Document downloaded from:

http://hdl.handle.net/10251/180737

This paper must be cited as:

Costa, A.; Yelshyna, A.; Moreira, TC.; Andrade, FC.; Julian Inglada, VJ.; Novais, P. (2017). A legal framework for an elderly healthcare platform: A privacy and data protection overview. Computer Law & Security Review. 33(5):647-658. https://doi.org/10.1016/j.clsr.2017.03.021

The final publication is available at

https://doi.org/10.1016/j.clsr.2017.03.021

Copyright Elsevier

Additional Information

A Legal Framework for Elderly Healthcare Platform: Privacy and Data Protection Overview

Angelo Costa*
Centro ALGORITMI, University of Minho, Braga, Portugal
acosta@di.uminho.pt

Aliaksandra Yelshyna
School of Law, University of Minho, Braga, Portugal
yelshyna@gmail.com

Teresa C. Moreira
School of Law, University of Minho, Braga, Portugal
tmoreira@direito.uminho.pt

Francisco C.P. Andrade
School of Law, University of Minho, Braga, Portugal
fandrade@direito.uminho.pt

Vicente Julián
Departamento de Sistemas Informáticos y Computación, Universitat Politècnica de València, Valencia, Spain
vinglada@dsic.upv.es

Paulo Novais
Centro ALGORITMI, University of Minho, Braga, Portugal
pjon@di.uminho.pt

Abstract

Cognitive problems are increasingly affecting the population, with the elderly being the ones that are the most affected. This problem requires a new approach in terms of medical and social actions, personalisation, and services. The Ambient Assisted Living area provides solutions to allow elderly people to stay in their homes safely and with the appropriate care. The number of Ambient Assisted Living projects is increasing rapidly, leading to large commercial deployment, most of these projects disregard the privacy and data protection of the users and the information that they process and save. The iGenda project is a Cognitive Assistant inserted in the Ambient Assisted Living area that provides help to users in their daily lives. However, since it requires a large amount of private and personal data that is transferred between the modules of the platform, fundamental rights may be at stake. This paper presents the iGenda platform, the principle rights of data protection and transmission, legal guarantees and latent ethical concerns. Furthermore, the dichotomy between current developments and legal and ethical aspects are explained. To overcome this problem, legal considerations and ethical considerations are presented, embracing appropriate solutions to features that present any threat.

Keywords: Healthcare Platform, Ambient Assisted Living, Data Protection, Privacy, iGenda

1 Introduction

Population evolution is suffering a paradigm shift. We are currently bearing witness to important changes in population and history: the birth is decreasing and the elderly population is increasing [1,2]. Increasing economic stability and medical improvements have increased human longevity and changed the conception of the age at which one is considered to be old. This same economic stability has also changed the way young couples, based on household income, plan their lives (increasingly focused on their careers) and they are limiting the number of children they have, in order to provide a very comfortable lifestyle to their offspring [1,2]. A very complex issue that arises from this evolution is the challenging demographic context that is threatening the sustainability of health systems.

Portugal is one of the European Countries with the lowest total fertility rate[1] – 1, 21%[2] -, and of course that is one of the biggest problems that we are facing and during the last years there was an increase in the number of elderly and a decrease in the number of young people and in the number of people aged between 15 and 64 years. According to the latest demographic predictions in the very long term Portugal will have a sharp population decline until 2060, as well as a dramatic change in the age structure. Also, per data presented in 2015 Portugal has, in all the 28 Member States of the EU, the 5th highest ageing index; the 3rd lowest working age population renewal ratio; the 3rd highest increase in the median age between 2003 and 2013 and is one of the lowest total fertility rate.

Changes in the population age structure result in the increase of ageing index: in 2014 for every 100-young people there were 141 elderly people residing in Portugal, a number that in 2013 was 136. The ageing index for the EU 28 in 2013 was 119 elderly people for every 100-young people. In terms of numbers, according to the UN report, in the year 2050 the elderly population is expected to be over 2 billion [3,4]. The report provides a grim perspective, since they assume that the current economic situation will become unsustainable in a few years and that measures must be implemented urgently to keep up with this population change scenario.

In terms of the medical attention, the elderly population requires a lot of medical care, ranging from periodical medical consultations to long periods of hospital admittance and costly operations. In terms of logistics, the extended duration of hospital occupation is a possibility, effectively reducing the capacity of new admittances and leading to a rupture in the process of medical response. Moreover, there are currently several countries that are crippled by a fragile economic recovery, which limits the resources that are available for investment in healthcare.

Another issue is the decrease of medical personnel in nursing homes and care centres, which results in a poor oversight of the elderly residents leading to a loss of quality of life [5,6]. Furthermore, this issue increases greatly the stress of the caregivers that are more prone to commit errors and endanger the life of the care-receivers.

Technology, namely the computer science area, has presented the Ambient Assisted Living (AAL) concept, which aim to provide technological solutions that are inexpensive and that can provide medical assistance through the use of devices and services [7–14]. These devices and services form a platform that is interactive and intelligent and can change environment characteristics to achieve a specific result. The main differences to the telemonitoring concept are the provision of intelligence to the devices (they can act without supervision) and the connectivity (most of the systems are composed of several sensors and are connected with intelligent homes and other services/users), greatly extending the limited telemonitoring features.

A few AAL examples can be: the BRAID project [15] consists in a set of devices (visual monitoring and handheld devices) coupled with software services that created an medical sphere

1 Indicates the average number of children per woman.

2 Per the data presented in www.pordata.pt.

around the users. The aim was to provide constant monitoring of the users and detect significant deviations to the expected pattern and provide that information to the caregivers or medical staff. This would alleviate the active monitoring by these people and shift that task to intelligent systems that were connected with them; the AAL4ALL is an AAL project (which is stated in the project's name) is a multi-company and institution effort to provide easy to use devices that are integrated with a central software system with the aim of monitoring elderly users and change their environment (with domotics/robotics), helping them on their daily tasks. The project has produced several devices like: fall detectors, movement detectors, water and gas leakage detectors, electrical devices controllers, smart visual monitors, among others. These devices are connected with a local home central system and the AAL4ALL server system that monitors constantly and analyses every situation for possible dangers to the users and how, with the help of the available devices, to provide help performing activities.

AAL platforms aim to provide a safe and welcoming environment that proactively responds to an individual's needs. These platforms are built to be used in a home environment (although they can be used in other environments, like hospitals) with cost/effect in mind. They provide affordable solutions that help to monitor each individual's health status and act upon critical events. This makes the medical network more effective (decreasing hospital stays and troubleshooting simple medical problems) while at the same time keeping a human touch (recurring to periodic contact with human assistants). The implicated costs are low as most of the small components are inexpensive and the software may run from a simple computer. A downside is that AAL systems and related services deal with large quantities of personal data and, especially, sensitive data (or special categories of personal data, art. 9 Regulation 2016/679, e.g., data concerning the health of the holder of data).

The usage of AAL systems can be (among several others): monitoring an agitated person so the system can intelligently change the lighting and introduce music to sooth that person; or if there is a fall, through visual or sensoring systems the platform can call a caregiver or emergency services for further assistance; or if a person forgets its keys, the platform should be able of locating them; or if the gas or electric devices are left open the platform can shut them down.

These concepts battle the issues that an aging society presents, which are high economic medical costs and the provision of medical services [16,17]. Furthermore, the medical staff often becomes overburden and is unable to provide proper care at hospitals or at home [5]. These areas have since raced to create new projects and new solutions that promote active aging to keep their users at home, while at the same time connecting them with their physicians and the medical care that they need. This includes optimising the visit to the hospital and, above all, responding to critical situations as fast as possible.

Since 2008, through its funding programs, the European Union (EU) has supported, active aging and elderly health and promoted the creation of practical solutions to combat the aging paradigm [18]. The EU has realised that technological solutions should be seriously considered, since it had become clear that aiming for home environments is also critical to the well-being of the elderly. Since 2012, the EU has actively supported AAL and AmI projects that validate the importance of these areas[3], and the result is the proliferation of new devices and software [3]. This call for innovation often collides with the current legal system, because the AmI and AAL projects rely heavily on personal data, monitor the home environment, and interact directly with the people that they monitor.

Privacy in AAL and AmI applications is an emerging problem which was born from the great success in recent years of these applications and the limited preparation of people regarding risk and safety in data sharing. Moreover, privacy is becoming an important issue in the EU due to changes in the dissemination of personal information caused using Internet and, especially social networks. This aspect is reflected in project calls launched by different European

3 http://ec.europa.eu/archives/ey2012/

governments and the EU itself, which launched the Horizon 2020 program to address these challenges.

The aim of this paper is to present the legal and ethical aspects related to AAL platforms, focusing on privacy and data protection, using the iGenda development as an example. This work presents a discussion of the dichotomy between the current laws and novel technology and what can be done to protect individuals versus the adoption or broadening of new laws that tolerate how technology has advanced.

The paper is structured as follows: section 2 presents an AAL platform, iGenda, showing the data transferred and user access to it; section 3 presents the current data protection framework and the legal accountability along with the legal aspects that are directly related to the AAL action area; sections 4 and 5 explain the legal requirements for multi-user and data access, the law procedures and the data storage access levels and dates expiration; section 6 discuss the data security requirements for current and future laws and how AAL platforms can follow them; in section 7 is the ethical concerns; finally, section 8 presents the conclusions of the paper.

2 The iGenda example

The iGenda project [19–21] is an example of a mobile and web AAL platform that monitors the elderly by using sensor systems, which collect and process vital data (electrocardiogram data, blood pressure and oximetry, among others). These procedures aim to improve the well-being of the care-receiver by creating a compendium of health data that can help to identify health problems or critical events. Furthermore, one of the goals is to be an intelligent agenda that intelligently plans events and leisure activities using profiling techniques to find user traits and likes. It is a social application that connects several different care-receivers, relatives, and medical personnel, which allows them to share medical and personal information and facilitates the creation of shared events.

The iGenda platform uses mobile and desktop devices to interface with its users and to provide an array of information to each one. There are three major actors in iGenda: the care-receivers (elderly or mentally impaired people), the caregivers (physicians or family/relatives), and the relatives (family and friends). The actors have specific roles and have access to tailored information about their sphere of connection, thus it is expected to be an exchange of information among them. Moreover, the relation between care-receiver and caregiver requires the exchange of very sensitive information, such as health data, and the persistency of it in the system. Apart from these three actors there is also the technician who is a trained professional that is responsible for the health of the iGenda system and who is bounded by an obligation of confidentiality.

The caregiver has access to a portal that displays all the people being cared by him/her. It contains the personal health record of each care-receiver and uses the care-receiver monitoring data to improve the data on the system databases, it also displays imminent or future critical situations. Moreover, iGenda has a profiler module, meaning that it can gather information about the user and construct a meta-association structure that enables the system to respond to non-user-guided information, such as prioritising events and suggesting leisure activities that are in line with the active-aging objective. The success of the platform is dependent upon the regular use of each user.

The several actors (i.e., people divided into workgroups) are linked and interact with iGenda. Most of each user's data is shared with one person or more based on to their social connection and access level. Fig. 1 shows the simplified data transmission between all the actors. All information collected via mobile device or web goes through the iGenda and is saved and processed. If one of the actors represented on the right side of the figure wants to get the information available and has the access level to do so, the information can be obtained.

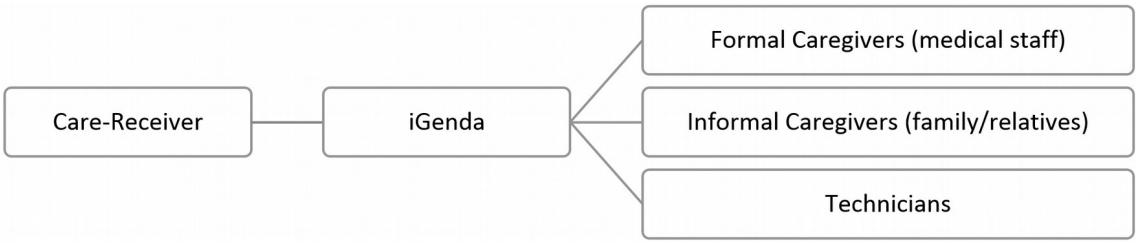

Figure 1: Actors involved in the data transmission.

The care-receiver is typically the information producer; the information is manually introduced by him/her or is generated by sensor systems. The caregivers also produce information but at a much lower rate. Most of the time they are information consumers at their own discretion. They are divided into two sub-groups: the formal caregivers and informal caregivers. The formal caregivers are mostly constituted by medical staff who have a higher level of access to the information available. Therefore, all private details are accessible to them. They may also edit and add information to the care-receiver profile (e.g., complementary exam results or updates of the health status). The informal caregivers are represented by family and relatives who have access to some information about the care-receiver. Most of the data it is not private since most of it is shared by the care-receiver (e.g., social events or status update). The informal caregivers play an important role in the care-receiver's life by engaging in social activities and promoting an active lifestyle. Finally, the technicians are the actors who are responsible for the iGenda maintenance and have clearance to edit and remove data, keeping the data on the platform error-free. Most of the work done is related to database structure maintenance, so they do not interact directly with the data itself. One of the core procedures to notify the formal caregivers is when there is a problem in a care-receiver profile. iGenda tends to be as automatic as possible, keeping its users from having to interact with the data. However, to achieve this the data must be stored for long periods of time (if it is relevant) and must be accessible by several people, as explained above.

The data protection and privacy issues will be explained in the following sections, highlighting the current legal limitations and the features of iGenda that have not yet been given legal considerations, and that affect most of the current AAL projects. Furthermore, there are some ethical issues that the iGenda presents regarding data protection and privacy themes. These ethical considerations are presented in section 8.

3 The Data Protection Framework for AAL Systems

iGenda (and AAL platforms in general) collects and processes health-related data which is particularly sensitive and therefore requires special protection in abidance with specific Data Protection Directives. Compliance with personal data protection rules, lawful processing of personal data (including health data), and data security is crucial for building trust in ALL solutions. In addition, security-related issues and data protection safeguards must be defined in the early stages of development of the AAL, because high security is essential for a successful implementation. Also, data protection should be incorporated in all the processes that are implemented by the vendors and service providers.

3.1 Transversal Data Protection in Electronic Systems

Personal data protection is a fundamental right in Europe, which is enshrined in article 8 of the Charter of Fundamental Rights of the European Union as well as in article 16 of the Treaty on the Functioning of the European Union (TFEU). The fundamental right to privacy with respect to the processing of personal data is protected in conformity with national measures implementing European Union provisions on the protection of personal data, specifically 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 (Personal Data Protection Directive) that was adapted in Portugal by the Law 67/98, 26 October on Data Protection (Portuguese Data Protection Act) and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

In the EU, the currently applicable Data Protection Directive 95/46/EC was intended to ensure that individuals keep effective control over their personal data. Meanwhile, a new General Regulation on Data Protection (Regulation 2016/679, due to replace the said Directive), was approved and will enter into force in May 2018. This GDPR aims to harmonise data protection rules in the EU, maintaining many of the previous principles and introducing new ones, including the principles of data protection by default, and data protection by design, which can be very important to the issue of AAL platforms and data minimisation to guarantee that data protection safeguards are taken into consideration at the planning phase of procedures and development of systems.

3.2 General Data Protection Principles

In terms of Personal Data, the Directive 95/46/EC establishes it as any information related to an identified or identifiable natural person, considered as the data subject, more precisely in article 2, paragraph a) of the Directive. An identifiable person is one who can be identified, directly or indirectly, specifically by reference to an identification number or to one or more factors that are specific to his/her physical, physiological, mental, economic, cultural, or social identity. "Processing of personal data" means any operation or set of operations, which is performed upon personal data, whether by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (article 2, line b) of the Directive)[4]. This may include the processing of sound and image data. In the Portuguese legal system there is a general prohibition of processing personal data. Article 35 of the Portuguese Constitution forbids the use of informatics for the treatment of data concerning the private life of the citizens [22]. In addition, both the Portuguese Law 67/98 and the European Directive 95/46/CE have stipulated that, within the prohibition of processing sensitive data, the following data must be included: data concerning not only the private life of the citizens, but also health data, sexual life data (and genetic data in the Portuguese law). However, there is an obvious exception to this general prohibition: this is the case when the data subject expressly consents through free informed will (which in the case of sensitive data must be issued in an express way) without any kind of coercion, in which the data subject must be totally aware of the effects arising out of his/her manifestation of will [23].

3.2.1 Data Protection by Design

Of course, for elderly people, consent can raise some problems because it must be given unambiguously by any appropriate method enabling a freely-given, specific, and informed indication of the data subject's wishes, either by a written statement, including electronic, oral or (if required by specific circumstances) by any other clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed[5]. The elderly can be in a situation of dependence that prevents them from giving this informed consent.

Privacy by design brings along the responsibility for the processor of data to apply the adequate technical and organisational measures due to efficiently ensure the compliance with the data protection principles and the rights of the holders of data (art. 23 no. 1 GRDP). This is especially relevant when dealing with medical information, that is subject to professional secrecy and special categories of personal data (art. 9 GDPR) (i.e., health data which reveals

4 "Opinion 4/2007 (WP 136) of the Article 29 Working Party on Data Protection on the concept of personal data" available on: http://goo.gl/TWb4M7

5 Recital 25 of the General Data Protection Regulation.

information relating to the past, current, or future physical or mental health of the patients, Recital 35 in the preamble of GRDP). We recommend that AAL platforms are created with a mechanism of privacy by design and a privacy impact assessment before it is used.

Requirements of "privacy by design" and "privacy by default" will become a lot stricter under GDPR. What will be facilitated is the cross exchange of health data while preserving a high level of protection. GDPR proposes an additional requirement that dictates how a company must design its devices and services: "The principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation."

According to the General Data Protection Regulation, approved by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, in Recital 78, "the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency regarding the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."
It is also of core importance to take into account Article 25 that establishes in Number 1 "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

3.2.2 Legal Enforcement on AAL platforms

Data consumers must comply with the general principles of data protection law established in the Data Protection Directive. One of them is the limitation principle or purpose principle (partially embodied in article 6, no. 1, paragraph b) of the Directive and in article 5, no. 1, paragraph b) of the Portuguese Data Protection Act, and art. 5 number 1 b) of the GDPR), which prohibits further processing that is incompatible with the original purpose(s) of the collection. Personal and health data collected via AAL should only be processed for the purpose of providing AAL services and should not be processed for any other purpose not disclosed to the users that are using the service.

The data quality principle requires personal data to be relevant and not excessive for the purposes for which it is collected. Therefore, irrelevant data should not be collected and if it has been collected it must be discarded (article 6, number 1, paragraph c) of the Directive). It also requires data to be accurate and kept up-to-date, according to article 6 number 1, paragraph d) of the Directive and article 5, number 1, paragraph d) of the Portuguese Data Protection Act. This principle is considered also in article 5 number 1 c) and d) of GRDP. The principle of proportionality requires that any measure affecting individual's rights is appropriate for achieving the objective pursued and does not go beyond what is necessary to attain it, assuring a balance between the collected data and the purposes of its collection and processing [23,14].

Article 6 of the Directive and article 5, number 1, paragraph c) of the Portuguese Data Protection Act, and 5 number 1 c) of GRDP, incorporate this principle by stating that personal data must be adequate, pertinent, and not excessive in relation to the intended and legitimate purposes for which it is collected and/or further processed.

Also, of core importance it the right of access to data which has been collected concerning the patients and to exercise this right easily and at reasonable intervals to be aware of and verify the lawfulness of the processing. For the purposes of iGenda, the patients need to have access to the personal data that concerns their health (e.g., data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided)[6].

According to the minimisation principle, the processing of personal data must be strictly limited to the minimum required to achieve the AAL objectives. In addition to the above, the data should not be retained in these systems for longer than necessary (see article 6, number 1, paragraph e) of the Directive and article 5, number 1, paragraph e) of the Portuguese Data Protection Act, and article 5 number 1 c) of GRDP). Each consultation of personal data that is available through the AAL should be justified by the existence of a real necessity to access specific data related to the care or treatment to be provided or the medicine to be prescribed or dispensed.

The retention principle specifies that the collected data should only be conserved for the time and the necessities of the initial purpose, i.e., the data should not be retained in these AAL systems longer than it is necessary to achieve the specified purposes for which it was initially collected. This retention principle is associated to the right to be forgotten and the right to be let alone [23]. To ensure this right, Article 12 of the Directive and article 11 of the Portuguese Data Protection Act provide the care-receiver with the right to access and verify, without any need of substantiation, the accuracy of the data concerning himself/herself and to ensure that the data is kept correct and up-to-date. This ensures informational self-determination. According to the article 16 of the GRDP the rights holder is entitled to obtain, without undue delay, the rectification of the personal data related to him. These rights fully apply to the collection of personal data in AAL platforms. Furthermore, the principles of fair and transparent processing require that the patients should be informed of the existence of the processing operation by iGenda and all its purposes, with the creation of profiles (or, at least, profiling without rules) not being possible. Profiling is another issue that is related to AAL platforms in general and to iGenda. This can be seen in article 4, Number 4 of GRDP which comprehends health data establishes that “profiling means any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements”. However, we must bear in mind that profiling is subject to the general rules of Data Protection, inter alia, legal grounds of processing and data protection principles. One solution could be the existence of specific safeguards, such as the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual[7]. This impact assessment would contribute to the reception of justified queries from the interested parties, thus allowing the modification of the system avoiding future predicaments.

Also, in accordance with article 10 of the Directive and in the terms of article 10, number 1 of the Portuguese Data Protection Act, the care-receiver must be provided with the following information: the purpose of the collection and processing of his/her personal data (e.g., for diagnosis, prevention), the identity of the data processor, the recipients of the data, and the existence of a right of access and rectification, the transfers of personal information outside the EU, and the disclosures of information to third parties (e.g., other healthcare professionals). The

6 See Recital 51 of the General Data Protection Regulation.

7 Similar to Recital 58 a) of the General Data Protection Regulation and infra 6.2.

provision of this information is necessary to satisfy the requirement of fair and lawful processing under the Data Protection Directive. In the GRDP Regulation these rights are established in article 13 numbers 1 and 2.

Furthermore, article 17 of the Directive and article 14 of the Portuguese Data Protection Act impose security related obligations upon the data processor to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organisational or technical. In GRDP there is the recognition that data protection must apply by design and by default (art. 25).

3.2.3 Data Health Standards

According to the European Court of Justice, the notion of "data concerning health" must be given a broad interpretation to include information concerning all aspects (both physical and mental) of an individual's health[8] in the terms of the Directive 95/46/EC. The European standard based on this directive are: the European Standards EN 14484:2003 "Health informatics – International transfer of personal health data covered by the EU data protection directive – High level security policy"; and EN 14485:2003 "Health informatics – Guidance for handling personal health data in international applications in the context of the EU data protection directive". (These standards are currently under revision.)

Article 29, Data Protection Working Party[9] provided further interpretation of this concept by recommending that health data should involve: any personal data that is closely related to the health status of a patient, such as data on consumption of alcohol or drugs, genetic data, and any other data contained in the medical documentation concerning the treatment.

A large amount of personal information flows between the various services of AAL platforms when monitoring the care-receiver using sensors and constructing profiles. This raises a delicate issue that is related to the collection, storing, and transmission of health data, which is considered by European and Portuguese law as "sensitive data", thus requiring reinforced protection. Nevertheless, monitoring and profiling must be done to accomplish the minimal requirements for the platform operation, which does not mean that legal aspects are breached.

Health data is in the special categories of data, according to the Directive (art. 8 number 1) and the Regulation (art. 9 number 1) and considered as sensitive data in Portuguese law (art. 7 number 1) and there is a prohibition of its general use. However, there may be some exceptions to the rule if the information is crucial to providing appropriate medical support. Therefore, identifiable health data may only be processed if at least one of the conditions established in article 8 number 2 and 3 of the Directive is satisfied (and article 9 number 2 and 3 for the GRDP). Clearly, processing health data can be authorised when there is an explicit consent of the care-receiver and also if additional data security measures are available, such as the logical separation between sexual life or genetic data and other personal data [23]. Accessing data may also take place when the care-receiver is temporarily unable to express consent (e.g., loss of total unconsciousness or coma) or when the data collection or its processing is absolutely indispensable in order to protect the care-receivers' vital interests: usually life or death situations; and in this case, the fundamental right to life will always prevail [24].

Also in the General Data Protection Regulation health data is a special category of data. This special data means, according with article 4, 15, "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" and that the processing of such data is, generally prohibited. This prohibition is established in article 9, number. 1, "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a

8 European Court of Justice, Judgment of 6 November 2003, Case C-101/01 - Bodil Lindqvist, 50 and 51.

9 This group was created by Article 29 of Directive 95/46/EC.

natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

However, number 2, h), permits in some cases the treatment of data when "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3", or "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject".

4 Legal Requirements for Lawful and Transparent Processing of Personal Data

In article 8, numbers 2 and 3, the Data Protection Directive stipulates mandatory derogations of the general prohibition of processing special categories of data and an optional exemption concerning health data in article 8, number 4 of the referred Directive (article 9 number 2, 3 and 4 of the GDP). It is important to consider the fact that all these derogations must be as limited as possible. In conformity with article 8, number 2, line a) of the Directive, the exception to the general prohibition of sensitive data processing can be the consent of the data subject. An important point is that to be valid, this consent must be a "freely given, specific, and informed indication of the data subject's wishes", as defined in article 2, line h) of the Directive.

Thus, the iGenda way of processing special categories of data (more specifically, health data) is legally possible upon the requirement of consent: consent is a cornerstone of the Data protection principles as can be seen in many of the Recitals of the Directive 95/46/EC and in the General Data Protection Regulation approved on 4th March 2015 by the European Council. As an example, Recital 25 establishes that: "Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, including electronic, oral statement or, if required by specific circumstances, by any other clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed". Also, Recital 32 is important when it establishes that: "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation. Specifically, in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that, and the extent to which, consent is given". For consent to be free, the data subject must be informed. Yet, for the processing of sensitive data, it is also required that the consent of the care-receiver fulfil the following conditions:

- It must be freely given: free consent means a voluntary decision issued by an individual person in possession of all of his/her faculties, taken in the absence of any kind of coercion and which can be taken out at any moment without any sort of penalisation;
- It must be specific: specific consent must refer to a well-defined, concrete situation in which the processing of heath data takes place. Consequently, a general agreement of the care-receiver just with an indication of a vague and generic purpose for the use of his/her data (e.g., the collection of his medical data and the subsequent transfers of this health and clinical data to the past and the future health professionals involved in treatment or among different medical entities and organisations) would not constitute consent in the terms of article 2, line h) of the Directive. Beyond that, each time the alluded finality is modified, it is mandatory to get a new consent for the care-receiver.
- It must be informed: informed consent represents a consent from the care-receiver based upon an appreciation and understanding of the facts and implications arising out

of his/her manifestation of will [23]. The individual consent must include accurate and full information of all relevant points. Specifically, those specified in articles 10 and 11 of the Directive (e.g., the nature of the data processed, purposes of the processing, the rights of the data subject, and the recipients of possible transfers). In GRDP these specifications appear in articles 13 (information to be provided when data is collected from the rights holder) and 14 (information to be provided when data is not collected from the rights holder).

As an extra requirement to the provisions of article 7 of the Directive (and article 9 of GRDP), consent in the case of special categories of data and therefore in any kind of AAL system (like iGenda) must be explicit (i.e., fully and clearly expressed). Additionally, the care-receiver must always be informed about the presence of sensors and cameras and what type of personal data is being processed and for what purposes the data is planned to be used, according to article 11 of the Data Protection Directive (and article 14 of GRDP). In obedience to article 10 of the Data Protection Directive (and article 13 of GRDP), each data subject has a right to know the identity of who is processing their personal data. Thus, the iGenda (seen in this context as the processor) always informs potential users at least about the following: identity and contact details, the precise categories of personal data the platform will collect and process, why (for what precise purposes), whether data will be revealed to third parties (and under what conditions), and how users may exercise their rights in terms of withdrawal of consent and deletion of data, ensuring the transparency of all of the process that capture and treat personal data [25]. To fulfil this legal requisite, every application has a readable, understandable, and easily accessible privacy policy, where all of the above-mentioned information is included. The consent will be received through a digital consent from filled by the user party.

Furthermore, article 18 of Directive 95/46/EC materialises the principle of transparency, setting out an obligation to notify the supervisory authority before carrying out any operation. In GRDP, article 30, there is an obligation for the data processor to keep a register of all the processing activities under his responsibility, and the processor must, when required, make this register available to the supervising authority (article 30 number 4 GRDP). At the same time, according to articles 12 and 14 of the Data Protection Directive (and articles 15, 16 and 17 of GRDP), the care-receiver can exercise his/her rights of access, rectification, deletion, and the right to object to data processing. Therefore, if the care-receiver exercises the right to access the data, the care-receiver will be provided with information about what is being processed and its source. If the platform takes automated decisions based on compiled data, the care-receiver is informed about the logic behind those decisions. The care-receiver should be able to ask about the access of each party and be allowed the possibility of rectification, deletion or blocking of any parties or entities involved in the exchange of information within iGenda. Thus, the care-receiver has a right of opposition: the rights holder can deny the collection and processing of his/her personal data and refuse access to optional information using privacy-friendly default options [23], with the downside of losing some or all iGenda features and services.

Regardless of the above referred rights, sometimes certain circumstances may arise under which the access of the users to their own information may not be beneficial or may even be harmful to them; this is called the right of no science or unknowingness [26]. There are social and psychological barriers that must be met which do not overlap or overrule the rules but that do require a different approach to data access (i.e., it is of the users' best interest not to show some information to them). For instance, the information about a diagnosis of a terminal disease may be delayed so that it can be communicated through a human intermediary and not by the platform. In these cases, human interaction is preferred.

5 Authorisation for Accessing Data: Categories of Data Storage

All AAL platforms need to collect health data about their users and persist that data for historical operations, personal health records and future medical actions based on previous conditions. Therefore, iGenda is confronted with the difficult decision of which categories of

personal data, particularly health data, should be collected and stored. Since it is necessary to consider the fundamental rights of the individual (especially regarding the right to be left alone or the right to be forgotten) so data must only be stored while it is indispensable.

In conformity with the principles of relevance and proportionality of data collection, every compilation of data must be limited to the data that is relevant and not excessive for the defined purpose of the processing (article 6, number 1, paragraph c) of the Directive and article 5 c) of GRDP – minimisation of data). This Directive directly and indirectly affects the process of keeping information about the medical history of the people that are supervised by AAL platforms. To provide a secure and reliable medical diagnosis, it is imperative to have knowledge about previous medical problems. Therefore, by shortening the lifespan of the information, the European norms restrict the provision of any type of diagnosis and just responds to immediate problems.

5.1 Social Features

iGenda provides a feature that is based on social interaction, meaning that it aims to connect several of its users and shares non-vital information among them. Although the information is non-vital, several aspects can be extracted when information is cross-linked. Thus, by propagating previous rules, each individual may require being exempt from this feature and requires that all information related to him/her be removed. This requires prior information about who, when and why someone wants to access to the data and about the potential consequences of not allowing access.

5.2 Profiling

The profiling technique is an essential feature in the iGenda. It automatically builds a database that mirrors the user's personality to better emulate the user's choices in non-critical decisions, and it requires a large amount of personal data. The iGenda uses profiling techniques based on artificial intelligence methods that through the usage of the system it learns users' preferences and likes. It then uses that information to proactively change the home environment and control devices emulating the user in certain decisions. Each user is clearly identified and each has its own profile type, such as care-receiver, the caregiver, and other users; however, there are various categories of personal data stored in these profiles that require different degrees of confidentiality. Therefore, each user has different access conditions to the database[10]. The Article 29 of the Data Protection Working Party provides information related to electronic health records that contain some similarities in terms of securing and anonymising personal information about the users, but the procedures have very little relation with the processes used by the iGenda.

Rather than excluding such data, which might be prejudicial for future successful medical care, special restrictions for access to such data are built into the system that includes explicit consent and special technical barriers for data protection. The bulk information is used in machine learning processes that are tightly related to each user. The anonymisation of the available information would provide bad results, like average results. When the potential users have a great number of conditionings, like health issues, average results are not advised as personalised results, thus the requirement of identifiable information by the system.

6 Data Security Requirement in AAL

Article 17 of the Data Protection Directive and Article 32 of GRDP impose security requirements, which specifies that appropriate technical and organisational measures must be taken to avoid unauthorised or unlawful processing of personal data to ensure that data remain confidential and to protect personal data against accidental or unlawful loss, damage, or

10 See Article 29 Data Protection Working Party. "Working Document on the processing of personal data relating to health in electronic health records (HER)" Adopted on 15 February 2007 (00323/07/ENWP 131).

destruction. The integrity of the system and personal data protection in iGenda can be guaranteed by making use of privacy-enhancing technologies and transparency-enhancing technologies [25]. The iGenda platform includes regular internal checks and controls of database access, which serve as a protection against intrusions. Accordingly, the module of the Agenda Manager keeps a record of every connection made through a Login register, which registers every communication tunnel established, such as in a log-style for security analysis. Although there is a large list of encryptions techniques (and the iGenda databases are AES-128 encrypted) like the ones presented by ENISA [27] are designed to keep databases secure from outside risks, while most of the iGenda risks come from internal interaction, e.g., technicians, caregivers, medical staff. Thus, the people with direct access to the iGenda information do not have these encryption barriers and can surpass the encryption protocols as they are authorised.

Nevertheless, in iGenda, as in any other AAL platform, there is clearly a permanent risk of loss of privacy and unauthorised access to ones' data. That is why the overall security for applications of this type must pay special attention to data protection and privacy. It must be ensured that the data security is implemented directly in the architecture of an AAL (privacy by design).

Besides that, the complexity of the platforms, the users typically do not understand the actions of ICTs (Information and Communication Technologies). This obliges resorting to technicians/engineers to keep the system working correctly, since the users (caregivers and care-receivers) are prone to introducing errors that they cannot correct. Furthermore, there is an inherent distrust of computer systems and their actions, which makes their adoption and understanding difficult.

The use of mobile devices and personal computers may become problematic due to the lack of security protocols, not by transmitting information but to rather determining whether the person who is operating the device is the same person that the information is directed to. It is reasonable to expect another person to access the information of a care-receiver on his/her behalf, which leads to a serious problem, which is insuring that the informed consent is really from the intended user. For instance, if a user has limitations (e.g., eyesight problems) another person (a relative, etc.) might read the information to him/her, breaching confidentiality and privacy and in some cases, providing consent for the original user without his/her knowledge. This ethical issue is more related to the social aspect but it is very important to address due to the implications that it has. Most AAL projects consider that the directed information is only read by the intended users; however, that is not the case in many of the environments [28]. Introducing security measures such as passwords are impeditive to the normal visual interface operation, and in the case of users with some form of dementia introducing these measures is even impossible. The advances in some devices provide fingerprint identification, which increases security and identification; however, the problem persists if the user’s disregard those features. Since there is no feasible solution that has a high level of acceptance and security for this issue, we suggest that the best way to enforce the security measures is to educate the users about the correct procedures to operate the platform.

7 Ethical Concerns

There are several ethical concerns about AAL projects, since most of the actions that AAL projects perform can become ethically questionable if they fail or the information that is transmitted is compromised by others who are not the original sender and receiver. For instance, the loss of trust and the possible misuse of data would have unimaginable repercussions if an attack occurred and information was stolen. Most of the information flowing in the iGenda is very sensitive, thus the leak of such information can lead to the loss of privacy if the information is posted on the Internet or even lead to identity theft. Principles that are applied in healthcare practice (confidentiality, informed consent, etc.) still do not have a parallel in AAL applications, which can pose a high risk due to the role of mediation that they assume by collecting and processing data.

iGenda presents ethical issues that affect all of its users, which can be grouped in the following way: care-receivers, caregivers (formal, informal, relatives, and friends), medical staff, and technicians [28–30]. Some of the issues that we believe to have the most ethical concerns related to the iGenda platform are presented below.

7.1 Informed Consent and Independence

There are two issues regarding informed consent and independence: the user's lack of understanding of the platform actions and the possible dependence of the users on the platform. The first issue requires the complete trust of the user, even if the users do not understand how their information is about to be used, shared and processed. The second issue (which also requires full trust in the system) is that the users tend to have a more dependent life. This contradicts the aim of AAL projects, which is to increase the autonomy of the users. In case of the iGenda an informed consent draft was prepared according to the current Portuguese legal parameters. We believe that it is not the best way to approach this issue, but at this moment it is the only measure we can implement.

7.2 Platform Alienation

Another issue is the user's sense of lack of control. Since most of the events and actions are automatised, the users may feel that they do not have any control over their own lives, which leads to the rejection of the platform [31–34]. The "transparent" and ubiquitous technology may provide few humanisation features, which to a human user may mean that they are no longer in control. Furthermore, the introduction of many sensors (more specifically cameras) makes the users aware that they are being monitored and may challenge the expected results due to an abnormal response of the users to the environment. In an effort to humanize the systems, Portet el al. [35] has proposed that the systems use voiced answers and visual cues to the changes that are happening, however, in our opinion, this conflicts with the expected transparency and integration in the user's lives. Moreover, the way that iGenda and most AAL operate require some fixed actions and procedures that obligate the users to engage, disregarding their own decision towards those actions. A possible outcome is a digital exclusion, creating negative feelings about the platform that they are somewhat obliged to use (due to the help that it provides and the limitations that the user has) contradicting the iGenda objective.

7.3 True Objective

Last is the ethical issue related to the objective of the iGenda, meaning, with the introduction of external care services who is going to benefit from its use. For the normal operation of iGenda, external services are required (formal caregivers and private medical services) to provide extra assistance and to compensate the presence of relatives and doctors on a regular basis. These services have high-level access to the information of their clients (users that pay for their service) and, to some degree, can manipulate their clients' information. This means that the iGenda platform could be used inappropriately, for instance free-time activities can be override by external managing services. Moreover, the iGenda petition for admittance can be done by people other than the final users and be repurposed, thus delivering all control to the external services. Furthermore, utility services (like electricity or internet) can greatly influence the operation of the system because it is very dependent on them. For instance, if there is a critical occurrence, iGenda may be unable to register. The ethical issue of trust abuse is very difficult to manage. Some technological solutions may be implemented to monitor it, but they can only serve after the abuse happens; therefore, they cannot help in preventing it. Another ethical issue may fall under the term of overlapping responsibilities, which establishes the normative of operations where each service is responsible for itself and its importance related to the responsibility for the remaining services (e.g., if there is an electrical failure, iGenda cannot be responsible for the absence of service during that period).

Mark R. Waser [36] states "All ethical agents must not only have the ethical decision-making rules but also methods to collect data, information and knowledge to feed to those rules; codified methods to determine the source, quality and accuracy of that input; trustworthy methods to recognise anomalous conditions requiring expert human intervention and simple

methods to get all of this into the necessary hands in a timely fashion". This may balance the responsibility of the ethical responsibility between all actors that make decisions on the platform, since responsibility currently cannot be attributed to machines or computer systems.

These are the most important and complex ethical issues identified in the operation of the iGenda. Some can be addressed more easily than others. There are issues that do not have a defined procedure or guideline of operation, so they must be carefully reflected and managed in the following developments of iGenda.

8 Conclusions

The investment in AAL projects and the technological advances of these platforms have shed new light on what data is required and how it is managed, introducing the theme of unsupervised data processing and cross-sharing of sensitive information. Some of the ethical concerns were addressed in section 7, and others still require more consideration and investigation [29,30].

This study focuses mainly on the analyses of technical features that may collide with legal requirements in terms of privacy and data protection. However, to mitigate the potential risks of privacy loss and unauthorised access to personal data as much as possible, care-receivers need to be enabled to make use of their legal right to informational self-determination by taking control of their own data flowing within the system. This must be done in a way that allows them to benefit from the iGenda services and, at the same time, to ensure that all guarantees of fundamental rights are respected.

Transparent and permanent cooperation and participation of the care-receivers is still required to ensure the exercise of their fundamental rights to informational self-determination; the only admissible exception of cases is when care-receivers are not able to give their free and informed consent and the collection and processing of the data becomes absolutely necessary to protect their vital interests. Nevertheless, the highly heterogeneous group of people using iGenda results in many legal requirements defined mostly by data protection laws and that must be taken into consideration right from the start.

From what we have could observe, AAL projects can follow current laws but not without losing important features that would be essential to improve one's health condition. There are few exceptions that may be implemented that can enforce legal aspects, but in our perspective, it is almost impossible to change the core design of AAL systems in such way that they can comply with current legal requirements. The rate at which technological solutions are advancing makes it clear that current directives and protections are inadequate and that it would be in everyone's interest to accommodate future developments by adjusting to the new data requirements. Moreover, the acceptability of AAL projects depends on being able to provide an adequately high level of data protection and privacy, which is why security-relevant issues must be considered.

The problem with these concerns is that they lack legal directives, so there are no guidelines to establish the correct implementation. Nonetheless, we can address recommendations that can help prevent erroneous actions committed by the users by resorting to social engineering:

- Train users by giving courses and explaining the technology that they are using. Take preventive measures and give information about how the life of a user is going to be affected by using iGenda.
- Include the users' input in the development of new features or the correction of current ones, generating a more user-friendly environment that the final users can relate to and thereby generate trust.

- Inform the users (specially the caregivers) about privacy issues and how to keep their information private, as well as explain the way information is processed and sent across the platform.
- Inform the staff (formal and informal caregivers and technicians) of their roles on the platform, explaining in detail the platform features that they will be operating.

Present confidentiality contracts to the staff and enforce regular reviews of their activity by an independent taskforce. This procedure also assures that the privacy and data protection are enforced from social engineering attacks.

In summary, this paper has presented several aspects that are related to the legal and ethical concerns that affect the data transmission and procedures of AAL projects. Because there is a large amount of data flowing through the systems the issues of privacy and data protection are not trivial nor easy to implement or enforce. In the sections 7 and 8, the data protection framework was presented, showing what procedures of the AAL platforms abide by the law and which do not as well as the ethical concerns that affect the users (with the iGenda as an example). Furthermore, it has been demonstrated that if the iGenda follows and enforces all current legal directives, it would jeopardise the user's privacy and security, and the platform would be severely crippled in terms of functionality.

Acknowledgements

This work has been supported by FCT - Fundação para a Ciência e Tecnologia within the Project Scope UID/CEC/00319/2013. A. Costa thanks the Fundação para a Ciência e a Tecnologia (FCT) the Post-Doc scholarship with the Ref. SFRH/BPD/102696/2014. This work is also partially supported by the MINECO/FEDER TIN2012-36586-C03-01.

References

[1] P.D. United Nations, Department of Economic and Social Affairs, Population Ageing and Development Database 2014, 2015. http://www.un.org/en/development/desa/population/publications/ageing/ageing-development-database-2014.shtml.

[2] United Nations, World Population Ageing 1950-2050 (Population Studies Series), United Nations, 2002. doi:10.2307/1524882.

[3] United Nations, Population estimates and projections section, 2012. http://esa.un.org/wpp/ppt/paa/PAA%7B_%7D2012%7B_%7DHeilig.pdf.

[4] European Commission, The 2015 ageing report: Economic and Budgetary Projections for the 28 EU Member States (2013-2060), 2015. doi:10.2765/973401.

[5] C. Harrington, J. Choiniere, M. Goldmann, F.F. Jacobsen, L. Lloyd, M. McGregor, V. Stamatopoulos, M. Szebehely, Nursing Home Staffing Standards and Staffing Levels in Six Countries, J. Nurs. Scholarsh. 44 (2012) 88–98.

[6] A. Matta, S. Chahed, E. Sahin, Y. Dallery, Modelling home care organisations from an operations management perspective, Flex. Serv. Manuf. J. (2012).

[7] J. Grauel, A. Spellerberg, Attitudes and requirements of elderly people towards assisted living solutions, in: M. Mühlhäuser, A. Ferscha, E. Aitenbichler (Eds.), Constr. Ambient Intell., Springer Berlin Heidelberg, Berlin, Heidelberg, 2008: pp. 197–206. doi:10.1007/978-3-540-85379-4.

[8] R. Magjarevic, Home Care Technologies for Ambient Assisted Living, in: T. Jarm, P. Kramar, A. Zupanic (Eds.), 11th Mediterr. Conf. Med. Biomed. Eng. Comput. 2007,

Springer Berlin Heidelberg, Berlin, Heidelberg, 2007: pp. 397–400. doi:10.1007/978-3-540-73044-6.

[9] A. Costa, P. Novais, R. Simoes, A Caregiver Support Platform within the Scope of an Ambient Assisted Living Ecosystem, Sensors. 14 (2014) 5654–5676. doi:10.3390/s140305654.

[10] M.J. O'Grady, C. Muldoon, M. Dragone, R. Tynan, G.M.P. O'Hare, Towards evolutionary ambient assisted living systems, J. Ambient Intell. Humaniz. Comput. 1 (2009) 15–29. doi:10.1007/s12652-009-0003-5.

[11] P. Rashidi, A. Mihailidis, A Survey on Ambient-Assisted Living Tools for Older Adults, IEEE J. Biomed. Heal. Informatics. 17 (2013) 579–590. doi:10.1109/JBHI.2012.2234129.

[12] H. Sun, V. De Florio, N. Gui, C. Blondia, Promises and Challenges of Ambient Assisted Living Systems, in: 2009 Sixth Int. Conf. Inf. Technol. New Gener., IEEE, 2009: pp. 1201–1207. doi:10.1109/ITNG.2009.169.

[13] Â. Costa, F.C.P. Andrade, P. Novais, R. Simões, Privacy and Data Protection in Elderly Healthcare: Threats and Legal Warranties, Proc. Sixth Int. Work. Juris-Informatics (JURISIN 2012). (2012) 7–22. http://repositorium.sdum.uminho.pt/handle/1822/23889.

[14] F. Andrade, J. Neves, P. Novais, J. Machado, A. Abelha, Legal Security and Credibility in Agent Based Virtual Enterprises, in: Collab. Networks Their Breed. Environ., Springer-Verlag, New York, 2005: pp. 503–512. doi:10.1007/0-387-29360-4_53.

[15] L.M. Camarinha-Matos, J. Rosas, F. Ferrada, A.I. Oliveira, BRAID Active Ageing Scenarios, 2011. http://www.braidproject.eu/sites/default/files/Ageing%7B_%7Dscenarios.pdf.

[16] W.J. Katon, E. Lin, J. Russo, J. Unützer, Increased Medical Costs of a Population-Based Sample of Depressed Elderly Patients, Arch. Gen. Psychiatry. 60 (2003) 897. doi:10.1001/archpsyc.60.9.897.

[17] P. Neuman, J. Cubanski, A. Damico, Medicare Per Capita Spending By Age And Service: New Data Highlights Oldest Beneficiaries, Health Aff. 34 (2015) 335–339. doi:10.1377/hlthaff.2014.1371.

[18] University of Southampton, Active aging on the up in EU, despite economic crisis and austerity -- ScienceDaily, ScienceDaily. (2015). https://www.sciencedaily.com/releases/2015/04/150415125827.htm (accessed November 14, 2016).

[19] Â. Costa, J.C. Castillo, P. Novais, A. Fernández-Caballero, R. Simoes, Sensor-driven agenda for intelligent home care of the elderly, Expert Syst. Appl. 39 (2012) 12192–12204. doi:10.1016/j.eswa.2012.04.058.

[20] A. Costa, P. Novais, J.M. Corchado, J. Neves, Increased performance and better patient attendance in an hospital with the use of smart agendas, Log. J. IGPL. 20 (2012) 689–698. doi:10.1093/jigpal/jzr021.

[21] P. Novais, R. Costa, D. Carneiro, J. Neves, Inter-organization cooperation for ambient assisted living, J. Ambient Intell. Smart Environ. 2 (2010) 179–195. doi:10.3233/AIS-2010-0059.

[22] G. Marques, L. Martins, Direito da Informática, 2nd ed., Almedina, 2006.

[23] C.S. e Castro, Direito da Informática, Privacidade e Dados Pessoais, Edi{ç}{õ}es Almedina, 2005.

[24] L.B. Correia, Direito da Comunicação Social, Almedina, 2005. http://books.google.pt/books?id=JLkZSQAACAAJ.

[25] P. Hert, S. Gutwirth, A. Moscibroda, D. Wright, G. González Fuster, Legal safeguards for privacy and data protection in ambient intelligence, Pers. Ubiquitous Comput. 13 (2008) 435–444. doi:10.1007/s00779-008-0211-6.

[26] P. Rothenpieler, C. Becker, S. Fischer, Privacy Concerns in a Remote Monitoring and Social Networking Platform for Assisted Living, in: IFIP Adv. Inf. Commun. Technol., 2011: pp. 219–230. doi:10.1007/978-3-642-20769-3_18.

[27] European Union Agency For Network And Information Security, Smart Hospitals, European Union Agency for Network and Information Security, 2016. doi:10.2824/28801.

[28] B. Hofmann, Ethical Challenges with Welfare Technology: A Review of the Literature, Sci. Eng. Ethics. 19 (2013) 389–406.

[29] P. Novitzky, A.F. Smeaton, C. Chen, K. Irving, T. Jacquemard, F. O'Brolcháin, D. O'Mathúna, B. Gordijn, A Review of Contemporary Work on the Ethics of Ambient Assisted Living Technologies for People with Dementia, Sci. Eng. Ethics. 21 (2015) 707–765. doi:10.1007/s11948-014-9552-x.

[30] J. van Hoof, H.S.M. Kort, P.G.S. Rutten, M.S.H. Duijnstee, Ageing-in-place with the use of ambient intelligence technology: Perspectives of older users, Int. J. Med. Inform. 80 (2011) 310–331. doi:10.1016/j.ijmedinf.2011.02.010.

[31] F.D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, MIS Q. 13 (1989) 319. doi:10.2307/249008.

[32] W. Wilkowska, M. Ziefle, Privacy and data security in E-health: Requirements from the user's perspective, Health Informatics J. 18 (2012) 191–201. doi:10.1177/1460458212442933.

[33] K. Arning, M. Ziefle, "Get that Camera Out of My House!" Conjoint Measurement of Preferences for Video-Based Healthcare Monitoring Systems in Private and Public Places, in: Incl. Smart Cities E-Health, Springer, 2015: pp. 152–164. doi:10.1007/978-3-319-19312-0_13.

[34] J.W. Patton, Protecting privacy in public? Surveillance technologies and the value of public places, Ethics Inf. Technol. 2 (2000) 181–187. doi:10.1023/A:1010057606781.

[35] F. Portet, M. Vacher, C. Golanski, C. Roux, B. Meillon, Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects, Pers. Ubiquitous Comput. 17 (2013) 127–144. doi:10.1007/s00779-011-0470-5.

[36] M.R. Waser, Implementation Fundamentals for Ethical Medical Agents, in: Mach. Med. Ethics, Springer, 2015: pp. 49–65. doi:10.1007/978-3-319-08108-3_4.