Privacy and Data Protection in Elderly Healthcare: Threats and Legal Warranties

Ângelo Costa[1], Francisco C.P. Andrade[2], Paulo Novais[1], Ricardo Simoes[3,4,5]

[1]CCTC-Departament of Informatics, University of Minho
[2] School of Law, University of Minho
[3]Institute of Polymers and Composites IPC/I3N, University of Minho, Guimarães, Portugal
[4]Polytechnic Institute of Cávado and Ave, Barcelos, Portugal
[5]Life and Health Sciences Research Institute (ICVS), School of Health Sciences, University of Minho, Campus de Gualtar, 4710-057 Braga, Portugal
acosta@di.uminho.pt, fandrade@direito.uminho.pt, pjon@di.uminho.pt, rsimoes@dep.uminho.pt

Abstract. The progressive aging of the population requires new kinds of social and medical intervention and the availability of different services provided to the elder population. New applications have been developed and some services are now provided at home, allowing the older people to stay home instead of having to stay in hospitals. But an adequate response to the needs of the users will imply a high percentage of use of personal data and information, including the building up and maintenance of user profiles, feeding the systems with the data and information needed for a proactive intervention in scheduling of events in which the user may be involved. Fundamental Rights may be at stake, so a legal analysis must also be considered.

Keywords: Healthcare Platform; Data Protection; Privacy; Ambient Assisted Living

1 Introduction

Aging is a natural process in the life of a person. As society, technology and healthcare advances life expectancy increases [1]. Every year the average death age increases meaning people age and live more. Also there is a tendency in the advanced countries to diminish the number of children. This enables a better quality of life of the family and enables spending contention. These two facts combined result in an aged population that cannot rely in the future workforce of the current teenagers. Furthermore there is an issue that is the great medical assistant that the elderly population need [2–4].

There is an obvious need to rethink health care planning and provision. Nursing homes are insufficient and most of the time families cannot maintain an elderly at home. Currently there are efforts to provide technological solutions in the medical and social domains. A common problem in using these applications is that not only they require total cooperation by the users, but also they often use user profiling. The ap-

plications require a huge collection of data in real time, being a way to get accommodated to the user preferences. User profiling requires interaction with humans by formulating questions, while the system evaluates answers that allow the profile creation.

Usually, these systems require a share of personal data (eventually sensible data) between system technicians and spread to health care professionals or user's family.

1.1 Motivation: Healthcare And Privacy

Medical Science is today developed in collaboration between human and technology. Despite the fact that the most relevant decisions are taken only by physicians, the truth is that computers provide nowadays an inestimable support through the use of decision support systems. They provide an easy access to data, tests results and may even present suggestions that will enhance the decision making process [5]. Many of the suggestions presented by applications based in the analysis of sensible data are then reviewed by medical care professionals. Computers must not decide anything concerning a citizen's health care problems [6]. Medical professionals have to follow strict deontological rules for the protection and safeguard of human life. These professionals are subject to secrecy and respect for privacy, nevertheless sensible data is being shared between persons and applications.

Every day technical staff process data and information concerning the users (the patients). Hospitals and health care units regard patient treatment essential, because of this fact they may sacrifice privacy to maintain a flux of data that is quite important for the availability of efficient and trustable health care services [7].

This scenario of privacy breaches is undesirable but strictly following the rules may lead to a worst clinical service. There must be a balance between the rights and legitimate concerns of users and the requirements of an efficient functioning of hospitals and health care units. Gathering and sharing data and information between hospitals, physicians and other professionals improves the health care services. Nevertheless it cannot be forgotten that privacy and data protection are fundamental rights of the patients.

This work is in the following of the work presented in Costa, Castillo, Novais, Fernández-Caballero, & Simoes, "Sensor-driven agenda for intelligent home care of the elderly". It is presented a cognitive assistant that uses visual monitoring systems to detect falls [8].

2 Cognitive Assistants on an Ambient Assisted Living Context

Long term memory loss is a complex issue, difficult to deal with and it mainly affects the older population. Cognitive impairments may be considered within three different groups: absence of cognitive impairments, light cognitive impairments and severe cognitive impairments. These kinds of impairments are different stages of memory loss [9–11]. In the first type there are no limitations or very light that do not affect the everyday life of the person. In the second stage, the person already faces some difficulties in his daily life, and memory loss starts to affect the execution of simple daily

tasks. The third stage corresponds to a situation in which a person needs constant vigilance, since it is no longer able to execute almost none of the simplest daily tasks. Persons included in the first or second stage are those that can be helped by the technologic resources [12]. Providing auxiliary means contributing to overcome the above referred memory losses.

Cognitive assistants may be described as follows: systems that help the user in the daily tasks, presenting real-time suggestions related to what the user is doing and revising the user actions and places where he was. However, projects directed to a real interactivity and total automation are not available yet. The projects developed still require great attention by the user. Both in what concerns the configuration of every option as well as the correction of mistakes of the application.

2.1 A Cognitive Assistant: iGenda

Project iGenda is being developed at University of Minho (Portugal) [6, 13, 14]. It is a project based in AAL (Ambient Assisted Living) environments that has as goal to be an intelligent agenda that automatically schedules events and leisure time activities. Events may result of appointments made by third persons and the system inserts the tasks and activities in the user's agenda. This development is aimed to the resolution of a quite common problem affecting older people, memory loss.

The iGenda can be perceived as a platform of services. Currently it has several available services, independent of the core structure. The services are: Personal sensor platform; Visual fall detection system; User profiling. Although independent, each one of them is part of the iGenda and uses its features. This means that there is a great trade of information between the services, as seen if Fig. 1. The information can be constituted by private content. Technicians can also access the information flowing in the system, as well introducing new information. Due to the complexity of this platform it manages very different type of information.

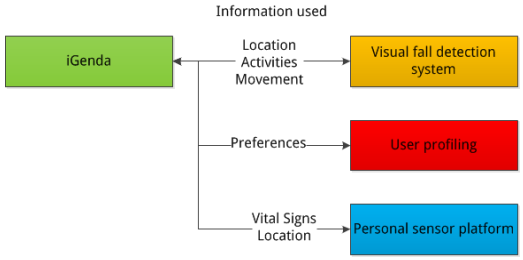

Fig. 1. : iGenda services and the information they send and receive.

In terms of the iGenda core, it operates in two distinct levels: on one side, the scheduling of events, on the other side, the management of leisure times. Scheduling of events is processed through the reception of new events by the system and, through a conflict resolution system, allocates them in an optimal timeframe. Also, it corrects errors and tries to overcome incompatibilities that might arise out of the process. The

function of leisure time management, on the other turn, ensures the scheduling of leisure activities, to make the user's life more active.

iGenda has three internal modules: the Agenda Manager, Conflicts Manager and Free Time Manager [15, 16]. The Agenda Manager is the portal of the system for the reception and sending of information. It is constituted by a message receiver, a security manager and a task deliverer. The received messages integrate a mechanism of safe electronic signature with an encryption key generated for each user. Thus, being ensured a level of security that only allows the destinee of the message to decrypt the message and have access to the message content. It also integrates in its database all the persons authorized to establish a connection with the user, serving as a protection against intrusions. The Agenda Manager keeps a record of every connection made through a Login register, ensuring the register of every communication. Conflicts Manager is essential for the scheduling. The decision making is done with resource to logical inference. Our approach to manage the incoming events is hierarchic. It balances the importance the sender gave with the classification the sender has. It is able to make changes to the received events, such as shortening and reallocating them to other timeframe. Also it is able to do these changes to already scheduled events if needed.

The person scheduling a new event may attribute a relevance value to the said event, but the system will always verify which base value is attributed to that user. Medical services will always have priority in the ranking. Meanwhile leisure activities will have a lower value.

Project iGenda is based on the idea of helping the user in programming leisure times, upon a collection of events and activities. This is undertaken through an automatic execution and selection of events and their addition to a calendar attributed to each user. The goal of Free Time Manager is to assure that leisure activities are inserted in the free spaces of the user's calendar. This function is quite important since it keeps the user active and connected to other users, helping him keep a social integration. The database will contain data on the different kinds of activities the user enjoys and can perform, either on his own or together with other persons. The Free Time Manager will verify the free space in the user's calendar and, using linear functions of distribution, it will schedule activities in the free spaces. If the activity involves other persons, iGenda will establish the required connection with other users, to assure a compatibility of the scheduled activities.

Decisions are made in real-time or through a questionnaire that will allow the user to evaluate the efficiency of the system. The results will be analyzed to improve the decision methods, by changing the overall preferences. The system also allows the family of the user visualize the user's calendar, to evaluate if the scheduled events are (or not) adequate for the user.

Connectivity and Interfaces

Ordinary use will be assured from a mobile device that the user will always keep with him. This device will have access to all the information available from the server and it will provide information captured from sensors, such as GPS.

The available interfaces are as simple as possible and they are built in accordance with the common rules of use and in a user-friendly way. The user may keep a window open with information (for instance, about recently schedules events or activities) and a supplementary window may be available for sending messages. The mobile device uses an Android operating system [17] and the interface is designed allowing the user to easily interact with the platform. It uses the most of the available services provided by the operative system, in order to diminish the need of supplementary applications. The modules have sophisticated agents available which are able to communicate through the network (LAN, WiFi, 3G). Each service and module transfers a large amount of sensible information, being each service responsible of a different type of information.

Next, it will be presented the services that are inherent to the iGenda, providing the architecture and how they work.

Personal sensor platform

Upon the development of the iGenda, several ideas have emerged to take advantage of its features. This allows an extension of the automatic and intelligent scheduling functions. That was the case of the personal sensor platform (PSP) [18, 19], having as goal mobile monitoring of the user using body sensors. By collecting vital data, it can remotely process it and send the updated information to the user's physician. He then can avail the user's health condition.

The sensors can collect electrocardiogram data, blood pressure, oximetry, among other data. Being these processed in order to aggregate information on the general health condition of the user. Data is then sent to the user's physician for a more detailed analysis. This monitoring function allows the user to be out of hospital, while ensuring the usual monitoring hospitals assure. Physicians will also be more available for real emergency situations, while keeping the required daily control on the user's health condition. They can base their decision on reports of the overall health condition. In this scenario, the interest of iGenda integration is obvious. It ensures the connection maintenance between the physician and the system user. If after a daily report the physician decides to call the user for an appointment, all he got to do is to use the iGenda. The event will be automatically scheduled and the user will be notified. The same could be said in situations when the user is the one willing to schedule the appointment. In this situation, the physician gets a notification of the user's wish, and the scheduling is left up to the physician while allowing him to send a reply.

The processing system will still be able to take some proactive decisions, based in normalized health conditions. For instance, if there is a relevant change in some of the health levels of the user.

Visual fall detection system

The visual fall detection system (VFD) monitors the user in his home [13, 20, 21]. This monitoring is aimed to keep the user safe, by detecting if any falls happen.

Falling is one of the events that usually occur to elderly persons. Due the fragility of the elderly persons falls should be avoided at all costs. The loss of balance and

falling can have neurological or physical origin. Currently there are no means to cure these problems. Therefore, prevention of falling is very difficult. Due to these facts, post-fall help is the best way to aid the person. Due to reduced mobility and disorientation elderly persons struggle to call for help. In extreme cases it may lead to death, as they cannot move, and have to stay in that position until help arrives. Help quite often arrives too late.

Technology has provided g-force sensors and accelerometers, miniaturized so they can be carried by a person. Although they have a high level of accuracy, they have a high amount of false positives.

Currently we can assume that an accurate method is to track the user with cameras. The cameras capture the human silhouette and process the image to verify if it corresponds to a "fallen position". The image capture consists in image blobs that are processed to extract common features that correspond to a human shape.

The continuous image capture and processing provides the system with a viable solution to detect a fall and engage the help system. The help system is the merging between the iGenda and the VFD.

By using the iGenda features the VFD is empowered with features that can directly interact with the user. The interface that iGenda provides is modular. Therefore, the VFD can communicate with the iGenda to ask a question to the user. For instance, if a user falls the system detects it, and it may question the user if he has no injuries. A triage right after the event can prevent further health complications. Also emergency services can be called if the user requires, or there is a lack of response by the user. The emergency operators can connect with the user home and use devices, such as speakers and microphones, to talk with the user.

The cameras available (normal spectrum and thermal spectrum) capture all the environment and have to be placed, at least, one in each division. The placement of the cameras is vital to capture all the events that occur.

User profiling

For the sake of adjusting the system to the needs of the user, it was built a personalized platform that keeps the profile of the user updated. This profile contains private and personal data of the user [22, 23]. The information is used to automatically build a database mirroring the user personality. This allows creating patterns that can help the system to formulate suggestions. The collected data are reviewed by specialists (subject to an obligation of sigil) who insert them in the database. Thereon a model is created, attributing significance values and establishing relations, improving efficiency. The profile also encompasses clinical reports of the user to keep the information available to all services.

This profiling system collects a great variety of data. But the association between data and information is not totally reliable. These operations may sometimes induce mistakes in the system and create unexpected results. To have this situation revised, the technicians must review again all the information. If needed, with the help of the user, it is possible to repair the associations.

A learning system will also collect data about the choices and activities of the user. The system will keep learning what the user does, what his favorite activities are, to be able to efficiently modify the decision algorithms.

2.2 Threats to Privacy and Data Protection

The iGenda project intensely uses personal and private data. Given its nature, the collected data must be reviewed by specialists, becoming a reliable and efficient system. Also the social interaction services may require that information becomes visible to other users. It is possible also that family or caregivers have full access to the system.

Data is processed and analyzed recurring to medical definitions. These support a decision flux that will be translated in an initial medical diagnosis. If there is an emergency situation, the system immediately notifies the Emergency Service and transmits to it the user's vital data and localization data.

The vital data captured by the sensors is then transferred for the main server, in order to be processed. Finally, it is created a clinical chart representing the user health condition that physicians can consult. Through the use of this health report, the system is capable of identifying eventual problems and automatically scheduling an appointment with the user's physician. The system will immediately notify both the patient and the physician of this scheduling.

The data goes through different technical revision, until it is inserted into the system. Authorized personal will be able to make required technical operations.

The possibility of sharing clinical data is also a quite relevant feature. Clinical reports may be shared among different medical entities and organizations. Electronic data files may be shared in projects such as VirtualECare, and then distributed to different hospitals and medical centers.

Concerning other persons involved, data may be shared among various persons of the family and even friends. These persons may be authorized by the user to have different types of access to data. The levels range from viewing, adding and altering events, or to seeing events that the user considers private.

The devices on this project are mainly wireless, flowing over-the-air communications between sender and receiver. Other type of communications, such as GSM, UMTS and WiFi, implies that a third party is involved. As it will be the case of the mobile service provider, that will also have access to the transmitted information.

For a proper functioning of the system it is essential that all the received information is stored. These systems obviously present a permanent risk of loss of privacy and access to data (and even sensible data) of the user by third parties.

3 Technical and Legal Warranties

This application processes vital and personal data and information of the user, making these accessible to third parties and even allowing them to know his precise localization. Thus being, this project intends a serious risk of privacy loss. Concerning this, it

is important to determine which personality spheres (of the user) are to be affected. German Jurisprudence considers not only a public sphere, but also a private and an intimate sphere [24]. Besides this, it was expressly recognized by article 8 of the European Convention on Human Rights the existence of a Fundamental Right to Privacy. Also European Union Chart of Fundamental Rights proclaimed, in its article 7, this same right, clearly intended for the protection of the citizen against illegitimate intrusion either by public authorities or other persons [25]. Besides the issue of privacy, the European Union Chart of Fundamental Rights also proclaimed the existence of a fundamental right to personal data protection [25, 26]. But these rights, although usually considered altogether, may require different approaches. For instance, meanwhile privacy may require prohibitions concerning monitoring or vigilance in certain spaces or situations, data protection may imply other kind of restrictions concerning the collection and processing of data[27] .

It is thus important to determine which legal obligations (and legal protection) arise from the above mentioned. This happens to be a quite delicate issue, since the project intends the collection, storing and transmission of health data, and this kind of data is considered by European law as "sensitive data" and thus requiring a reinforced kind of protection. In this regard, it is important to look at the legal framework and try to understand if (and to what extent) there are any exceptions to this consideration of health data as "sensitive data". Issues such as the distribution of data, monitoring through the use of cameras and sensors, and the construction of user profiles, may indeed become an open door for intrusion in the user's privacy and for the (eventually illegitimate) use of the user's personal data. And it must also be considered that it is not just a question of collecting data, but mainly the possibility of building true knowledge from the use of such data. It becomes possible the transformation of data into information and a connection of such information with context, thus allowing the attribution of meaning to the collected elements.

3.1 Privacy

The right to intimacy and to private life are closely connected to personality and personality rights [12, 28]. Every person has the right to decide by himself alone what and when shall be shared with third persons, thus allowing everyone to have a control on His own life and experiences, concerning the spheres in which it is not allowed an intromission, neither by the State authorities nor by third persons [28]. This is a right intimately connected to personal freedom, to the construction of the identity, to the control everyone should have on the aspects of his identity one intends (or not) to project to the world [25].

This right to privacy is now, due to technological developments, particularly threatened. The technological possibilities of monitoring have increased enormously, especially if we think on the use of RFIDs and other technologies allowing a constant monitoring on what we do and wherever we go [27] and the establishment of connections between persons and objects, thus permitting a constant following of someone. Besides this, the possibilities of data collection and data mining, the building up of user profiles, the use of sensors able to monitor blood pressure, heart beating, body

temperature, facial expression and even the possibility of a constant observation choices, behavior, emotions, making us wonder if persons are still able to live according to autonomous and free options [29]. Besides that, is becomes clear that monitoring brings along a progressive blurring of the distinction between public and private spheres, as well as a danger of Data Vigillance or "Dataveillance" [27]. So, it becomes urgent to remind that intimacy and private life are to be protected, and warranties of confidentiality seek to strengthen two different aspects of intimacy : on one side, a negative aspect of intimacy which excludes from third persons the knowledge of what is own to the individual; on other side a positive aspect of intimacy, assuring a control by the individual on data and information of his own [28].

3.2 Personal Data

Personal data are data relating to an individual person, either identified or identifiable, considered as data holder [12]. Health data are data concerning all aspects, both physical and psychological, of the health condition of a person, as it was referred by the Court of Justice of the European Union on the interpretation of article 8 of Directive 95/46/CE (Process C-101/01, decided on the 6th November 2003). Health data are considered to be sensitive data according to Portuguese and European law and its processing may not be authorized in all situations, unless there is a consent of the holder of the data and additional data security measures are available, such as the logical separation between health data and other personal data (article 15 nr. 3 of the Portuguese Law 67/98).

Under the Portuguese legal system there is a general prohibition of processing personal data. The Portuguese Constitution even prohibits, in its article 35, the use of informatics for the treatment of data concerning the private life of the citizens [30]. On the other side, both the referred Portuguese Law 67/98 and the European Directive 95/46/CE have specified that within the prohibition of processing sensitive data it must be included data concerning non only the private life of the citizens, but also health data, sexual life data and genetic data (Law 67/98 article 7).

However, there is an obvious exception to this general prohibition: it is the case when the holder of the data expressly consents through a free informed will, which in the case of sensitive data must be issued in an express way, without any kind of coercion, and informed in a sense that the holder of the data must be totally aware of the effects arising out of his manifestation of will [12]. Of course, this implies the existence of a right to information, including the right of the data holder to know exactly what data about him are on the files. On the other side, there is a requirement of consent that will not be met if there is just an indication of a vague and generic finality for the use of the data. And of course, the data holder must be able to have a right of control on the data, in the sense that he must have the right to ask for an updating, correction or removal of the data. Last, but not least, the data must be kept correct and accurate, and they must be used in a secure and confidential way and according to the finality invoked for its collection [26]. Every time the invoked finality is modified, it is mandatory to get a new consent of the holder [12].

This requirement of a free and express consent is obviously related with the legal principles of personal data protection: first of all, a principle of transparency, meaning that the person responsible for the data processing must be clearly identified and the data holder must be informed on the finalities of the collection and processing and also on the delays for keeping the data as well as the possibility and conditions of its communication to third parties. Besides that, this principle of transparency also implies the existence of a right of the holder to information and to access to the data.

Every time it will be legally required, the person responsible for the data processing must fulfill some legal obligations, such as register, authorization requirement or notification to the National Commission for Data Protection [12]. But it also mandatory the obligation of conformity with the principle of finality: data can only be used according to the finality invoked for its collection. The goals of the data processing must always be expressly indicated and data can not be used contrarily to the said finality. Thus being, there is no doubt that consent must be unequivocal and informed [27]. And the principles of Data Protection must always be applied [27].

Yet, this finality principle has to be considered in relation to another quite relevant legal principle: the collected data must be only the adequate and needed data, that is to say the necessary data for the indicated purpose and its collection and processing must not go beyond what is really necessary for such finalities to be reached. Thus being, a principle of proportionality must also be respected, assuring a balance between the collected data and the purposes of its collection and processing [12]. On the other side, there is also a recognition that criteria for consideration of a need of data collection must considered objectively and according to the expressly referred finalities.

It must not be forgotten the legal rights of the data holder: first of all, the right to be forgotten and the right to be let alone [12]: data must be preserved only during the time necessary for the prosecution of the finalities of collection and processing. An adequate delay for the conservation of data may have to be established. A perpetual appropriation of various aspects of the private life of the holder of data would certainly be totally unlawful! [31]. Thus being, there authors that refer the need to ensure an informational self-determination [12, 29]. In order to ensure this right, there must be a right of the data holder to access to the data – a right of consultation without any need of substantiation. And of course, the data holder must have a right of rectification and of updating the data. For this right to be exercised, the data holder must be able to verify if the data concerning himself are (or not) correct and updated. And, as it was already referred, data must not be kept beyond the necessary delay.

An exception to the requirement of free and informed consent occurs when the data holder is temporarily unable to express consent (for instance, because he is in coma or totally unconscious) and, yet, the data collection or processing is absolutely essential in order to protect a vital interest of the data holder. This could well be the case of monitoring persons in coma or in intensive care units [12].

Another important exception is the treatment of medical data for purposes of preventive medical actions, medical diagnosis, medical care and treatment, provided on one side that these actions are undertaken by a physician or health professional and that these professionals are subject to an obligation of secrecy and on the other side

that the National Data Protection Commission is notified and all warranties for the security of information are observed [12].

The Portuguese National Data Protection Commission has even stated that telemedicine actions are to be considered as medical data processing for the purposes of the Law, thus opening a window for the possibilities of telemedicine intervention, provided that the above referred requirements are observed. Anyway, this treatment of data will only be admitted if it is undertaken by a health professional or other professional subject to the obligation of secrecy. Data relating to health condition, sexual life or genetic data must be logically separated from other personal data [12].

But even considering that the collection and processing of such data may be not only admitted but even highly beneficial for the data holder, it must never be forgotten the obligation of observing the fundamental principles of data protection: the finalities of data collection must be known in advance, and it must also be lawful and legitimate, and the use of such data must respect the referred purposes.

Some difficulties may yet arise out of the consideration of the fundamental rights of the data holder, especially concerning the right to be forgotten and the right to be let alone. This means that data must only be preserved while it is absolutely needed for the purposes of data collection and treatment. For instance, in Portugal, the Data Protection National Commission will establish the delays under which data may be lawfully used according to said finalities. In the end of the established delay, data must be deleted, in order to warrant the right to be forgotten. Another aspect refers to the right of the data holder to data deletion or, at least, to a blockage of the access to the data, when these are not updated or are kept beyond the established delay. Furthermore, the data holder must always be informed about the presence of tags and readers, about the purposes under which data is lawfully collected and processed, about who is the person responsible for the data treatment, and whether or not data will become (and under what conditions) available to third parties [27]. Last, but not least, the data holder has a right of opposition – he may oppose to the collection and processing of his personal data, based upon legitimate reasons [12].

Thus being said, in accordance to the Directive 95/46/CE important requirements related to the quality of data are referred and data must be:

- Processed in a loyal and lawful way ;
- Collected for legitimate and expressly specified purposes, and never in any way incompatible with such purposes;
- Data must be adequate, relevant and not excessive, having in consideration the purposes of its collection and treatment;
- Data must be accurate, correct and updated; all reasonable steps must be taken in order to warrant that incorrect or incomplete data, having in consideration the purposes of collection and processing, must be corrected or deleted;
- Data must be kept in such a way that it will allow the identification of the data holder only during the time needed for the purposes that were intended for the data collection and processing.

In data protection domain, a main concern will be to ensure that the data holder has a control on his own data. In order for this to be achieved, both law and technology

have important roles. Particularly relevant will be the so called Transparency Enhancing Technologies [27], as instruments capable of helping in the fulfillment of the requirements of informational self-determination.

The main issue is the consideration of systems oriented to persons using sensitive information about the data holder. It is important to ensure that these services are not simply considered as illegal and thus prohibited, based on a too rigid application of legal principles and of the human rights, without considering other fundamental rights such as the right to health care. The important thing is unquestionably the protection of the data holder and of the data flowing within the system, in a way allowing the data holder to benefit from the available services and, at the same time, having all warranties of being always his fundamental rights legally protected.

4 Conclusions and Challenges

Health care services require that personal data and even sensitive data are stocked within information systems, and then made available to physicians and paramedical professionals and even to other persons, such as the user's family or friends. In the Portuguese legal system, processing health data may be admitted whenever necessary for preventive care, diagnosis, and medical treatment, whenever these services are provided by a physician or other healthcare professional subject to obligations of secrecy.

In this context, telemedicine operations may well be admitted, being this an open window for taking advantage of the benefits offered by the new methods of medical intervention, provided that the legal requirements are observed. In the project herein referred, there are possibilities of having to use monitoring and profiling in accordance with the legal requirements. It will be mandatory, however, to constantly focus upon the fundamental rights of the holder of data in a perspective of a fully warranty of the exercise of the right to informational self-determination. Having this in mind, a permanent cooperation and participation of the user is required, with the only admissible exception of cases when the user is not in conditions of giving his free and informed consent (for instance, due to being in coma or unconscious) and the collection and processing of the data becomes absolutely necessary for protecting the vital interests of the user.

Although it is admissible that these systems may respect legal requirements concerning the rights and warranties of the data holder, it must nevertheless be recognized that there are permanent risks of Dataveillance [32]. On the other side, we must distinguish between requirements concerning privacy and requirements concerning data protection, between warranties of opacity and warranties of transparency [27].

Thus being, it becomes important to understand that it is not enough to have a legal affirmation of rights. It is also quite important to ensure the effectiveness of the rights. On this respect, we must recognize an important role that may be played by technology itself, mainly privacy enhancing technologies and transparency enhancing technologies[27].

It will thus be quite interesting to point out that on one side technology brings along innumerous and quite serious threats to the human rights to privacy and data protection. But, on the other side, we may wonder whether technology may be also considered as an important part of the solution for the innumerous problems it creates, while enhancing technological uses in compliance with the legal requirements of privacy and data protection [33].

Acknowledgments

This work is partially funded by National Funds through the FCT - Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) within projects PEst-OE/EEI/UI0752/2011, PEst-C/CTM/LA0025/2011 and AAL4ALL QREN 13852.

References

1. Nations, U.: World Population Ageing 1950-2050 (Population Studies Series). United Nations (2002).
2. Chisholm, D., Evans, D.B.: Economic evaluation in health: saving money or improving care? Journal of Medical Economics. 10, 325–337 (2007).
3. Charness, N.: Aging and human performance. Human Factors The Journal of the Human Factors and Ergonomics Society. 50, 548–555 (2008).
4. Department of Health: NHS inpatient elective admission events and outpatient referrals and attendances. (2011).
5. Ball, M., Lillis, J.: E-health: transforming the physician/patient relationship. International Journal of Medical Informatics. 61, 1–10 (2001).
6. Costa, A., Novais, P., Corchado, J.M., Neves, J., Costa, Â.: Increased performance and better patient attendance in an hospital with the use of smart agendas. Logic Journal of IGPL. (2011).
7. Jones, P., Marsh, D.: The Essentials of EDI Law. Blackwell Publishers (1994).
8. Costa, Â., Castillo, J.C., Novais, P., Fernández-Caballero, A., Simoes, R.: Sensor-driven agenda for intelligent home care of the elderly. Expert Systems with Applications. 39, 12192–12204 (2012).
9. Mohs, R.C.: How Human Memory Works, http://health.howstuffworks.com/human-memory.htm/printable.
10. Craik, F.I.M., Winocur, G., Palmer, H., Binns, M.A., Edwards, M., Bridges, K., Glazer, P., Chavannes, R., Stuss, D.T.: Cognitive rehabilitation in the elderly: effects on memory. (2007).
11. Barker, A., Jones, R., Jennison, C.: A prevalence study of age-associated memory impairment. The British Journal of Psychiatry. 167, 642–648 (1995).
12. Castro, C.S. e: Direito da Informática – Privacidade e Dados Pessoais. Almedina (2005).
13. Costa, Â., Castillo, J.C., Novais, P., Fernández-Caballero, A., Simoes, R.: Sensor-driven agenda for intelligent home care of the elderly. Expert Systems with Applications. 39, 12192–12204 (2012).
14. Costa, Â., Novais, P.: An Intelligent Multi-Agent Memory Assistant. In: Bos, L., Dumay, A., Goldschmidt, L., Verhenneman, G., and Yogesan, K. (eds.) Handbook of Digital Homecare - Successes and Failures. pp. 197–221. Springer (2011).

15. Gawinecki, M., Frackowiak, G.: Multi-Agent Systems with JADE: A Guide with Extensive Study. IEEE Distributed Systems Online. 9, 4–4 (2008).
16. Bellifemine, F.L., Caire, G., Greenwood, D.: Developing Multi-Agent Systems with JADE. Wiley (2007).
17. Yu, J., Liu, M.: Secondary Development on Android Intelligence Mobile Phone Platform. Management and Service Science MASS 2010 International Conference on. pp. 1–4. IEEE (2010).
18. Costa, Â., Novais, P.: Mobile Sensor Systems on Outpatients. International Journal of Artificial Intelligence. 8, 252–268 (2012).
19. Costa, Â., Barbosa, G., Melo, T., Novais, P.: Using Mobile Systems to Monitor an Ambulatory Patient. International Symposium on Distributed Computing and Artificial Intelligence (DCAI'11) Salamanca. pp. 337–344. Springer (2011).
20. Montotya, J.C.C., Serrano-Cuerda, J., Sokolova, M.V., Fernández-Caballero, A., Costa, Â., Novais, P.: Multispectrum Video for Proactive Response in Intelligent Environments. The 8th International Conference on Intelligent Environments, IE'12 (2012).
21. Costa, Â., Montotya, J.C.C., Novais, P., Fernández-Caballero, A., Bonal, M.T.L.: Sensor-Driven Intelligent Ambient Agenda. In: Novais, P., Hallenborg, K., Tapia, D.I., and Rodríguez, J.M.C. (eds.) Ambient Intelligence - Software and Applications. pp. 19–26. Springer Berlin / Heidelberg (2012).
22. Marques, V., Costa, A., Novais, P.: A dynamic user profiling technique in a AmI environment. 2011 World Congress on Information and Communication Technologies. pp. 1247–1252. IEEE (2011).
23. Schiaffino, S., Amandi, A.: Intelligent User Profiling. Artificial Intelligence. 9, 193–216 (2009).
24. Farinho, D.M.S.: Intimidade da Vida Privada e Media no Ciberespaço. Almedina (2006).
25. Rouvroy, A.: Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. Studies in Ethics, Law, and Technology. pp. 1–51. Berkeley Electronic Press (2008).
26. Miguel, C.R.: El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea. Temas de Direito e Informática e da Internet. pp. 17–71. Coimbra Editora (2004).
27. Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., González Fuster, G.: Legal safeguards for privacy and data protection in ambient intelligence. Personal and Ubiquitous Computing. 13, 435–444 (2008).
28. Janeiro, D.B.: La protección de datos de character personal en el derecho comunitario. Estudos de Direito da Comunicação. p. 305. Almedina (2002).
29. Rouvroy, A., Poullet, Y.: The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. Reinventing Data Protection. pp. 45–76. Springer (2009).
30. Marques, G., Martins, L.: Direito da Informática. Almedina (2006).
31. Cueva, P.L.M. de la: Informática y Protección de Datos Personales. Cuadernos y Debates, Nº 43. p. 193. Centro de Estudios Constitucionales (1993).
32. Clarke, R.: Information technology and dataveillance. Communications of the ACM. 31, 498–512 (1988).
33. Winn, J.K.: Technical Standards as Data Protection Regulations. In: Gutwirth, S., Poullet, Y., Hert, P., Terwangne, C., and Nouwt, S. (eds.) Reinventing Data Protection? pp. 191–206. Springer Netherlands, Dordrecht (2009).