethical policy regulations.

Document Status	
Deliverable Lead	Lucile Danglas, Marta Ribeiro, Magda Rosenmoller (IESE)
Internal Reviewer 1	Mona Komulainen (ESE)
Internal Reviewer 2	Emilia Garcia Nieto (WORLDLIN)E
Type	Deliverable
Work Package	Work package 9 - Impact
ID	D9.6.1 Standardization, Policy and Ethical Issues Report
Due Date	30.09.2014
Delivery Date	30.09.2014
Status	Final

Document History	
Contributions	**V0.1 IESE** **V0.2 ESE** **V0.3 IESE** **V0.4 WORLD** **V1.0 IESE**
Final Version	30.09.2014

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 report summarizes the standards, ethical and policy issues that are relevant for the development of ALFRED project and commercialization of ALFRED products.

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. For instance, a voice controlled interface needs to access the different components of the system to support social activity, monitor vital signs and stimulate gaming engagement. 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. Quality management standards were also identified to support product development and quality monitoring to ensure that ALFRED products/services meet end user's requirements. As such, the documentation of standards has been of high relevance for the development of the ALFRED solution.

In addition, a review of the policy framework was conducted at the global and European levels in the field of mobile and mobile health applications to assess the regulatory context of the development of mobile health devices. In particular the important distinction between mobile wellness/fitness and health devices and its implications on the business model of ALFRED were exposed.

Finally, this document highlights the main ethical issues arising during the research and commercialisation phases, especially with regards to the involvement of end users. ALFRED will require access to the user's personal and health related information. Recommendations to ensure data protection and privacy from a standard as well as regulatory and ethical perspective are provided.

Overall, this documentation constitutes a roadmap for the further development of the ALFRED solution and will be updated throughout the whole duration of the project to adapt to technical evolution and reflect changes in the regulatory and market environment. Updates will be provided in the subsequent deliverables 9.6.

Table of Contents

List of Figures

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 out 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, considering his interests and his social environment.
- A more **Effective & Personalized Care** by allowing medical staff or carer to access vital signs of older people monitored by (wearable) sensors.
- **Physical & Cognitive Impairments Prevention** by incorporating serious gaming to improve the physical and cognitive condition by offering games and quests to older people.

1.1 ALFRED Project Overview

One of the major problems today 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). ALFRED will allow overcoming this problem with an interactive virtual butler for older people, which is fully voice controlled.

The ALFRED project is wrapped around the following very clear main objectives:

- Empowering people with age related dependencies to live independently for longer by delivering a virtual butler with seamless support for tasks in and outside the home. The virtual butler ALFRED will have a very high end-user acceptance by using a fully voice controlled and non-technical environment.
- Prevailing age-related physical and cognitive impairments with the help of personalized, serious games.
- Fostering active participation in society for the ageing population by suggesting and managing events and social contacts.
- Improved care process through direct access to vital signs for carers and other medical stuff as well as alerting in case of emergencies. The data is collected by unobtrusive wearable sensors monitoring the vital signs of older people.

To achieve its goals, the project ALFRED conducts original research 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 and medical 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 standard and regulatory framework which should apply to the research and development and the entry to market of ALFRED products to achieve technically successful and commercially sustainable solutions. It reviews the status of policies and standards at the global, European and national levels and highlights their implications for the development and marketing of ALFRED.

The deliverable also draws attention to the ethical issues related with the management of end users' data during the research and development of the project and also while 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 ALFRED and can therefore be used by external parties in order to get according insight into the project activities.

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

1.4 Abbreviations and Glossary

A definition of common terms and roles related to this deliverable can be found in the part 6 of this document. Further definitions related to the realization of ALFRED 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. It also includes a glossary.
- Chapter 2 describes the role of standards in shaping the technical development of ALFRED to ensure safety and proper use. It also aims at facilitating interoperability between the interfaces of different components and devices to foster the implementation of an eHealth based integrated healthcare sector.
- Chapter 3 focuses on the policy framework at the global, EU and national levels that will have an influence on the entry to market of the ALFRED products. In particular, it highlights the delicate distinction between wellness and medical devices and their respective implications for developers and manufacturers.
- Chapter 4 reviews the ethical issues raised in AAL in general and the specific one which applies to ALFRED's research and development. In particular, due to ALFRED access to its user's personal and health related information to carry out its virtual assistant functions, great consideration needs to be given to protect user's personal and medical information as well as privacy.

2 Standards to Be Taken into Account in the Design of the ALFRED-solution

A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are uniformly fit for their purpose (http://www.iso.org/iso/home/standards.htm).

Standardisation is the process of developing and implementing technical specifications to maximize interoperability, privacy and accessibility thereby supporting market acceptance and the efficient and effective use of ICT applications and services. Integration of technical and business standards in the development of the ALFRED-solution is essential to ensure its authorisation on the market and its proper functioning.

"Highly integrated and at the same time distributed applications with a high communication capability are needed to provide the required environmental and processing intelligence for the user. Capturing of the required data (vital parameters, environmental data) takes place via sensors either close to the human body, or integrated into the environment. The variety of ICT technologies used ranges from intelligent data processing to automated decision support. The interaction of the user with the various applications should be as intuitive as possible. The system should adapt to the user context and the physiological and cognitive conditions of the user. The user can display and, if needed, interact with the data using ergonomic user interfaces and terminal devices, whereas older people, physicians or nurses and carers might be users of the system. Therefore, AAL applications always address interfaces to other systems within an eHealth based integrated healthcare sector" [VDE08].

The ALFRED-system, like other AAL applications, 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 different pillars.

2.1 Existing Sources of Standards

2.1.1 Introduction to Standards

Standards define consistent ***interfaces*** enabling the interoperability and exchangeability of different components; they define safety requirements or permit service offerings to be compared. Standards can establish a wide range of specifications for products, processes and services

- Prescriptive specifications obligate product characteristics, e.g. device dimensions, biomaterials, test or calibration procedures, as well as definition of terms and terminologies.
- Design specifications set out the specific design or technical characteristics of a product.

- Performance specifications ensure that a product meets a prescribed test, e.g. strength requirements, measurement accuracy, or battery capacity.
- Management specifications set out requirements for the processes and procedures companies put in place, e.g. quality system for manufacturing or environmental management systems.

Standard documents are voluntary, neutral recommendations that can be used by everyone – they become mandatory only if a law explicitly requires compliance with a certain standard or set of standards. They are developed by expert committees such that they solve certain tasks in a way that does not favour any specific party (individual or organisation) – this vendor-neutral nature is a mandatory requirement for all official standards published e.g. by standards bodies such as CEN, CENELEC or ETSI at the European level and ISO, IEEE, W3C, IEC at the international level (Table 1).

Table 1: Main Elements of the Standardization Landscape at the International and European Levels

Standardization	General	Electrical Technology	Telecommunication
International level	ISO	IEEE	ITU
European level	CEN	CENELEC	ETSI World Class Standards

To ensure that the ALFRED system can become established on the European Single Market and beyond, its standardization activities should take place on an international or at least European scale.

2.1.2 European Standards

- The European Committee for Standardisation (CEN) is one of three European Standardization Organizations (together with CENELEC and ETSI) that have been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level. This important work brings concrete benefits, such as: improving safety, quality and reliability of products, services, processes; reinforcing the Single Market and supporting the economic growth and the spread of new technologies and innovation.
- The European Committee for Electrotechnical Standardization (CENELEC) is responsible for standardization in the electrotechnical engineering field. CENELEC prepares voluntary standards that facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market.

- The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

2.1.3 International Standards

- The International Organisation for Standardization (ISO) defines a standard in the medical device domain as follows*: "Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines or definitions of characteristics, to ensure that materials, products, process and services are fit for their purpose"*.
- The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards as well as professional and educational activities. IEEE is a leading developer of international standards that underpin many of today's telecommunications, information technology, and power generation products and services.
- The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web. W3C's standards define key parts of what makes the World Wide Web work.
- The Standards and Interoperability (S&I) Framework is a collaborative community of participants from the public and private sectors who are focused on providing the tools, services and guidance to facilitate the functional exchange of health information (http://wiki.siframework.org).

2.2 Technical Standards Issues

The vision and promise of the ALFRED system is to provide a virtual butler to support and monitor the elderly user in various functions as well as to foster its autonomy and its active participation in society. The realisation of this system requires the integration of different system components (see example on Figure 1 below):

- Medical Device Technologies
- Communications Technologies
- Network Infrastructure, including access to the Internet
- Software Technologies
- Technical Support: device, accessory and component (tablet, app, pcs, watch, sensors etc.)

All these different components need to follow established standards to ensure interoperability, safety and risk management, usability and accessibility, privacy and data protection, and service functioning.

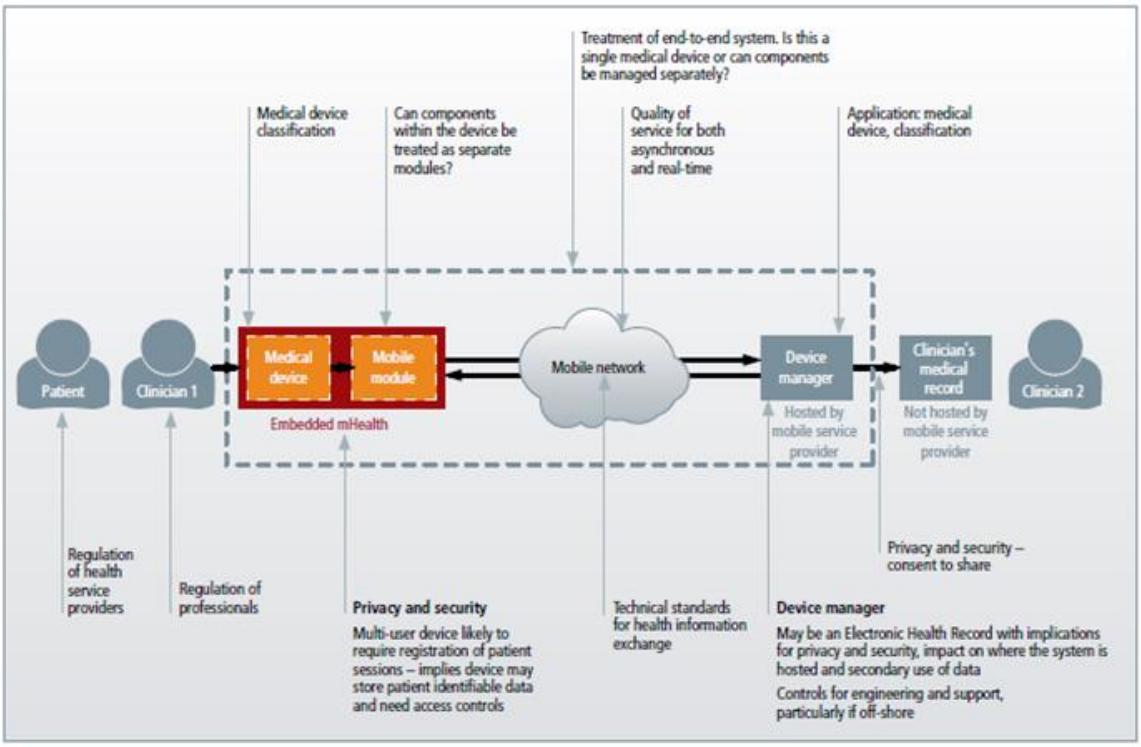

Figure 1: Policy and Regulation That Could Apply to Remote Monitoring Solutions [GSM12-1]

2.2.1 Interoperability

The implementation of this vision requires many “building blocks”: system components and human services need to integrate, to work together, in order to provide this desired ambient support for the user. This ability of two or more systems to work together to perform a task by communicating via their interfaces is called “interoperability”. The development of standards is essential to enable interoperability among applications and systems and ensure the proper functioning of ALFRED. The concept of interoperability can be broken down into several levels, as described for example in ETSI ETR 130:1994 [ETSI130]:

- *Protocol interoperability* is the ability of a remote system to exchange data packages via the basic communication system.
- *Service interoperability* (or syntax interoperability) is the ability of a remote system to offer a sub-set of a remote service according to a functional specification.
- *Application interoperability* (or semantic interoperability) is the ability of a remote system to warrant consistent implementation of syntax and semantics of the exchanged data.
- *Interoperability for the user* applies when the user can exchange information using the remote system.

These levels build consecutively on each other. Interoperability for the user presumes that the participating systems can exchange and interpret the data correctly. This demands the ability to exchange messages or commands, which in turn requires a functioning interface

to exchange bits and bytes. In the end, the objective of all measures involved in conformity review (i.e. checking that system interfaces comply with the interface specifications) and interoperability review (i.e. checking that two or several systems "match") consists of safeguarding interoperability as seen by the user.

2.2.2 Safety and Risk Management

The malfunction of a component of the ALFRED system may pose a safety threat to the user. Therefore, both the product safety (including electromagnetic compatibility) and the risk management are relevant topics in the product design. In the lifecycle management processes must be integrated a process which identifies hazards to the user from the use of the application. Furthermore, this process estimates the associated risks and aims to eliminate or minimize those by designing and determining information about residual risks to be transferred to the user.

Both safety and risk management are covered by standards, many of which (in the case of product safety) are legally required for all products brought to market in the EU (recognizable by the CE mark on the product). For instance, the standard reference for the definition of a risk management approach to product and system development for medical devices is the ISO 14971 Medical devices – Application of risk management to medical devices [ISO14971].

Guidance on the application of ISO 14971 to medical device software:

- IEC/TR 80002-1 Medical device software - Part1 [IEC80002]

Additional standards can guide the development of the ALFRED-system to ensure its safety:

- IEC 62366 Medical devices. Application of engineering suitability for use on medical devices [IEC62366]
- IEC 60601-1 Electrical equipment. Part 1: General requirements for basic safety and essential performance [IEC60601].

2.2.3 System Quality Management

The developer must define, implement and maintain a system of quality management related with the hazard class of applications. They may be taken as general reference standards like ISO 9000 family [ISO9000, ISO9001]. ISO13485 [ISO13485] and ISO13488 [ISO19488] are specific ISO quality systems standards for medical device manufacturing.

Guidance on the application of ISO 13485 to medical devices:

- CEN ISO / TR 14969 IN Medical devices. Systems of quality management [ISO14969]

The organizational structure should include the figure of the head of compliance, whose training and experience must be commensurate with the risk of the generated applications.

2.2.4 Usability and Accessibility

For an information system to be used, it must be easy and straightforward to operate. This property is defined as “usability”. Usability refers to “the extent to which a product can be

used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" (ISO 9241 [ISO9241-1, ISO9241-2, ISO9241,3]). In other words, usability describes the ease of use of a product. Whereas accessibility refers to the degree to which a product is available to as many people as possible, in particular people with disabilities or special needs. Both topics are important for the ALFRED system since its target user groups are older adults with relatively limited experience with technology and who might have various age-related disabilities and special needs. It is, therefore, important to consider these factors in the product design. A large number of standards is available helping the system architects to improve the usability of a system and to achieve a "design for all" that makes the system accessible to as many users as possible.

2.2.5 Privacy and Data Protection

The ALFRED components will collect personal data, including health data, of its elderly users, which requires protection under the EU data protection directive 95/46/EC [EC95]. Furthermore, unauthorized interference with the system (such as abusing system actors to facilitate burglary) may pose security and safety risks. In addition to the standards on risk management, there are also standards covering the topics of data protection and system security, which may help system designers to appropriately address these issues.

Privacy implementation always entails a combination of technical and organizational measures. Security includes encryption from the infrastructure to the end-user service, integrated governance and compliance management, identity and access management, security analytics, integrated backup and recovery, etc.

Various ISO/IEC working groups are currently working on international specifications for data protection. In concrete terms, these are:

- ISO/IEC FDIS 29100: Privacy framework (definition of privacy requirements in processing personal data in the information systems of all countries) [ISO29100],
- ISO/IEC CD 29101: Privacy reference architecture (best practices for consistent technical implementation of privacy principles) [ISO29101] and
- ISO/IEC WD 24760: Framework for identity management (framework for secure, reliable privacy conformity management of identity information) [ISO24760].

The use and disclosure of security and risk management standards and specifications are also important. The ISO/IEC 2700 standards series is relevant in this context. In addition, the BSI standards[1] on IT baseline protection are of particular significance. Attention is required in particular to ensure that pseudonyms are used for data in the AAL system.

2.2.6 Process and Service Level

In addition to the technical aspects, also the service level aspects and business processes of the ALFRED-system need to be well-designed. There is a number of specifications addressing requirements and quality criteria.

[1] BSI: Bundesamt für Sicherheit in der Informationstechnik, Germany [Federal Office for Information Security]

2.2.7 Lifecycle Management of the App

The processes of design, development and maintenance of the application must be systematized, including the verification and validation phases of the requirements before the release of the software, and with the evidence of implementation in the case of the App to be certified.

The rule that is usually taken as a reference for managing the software lifecycle is the IEC /EN 62304 - Medical device software: Processes of the software life cycle [IEC62304.

2.2.8 Evaluation and Clinical Monitoring

The effectiveness and security requirements defined for the design and development of the application should be based on relevant clinical data obtained from scientific literature searches, clinical experience, or clinical research.

On the other hand, the confirmation of compliance of these requirements in the intended use, the evaluation of the undesirable side effects and the acceptability of the benefit / risks should also be based on clinical data.

2.2.9 Post-Marketing Surveillance Plan

The aim is to channel information from professionals, users or other stakeholders on incidents, complaints or alleged incidents involving the use of the application. Part of this plan will be dedicated to post-market clinical follow-up, designed to confirm the effectiveness and application security, the acceptability of the risks identified and the detection of emerging risks on the basis of objective evidence.

The European Commission’s guide for the development of the monitoring system also provides indication to obtain performance information once the product is on the market to allow for a better control of product hazards [MEDDEV09].

2.3 Specific Standard Requirements for the ALFRED System

The ALFRED solution elements may include sensors, software, mobile ICT-devices and an associated network infrastructure. Each of these elements should be classified as a device, an accessory or a component, depending on the construction of the specific element and the intended use. Specific standards apply to each of these elements. The product must to be considered as two independent devices: the App and, for example, the sensorized t-shirt. In some cases, the rules may be specific to the software's global standards guides or to medical devices.

The following sub-chapters sum the ALFRED-system components and their main functions.

2.3.1 Personal Assistant

The **Personal Assistant (PA)** provides the graphical user interface and is the central access point between the ALFRED components, third-party apps, and games. It must permit users to fulfil their tasks and objectives in an effective, efficient and assenting

manner. However, the usability of a user interface is always highly dependent on the context.

The ISO/IEC has published the following additional standards related to usability:

- ISO/IEC 9126 Software engineering - product quality. This standard refers to the quality of whole software products. Usability is part of the standard and is supplemented by understandability, learnability, attractiveness and conformity [ISO9126];
- ISO/IEC 12119 Software packages. Quality requirements and testing: This standard also stipulates criteria for the quality of software. It does not address usability directly, but demands reliability and usefulness (learnability) [ISO12119];
- EN ISO 9241 Ergonomic requirements for office work with visual display terminals: This standards series currently consists of about 30 parts describing the guidelines for man/computer interaction. In EU law it acts as the guideline for the assessment of usability. The parts include among others the design of classic input and output devices and the design of interactive dialogue systems [ISO9241];
- EN ISO 9241-20 Part of the standards series Ergonomic requirements for office work with visual display terminals: Accessibility guidelines for information/communication technology equipment and services. This part of the international standard is intended for use by those responsible for planning, design, development, acquisition and assessment of information/communication technology equipment and services [ISO9241];
- EN ISO 9241-171 Part of the standards series Ergonomic requirements for office work with visual display terminals: Accessibility guidelines for software. This part of ISO 9241 makes demands and recommendation for the design of accessible software for use at work, in the home, in the education sector and in the public domain. It deals with problems related to the design of software that is accessible for people with the widest possible range of physical, sensory and cognitive abilities, including those with temporarily impaired capabilities and older persons [ISO9241];
- EN ISO 9241-210:2010 Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems (ISO 9241-210:2010). In contrast to ISO/IEC 9126 and ISO/IEC 12119, which refer to the product, this standard refers to process quality. Its core focus is human-centred design that puts the focus on the user in all phases of the development process [ISO9241];
- EN ISO 14915 Software ergonomics for multimedia user interfaces. This standard focuses on media and navigation. It names the principles such as target orientation, understandability, structure and user motivation [ISO14915-1, ISO14915-2];
- EN ISO 11064 Ergonomic design of control centres. This standard stipulates environment-related requirements for control centres, regulating their design processes and working conditions [ISO11064];
- IEC 60601-1-6 Medical electrical equipment - Part 1-6: General requirements for basic safety and essential performance - Collateral standard: Usability. As in DIN EN ISO 14915, this standard describes the requirements made of the process. Here again the focus is on usability, while basic safety is another essential aspect and prerequisite for CE marking [IEC60601];

- EN 62366 Medical devices - Application of usability engineering to medical devices. This standard stipulates the obligation for compliant process and risk management and is prerequisite for CE marking [IEC62366];
- ISO/IEC Guide 71 Guidelines for standards developers to address the needs of older persons and persons with disabilities. This document provides guidelines for designing accessible systems for older persons and persons with special needs. It helps to improve the general situation of the elderly and the disabled. The intention is not just to inform developers but to support authors of specifications in this field. ISO/IEC Guide 71 is available as European guidelines in English and German [ISO71].
- ISO/TR 22411 Ergonomics data and guidelines for the application of ISO/IEC Guide 71 to products and services to address the needs of older persons and persons with disabilities is an important collateral document containing instructions for using the ISO/IEC Guide 71. The Technical Report contains ergonomic data and knowledge about human capabilities in the sensory, physical and cognitive sphere and when suffering from allergies [ISO22411].

Machine-to-Machine is a newly developed ETSI specification that stands for the automated exchange of information between machines. It describes generally useful M2M functions such as security, data transmission, boot strapping and an application programming interface for services. The API permits communication between individual M2M components (such as sensors and actuators), M2M gateways and service platforms. Systems and machines should exchange data in a completely automated process without human interaction. M2M abstracts from the basic LAN and WAN technology. ETSI-M2M as developed on the basis of requirements from a number of use-case documents. Relevant examples in the AAL context are “eHealth” [TR102732] and “Connected Consumer” [TR102857]. The notable specifications of ETSI-M2M are:

- TS 102 689: M2M service requirements [TS102689]
- TS 102 690: M2M functional architecture [TS102690]
- TS 102 921: M2M mla, dla and mld interfaces (draft) [TS102921]

2.3.2 Health Monitor

The **Health Monitor (HM)** provides access to the external sensors and wearables which are part of the ALFRED solution, collects raw sensor data and processes it to health information. Separate standards apply to the sensors and actuators of other branches of industry, which are listed below. Reference is provided for details:

- ISO/IEEE 11073: Health informatics – Personal health device communication. This standards family defines an application protocol for networking vital sign sensor devices using USB and Bluetooth among others. But in practice, up to now the individual device vendors use their own proprietary interfaces. Some parts of this standards series are also available as EN ISO 11073 [ISO11073].

It is also worth mentioning new de-facto standards such as BlueRobin, primarily serving medical sensors. Most applications are unidirectional, although there is an increasing trend towards bidirectional (complex) application.

2.3.3 Context-Aware Dialogue Engine

The **Context-Aware Dialogue Engine (CADE)** is responsible for the spoken interaction between the end user and the ALFRED system. It receives input from the microphone, interprets recognized speech, interacts with apps and games, and provides spoken output.

2.3.4 ALFREDO Marketplace

The **ALFREDO Marketplace (AM)** is the repository for all ALFRED apps. It provides management functionalities to the end user, such as finding, installing, updating and deleting an ALFRED app. It also enables developers to upload and manage ALFRED apps.

2.3.5 Personalisation Manager

The **Personalisation Manager (PM)** is the central hub for all user profile information. It processes raw data in order to acquire new, more complex knowledge about the user. All this information is then provided as a service to the other components of the ALFRED system.

2.3.6 Event Manager

The **Event Manager (EM)** gathers event information, which is automatically collected by crawling specific domains in the Internet and manually through user input in a web portal.

2.3.7 Game Manager

The **Game Manager (GM)** provides and manages the serious games of the ALFRED system. It uses information for the Personalisation Manager, Health Monitor and the ALFREDO Marketplace in order to suggest and adapt games to the end user.

2.3.8 Knowledge and Information Storage

The **Knowledge and Information Storage (KIS)** acts as a provider of various types of databases to the components of the ALFRED system. It thus enables the other components to store all data save and secure, ensuring data sustainability and privacy.

2.4 Standards Framework Definition for Multiple Stakeholders

Technical standards describe the responsibilities of various stakeholders. In the case of the ALFRED solution, they define a specific framework for manufacturers, specification developer, component supplier, app distributor, application programming interface developer.

- **Manufacturers**: they are responsible for defining the intended use of the device and its specification.
- **Specification developer**: in case specification development is contracted out to an organisation that will not manufacture the device, the manufacturer will specify to the specification developer the quality standards that must be applied (such as ISO 13485, ISO 14971 and software standards) [ISO13485, ISO14971].

- **Component supplier:** the manufacturer must put in place quality and service level agreements to ensure that components are supplied to an appropriate quality standard.
- **App distributor:** App authors are generally required to follow limited template development rules and some distributors undertake perfunctory peer review to check performance of the app. Currently distributors (e.g. iTunes) are exempt from medical device regulation.
- **Application programming interface developer:** an API developer can, in theory, aim at being "medical use ready": This claim does not sufficiently define its intended use or identify a complete test programme; therefore it cannot yet be classified or approved as a medical device. The analogy would be the same as any component that meets a certain recognised standard (for example a polymer meeting USP Class 6, or an accessory/component meeting Continua), but is not an approvable product in its own right. These components would be marketed as potentially suitable for use in medical products and then evaluated within the context of the product into which they have been incorporated. Being "continua ready" should therefore not impact the certification of a device with no specific medical intended use. However, for the API to be useful for medical devices, any software should be developed with medical regulations in mind (e.g. ISO 13485) as it's often harder to retrospectively validate software for medical applications, should this become the intended use. On the other hand, an API can be marketed with a (or multiple) specific medical intended use (for example, being an accessory of a specific medical App): Then the development process is impacted by med device regulations which involve supporting specification, testing and documentation according to ISO 13485/CFR 820.

2.5 Business and Quality Management Standards

Regulations are necessary tools to safeguard end-users and support the product development. Throughout all the development and production process, managing quality is essential to reach quality and sustainability objectives and ensure the end users' satisfaction. It implies all the organizational structure, policies, procedures, processes and resources needed to implement quality management. Depending on the characterisation of the final ALFRED product (wellness or medical intended use), different levels of manufacturing practices should be followed. Specific Quality System requirements apply to medical devices

2.5.1 Business Management Standards

ISO management system standards provide a model to follow when setting up and operating a management system. The benefits of an effective management system include:

- more efficient use of resources
- improved risk management, and
- increased customer satisfaction as services and products consistently deliver what they promise [ISO19011].

More specifically, ISO 22301 specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure your business recovers from disruptive incidents [ISO22301].

2.5.2 Quality Management System

The ISO 9000 family addresses various aspects of quality management and contains some of ISO's best known standards. The standards provide guidance and tools for companies and organizations who want to ensure that their products and services consistently meet customers' requirements, and that quality is consistently improved. They define the quality measures for both production and quality control as well as the general measures to ensure that processes necessary for production and testing are clearly defined, validated, reviewed, and documented.

Standards in the ISO 9000 family include:

- ISO 9001:2008 - sets out the requirements of a quality management system [ISO9001]
- ISO 9000:2005 - covers the basic concepts and language [ISO9000]
- ISO 9004:2009 - focuses on how to make a quality management system more efficient and effective [ISO9004]
- ISO 19011:2011 - sets out guidance on internal and external audits of quality management systems [ISO19011].

These standards are based on a number of quality management principles including a strong customer focus, the motivation and implication of top management, the process approach and continual improvement. Using Quality Management system helps ensure that customers get consistent, good quality products and services, which in turn brings many business benefits.

2.5.3 Guidelines for Certification

Product certification or product qualification is the process of certifying that a certain product has passed performance tests and quality assurance tests, and meets qualification criteria stipulated in contracts, regulations, or specifications. Apart from facilitating access to market, it contributes to add more credibility to manufacturers and developers by demonstrating to end-users, customers, competitors, suppliers, staff and investors that they are committed to being quality standards.

In the field of the mobile and health apps, there are several institutions around the world promoting recommendations and practical guidelines for their design, implementation and use, such as the Food and Drug Administration, Happtique, Devices 4 Limited or mHIMSS [D4L12]. Additional Resources to Supplement Apps Market Review are shown in Table 2.

Other institutions, such as the European Commission, the National Library of Medicine or the National Health Service (UK), are promoting a repository website where some apps are included after being submitted to some kind of screening process. The CE Mark for medical devices (European Commission) could be applied in some kinds of apps used in clinical environments. The main recommendations include standards related to

accessibility, privacy and confidentiality, technical aspects, security and scientific accuracy [ML13].

- The FDA has approved approximately 75 apps that comply with their recommendations for interoperability and security. The FDA issued the Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff on September 25, 2013, which explains the agency's oversight of the mobile medical apps as devices and their focus only on the apps that present a greater risk to patients if they don't work as intended and on apps that cause smartphones or other mobile platforms to impact the functionality or performance of traditional medical devices [FDA03].
- The Health App Certification Program (HACP) – Happtique: Operating as a complement to FDA oversight, the HACP is the mHealth application certification program of the New York-based mobile healthcare provider Happtique. It developed a set of final standards for mHealth applications to evaluate and certify mHealth apps in terms of their operability, privacy, security and content. It provides the market with a means to self-regulate, raising the bar for all developers while increasing consumer and provider confidence in this rapidly growing industry. Each app examined for certification is submitted to both technical testing--the verification of privacy, security, and operability standards by global testing leader Intertek--and content testing, as completed by relevant, independent clinical experts [Happ01].

Table 2 Other Resources to Supplement Apps Market Review

Resource	Description
mHIMSS	Analyzed more than 43,000 healthcare apps available on iTunes; Provides a Roadmap that shares best practices for implementing mobile and mHealth strategies
iMedicalApps.com	Physician curated and generated reviews with indexed search functions by app type, physician specialty, and device platform
KLAS	Reviews on "mobile data systems"
Mobilehealthnews	News and Reviews on the latest medical apps

3 Regulatory Framework for Health Related Services on Communication Devices

In the rapidly evolving field of telecommunications, countries around the world face the complex challenge to adapt to the new developments. Increasingly, the mobile technologies are used as a support for medical devices. Policy makers and regulatory bodies have been reviewing existing frameworks, enacting legislation and creating new regulatory authorities to implement their legal and regulatory framework.

Health-related services on smartphones, tablet, PCs and other communication devices can be divided in apps; on one side, the mobile applications related to health and, on the other side, the apps related to wellness. Sometimes the distinction of these type types of apps is blurred, as the both focus on various aspects of promoting health. Solutions across the patient pathway include wellness, prevention, diagnosis, treatment and monitoring and entail direct touch points with patients.

The devices that potentially affect users' health must comply with specific regulations to ensure patients' and users' safety. The objective of this chapter is to determine which regulations may apply to the ALFRED-system. This will depend on the ALFRED solution's use as (i) *health* or (ii) *wellness device*. When considered a *health application*, users (medical professionals or lay persons) should be clearly aware of its regulatory status as a mobile health solution. Different legal dispositions apply.

3.1 Determination of Regulations Applicability: Wellness VS Medical Devices

Although they are often used interchangeably under the term mHealth apps, there is a distinction in the regulations that apply to medical devices and wellness applications. While the wellness applications are considered to have a mild impact on the user's health as those only focus on general health and wellness and promote wellness awareness, the medical devices are used to support the diagnostic and treatment of diseases and as such are subject to more stringent regulations to protect the patient's safety. Defining whether a product is a medical device represents the first step in the identification of the applicable regulations and the consequent potential impact of medical device regulations for new products (see below Figure 2 Guidance on Medical Definition).

The distinction between medical and wellness devices is sometimes difficult to establish. In particular, the determination of the regulation that would apply to mobile applications directly accessible to consumers, with no medical supervision, is complicated and subject to interpretation. For example, the distinction between Mobile Medical Apps and Mobile Wellness Apps can become unclear as healthcare models become more patient-centric. Today, the impact on quality of life or health outcomes may be significantly improved through preventive and self-monitoring activities. Some mHealth solutions, such as health and fitness Apps, intended to support general consumer wellness could arguably, if integrated in a diagnosis and treatment regimen, be classified as a medical device.

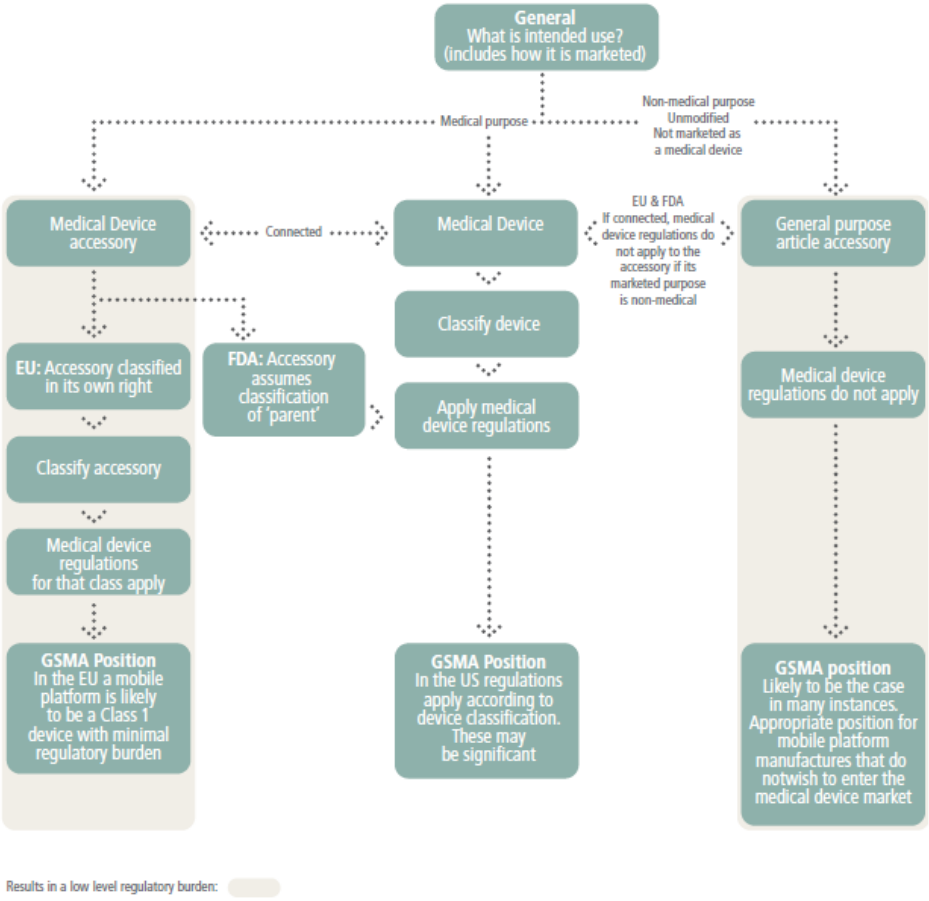

Figure 2: Guidance on Medical Device definition [GSM12-2]

In doubt a manufacturer can consult with a notified body or a supervisory authority to determine whether or not a product falls into the scope of the Medical Device Directive. This has far-reaching legally binding consequences for the manufacturer, the operator and the user.

3.1.1 Determination of the "Intended Use" of the Product

Under which circumstances might a product intended to support self-awareness and well-being become subject to the medical device regulation?

Determination with respect to applicability of medical device regulation to a product or service is based on the **intended purpose (also referred to as "intended use")** of the product and its mode of action[2]. Considering a product's intended use in conjunction with the regulator's definition of what constitutes a medical device enables manufacturers to decide with reasonable clarity, whether the product will fall within the scope of the regulation [GSM12-2]. The intended purpose of the medical device is examined in very similar terms by the EU and US legal bodies (see Table 3 - Comparison of the focus of

[2] The principle of considering the "intended use" of the product in medical device regulation is common to the both, the EU and the US.

legislation of medical and wellness devices between the US and the EU legal bodies) In this respect, when there are no claims made regarding the suitability of a network or a mobile device for medical purposes, medical device regulation should normally not apply.

Table 3: Comparison of the Focus of Legislation of Medical and Wellness Devices between the US and the EU Legal Bodies

	Medical devices	Wellness Devices
U.S. FDA	Focus on diagnosis and treatment of diseases	Focus on general health and wellness and promote awareness and wellness
E.U. Medical Device Directive	Focus on diagnostic and/or therapeutic purposes	Lifestyle and wellbeing apps primarily include apps intended to directly or indirectly maintain or improve healthy behaviours, quality of life and wellbeing of individuals

For example, an app that records how many miles an individual runs is a wellness app. But if the same app claims to track exercise to help address obesity, then it can be linked to a disease state and transforms into a medical app – which may then be regulated by the FDA or the European Medical Devices Directive.

On both the Apple and Android platforms there are two distinct categories: “Medical” that targets the health care professionals and “Healthcare & Fitness” is often used to describe apps for use by patients and the general public. It is important to stress that the allocation of apps to these categories is not closely curated – developers may submit their app categorised as they feel appropriate, and may list the same app under multiple categories.

3.1.2 Risk Assessment and Medical Device Classification

The purpose of medical device regulations is to minimise risks for the patient, the user and third parties caused by the use of the medical device through mandatory requirements concerning the production processes, documentation, certification, distribution channels, training, limitation of use, operation, incident reporting and maintenance.

All medical devices require adoption of a risk based approach to product and system development in accordance with ISO 14971:2007 Medical devices - Application of risk management to medical devices [ISO14971]. In support of this, the regulatory process evaluates each device on a case-by-case basis to discriminate between high, medium and low risk devices. This evaluation is based on the risk of harm posed to the users and not technological complexity. It is this risk based approach that ensures regulatory controls are applied in a proportionate and appropriate way, avoiding over-regulation of low risk devices (see Figure 3 Increasing levels of risk of harm to users is mitigated by applying an incremental level below). Depending on the classification, quality management systems, risk management and post-market surveillance processes have to be established by the organisation placing the device on the market, and verified in a regulatory compliance audit. Risk assessment forms the basis of the medical regulatory approval process.

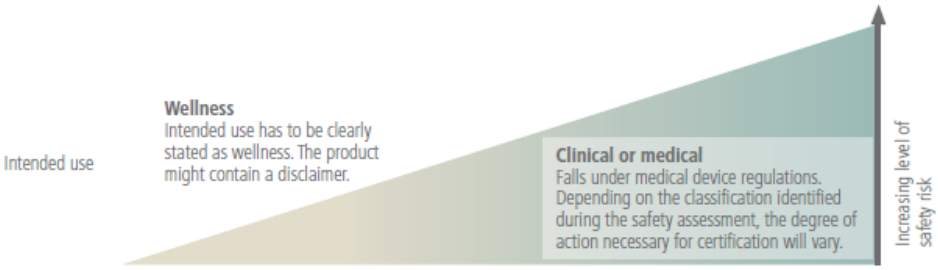

Figure 3: Increasing Levels of Risk of Harm to Users Is Mitigated By Applying an Incremental Level [GSM12-1]

Similarly in the US the FDA is taking a tailored, risk-based approach that focuses on the small subset of mobile apps that meet the regulatory definition of 'device' and that are intended to be used as an accessory to a regulated medical device, or transform a mobile platform into a regulated medical device. Mobile apps span a wide range of health functions. While many mobile apps carry minimal risk, those that can pose a greater risk to patients will require FDA review.

According to the FDA, there are three categories of apps identified [FDA14]:

- Apps "for the purpose of displaying, storing, analysing, or transmitting patient specific medical device data"
- Apps that "transform or make a mobile platform into a regulated medical device or performs similar medical device functions"
- Apps that "allow the user to input patient-specific information and - using formulae or a processing algorithm - output a patient-specific result, diagnosis, or treatment recommendation that is used in clinical practice or to assist in making clinical decisions".

3.1.3 ALFRED Wellness / ALFRED Medical

The ALFRED system will be constituted of a mobile device (phone, tablet, watch or other) and of a platform for apps. Regulations applying to the App writers, App distributors, and manufacturers of the device should be identified. Potential development of the ALFRED solution could lead to the commercialisation of different products and services, falling either under the wellness field or the medical application.

The main discussion about mHealth applications is the need to define a framework for the Health Apps Certification that would help to reach the effectiveness standards and the minimal security levels. This framework exists with the Directive 93/42/CE about sanitary products [MDD07]. In addition, the CE is going to publish soon a new sanitary product regulation that will incorporate new requirements and will revise the existing ones.

The interpretation difficulty of the current legislation can be solved with a conceptualization of the normative requirements and the identification of a few steps that help to orientate in the certification of the Health App.

First, it's necessary to know if the App belongs to the mHealth applications group knowing if it belongs to some of the three possible groups of the Health Apps:

1. Health Apps that are not considered sanitary products
2. Health Apps that are assimilated as sanitary products but have a low risk for the user.
3. Health Apps that are considered sanitary products and have a medium-high risk for the user.

To determinate which group a mHealth application belongs, the following four questions should be responded:

- Is it a computer program?
- Does it generate or modify data?
- Is it intended to benefit the individual patients?
- Is it designed for use as a medical device?

If the answer is affirmative in all four cases, the app is considered a medical device and therefore belongs to group 2 or 3. Moreover, if it is designed to benefit the individual patients, it is likely that it should keep in line with the personal data protection legislation.

Once the mobile application has been categorized as a medical device, the next step is to classify according to the risk to the user. The CE offers the 2.4 MedDev guide to support this process with a series of rules and diagrams [MEDDEV09].

However, one can state on a more general term that if an app does neither implement a function of measurement nor use invasive accessories or control risk devices (such as blood pressure monitors or insulin pumps), the app is associated with a low risk or Class I. The next table shows the annexes that the different classes of clinical products must comply (see Table 4 Conformity Assessment Procedures for mHealth Applications).

Table 4 Conformity Assessment Procedures for mHealth Applications

CONFORMITY ASSESSMENT PROCEDURES	**CLASSES**					
ANNEXES	I	I Sterile	I measure	IIa	IIb	III
II (+ section 4)						✓
II (- section 4)		✓	✓	✓	✓	
III					✓	✓
IV		✓	✓	✓	✓	✓
V		✓	✓	✓	✓	✓
VI		✓	✓	✓	✓	
VII	✓	✓	✓	✓		

For the applications with Class I the Directive allows a self-certification process in which the developer declares conformity with the requirements for such applications and incorporates the CE marking to the app.

For certification of medium and high risk applications (Classes II and III), the Directive requires the involvement of so-called organized Reportable Organizations that are accredited by the national competent authority, with a degree demanding commensurate with the risk of application. In these cases, these Organizations are who issue the declaration of conformity and assigned certification numbers which must to be placed next to the CE mark.

3.1.4 Legal Prospects

Depending on the ALFRED system's classification as a simple mobile health application or as a medical device, requirements in terms of regulations and standards to meet will vary greatly. In contrast to the regulations in the telecommunications industry, the medical device regulations can appear complex. In Europe, routes to approval depend on the medical device classification. In order to meet with the MDD essential requirements, manufacturers must provide and demonstrate that they have:

- Technical documentation which must contain full construction details and test data known as design validation and verification for your medical device (ISO / TR 16142) [ISO16142].
- Performed a safety assessment that includes a construction evaluation, the specification of the materials used, the bio-compatibility analysis and the analysis of the potential risks during use.
- A quality system, which can be achieved by conforming to ISO 13485 [ISO13485].

Ultimately, the regulatory landscape is evolving rapidly as more products are being developed to address health, wellness, or medical purposes, which, though not clearly intended as medical devices, could be re-classified as such following a potential change in the regulation. In its 2012 report, GSMA recommends manufacturers to be "prudent and keep uppermost in mind the concepts of intended use´ and ´potential to cause harm' [GSM12-1]. Updates will be provided in the subsequent deliverables 9.6.

3.2 Multiple Sources of Regulations

3.2.1 Sources of Regulation at the EU Level

At the European level, there is no specific agency in charge of evaluating and approving the entry to the market of medical devices. The European Medicines Agency is responsible for the scientific evaluation of medicines developed by pharmaceutical companies for use in the European Union, and it can be consulted on medical devices that contain medicinal substances. However, it plays no role in the device industry. Instead, medical devices are evaluated by the medicines regulatory authorities in each Member State.

Private reviewers, known as notified bodies and certified by member state governments, are in charge to assess the device for safety according to standards set out by European

Commission directives and grant a so-called CE mark associated with market authorisation. The mobile medical apps are medical devices that are mobile apps, and as such fall under the EU regulatory frameworks for both medical devices and telecoms.

- The EU Radio and Telecommunications Terminal Equipment (RTTE) Directive, is the main route to compliance for Radio and Telecoms equipment that is marketed in the EU. Compliance with this Directive is required in order to place a CE Mark on these products [RTTE99].
- The EU Medical Devices Directives (MDD) which may place a higher burden of design control, testing and Premark and clearance. (Directive 93/42/EEC, *under revision, new directive to be adopted in 2014 [MDD07]*)

The quality assurance requirements for each Directive, whilst similar, lead to the application of different harmonised standards (ISO 9001 and ISO 13485).

3.2.2 Adaptation at the Country Level

There is no central European register of registered medical devices. Each national Competent Authority manages its own register, and a manufacturer needs only to register in one member state to place its device on the market across the EU, as there is mutual recognition.

The transposition of the EU Directive on Medical Devices in each Member State is carried out with the support of “MEDDEV Guidance Documents”[MEDDEV09]. These documents are the strongest documented consensus of how directives or specific parts of a directive are interpreted. These instructions reflect the consensus position of the national members of the competent authorities on such issues as the demarcation between the MDD and AIMDD Directive, definition of an accessory, classification of devices, translation procedures and much more. The opinion of this group is not legally binding but is considered the "highest" of guidelines in the industry.

However, there may be variations in how this and other Directives have been transposed into the national law from country to country. The individual competent authorities may have differing interpretations on the meaning of what was originally approved, and additional differences can occur due to the simple translation errors. A procedure for decisions on whether or not a product falls under the medical device definition may have been established for the appropriate and efficient functioning of Directive 93/42/EEC as regards to classification issues.

3.2.3 Overview of the US Regulation

The FDA provides regulations and delivers market authorisation for medical devices. Recently it published its final guidelines for regulating mobile medical applications to clarify associated legal requirements. Importantly, it states that its regulatory coverage would focus only on the apps that present a greater risk to patients if they don’t work as intended and on apps that cause smartphones or other mobile platforms to impact the functionality or performance of traditional medical devices. For these mobile medical apps, the FDA will apply the same risk-based approach as the agency uses to assure the safety and the effectiveness for other medical devices.

3.2.4 Additional European Regulations

- Liability for defective products (1985/374/EC &1999/34/EC [EC99-1])
- General product safety (2001/95/EC [EC01])
- Sale of consumer goods (1999/44/EC [EC99-2])
- Information society services and ecommerce (2000/31/EC [EC00])
- Data Protection (1995/46/EC [EC95])
- Misleading and comparative advertising (2006/114/EC [EC06])
- Unfair business-to-consumer commercial practices (2005/29/EC [EC05])

4 Essential Ethical Issues of Managing Users Related Information and Legal Requirements

During the recent years, the mobile technology solutions adapted for older adults have been developing and expanding rapidly. These solutions are intended for the older users and their carers enabling to monitor users' health and safety and to promote social inclusion and autonomous lifestyle. In particular, mHealth is an emerging and rapidly developing field that has the potential to play a part in the transformation of the healthcare paths and to increase the quality and efficiency of the healthcare system by facilitating the integration of the use of electronic devices and applications to monitor and share patients' health related information [VPZ12].

Furthermore, the ALFRED solution faces the major challenge to protect its users' personal and medical information and their private lives as the system requires access to its user's personal and health related information enabling to monitor their health status. The research in the ALFRED project and the development of the ALFRED solution should also be conducted in the respect of the ethical guidelines that ensure the end-user's protection and rights.

4.1 Introduction to Ethical Issues in Assisted Living Solutions and in the ALFRED System

Social applications, mHealth solutions and related devices can collect large quantities of medical, physiological, lifestyle, daily activity and environmental information (e.g. data stored by the user on the device and data from different sensors, including location) and process them. The rapid development of the mHealth sector raises concerns about the appropriate processing of the data collected through the apps or solutions by individuals, app developers, health professionals, advertising companies, public authorities etc.

There are legitimate concerns about the security of the individuals' personal data when using mobile technologies as this sensitive data could be accidentally exposed or easily leaked to unauthorised parties (e.g. employers or insurers). All the relevant ethical issues related to the ALFRED system and the ALFRED research project are reviewed in this chapter.

4.1.1 Ethical Issues related to Processed Personal Data and Respect of Private Life

Definition of personal data*:* Any data that can be connected to and identifies an individual, such as a name, a telephone number, a photo etc. [EC14]*.*

Definition of private life: The definition of private life is rather open in international legislation; this notion concerns the individual's freedoms, family and home. As a result, the right to private life includes a wide range of overlapping and interrelated rights protecting the individual's freedom. Moreover, the right to privacy is the right to individual autonomy. The right to privacy encompasses the right to protection of a person's intimacy,

identity, name, gender, honour, dignity, appearance, feelings and sexual orientation and extends to the home, the family and correspondence.

Information relating to individuals is collected and used in many aspects of everyday life. These data may subsequently be used for other purposes and/or shared with other parties. Personal data can be any data that identifies an individual, such as a name, a telephone number, or a photo. Advancement in computer technology along with new telecommunications networks is allowing personal data to travel across borders with greater ease. As a result, data concerning the citizens of one Member State are sometimes processed in other Member States of the EU. Therefore, as personal data is collected and exchanged more frequently, regulation on data transfers becomes necessary.

Data controllers are the people or body which determines the purposes and the means of the processing, both in the public and in the private sector. Data controllers are required to observe several principles. These principles not only aim to protect the data subjects but also are a statement of good business practices that contribute to reliable and efficient data processing. Each data controller must adhere to the data processing rules of the Member State where he or she is established, even if the data processed belongs to an individual residing in another State. When the data controller is not established in the Community (e.g., a foreign company), he or she has to comply with the laws of the Member State(s) if the processing equipment (e.g., a computing centre) is located within the European Community [OECD13].

4.1.1.1 European Regulatory Framework

Personal data protection is a fundamental right in Europe, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, as well as in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) [TEU92].

It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data.

In the EU, the currently applicable Personal Data Protection Directive is being revised in order to better respond to challenges posed by the rapid development of new technologies and globalisation while ensuring that individuals retain effective control over their personal data: the Commission's proposal for a General Data Protection Regulation will provide for further harmonisation of data protection rules in the EU, ensuring legal certainty for businesses and increasing trust on eHealth services with a consistent and high level of protection of individuals [EC14]. Within the ALFRED project and in the next Deliverable 9.6, the situation of the revised Personal Data protection directive will be updated to ensure that the ALFRED solution respects the highest standards of personal data protection.

- **European Convention for the Protection of Human Rights of 4 November 1950 [EC50]**

Article 8 of the European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society"

- **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 [EC95]**

The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 intends to ensure the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive lays down a series of rights of the data subject, for instance a demented patient. These are:

- The right of access to his/her personal data;
- The right of erasure, blocking, or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate;
- The right to be informed of all relevant details relating to the data processing and the rights granted to him/her;
- The right to a judicial remedy for any breach of the above mentioned rights.

All these are applicable to ALFRED. The first three aforementioned rights may be restricted if this is necessary for reasons relating to the protection of the data subject or the rights and freedoms of others or to prevent a criminal offence or for reasons relating to public security.

The rules according to the directive are:

- Data must be processed fairly and lawfully.
- They must be collected for explicit and legitimate purposes and used accordingly.
- Data must be relevant and not excessive in relation to the purpose for which they are processed.
- Data must be accurate and where necessary, kept up to date.
- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them.
- Data that identifies individuals must not be kept longer than necessary.

The Directive states that each Member State must provide one or more supervisory authorities to monitor the application of the Directive. One responsibility of the supervisory authority is to maintain an updated public register so that the general public has access to the names of all data controllers and the type of processing they do.

In principle, all data controllers must notify supervisory authorities when they process data. Member States may provide for simplification or exemption from notification for specific types of processing that do not entail particular risks. Exception and simplification can also be granted, in conformity with national law, when the controller has appointed an independent officer in charge of data protection. Member States may require prior checking, to be carried out by the supervisory authority, before data processing operations that involve particular risks may be undertaken. The member states to determine the specific data processing operations that involve particular risks for the users.

When can personal data be processed?

Personal data can only be processed (e.g., collected and further used) if:

- The data subject has unambiguously given his or her consent, i.e., if he or she as agreed freely and specifically after being adequately informed;
- Data processing is necessary for the performance of a contract involving the data subject or in order to enter into a contract requested by the data subject, e.g., processing of data for billing purposes or processing of data relating to an applicant for a job or for a loan;
- Processing is required by a legal obligation;
- Processing of data is necessary to protect an interest that is essential for the data subject's life. An example is in the case of a car accident and the data subject is unconscious; emergency paramedics are allowed to give blood tests if it is deemed essential to save the data subject's life;
- Processing is necessary to perform tasks of public interests or tasks carried out by official authorities (such as the government, the tax authorities, the police, etc.).

Finally, data can be processed whenever the controller or a third party has a legitimate interest in doing so. However, this interest cannot override the interests or fundamental rights of the data subject, particularly the right to privacy. This provision establishes the need to strike a reasonable balance, in practice, between the business's interest of the data controllers and the privacy of data subjects. This balance is first evaluated by the data controllers, under the supervision of the data protection authorities, although, if required, the courts have the final decision. (See Table 5 for a Summary of the processing principles applying to personal data)

Table 5 Summary of the Processing Principles Applying to Personal Data

Processing Principles	Description
Collection	Data to be fairly and lawfully obtained
Proportionality	Personal data should be adequate, relevant and not excessive to the purpose for which it is collected
Use	No disclosure, transfer or other use except those needed to achieve the purposes specified except: – With consent of data subject – Pursuant to law
Data Quality	As needed for specified purposes, collected and stored data should be accurate, complete & up-to-date
Transparency	Data subjects should have the means to know existence and nature of processing; purposes of their use; the identity and location of the entity controlling the processing; whether any data is likely to be transferred and to whom

Access and Correction	Data subjects should be allowed to access their data and make corrections to any inaccurate data
Objection	Data subjects should have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data
Transfers	Transfer of personal data to third (non-EU) countries are prohibited except under limited specific circumstances
Security	Appropriate measures by data controller to guard against: – Loss or destruction of data – Unauthorised processing or disclosure "at the time of the design of the processing system and at the time of the processing itself"
Accountability	Data subjects should have a method available to them to hold data collectors accountable for not following the above principles

- **Charter of Fundamental Rights of the European Union of 7 December 2000 (Article 7 and 8) [CFR00]**

The Charter of Fundamental Rights in the course of the respective legal trend dedicates a separate article to the protection of personal data. Article 7 of the Charter specifies the right of every individual to "respect for his or her private and family life, home and communications". Article 8 sets out the right to the protection of personal data of an individual and, thus, the protection of personal data has now its own legal basis, beyond the right to respect for an individual's private life and the protection of the human dignity. Art. 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Finally, Article 8 sets out the need for an independent authority, which shall control the compliance with the data protection rules.

- **European Directive on Privacy and Electronic Communications (02/58/EC) (Article 3 and 4) [EC02]**

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) harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communications equipment and services in the Community.

For this purpose, Directive 02/58/EC particularises and complements 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 and also provides for protection of the legitimate interests of subscribers who are legal persons (in distinction to Directive 95/46/EC).

4.1.1.2 International Regulatory Framework

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology (IT). The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970 This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978).

At an international level, the ALFRED consortium acknowledges heterogeneity in international data protection jurisdiction, starting with the Organisation for Economic Cooperation and Development (OECD) guidelines including the “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (1981) and “Guidelines for the security of information systems” (1991/92) [OECD13].

- **Universal Declaration on Human Rights (1948) [UN48]**

This Declaration of the United Nations marked the modern protection of privacy, and specifically protected territorial and communications privacy. Article 12 states:

“No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.”

- **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981) [OECD13]**

The OECD eight core Privacy Principles provide the most commonly used privacy framework and they are reflected in existing and emerging privacy and data protection laws (see Table 6).

Table 6 OECD Privacy Principles (Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data.[OECD13])

Principle	Description
Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.
Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual Participation Principle	An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability Principle	A data controller should be accountable for complying with measures which give effect to the principles stated above.

4.1.1.3 National Regulatory Framework

In addition to the international and European Union standards, partners will act in accordance with national conventions. All partners will strictly adhere to the legal regulations and guidelines presented by the European Union and all participating countries. In a subsequent section, national codes of conduct and laws for the protection of data, including all subsequent and future amendments that may apply, are identified while adhering to the European Data Protection Law [EC14].

The Data Protection Acts, in each respective country, may differ slightly in their terminology; however, they all provide the same fundamental rights which the end-users of the ALFRED- system should be entitled to. These fundamental rights provide individuals with secrecy of the data concerning the individual and the right to rectification of incorrect data, so long as there are no issues overriding the interests of others. This follows the European Data Protection Law.

4.1.2 Ethical Issues Related to Processed Medical Data

"All *that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."*

Hippocrates, from the Hippocratic Oath

The protection of medical data dates back to the classical period of Ancient Greece history when Hippocrates wrote the oath which every new physician was required to swear, upon a number of healing gods, to uphold specific ethical standards. The eleventh area covered is Confidentiality which simply mentions that a doctor will not repeat anything that is seen or heard. Further legislations have come to strengthen this right of users and patients to have their medical data protected. The ALFRED solution must ensure the respect of the ethical processes related with the access, process and use of the end users' medical data.

4.1.2.1 European Regulatory Framework

- **European Union Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine**: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997 [CHR97]

Article 3 (under Chapter 1 – General provisions) recalls the commitment of Parties to the Convention to provide equitable access to health care. Article 5 (under Chapter 2 – Consent) highlights the obligation for a person to give his/her free informed consent before any intervention in the health field can be carried out on this person. Exceptions may occur for the protection of persons who have a mental disorder (article 7), in case of an emergency situation (article 8), and if wishes have been previously expressed (article 9).

Importantly, article 10 of Chapter 3 protects the right to private life and to information as follows:

- Everyone has the right to respect for private life in relation to information about his or her health.
- Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.

- In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.
- **European Union Data Protection Directive** (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data); to be replaced in the future by European General Data Protection Regulation [EC95]

The European Data Protection Directive 95/46/EC is one of the major instruments of EU data protection law. Data protection plays a significant role to reduce or even inhibit the processing of sensitive data (Art. 8 of Directive 95/46/EC), which encompasses “personal data concerning health”.

The meaning of the term “personal data concerning health” has been carefully studied by the Committee of Experts on Data Protection in connection with its work on medical data banks. It includes information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased.

The European data protection legislation grants patients (as data subjects) a number of rights once identifiable data are processed. These rights are the following:

- to be aware of the processing of their data, its purposes, the identity of the data controller, the identity of the possible recipients of the data;
- to have access to a copy of the information comprised in their personal data;
- to object to processing;
- to prevent processing for direct marketing;
- to object to decisions being taken by automated means;
- in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed;
- to claim compensation for damages caused by a breach of the Privacy Directive.

Member States are allowed to apply more stringent rules to legitimize the data subject’s consent, be it through the requirement of ‘written consent’ or preventing consent from being the sole basis to authorize the generally prohibited processing of personal health data. The data subject may always revoke the given consent at any time and without justification. This will impede further processing, but not making past operations retrospectively unlawful.

On 25 January 2012, the Commission proposed a comprehensive revision of the current Data Protection Directive which among other issues aims to address key aspects of processing personal health data, to ensure on the one hand privacy for patients while still enabling the EU to meet the other legitimate objectives in the Treaties such as a high level of health protection. The final text will set the rules under which personal data are to be handled in the EU, including in the field of health and research. It is expected that it will introduce much more stringent requirements for explicit consent to use personal data for health or scientific research than under current legislation [EC14].

4.1.2.2 International Regulatory Framework

Internationally, the OECD Privacy Principles from the OECD Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data provide the most commonly used privacy framework, they are reflected in existing and emerging privacy and data protection laws, and serve as the basis for the creation of leading practice privacy programs and additional principles [OECD13].

The OECD Privacy Principles tie closely to European Union (EU) member nations' data protection legislation (and cultural expectations), which implement the European Commission (EC) Data Protection Directive (Directive 95/46/EC), and other "EU-style" national privacy legislation.

4.2 Ethical Guidelines in the Design of the ALFRED Technology

The most important sensitive data protection issues (for the both personal and medical data) that should be considered in the system development of ALFRED will be summarised under this section.

Compliance with personal data protection rules, with information of the data subject, data security, and the lawful processing of personal data, including of health and medical data, is therefore vital for building trust in technological systems that process personal and sensitive data. Guidance exists on data protection requirements for 'apps' [ECGP14, EMC14].

4.2.1 Privacy and Confidentiality

Definition of **privacy**: Only authorized (by the patient) people can see data.

Definition of **confidentiality**: The ethical principle or legal right that a person or a physician or other health professional will hold secret all information relating to a patient, unless the patient gives consent permitting disclosure.

Consent models to user authorization of access to his personal data:

- **No consent:** Health information automatically included—patients cannot opt out
- **Opt-out:** Default is to be included, but the patient can opt out completely
- **Opt-out with exceptions:** Default is to be included, but the patient can opt out completely or allow only select data to be included
- **Opt-in**: Default is not included; patients must actively express consent to be included, but if they do so then their information must be all in or all out
- **Opt-in with restrictions:** Default is that no patient health information but patients can opt-in allowing only select data to be included

4.2.2 Security

Definition of **security**: Data is protected from unauthorized access, during collection, storage, use and access and particularly during transport (from device to device, or within the healthcare context from doctor to doctor, doctor to patient).

The following practices can be used to protect health data:

- **Anonymisation** is the process used to strip personal data from all elements likely to help identify directly or indirectly the data subject (e.g. name, age, address, social security number, etc.). These elements are deleted to ensure re-identification is not possible.
- **Pseudonymisation** is the process of disguising identities - the aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity. This is particularly relevant in the context of research and statistics. Disguising identities can also be done in a way that no re-identification is possible, e.g. by one-way cryptography, which creates in general anonymised data.
- **Encryption** is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent hacking but it reduces the likelihood that the hacker will be able to read the data that is encrypted.

The consortium will pursue the fulfilment of the European Directive and other regulations to ensure the security of data collection, storage, use and access for the ALFRED solution's users.

- **Risk Related to Data and Privacy**

All sensible data will be encrypted and protected during storage and transmission (which takes place across third-party networks (such as the Internet) so that user's identity and privacy will not be compromised. Integration with standards available security and authenticity technologies, such as single sign-on management will be analysed.

- **Data Storage and Transfer**

Ambient Assisted Living research ethics focus on the importance of secure storage, management, and accessing of the related information; data must be stored in a secure environment with control access and other security measures obeyed (e.g., proper temperature control). Additionally, sensitive information needs to be stored in the appropriate hardware means, in the appropriate structure and format, corresponding to the related requirements (e.g., paper, disk, etc.). Accessibility to the information needs to be maintained controlled and the networking configurations should not allow data duplication of circulation [GCE12].

Data transfer in both electronic and other ways will, therefore, be monitored. Data storage and management considerations also impose thoughts concerning (a) the duration of storage of the sensitive information and (b) if any back up policies shall be implemented. For example, the duration of the storage should define the extent of time needed until destruction of the data occurs, in accordance with the level of importance of the data. This procedure ensures avoidance of the inappropriate use and dissemination of the information.

- **Need to Keep Up with New Technologies for Security Reasons**

The security of precious data demands the ability to avoid data theft regardless of the level of cracking techniques. Therefore, the encryption, file and record locking, integrity, the passwords mechanisms as well as the traceability of the data acquisition systems will have

be constantly updated to prevent the possibility of decoding the data management system in any level and disseminating private information.

4.2.3 Trust

Definition of **trust**: people/organizations (including physicians, hospitals, patients in the healthcare context) are who you think they are.

Standard internet security techniques provide authentication and encryption of the communication with a service provider. However they do not provide the user with the means to control or even know how a service provider will actually use their personal information. Mechanisms should be implemented to allow users to make an informed decision to trust a service provider on the basis of facts, such as reputation and security attributes.

Assistive and healthcare electronic services offer important economic and social benefits for our society. End users rely on these services for their safety and care and for improving their quality of life. Trust is a pre-requisite for the acceptance of these services by the end-users.

Importantly, when electronic services include a component of healthcare (e.g. to implement or extend medical treatment), trust establishment is crucial for physicians and service providers. In particular, healthcare providers need to trust the patient data they obtain remotely from the measurement devices deployed in patient's home. It is crucial for them to know that a vital sign of a registered user is measured (not of his friends/children), that the measurement was taken with a certified device, under standardized conditions (e.g., with the blood pressure cuff on the arm at the heart level) and that it is not obtained as a result of device malfunctioning.

4.2.4 Accessibility

ICT accessibility is a term used to describe the degree to which ICT is accessible by as many people as possible. Impairments affect the user's ability to perceive, understand or physically manipulate things. This can be either permanent or temporary and may be due to various physical, mental or environmental conditions.

Accessibility barriers occur when the design of ICT fails to allow for the variation in users' abilities. Accessibility is not to be confused with 'usability' which is used to describe the extent to which a product (e.g. device, service, and environment) can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

The highly heterogeneous group of people using the ALFRED system results in a large number of functional and non-functional user requirements (defined in the deliverable D2.3) that have to be taken into consideration in order to widen accessibility to the solution.

Physical and cognitive issues should be taken into account when designing the ALFRED system in order to enhance an equitable access to its functionalities. Enhanced "Mobile accessibility" i.e. making websites and applications more accessible to people with disabilities when they are using mobile phones should be targeted when possible. WAI's

work in this area includes people using a broad range of devices to interact with the web: phones, tablets, TVs, and more.

Moreover, some socio-economic factors may also influence the general access and the use of the ALFRED solution. While the home-based mobile solutions have long shown promise in helping older people to live more independently, a key barrier has been the cost of placing an internet unit in the home as well as the cost of acquiring the assistive device. Furthermore, the lack of usage skills and self-confidence of older end users can also slow down their purchasing motivation. Solutions that enable the users to connect to their social network or care manager via a cell phone with pre-loaded applications, eliminating the need for a landline, Internet access or Wi-Fi connectivity, might better enhance equity.

In a way to strengthen accessibility, the ALFRED system research and development involves the target end-users in the different development phases. Active end-user involvement in the developing process represents a key feature of the design for all on the route to innovation and new product development. The term Design for All is a process whereby designers, manufacturers and service providers ensure that their products and environments address users irrespective of their age or ability. It aims to include the needs of people who are currently excluded or marginalised by mainstream design practices and links directly to the concept of an inclusive society.

4.3 Ethical Guidelines in Research and Development of the ALFRED Project

The ethical issues formerly described should not only apply to the design of the ALFRED solution but also to the research activities undertaken during the development of the ALFRED project. In addition to these general regulations, guidelines specifically developed to cover research ethics will be respected to best protect all groups involved in the research: participants, institutions, funders, and researchers throughout the lifetime of the research and into the dissemination process. The partners will have clear, transparent, appropriate and effective procedures in place for ethics review, approval, and governance whenever it is necessary. This chapter will provide guidelines so that research in the ALFRED project is designed in a way that the dignity and autonomy of research participants are protected and respected at all times, in particular when involving end users in focus groups, prototype and usability evaluations.

4.3.1 International Policies and European Union Regulations

In addition to the regulations previously mentioned regarding the protection of personal and medical data and privacy, the ALFRED consortium acknowledges the following guidelines and regulations of the EU to ensure an ethical research process:

- **The Nuremberg Code of 1949 on Research Ethics Principles for Human Experimentation [IMT49]**

The Nuremberg Code is a set of guidelines for research ethics principles for human experimentation set as a result of the Nuremberg Trials at the end of the Second World War. The Nuremberg Code consists of ten points of which the voluntary consent of the

research participants is absolutely essential. This means that the person involved should have the legal capacity to give consent and be able to exercise free power of choice. The research participant should have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him or her to make an informed decision. The research participant should be aware of the nature, duration, and purpose of the experiment, the method, and means by which it is to be conducted. Furthermore, the Nuremberg Code states that the experiment should be for the good of society and not inflict unnecessary physical or mental suffering and injury.

- **The Helsinki Declaration of 1964 on the Conduct of Clinical Research [WMA64]**

All consortium members are aware of the Helsinki Declaration of 1964 (Recommendation for conduct of clinical research), as lastly amended in Edinburgh in October 2000. All national legal and ethical requirements of the Member States where the research is performed will be fulfilled. There will be arrangements for protecting the confidentiality of personal data of participants at any time of the research. Potential safety implications of the ALFRED system will be clearly indicated. This means, in detail, that:

- All the test subjects will have the ability to give informed written consent to participate;
- All the subjects will be strictly volunteers and are able to withdraw from the trials at any time without any restraints;
- All personal data collected during the Pilots on the preferences and habits of subjects will be strictly confidential.

In addition, all test volunteers, following detailed oral information, will receive in their own language:

- A commonly understandable written description of the project;
- The project objectives;
- The planned project progress;
- The related testing procedures;
- Advice on unrestricted disclaimer rights on their agreement;
- Access to a complaints procedure.

The written information, as well as the sought informed consent, corresponds to the revised version of the mentioned Declaration of Helsinki. Participants with legal guardian aids, as well as participants who cannot rationalize the expected end-user activities and goal based on any impairment of their cognitive abilities, will be excluded from any project study.

- **European Union Convention For the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine**: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997 [CHR97]

Chapter 5 on Scientific Research provides general guidelines on the protection of persons undergoing research.

4.3.2 National Regulations

In addition to the international standards, partners will act in accordance with community law as well as national conventions. User studies will be carried out in Germany, France and the Netherlands; in each case, respective national laws will apply.

4.3.2.1 **The Netherlands**

The Dutch Data Protection Authority (CBP) supervises compliance with legislation regulating the use of personal data. The CBP primarily supervises compliance with and application of the Dutch Data Protection Act [Wet bescherming persoonsgegevens (Wbp)], the Police Data Act [Wet politiegegevens (Wpg)], and the Municipal Database (Personal Files) Act [Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA)].

The CBP is convinced that self-regulation will contribute effectively to the achievement of the individual's fundamental right to the protection of their privacy. As such, the Authority is promoting the appointment of a data protection officer and is encouraging companies to formulate a code of conduct for their branch of industry or sector. Based on this statement, the NFE has created a code of conduct for our sector as a charity foundation for the elderly. This code of conduct refers to all projects of the NFE that involve volunteers and is focused on issues of privacy and data protection. The code of conduct is still in progress and will be submitted to the CBP committee when finished. Some of the main regulations that have been defined at the moment are:

- Only necessary data of volunteers is collected, not more than absolutely required for the project;
- Personal data is only saved for the time required for the project;
- Personal data is only used for the objectives of the project;
- Reports on projects will never identify individual persons unless express permission has been given;
- The volunteer is informed on the objectives of the project, on the nature of the National Foundation for the Elderly and on other involved organisations.

In compliance with the Dutch Data Protection Act (Wbp) and the code of conduct for our sector, the NFE created an informed consent form that has to be signed by all participants of the interviews, focus group, and pilots that will be executed within the ALFRED project. This form clearly states the privacy rights of the participants and the compliance of the project with these rights.

4.3.2.2 **Germany**

In Germany the data protection law (Bundesdatenschutzgesetz/BDSG) regulates the handling of personal data which are handled manually or in information and communication systems. It implements the data protection guideline 95/455/EG. § 1 paragraph 1 BDSG protects the individual from being affected by the handling of their personal data in their personal rights.

A fundamental principle of the law is the so-called principle of prohibition with permission. This means that the collection, processing and use of personal data is prohibited in principle. It is only allowed if either a clear legal reason is given (i.e., the law allows the

data processing in this case) or if the person has (usually in writing) explicitly given their consent to the collection, processing and use (§ 4 paragraph 1 , § 4a). The procedures used with automated processing must be checked by (regulatory or operational) data protection officer or (if one is not present) to the competent supervisory authority notifiable (§ 4d).

The defined principle of data economy and data avoidance means that all data processing systems should align to use no or as little personal data as possible and make use of the possibilities of anonymity and pseudonyms.

On the basis on the Berliner Datenschutzgesetz – BlnDSG - which is a district specific version of the BDSG the Charite has created documents that ensure that the collected data of our participants are handled according the current data protection laws."

4.3.2.3 **France**

In France, the Law No. 78-17 of January 6, 1978 "relating to computers, files and liberties" (amended in 1988, 1992, 1994, 1996, 1999, 2000, 2002, 2003, 2004 and 2006), regulates the implementation of treatment of personal data [CNIL78].

It mainly includes:

- conditions of lawfulness of the processing of personal data (chapter 2)
    - conditions to the processing of personal data for the purpose of medical research (chapter 9)
- the preliminary formalities prior to commencing data processing (chapter 4);
- the obligations of data controllers (chapter 5);
- the rights of individuals (chapter 5);
- control and sanctions issued by the CNIL, the criminal provisions (chapters 7 and 8);
- Various provisions (health, journalism and art literature, transfer outside the European Community (EC) etc.).

It also established the missions of the National Commission on Informatics and Liberties (CNIL). The CNIL is in charge to protect consumers against misuse of computer data. Faced with the dangers that IT can bring to bear on the freedoms, the CNIL main task is to protect the privacy and individual or public liberties.

The CNIL is responsible for ensuring compliance with the law "and freedom" through six key responsibilities:

- Identify files: The CNIL advises on all automated processing of personal data in the public and private sector. All files must be declared in order to be registered.
- Control: By conducting audits, the CNIL monitors the security of information systems by ensuring that all precautions are taken to ensure that data is not disclosed to unauthorized persons.
- Regulate: The CNIL regulatory power is used for the development of standards for the most common treatment, so they do not have a risk of harm to the privacy of the individual and his freedom.
- Investigate complaints about improper use of files.

- Inform: The CNIL must inform all persons concerned who practice automated data processing. It must respond to requests for consultations with government and keep abreast of developments in technology to analyse the effects of their use on the right to respect for private life.
- Guarantee the right of access to computer files.

4.3.3 Implementation in the ALFRED Project: Data Treatment and Privacy

Based on the European guidelines and regulations, and the objectives of the ALFRED project, a special attention will be given to the safe treatment of personal data and respect of privacy. As mentioned, the consortium will follow the 95/46/EC Privacy directive of 4th April 1995 about individual protection for the personal data management and processing [EC95].

Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data include address, bank statements, credit card numbers, and so forth. Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (Directive 95/46/EC, Article 2b). Recommendations are separated on seven categories, following the EU Directive 95/46/EC categorization:

- **Notice -** Subjects whose data is being gathered should be notified of this action.
- **Purpose -** The collection of data should be preferred only for specific purpose(s).
- **Consent -** Personal information should not be transmitted to third parties without permission from its subject.
- **Security -** Once acquired, personal data should be retained in safe and secure place, protected from potential abuse, theft, or loss.
- **Disclosure -** Research participants, whose personal data is being obtained, should be informed of the project collecting such data.
- **Access -** Research participants are enabled to demand access to their personal data and allowed to reform any wrong information.
- **Accountability -** Research participants should be able to set the personal data collectors responsible for the application of all seven of these principles above.

4.3.3.1 **Informed Research Participants**

Informed consent is an important part of the research process during the ALFRED project. The protection of the privacy of the research participants is a responsibility of the researchers involved in the studies that include end users. Privacy means that the participants can control the access to their personal information. The participants should be informed about the confidentiality policy that is used in Work Package (WP) 2 “Concept, Requirements & Specification” of the ALFRED project and the tasks related to the user involvement (task 2.3 “User Stories and Requirements Analysis”). All involved research participants will be informed previously that their data will be protected and encrypted and that all the collected data is used strictly for research purposes in the framework of the ALFRED project and the data is only share within the consortium partners. Furthermore,

all processed that is likely to be used in the dissemination activities of the project will be made anonymous and the end-users consent is required. Investigators from the ALFRED project and partners must educate potential subjects to ensure that they can reach a truly informed decision about whether or not to participate in the research. Their informed consent must be given freely, without coercion, and must be based on a clear understanding of what participation involves. A signed informed consent form will provide them the information about how data will be handled and they will give their consent to the consortium to use the data for scientific purposes. Both the researchers from the end user partners and users will sign the consent form.

This issue will be further elaborated on in a specific section on the informed consent (see 4.3.6).

4.3.3.2 Data Processing and Protection

- **Anonymization**

Anonymization will be used to protect the user's identity. This means that only relevant attributes, i.e., gender, age, etc., are documented. The identity of participants will only be maintained in the consent form. The name of the persons and any kind of identification data will appear on the consent forms, of which one copy is kept by the project's test facilitator and the other one by the person participating to the ALFRED user study phase. All data will then be anonymized by assigning a numerical code to each user (local database), and stored accordingly (e.g., Subject 1, Subject 2, etc.). All data will also be anonymized in internal reports, internal communications and external publications (e.g., paper publications or the deliverables).

- **Risk related to data and privacy**

The consortium will pursue the fulfilment of the European Directive during the project and all sensible data will be encrypted and protected during storage and transmission (which takes place across third-party networks (such as the Internet) so that user's identity and privacy will not be compromised. Integration with standards available security and authenticity technologies, such as single sign-on management or LDAP will be analysed. Various implementations will provide a level of user-security in accordance with open-source security standards. State of the art firewalls, network security, encryption, and authentication will be used to protect collected data. Firewalls prevent the connection to open network ports and exchange of data will be through consortium known ports, protected via IP filtering and password. Where possible (depending on the facilities of each partner and pilot site), the data will be stored in a locked server, and all identification data will be stored separately. A metadata framework will be used to identify the data types, owners, and allowable use. This will be combined with a controlled access mechanism and in the case of wireless data transmission with efficient encoding and encryption mechanisms. Pretty Good Privacy (PGP) technology could be used to provide cryptographic privacy and authentication for data communication. PGP could be used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions.

- **Need to keep up with new technologies for security reasons**

The security of precious data demands the ability to avoid data theft regardless of the level of cracking techniques. Therefore, the encryption, file and record locking, integrity, the passwords mechanisms as well as the traceability of the data acquisition systems will have to be constantly updated to prevent the possibility of decoding the data management system at any level and disseminating private information.

- **Data storage and transfer**

In the scope of the ALFRED project's WP2 "Concept, Requirements & Specification" related to the user requirements studies and WP8 "Piloting and Validating" related to the ALFRED pilot studies, the ALFRED project will record and store information about the involved end users. This document provides the end user partners of the project (ESE, NFE and CHA) with concrete guidelines for data handling to the partners and will ensure that they follow best practices and give appropriate assurances regarding data acquisition, processing, storage, and transmission. Each end user partner will be accountable and in case of information compromising.

Any questionnaires or input acquired in the scope of the ALFRED user involvement processes (especially WP2 and WP8) will be handled in the strictest confidence – the results will be entered immediately into a database or XLS files from where each set of results will be given an automatic number and the personal details omitted. The questionnaires themselves will be kept in a folder, which is kept in a lockable drawer. The questionnaires will be destroyed at the end of the project. Additionally, all personal data can be modified and even erased on request from the person, e.g., on an XLS file or via an easy to use interface on the related ALFRED databases. Also, the user should be able to inquire about his/her stored data.

- **Secure data destruction**

In order to prevent the crack of sensitive data and the leak of insecure information, the project intends to apply safe methods one destructing its data, after the extent of their need. The aim is to guarantee that data is completely destroyed with absolutely no chance of retrieval and deny unauthorized access to any information. The way of destruction depends on the type of the files. Various techniques will be applied in paper, CDs, DVDs, floppy disks, USB drives, etc. The responsible deconstruction staff that will deal with encrypted data will be examined and have signed confidential agreements.

4.3.4 ALFRED Ethical Procedures

The ALFRED partners will apply well-established procedures, which are commonly used in research involving humans (including ethical clearance) and well-known to the end user partners. The main ethical management guidelines and principles to be followed in ALFRED are summarized in the following:

- **Respect of and compliance with national rules and regulations**

The user study participants, who will be involved in the project, will take part in a pilot study. The pilot study will be conducted in a 'natural' environment on the home computer and other electronic devices of older and younger end users. This is the most appropriate means of protection, since it means that the legal, professional, religious, and other contexts of the country in question will be taken into account and the evaluation will be

more independent than relying only on the ALFRED ethical guidelines. Thus, the consortium shall implement the project in full respect of the legal and ethical national requirements and code of practice. When authorizations have to be obtained from national bodies, those authorizations shall be considered as documents relevant to the project.

- **Protection of personal data and measures to guarantee security and confidentiality**

In general collection, storage and distribution of all data will be subject to standard requirements, involving briefing and consent of participants. Users will be informed of the purpose and nature when personal data is collected and will have to consent in writing. The researcher of the study and his/her co-workers will inform participants that they are in a position to refuse to participate, especially if they have a direct or indirect financial or contractual link with the research organisation.

- **Enforcement of standard privacy rules**

Standard database privacy rules will be enforced. Ownership of data will be made explicit to the participants. Each participant will have an opportunity to receive a copy of the stored data. Efforts will be made to ensure the traceability of material in such databases. Personally identifiable data transfer collected within the EU will not be made available to parties outside the EU unless the countries concerned comply with the EU directive 95/46/EC. Personally identifiable data will not be made publicly available unless it is accompanied by a certificate from the originator of the database specifying the conditions under which it may be released and the warrant for so releasing it.

- **Relation with research participants**

With the involvement of research participants it will be important to take into account that we are working with older people who may be frail. Friendliness, service quality and consulting authority are important. The following criteria related to the ALFRED target user group should be particularly noted:

- Older people are sensitive to politeness, obligingness and assistance.
- Older people are especially timely; they usually come in time, often even earlier than agreed, so punctuality is important. They are willing to wait a little, but it must not take too long.
- Older people are pleased with little surprises; small gestures for purchases and gifts are almost always accepted with joy. Personal good wishes on special occasions are very well received.
- Older people are less confident; many have fears to be overreached or not to be well versed with technology and electronics. Moreover, they fear to buy something wrong or to receive no service afterwards. Therefore, they like sellers who they know and who they trust.
- Older persons need acknowledgment and appreciation; they want to be taken seriously and importantly.

For the research activities, it will be important to treat the research participants according to well-accepted principles, which seem obvious but are often forgotten.

- Give Clear instructions in simple, short sentences.

- A caring, but also specific and clear, tone should be used.
- Repeat important information when needed several times.
- Let them always finish their sentences.
- Take them serious.
- Make sure that they understand everything what you tell them (no foreign words).
- Speak loud and clearly.
- Write complicated procedures down.
- Always maintain eye contact.

4.3.5 Local Ethical Procedures

Each end user partner will be responsible for establishing and implementing all ethical procedures that are relevant to the respective country (see Section 4.2) and, when necessary, request of permissions from relevant authorities, drafting of material necessary for obtaining permissions, drafting of informed consent forms, etc. The three end-user parties in the project will also approve all research activities involving human participants. Their responsibility is to guarantee the best quality of social, psychological, and public health attention to older people and to maintain the fundamental ethical principles that research involving potentially vulnerable human beings need to be considered.

The end user partner managers will also review those ALFRED deliverables that entail ethical issues, notably of the project. An audio-conference or physical meeting will be held when appropriate in order to discuss the status and evolution of the ALFRED project's ethical procedures. These communication activities will be more frequent during the phases of evaluation and pilot studies. If necessary, one or more independent ethic experts will be invited to advise the ALFRED partners on a merit and need basis with respect to the establishment of ethical procedures.

4.3.6 Informed Consent

In order to provide research participants with the maximum transparency, the ALFRED project will implement informed consent. By signing informed consent documents, research participants agree to a controlled breach of their privacy for a specific purpose and a specific period of time. In case an individual does not agree with such a temporary breach, he/she retains the right to withdraw. Individuals need to be aware of the:

- Methods used for handling personal data,
- Justification for requesting/obtaining their data,
- Duration of data use and storage, and
- Guarantees concerning the rightful use of data.

Therefore, any research action that might impede privacy requires informed consent. This means that in the Ethical Issues (see Annexe 9.1 Participant's Informed Consent for ALFRED Focus Groups) if the applicant ticks one of the two privacy topics, the "informed consent" section also needs to be ticked.

The main aspects of 'informed consent' are the following:

- The potential participant must be given sufficient information in order to be able to make a choice of whether or not to participate that is based on an understanding of the risks and alternatives in an environment, which is free from any coercion.
- The decision of the potential participant on the consent issue must be evidenced. The participant needs to agree that her/his data will be used for a specific research scope and is aware of the meaning of such use.

The ALFRED project will employ informed consent processes associated with all its users. This is also a requirement imposed at the national level (i.e., the countries of the various partners). The informed consent is the process by which a participant will be fully informed about the research in which he/she is going to participate. It originates from the legal and ethical rights a participant has to direct what happens to his/her body and personal data and from the ethical duty of the researcher to involve the participant in research. Seeking the consent of an individual to participate in research reflects the right of an individual to self-determination and also his/her fundamental right to be free from bodily interference, whether physical or psychological and to protect his/her personal data. These are ethical principles recognised by law as legal rights. A distinction between three informed consent elements is possible: the information given, the capacity to understand it, and the voluntariness of any decision taken. Respect for persons requires that participants, to the degree they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided when adequate standards for informed consent are satisfied. The written information, as well as the sought informed consent corresponds to information gathered from the revised version of the Helsinki Declaration of 1964, as lastly amended in Tokyo, 2004, and the Convention of the Council of Europe on Human Rights and Biomedicine (1997).

In order to involve a human being as a participant in research, the ALFRED researcher will obtain the legally effective informed consent of the participant or the participant's legally authorized representative. All investigators within ALFRED will seek such consent only under circumstances that provide the prospective participant or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence. The information given to the participant or the representative will be in language understandable to the participant or the representative. No informed consent, whether oral or written, may include any exculpatory language through which the participant or the representative is made to waive or appear to waive any of the participant's legal rights, or releases or appears to release the investigator, the sponsor, the institution, or its agents from liability for negligence.

5 Conclusion

This deliverable describes the various regulations in terms of technical and management standards, policies and ethics that may apply to both the ALFRED project and then the ALFRED system. It describes the regulatory framework for the product research, development and access to market as well as defines the important guidelines for the evolution of the project. In the next steps, it will be important to match the technical specifications of D2.5 with the regulatory requirements specified in this deliverable to ensure safety, security, interoperability, privacy, usability and performance.

Furthermore, the mHealth market is still immature, both in terms of framework and consumers, and is evolving quite rapidly, with hundreds of new health apps being launched every month. As an example, according to a 2014 study by research2guidance [GSM14], the mHealth app market is expected to grow to a substantial size of more than USD 26bn in 2017. This means that, in the period of 3 years, this market is forecasted to grow 7 times its actual size. The biggest growth will occur between 2016-2017.

This exceptional growth occurs within a regulatory framework that does not draw a clear line between wellness and medical devices and leaves a margin for developers and manufacturers to position themselves. Regulatory bodies at the EU level are expected to step in to breach the policy gap in this sector. To be on the safe side, it might be recommended to design ALFRED in a way that it does not fall under the medical devices regulations or to be ready to demonstrate safety and performance.

This deliverable will be updated at M 24 and 36 to reflect the evolution of the development of the ALFRED system on the one hand, and of the EU and US policy framework and mHealth applications market and on the other hand. In order for the ALFRED system to deliver its full potential, its technical specifications should meet all the existing standards as well as complete the performance tests.

6 Glossary

Accessories

In the US[3]

According to the FDA an accessory is a finished device that is "distributed separately but intended to be attached to or used in conjunction with another finished device" often referred to as a 'parent device'.

In Europe[4]

According to the European regulators[5] an "accessory means an article which whilst not being a device is intended specifically by its manufacturer to be used together with a device to enable it to be used in accordance with the use of the device intended by the manufacturer of the device".

Authorised Representative[6]

Any natural or legal person established in the Community who, explicitly designated by the manufacturer, acts and may be addressed by authorities and bodies in the Community instead of the manufacturer with regard to the latter's obligations under the Directive.

CFR - Code of Federal Regulations

Code of Federal Regulations is the collection of rules and regulations related to multiple departments and agencies of the American federal government. Title 21 is related to Food and Drugs and contains 1499 parts covering specific regulatory areas.

Class I medical devices with measuring function

Are considered Class I medical devices which measure physiological parameters or energy, respectively, substances delivered to or removed from the body and display or indicate its value in a unit of measurement (example: urine bags or thermometers).

Conformity Assessment

It is the process to verify the conformity of a medical device with the essential requirements. This process depends on the medical device classification, according to the procedures described in the MDD.

Component

Components are defined by the FDA[7] as " […] any raw material, substance, piece, part, software, firmware, labeling, or assembly which is intended to be included as part of the finished, packaged, and labeled device" Components are assembly parts to a medical device sourced by the manufacturer.

Component Supplier

[3] Section 201 (h) of the Federal Food, Drug and Cosmetic Act
[4] Directive 2007/47/EC (21 March 2010), amending the Directive 93/42/EEC
[5] MDD; Article 1 (2) (b)
[6] MDD; Article 14 (2) (j)
[7] According to 21CFR820 Sec. 820.3(c)

A component supplier is defined as a person or entity supplying parts to a medical device manufacturer. Very often component suppliers are not the manufacturer of the medical device. They therefore have no legal obligation to comply with the various regulatory bodies but they need to fulfil the manufacturer's quality requirements. Medical device manufacturers need to ensure that their component suppliers deliver parts of a satisfactory quality. This might mean keeping complete audit trails and comply with specific quality standards.

Design Controls

Design controls are defined by the FDA[8] as "an interrelated set of practices and procedures that are incorporated into the design and development process, i.e., a system of checks and balances. Design controls make systematic assessment of the design an integral part of development. […] Design controls increase the likelihood that the design transferred to production will translate into a device that is appropriate for its intended use."

Design Verification

According to the FDA[9] design verification means the "confirmation by examination and provision of objective evidence that specified requirements have been fulfilled"

Design Validation

Design Validation means "establishing by objective evidence that device specifications conform to user needs and intended use(s)."

EU Directive[10]

Directives are used to bring different national laws into line with each other, and are particularly common in matters affecting the operation of the single market (e.g. product safety standards). They lay down certain end results that must be achieved in every Member State. National authorities have to adapt their laws to meet these goals, but are free to decide how to do so. Directives may concern one or more Member States, or all of them. Each directive specifies the date by which the national laws must be adapted - giving national authorities the room for manoeuvre within the deadlines necessary to take account of differing national situations.

EMA - European Medicines Agency[11]

According to their website the European Medicines Agency34 is "a decentralised agency of the European Union, located in London. The Agency is responsible for the scientific

[8] Design Control Guidance For Medical Device Manufacturers relating to relates to FDA 21 CFR 820.30 and Sub-clause 4.4 of ISO 9001. It can be found at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070627.htm

[9] Design Control Guidance For Medical Device Manufacturers relating to relates to FDA 21 CFR 820.30 and Sub-clause 4.4 of ISO 9001. It can be found at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070627.htm

[10] http://ec.europa.eu/eu_law/introduction/what_directive_en.htm

[11] http://www.ema.europa.eu/ema/index.jsp?curl=pages/about_us/general/general_content_000235.jsp&mid=

evaluation of medicines developed by pharmaceutical companies for use in the European Union."

GMP - Good Manufacturing Practice

Good manufacturing practices are policies and systems needed to manufacture and test aspects of production that can impact the quality of an active pharmaceutical product, diagnostic tool, food, and medical device. They include the establishment of quality controls and quality systems and are, in some countries, required by law in order to safeguard the health of the public.

Intended Use / Intended Purpose

In the US

It corresponds to the use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer.

In Europe [12]

It corresponds to the use for which the device is intended according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional material.

ISO Standards

International Organization for Standardization is a non-governmental organization having members mandated by local governments as well as, private sector national partners and industry associations, therefore forming a bridge between the public and private sectors. Its mission is to develop and publish international standards enabling a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.

Manufacturer

The FDA[13] defines manufacturers as "any person who designs, manufactures, fabricates, assembles, or processes a finished device. Manufacturer includes but is not limited to those who perform the functions of contract sterilization, installation, relabeling, remanufacturing, repacking, or specification development, and initial distributors of foreign entities performing these functions".

Medical Device

In the US

A medical device is defined in the USA as "… an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is … [either] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals … [or] intended to affect the structure or any function of the body of man or other animals."

In Europe

[12] MDD directive 93/42

[13] Quality System Regulation 21 CFR 820 - Basic Introduction available at http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm126252.htm

In Europe a Medical Device is defined as “any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of: diagnosis, prevention, monitoring, treatment or alleviation of disease, diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, investigation, replacement or modification of the anatomy or of a physiological process, control of conception, and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted by such means.”

MDDS - Medical Device Data System

The FDA[14] defines an MDDS as “a device that is intended to provide one or more of the following uses, without controlling or altering the functions or parameters of any connected medical devices: The electronic transfer of medical device data; The electronic storage of medical device data; The electronic conversion of medical device data from one format to another format in accordance with a preset specification; or The electronic display of medical device data. An MDDS may include software, electronic or electrical hardware such as a physical communications medium (including wireless hardware), modems, interfaces, and a communications protocol. This identification does not include devices intended to be used in connection with active patient monitoring”. The FDA clarified further that an MDDS36 is NOT “general-purpose IT infrastructure used in health care facilities that is not altered or reconfigured outside of its manufactured specifications. Modifications within the off-the-shelf parameters of operation are still considered general IT infrastructure and not MDDS. For example, components with the following functions by themselves are NOT considered MDDS if they are used as part of general IT infrastructure even though they may transfer, store, display or convert medical device data, in addition to other information: The electronic transfer of medical device data [such as] Network Router, Network Hub, [or] Wireless access point; The electronic storage of medical device data [such as] Network Attached Storage (NAS) [or] Storage area network (SAN); The electronic conversion of medical device data from one format to another in accordance with a preset specification [such as] Virtualization System (ex: VM Ware) [or] PDF software.“

Mobile Health (“mHealth”)**Invalid source specified.**

Mobile health (hereafter “mHealth”) covers “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices”. It also includes applications (hereafter "apps") such as lifestyle and wellbeing apps2 that may connect to medical devices or sensors (e.g. bracelets or watches) as well as personal guidance systems, health information and medication reminders provided by sms and telemedicine provided wirelessly.

[14] FDA guidance on Identifying an MDDS that can be found on http://www.fda.gov/MedicalDevices/Productsand

Mobile Medical Apps[15]:

"The author is defined as the person or entity that initiated and developed specifications for the mobile medical app while the developers are only responsible for performing design and development activities to transform the author's specifications into a mobile medical app".

Mobile Medical Apps Manufacturer

Mobile medical apps manufacturer is further defined in the Mobile App guidance draft document[16] to "include anyone who initiates specifications, designs, labels, or creates a software system or application in whole or from multiple software components. […] [It includes] a person or entity that creates a mobile medical app by using commercial off the shelf (COTS) software components and markets the product to perform as a mobile medical app, [someone that] provides mobile medical app functionality through a "web service" or "web support" for use on a mobile platform. For example, a manufacturer of a mobile medical app that allows users to access the application's medical device functionality over the web is considered a mobile medical app manufacturer. [It also includes a person or entity that] initiates specifications or requirements for mobile medical apps or procures product development/manufacturing services from other individuals or entities (second party) for subsequent commercial distribution. For example, when a "developer" (i.e., an entity that provides engineering, design, and development services) creates a mobile medical app from the specifications that were initiated by the "author," the "author" who initiated and developed specifications for the mobile medical app is considered a "manufacturer" of the mobile medical app under 21 CFR 803.3. […] [In other worlds] manufacturers of a mobile medical app would include persons or entities who are the creators of the original idea (initial specifications) for a mobile medical app, unless another entity assumes all responsibility for manufacturing and distributing the mobile medical app, in which case that other entity would be the "manufacturer." Software "developers" of a mobile medical app that are only responsible for performing design and development activities to transform the author's specifications into a mobile medical app would not constitute manufacturers, and instead the author would be considered the manufacturer"

Quality Systems

As defined in Design Control Guidance For Medical Device Manufacturers § 820.3 (v) Quality system means "the organizational structure, responsibilities, procedures, processes, and resources for implementing quality management"

Risk Management

Risk management is defined by the FDA[17] as "the systematic application of management policies, procedures, and practices to the tasks of identifying, analyzing, controlling, and monitoring risk. It is intended to be a framework within which experience, insight, and

[15] Draft guidance for industry and FDA administration staff, Mobile Medical Applications" Issued on July 21, 2011

[16] Draft guidance for industry and FDA administration staff, Mobile Medical Applications" Issued on July 21, 2011

[17] Quality System Regulation 21 CFR 820 - Basic Introduction available at http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm126252.htm

judgment are applied to successfully manage risk. It is included in this guidance because of its effect on the design process. Risk management begins with the development of the design input requirements. As the design evolves, new risks may become evident. To systematically identify and, when necessary, reduce these risks, the risk management process is integrated into the design process. In this way, unacceptable risks can be identified and managed earlier in the design process when changes are easier to make and less costly."

Sensors

Sensors used in the field of AAL are either installed permanently in the building, i.e. the user's home (ambient) or are carried as mobile sensors by the user. They can encompass ambient parameters (e.g. temperature, brightness, presence, movement, fire), the use of devices and objects (e.g. light barrier, door contacts) or information about the user (vital signs such as pulse, blood oxygen saturation, ECG, position, movement). Sensors transfer the registered data by cable or cordless connection to a gateway where the data are collated and evaluated.

Specification Developers

Person or entity creating the initial specifications for a product. The specification developer may or may not be the manufacturer.

User Interface

This describes components for interaction between the user and the AAL system, including the classical graphic user interface of a computer (monitor, keyboard, mouse), use of the television with remote control, touch panels, voice input/output or multimodal user interfaces.

User Requirements

The highly heterogeneous group of people using AAL systems results in a large number of functional and non-functional user requirements that have to be taken into consideration right from the start.

Wellness

The definition of wellness is still something that has not been fully defined by international regulators. In general it can refer to related but slightly different concepts depending on the context this term is used. The term has been defined by the Wisconsin-based National Wellness Institute as "an active process of becoming aware of and making choices toward a more successful existence". The New York Times[18] has recently traced the historical changes in the meaning of this word as follow: Though the Oxford English Dictionary traces wellness (meaning the opposite of illness) to the 1650s, the story of the wellness movement really begins in the 1950s. New approaches to healthful living were emerging then, inspired in part by the preamble to the World Health Organization's 1948 constitution: "Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity." Halbert L. Dunn, chief of the National Office of Vital Statistics, was looking for new terminology to convey the positive aspects of health that people could achieve, beyond simply avoiding sickness. In a series of papers and lectures

[18] http://www.nytimes.com/2010/04/18/magazine/18FOB-onlanguage-t.html

in the late ’50s, Dunn sketched out his concept of “high-level wellness,” defined as “an integrated method of functioning, which is oriented toward maximizing the potential of which the individual is capable.”

7 References

[VDE08] VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V (Hrsg.): Positionspapier Intelligente Assistenzsysteme im Dienst für eine reife Gesellschaft., Frankfurt, 2008. ISBN-978-3-8007-925512-12-4. Available: http://www.vde.com/de/fg/dgbmt/arbeitsgebiete/intelligente_assistenzsysteme/documents/vde%20positionspapier%20intelligente%20assistenzsysteme%202008.pdf

[GSM12-1] GSMA Connected Living Programme: mHealth, “Understanding Medical Device Regulation for mHealth. A Guide for Mobile Operators,” GSMA, Version 1, Feb. 2012. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmaunderstandingmedicaldeviceregulationformhealthreport1.pdf [Accessed: Sep. 29, 2014].

[ETSI130] ETSI ETR 130-1994, Methods for Testing and Specification (MTS); Interoperability and Conformance Testing A Classification Scheme, European Telecommunication Standard (ETS), Jan. 1, 1994.

[ISO14971] ISO 14971:2007, Medical devices -- Application of risk management to medical devices

[IEC80002] IEC/TR 80002-1:2009, Medical device software -- Part 1: Guidance on the application of ISO 14971 to medical device software

[IEC62366] IEC 62366:2007, Medical devices -- Application of usability engineering to medical devices

[IEC60601] IEC 60601-1-11:2010, Medical electrical equipment -- Part 1-11: General requirements for basic safety and essential performance -- Collateral standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment

[ISO9001] ISO 9001:2008 Quality Management Systems – Requirements

[ISO9000-1] ISO 9000:2005, Quality management systems - - Fundamentals and vocabulary

[ISO9000-2] ISO 9000:2009, Managing for the sustained success of an organization – A quality management approach

[ISO13485] ISO 13485:2003, Medical devices -- Quality management systems -- Requirements for regulatory purposes

[ISO13488] ISO 13488:1996, Quality systems -- Medical devices -- Particular requirements for the application of ISO 9002

[ISO14969] CEN ISO/TR 14969:2005, Medical devices. Quality management systems. Guidance on the application of ISO 13485:2003

[ISO9241-1] ISO 9241-20:2008, Ergonomics of human-system interaction — Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services

[ISO9241-2] ISO 9241-171:2008, Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility

[ISO9241-3] ISO 9241-210:2010, Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems

[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, 2014].

[ISO29100] ISO/IEC FDIS 29100:2011, Information technology — Security techniques — Privacy framework

[ISO29101] ISO/IEC 29101: Information technology — Security techniques — Privacy architecture framework

[ISO24760] ISO/IEC WD 24760: Information Technology — Security Techniques — A Framework for Identity Management

[IEC62304] IEC/EN 62304, Medical Device - Software Life Cycle Processes

[MEDDEV09] European Commission DG Enterprise and Industry Directorate F-Consumer Good Unit F3-Cosmetic and Medical Devices: Guidelines on a Medical Device Vigilance System, MEDDEV 2.12-1 rev 6, December 2009. Available: http://ec.europa.eu/health/medical-devices/files/meddev/2_12_1-rev_6-12-2009_en.pdf

[ISO 9126] ISO/IEC 9126-1:2001, Software engineering -- Product quality -- Part 1: Quality model

[ISO12119] ISO/IEC 12119:1994, Information technology -- Software packages -- Quality requirements and testing

[ISO9241] EN ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability

[ISO14915-1] ISO 14915-1:2002, Software ergonomics for multimedia user interfaces -- Part 1: Design principles and framework

[ISO14915-2] ISO 14915-2:2003, Software ergonomics for multimedia user interfaces -- Part 2: Multimedia navigation and control

[ISO11064] ISO 11064-4:2013, Ergonomic design of control centres

[IEC60601] IEC 60601-1-6,Medical electrical equipment - Part 1-6: General requirements for basic safety and essential performance - Collateral standard: Usability

[ISO71] ISO/IEC Guide 71:2001, Guidelines for standards developers to address the needs of older persons and persons with disabilities

[ISO22411] ISO/TR 22411 Ergonomics data and guidelines for the application of ISO/IEC Guide 71 to products and services to address the needs of older persons and persons with disabilities is an important collateral document containing instructions for using the ISO/IEC Guide 71.

[ETSI102732] ETSI TR 102 732 V1.1.1 (2013-09), Machine-to-Machine Communications (M2M) - Use Cases of M2M applications for eHealth. Available: http://www.etsi.org/deliver/etsi_tr/102700_102799/102732/01.01.01_60/tr_102732v010101p.pdf

[TS102689] ETSI TS 102 689 V1.1.1 (2010-08), Machine-to-Machine communications (M2M) - M2M service requirements

[ETSI102690] ETSI TS 102 690 V2.1.1 (2013-10), Machine-to-Machine communications (M2M) – Functional architecture. Available: http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/02.01.01_60/ts_102690v020101p.pdf

[TS102921] ETSI TS 102 921 V1.1.1 (2012-02), Machine-to-Machine communications (M2M) - mIa, dIa and mId interfaces. Available at: http://www.etsi.org/deliver/etsi_ts/102900_102999/102921/01.01.01_60/ts_102921v010101p.pdf

[ISO11073] ISO/IEEE 11073, Health informatics – Medical / health device communication
[ISO19011] ISO 19011:2011, Guidelines for auditing management systems
[ISO22301] ISO 22301, Business Continuity Management
[ISO9004] ISO9004:2009, Quality management systems -- Guidelines for performance improvements
[D4L12] Devices 4 Limited, "Regulation of Health Apps: a Practical Guide," Devices 4. Ltd, Jan. 2012. Available: http://www.d4.org.uk/research/regulation-of-health-apps-a-practical-guide-January-2012.pdf [Accessed: Sep. 29, 2014].
[ML13] M. A. Mayer and A. Leis, "Designing and Using Mobile Health Applications (Medical and Health Apps): Practical Guidelines Are Needed" In iPROCEEDINGS Medicine 2.0 London – Sept 23-24, 2013, www.medicine20congress.com
[FDA03] FDA, Guidance for Industry and Food and Drug Administration Staff - Non binding recommendations, FDA, Sept. 25, 2003. Available: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf [Accessed: Sep. 29, 2014].
[Happ01] Happtique, https://www.happtique.com/
[GSM12-2] GSMA Connected Living Programme. mHealth, "mHealth and the EU regulatory framework for medical devices," GSMA, London, 2012. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/mHealth_Regulatory_medicaldevices_10_12.pdf [Accessed: Sep. 29, 2014].
[FDA14] Federal Drug Administration, Guidance on Mobile Medical Applications: http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm, Page Last Updated: 06/04/2014
[MDD07] European Directive 2007/47/EC of The European Parliament and of Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biotical products on the market, [EU Medical Device Directive], Official Journal of the European Union 21.09.2007, Sept. 9, 2007. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:en:PDF [Accessed: Sep. 29, 2014].
[RTTE99] European Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity [R&TTE Directive], Mar. 9, 1999. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=Ks5xJq1Mpv5J0WwQfSkpp6K6GxRBXnjWpL4J6Fk0L9vHs9nYyQzw!-1358510149?uri=CELEX:31999L0005
[EC99-1] European Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Official Journal, L 141/20, May. 10, 1999. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:141:0020:0021:EN:PDF
[EC01] European Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, Official Journal, L 11/4, Dec. 3, 2001.

Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:011:0004:0017:en:PDF

[EC99-2] European Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, Official Journal, L 171, May. 25, 1999. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0044

[EC00] European Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ['Directive on electronic commerce'], Official Journal, L 178, Jun. 3, 2000. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000L0031

[EC14] European Commission, “Progress on EU data protection reform now irreversible following European Parliament vote,” Strasbourg: Memo/14/186, Mar. 12, 2014. Available: http://europa.eu/rapid/press-release_MEMO-14-186_fr.htm

[EC06] European Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, Official Journal, L376/21, Dec. 12, 2006. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0021:0027:EN:PDF

[EC05] European Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, Official Journal, L149/22, May. 11, 2005. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:en:PDF

[VPZ12] S. Vavilis, M. Petkovic and N. Zannone, “Impact of ICT on Home Healthcare,” In *Proceedings of the 10th IFIP Human Choice and Computers International Conference (HCC 2012)*, Springer. 2012.

[OECD13] Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013. Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [Accessed: Sep. 29, 2014].

[TEU92] Treaty on the European Union [TEU], Maastricht, Feb. 7, 1992

[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].

[CFR00] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 2000/C 364/01, Dec. 18, 2000. Available: http://www.europarl.europa.eu/charter/pdf/text_en.pdf [Accessed: Sep. 29, 2014].

[EC02] European 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], Official Journal, L 201, p. 37, Jul. 12, 2002.

[UN48] United Nations General Assembly, *Universal Declaration of Human Rights*, 217 A (III), Dec. 10, 1948. Available at: http://www.refworld.org/docid/3ae6b3712c.html [accessed 30 September 2014]

[CHR97] Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997

[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 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5147 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5147 [Accessed: Sep. 29, 2014].

[EMC14] EMC Healthcare Solutions, “Trusted IT Solutions for Healthcare Providers: Best practices for healthcare privacy and security requirements,” EMC White Paper, Jan. 2014 Available: http://www.emc.com/collateral/white-papers/h12709-trusted-it-solutions-healthcare-wp.pdf [Accessed: Sep. 29, 2014].

[GCE12] German Commission for Electrica, electronic & Information Technologies of DIN and VDE, “The German AAL Standardization Roadmap,” VDE Association for Electrical, Electronic & Information Technologies, Jan. 2012. Available: https://www.dke.de/de/std/Informationssicherheit/Documents/German%20AAL%20Standardization%20Roadmap%20[1].pdf [Accessed: Sep. 29, 2014].

[IMT49] International Military Tribunal. "Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No. 10",Washington, D.C.: U.S. Government Printing Office, Vol. 2, pp. 181-182, 1949.

[WMA64] World Medical Association General Assembly, “Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects”, Helsinki, Finland, Jun. 10, 1964

[CNIL78] Law 78-17 of January 6, 1978, Concerning Information Technology, Files, and Liberties [Loi 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés], Official Journal of the French Republic [Journal Officiel de la République Française], p. 227, art. 31, at 229, Jan. 7, 1978. Available: http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf [Accessed: Sep. 29, 2014].

[GSM14] GSMA/PWC Report, “Touching Lives through Mobile Health Assessment of the Global Market Opportunity”, PricewaterhouseCoopers Private Limited, Feb. 2012. Available: http://www.pwc.in/assets/pdfs/telecom/gsma-pwc_mhealth_report.pdf [Accessed: Sep. 29, 2014].

8 Additional Documents of Interests:

- COCIR, “Contribution to the General Data Protection Regulation1 and European Parliament,” LIBE Report, Mar. 7, 2014. Available: http://www.cocir.org/site/fileadmin/4.4__eHealth/Data_Protection/COCIR_position_paper_on_data_protection_7_March_2014.pdf [Accessed: Sep. 29, 2014].
- European Commission, Borderline and classification issues on Medical devices. Available: http://ec.europa.eu/health/medical-devices/documents/borderline/index_en.htm
- European Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Jan. 28, 1981. Available: http://conventions.coe.int/Treaty/en/Treaties/Word/108.doc [Accessed: Sep. 29, 2014].
- European Digital Rights, Annual Report January 2013 – December 2013, EDRi, Brussels. Available: http://edri.org/wp-content/uploads/2014/04/EDRi_Annual_Report_2013.pdf [Accessed: Sep. 29, 2014].
- European Digital Rights, “An Introduction to Data Protection,” *The EDRI papers*, Issues 06, 2013. [Online]. Available: http://www.edri.org/files/paper06_datap.pdf [Accessed: Sep. 29, 2014].
- Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) General Data Protection Regulation, 25.01.2012. Available: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011
- Medicines and Healthcare Products Regulatory Agency (UK), Guidance on Medical device Stand-alone software (including apps) Regulating Medicines and Medical Devices, MHRA, Mar. 21, 2014. Available: http://www.mhra.gov.uk/Howweregulate/Devices/Software/index.htm
- Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare Within the Regulatory Framework of Medical Devices, ec.europa.eu/health/medical-devices/documents/guidelines/index_en.htm (February 2012).
- L. Rölker-Denker and M. Eichelberg, “D4.4 Report on Standards and Certification in AAL,” Next Generation European Ambient Assisted Living Innovation Alliance AALIANCE2, Sept 30, 2013.
- Sharkey and N. Sharkey, “Granny and the robots: ethical issues in robot care for the elderly,” *Ethics of Information Technology*, vol. 14, no. 1, pp27-40, 2012.
- R. Sparrow and L. Sparrow, “In the hands of machines? The future of aged care,” Minds & Machines, vol. 16(2), pp. 141-161, 2006. DOI 10.1007/s11023-006-9030-6
- World Health Organisation, Meeting Report. At Forum on Health Standardization and Interoperability, 3-4 December 2012, Geneva, Switzerland. Available: http://www.who.int/ehealth/WHO_Forum_on_HDSI_Report.pdf [Accessed: Sep. 29, 2014].

- World Health Organisation, “Legal Frameworks for eHealth: based on the findings of the second global survey on eHealth”. WHO, Geneva, Switzerland, Global Observatory for eHealth Series, v. 5. 2012. Available: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf [Accessed: Sep. 29, 2014].
- http://ec.europa.eu/enterprise/sectors/ict/standards/index_en.html
- http://www.w3.org/
- https://www.cen.eu/Pages/default.aspx
- http://ec.europa.eu/justice/data-protection/law/index_en.htm

9 Annexe

9.1 Participant's Informed Consent for ALFRED Focus Groups

PARTICIPANT'S INFORMED CONSENT FOR ALFRED FOCUS GROUPS

Me, the signatory,

Surname	
First Name	

accept freely and voluntarily to participate in the focus groups of the ALFRED project. I certify that I have been informed about the ALFRED project and that I have received all necessary information regarding my involvement in this phase and had sufficient time to decide whether I want to participate in this discussion. Furthermore, I confirm that I have had an opportunity to ask questions about the details of my involvement in the focus group and other aspects of the ALFRED project.

I understand that,

- My participation is voluntary and I can withdraw from the group at any time and without delay;
- I can obtain, correct and delete the information derived from my participation in the focus group discussions;
- The focus groups discussions will be recorded (audio/ video);
- All collected information will be analysed for research purposes only and can be used anonymously in ALFRED project related publications

Date: / /

Signature: