A Personalised Integrated Care Platform

(Grant Agreement No. 689209)

D3.4 Ethical Analysis of Monitoring and Privacy Impact Assessment

Date: 01-10-2018

Version 1.0

Published by the PICASO Consortium

Dissemination Level: Public

Co-funded by the European Union's Horizon 2020 Framework Programme for Research and Innovation under Grant Agreement No 689209

Document control page

Document file: D3.4 Ethical Analysis of Monitoring and Privacy Impact Assessment.docx
Document version: 1.0
Document owner: IN-JET

Work package: WP3 – Integrated Care Models, Multi-morbidities, and Privacy
Task: T3.3 – Ethical Analysis and Privacy Impact Assessment
Deliverable type: [R]

Document status: ☒ approved by the document owner for internal review
☒ approved for submission to the EC

Document history:

Version	Author(s)	Date	Summary of changes made
0.1	Trine F. Sørensen (IN-JET)	31-07-2018	ToC
0.2	Trine F. Sørensen (IN-JET)	19-09-2018	Section 2
0.3	Paul Quinn (VUB)	25-09-2018	Section 3
0.4	Trine F. Sørensen (IN-JET)	26-09-2018	Final editing, summary, introduction and conclusion. Ready for internal review.
0.5	Trine F. Sørensen (IN-JET)	01-10-2018	Review comments considered
1.0	Trine F. Sørensen (IN-JET)	01-10-2018	Final version submitted to the European Commission

Internal review history:

Reviewed by	Date	Summary of comments
Agostino Chiaravalloti (UTV)	28-09-2018	Minor comments.
Armanas Povilionis (INUIT)	01-10-2018	Minor comments and corrections.

Index:

1 Executive Summary

This deliverable first of all presents an ethical analysis of surveillance and monitoring, first from a general perspective and next focused on the healthcare and PICASO context. The ethics of surveillance raises a number of issues but in this deliverable, we will focus on stigmatisation and human dignity. Both issues are extremely important in the context of healthcare in general and with specific focus on the patient, notably a chronic patient, in particular. Surveillance, monitoring, stigmatisation and human dignity cannot be separated from a discussion on privacy and protection of personal data, especially as the digitalisation of societies, and of healthcare, increases and spreads.

The ethical analysis is followed by a data and privacy impact assessment. The requirements of the GDPR (General Data Protection Regulation) have assessed and related to 'PICASO as a research project'. These requirements have been grouped into five:

- The need to conduct an Impact Assessment
    - Several deliverables are considered to jointly fulfil the needs of such an assessment
- The need to identify data controllers and data processors
    - The hospital partners in the project are the data controllers and other partners are the data processors. A data protection agreement has been made between the parties
- The need to comply with data protection principles as outlines in the GDPR
    - The principles are explained and related to concrete actions implemented in PICASO
- The need to ensure that consent meets the standards of the GDPR
    - The consent forms used in the PICASO trials have been checked by the DPOs of the hospital partners, the ethics bodies of each hospital and VUB (in its role on the PICASO Ethical Board).
- The need to facilitate data subject rights
    - The main rights and their associated requirements for PICASO, e.g. specifying required information that must be relayed to the patient when obtaining informed consent (see also D3.3).

This deliverable will therefore provide the reader (including project partners) with a good understanding of the PICASO project's ethical and legal requirements towards the data subject and how these requirements have been fulfilled in the project.

2 Introduction

The PICASO project provides an ICT platform, which supports a better coordination of care plans for people with multimorbidities. One of the project's ambitions is to facilitate patients to actively participate in their own care based on monitoring physiological parameters at home and sharing the data with formal and informal carers using PICASO. Patients will thus be closely monitored during the PICASO trials and while only non-intrusive technologies (i.e. the devices used induce minimal impact on the patient and his/her mobility), the notion of monitoring, the perception and real experiences of being monitored pose some complex and interesting questions from both an ethical and legal point of view.

This deliverable is part of task T3.3 Ethical Analysis and Privacy Impact Assessment. It consists of two main parts. The first part of this deliverable will analyse the use of monitoring techniques from an ethical perspective with focus on stereotyping and stigmatisation. The second part looks at the legal requirements related to privacy and data protection in the form of an impact assessment of the project.

2.1 Purpose, context and scope of this deliverable

The ethical analysis will be related to the PICASO home-monitoring solutions used by the patients in the two trials to monitored selected health parameters: 1) blood pressure, weight and activity (steps per day) are measured and monitored using the provided devices and the PICASO App for transferring data to the clinic, 2) Well-being and medication adherence are monitored with the use of questionnaires patients have to answer directly in the PICASO Patient Dashboard.

The analysis will help to understand why it is important to consider the ethical aspects of using surveillance and monitoring technologies in a healthcare context and how the project has approached these issues. The concept of (human) dignity will be also be analysed as it is central to our understanding of privacy and data protection and the threats to these in a digital age. There is a clear link between the analysis and the Ethical Guideline and Principles in the project, and the forthcoming empirical research into patient empowerment in the PICASO context will provide deeper reflection on some of the issues discussed in this deliverable.

Please note that at the time of submission of this deliverable, the trials are still in very early stages and empirical experience and knowledge gained through the trials is thus limited. We therefore refer the reader to forthcoming deliverables which will also document PICASO specific data on the ethical challenges and issues experienced in the trials (directly or indirectly):

- ID3.8 Annual Compliance Monitoring Report 2 (M38)
- D3.6 Practical Implementation of Patient Empowerment and Joint Care (M36)
- D8.9 Third Annual Trial Progress and Ethical Report (M41).

The second part of the deliverable analyses the main privacy and data protection requirements as they apply to the project. It draws on the earlier analysis is in D3.5 but is presented in a summarised way and highlights concrete actions and/or implementations to be taken in and by the project, focusing on the patient (the data subject) with specific rights as endorsed by the GDPR.

2.2 Intellectual Property (IP)

This work may be cited by reference.

2.3 Content and structure of this deliverable

Section Three presents an ethical analysis of surveillance and monitoring, first from a general perspective and context, and secondly in the healthcare and particularly PICASO context. Section Four represents the privacy impact assessment of PICASO, focusing particularly on providing a good overview of the legal requirements related to the processing of personal data in 'PICASO as a research project'. Section Five sums up the concluding remarks on how to use this deliverable and on the continuing work related to ethics in the project.

3 The ethics of health monitoring and surveillance

Surveillance is targeted observation, tracking and monitoring with a clear purpose and the ethical complexity of surveillance has only increased with the technological developments allowing surveillance to go far beyond traditional CCTV installations.

The discussion of surveillance from an ethical perspective is very valuable as it contributes to understanding that surveillance is not a value-free and objective practice. It also makes it clear that surveillance should be placed in context, i.e. considering how surveillance is used, by whom, and why. The ethical dilemma of surveillance and health monitoring is rooted in the consoling the perceived benefits with the perceived harms; it is rooted in the generally accepted notion that surveillance in itself is not necessarily bad, but it is how and why it is used that must be questioned. The overall threat of surveillance is related to privacy, or more precisely the intrusion on and threat to privacy. How one can ensure that monitoring and surveillance technologies do not violate the individual's right to privacy or in any way endangers the protection of personal data? What impact on the individual's personal life will the technology have? These and other questions on surveillance and privacy also highlights that issues of stigmatisation, dignity and autonomy are important to consider in an ethical discussion and analysis.

The following sections will take a closer look of the above issues, relating them to the healthcare context in general and the PICASO context in particular.

3.1 Surveillance – an ethical dilemma

The ethical dilemma of surveillance is rooted in a general notion that surveillance in itself is not necessarily bad. The ethical discussion of surveillance is nevertheless very valuable as it has contributed to understanding that surveillance is not a value-free and objective practice; stereotyping, stigmatisation and prejudice are deeply embedded in the many surveillance practices which in turn has an effect on notions of privacy and autonomy, trust and power.[1]

Power and power structures are ingrained in the use of surveillance. There is a great dichotomy between the surveillant and the surveilled; a dichotomy that illustrates the power relationship between the two. Surveillance is targeted observation, tracking and monitoring with a clear purpose, but today (much due to technological advances) there is also a strong element of counter surveillance – "Who is watching us?"

We can easily find example of this counter surveillance, or sousveillance as it has also been phrased, in relation to traditional use of public surveillance and CCTV (so in non-health related scenarios). The boundary between who is watching and who is being watched have become more blurred.[2] In essence, sousveillance means bringing means of surveillance down to human level, either physically or hierarchically, and both sousveillance and traditional surveillance have become normal practices in most societies today.

This discussion on sousveillance is not easily transferred to the healthcare context. But let's consider that patients share self-monitoring data with their physician. Thanks to technology – such as those offered by PICASO – the patient can at any time point to specific data values and question why the physician did not react (in time) to the data. Consider the scenario where a self-monitoring service has been implemented with a chronic patient with the objective of improving the (remote) monitoring of vital health parameters. The patient is continuously sending the data to the physician, in the expectation that any abnormal data will immediately be caught by the physician who will then activate the appropriate action. This could be a change in medication, a face-to-face consultation, or even an emergency hospitalisation. If such action was not taken in due time resulting in serious consequences for the patient's health, the patient would now have a digital record to illustrate where action should have been taken, thus holding the physician responsible and liable for medical negligence or even malpractice. It is not conventional sousveillance as a countermeasure to CCTV practices;

[1] This is of course most evident in the predominant use of surveillance, CCTV, as a means to improve public safety and security. Most people may think of this in the context of police work, of crime prevention and in solving crime; CCTV is a powerful source of evidence. But public surveillance, not in the form of CCTV, is also a very important measure in the context of public health. As in the crime context, public health surveillance is used as a preventative measure; to prevent the spread of epidemics which of course can only be done if we know of outbreaks – a knowledge based on data from public health surveillance. Both types of surveillance are justified as being done for the public good. This, however, does not make it value-free or without consequences or ethical problems.

[2] In the context of sousveillance, the power relation is less rigid as mobile phones with built-in cameras are widespread allowing the public to record events as they happen: "In an inversion of the usual relationship between watcher and watched, these [phones with built-in cameras] are increasingly being used to hold the powerful to account – witness their role in the Arab revolutions, and in cases of police misbehaviour in the USA and UK. The output of this sousveillance by members of the public can be distributed using the Internet, to form a synopticon, in which the many watch the few." (Moran, 2015).

patients are not subjecting their physician to surveillance by capturing their actions on camera, but by having a digital record of the health data they have shared with their physicians, patients are now able to pinpoint exactly where the physician should have reacted.

The question of "Who is watching us?" is therefore very relevant in relation to home and self-monitoring services as part of the provided healthcare services. It put enormous pressure on physicians and it raises all kinds of liability issues, and if the shared health data is not assessed by the physician in time it threatens the very practise of self-monitoring.

3.1.1 Surveillance and Who is watching us - The PICASO context

As indicated above already, there are potential negative effects of surveillance and surveillance is not value-free or objective. It raises several ethical issues and when applying surveillance technologies in the context of health and healthcare it is important to be aware and understand these ethical issues. Only by understanding what is at stake can we take the necessary precautions to minimise any negative or damaging effects on the people subjected to monitoring and surveillance.

The use of surveillance and monitoring technologies in PICASO, primarily in the home-monitoring solution PICASO offers, are of course not value-free and therefore also depend on a careful consideration of the ethical implications and how to best overcome these. The home-monitoring feature of PICASO has two aspects: 1) external monitoring i.e. the formal/informal carer monitoring the patient's health related parameters and medication intake and hence (in)directly monitoring patient adherence to his/her care plan, 2) and internal monitoring i.e. the patients is monitoring him/herself. While it is clearer that there are some ethical concerns related to the former, especially as this type of monitoring is also most similar to the overall use and purpose of surveillance and has a clear division between the observer and the observed (with clear power structures embedded), it is probably less so with respect to the latter.

However, there are still some ethical issues to consider in the context of self-monitoring. For example, when self-monitoring health related parameters the patient will always face the dilemma of whether or not to share the data. With a solution like PICASO, the patient is supposed to submit x number of data (measurements) in accordance with the pre-scribed care plan. The patient has to actively submit (send) data, thus retraining control of whether or not to share data. However, the minute the patient does not send data, he/she will be questioned as to why that is. So, there will always be an element of external monitoring. Moreover, the patient may find him/herself in a personal (ethical) dilemma of whether or not to send the data; it could be that the data does not live up to expectation, e.g. activity level is less than agreed/recommended by the carer. The patient can choose not to share this data and then risk being questioned as to why, or send it and risk being "scolded" for not following or living up to the set target (recommendation/care plan). Either way, there is always a risk that a negative reaction (external or internal) and/or of a feeling of intrusion (into one's privacy). On the other hand, a "bad" result could be used positively to motivate the patient to do better, thereby ultimately also improving how the condition is managed and health improved. The point is that it is necessary to be aware of these complex issues and potential ethical problems, and not to think that fulfilling legal requirements (e.g. the patient has consented to be monitored) does not mean that a solution or service is home-free from an ethical point of view.

Therefore, we also need to consider that although all end-users in PICASO will have given their informed consent to be monitored it is only when they have been subjected to it for a while that they can truly understand what kind of impact it has on their lives, as well as on their perceptions and attitudes towards being monitored. People may imagine how they will feel about being monitored but the real experience of being monitored may be different (negatively or positively). In particularly, the behavioural and home environment surveillance and monitoring may cause end-users to feel that their privacy has been invaded. Consent must not be considered a "holy grail" that absolves us from any responsibility towards the patients or other users whose personal data is being collected and processed. That responsibility includes taking all precautionary measures to minimise potential harms and maximise potential benefits to patients. It also includes making sure that the actual process of collecting consent is conducted in an ethically sound manner. For this reason, the PICASO Ethical Guidelines includes the principle of beneficence and has described that ideal process for collecting informed consent from patients and other external users in the trials.

Moreover, although patients were given detailed information about the trials and have given their consent, any concerns expressed by patients or their informal carers at any time during the trial must therefore be taken seriously; the patient may wish to have the data protection and security measures explained and demonstrated, or the patient may wish to withdraw from the trial. All concerns and actions taken to alleviate and solve the issue will be documented in annual compliance monitoring report. It will also be described for

the evaluation report. At the time of writing, no concerns about invasion of privacy or data protection have been raised.

The question of "Who is watching us?" was considered in the design and protocols of the PICASO trials; it was made explicitly clear to patients in the trials that the health data that they share with the trial clinicians would not be monitored 24/7, nor did the trial itself replace any existing care plans or appointments. Nevertheless, the project was acutely aware of this issue and a technical user requirement was thus precisely to allow the system to only flag data that falls outside the predetermined parameters; clinicians are interested in abnormal data and it will be much easier for them to get an overview of the patient's health status if they can focus only on such abnormal data. In effect, the care would become more efficient and effective, also decreasing the clinician's workload.

Looking ahead, the possibility to flag abnormal data is a useful functionality in PICASO but healthcare providers would still need to have precise protocols in place for how flagged data will be handled, and patients would have to be carefully informed about these protocols. It could be that the patient notified him or herself of abnormal data and instructed to seek medical advice. The instructions accompanying the blood pressure device used in PICASO contains such advice as the device itself is able to indicate irregular data. For patients to be aware of this advice they would probably have to consult the instructions at the time. In contrast, PICASO could push a message or notification directly to the patient. There are concerns, however, that by notifying patients of abnormal or irregular measurements there is a risk to unnecessarily worry and stress them.

Considering the chronic disease of the patients involved in the UTV trial, the trial owners expressed deep concern of the potential risks associated with giving the trial patients access to historical blood pressure measurement data in the Patient Dashboard. Hence, the historical overview (graphs and tables) in the Patient Dashboard is not accessible.

In this case, the concern was only related to access to the historical data, not to notifications. There were concerns that seeing fluctuations, which would likely be harmless and normal fluctuations, would cause anxiety and fear in the patients. Patients are of course still able to keep a manual record of their measurements thereby granting themselves access to their historical data as noted down by themselves. So, it is a matter of directly providing them with the historical data and thereby being a force factor in triggering anxiety. Again, it is a case of weighing possible benefits against possible harms, and there are several questions that begs consideration: Should patients at least not have the option to choose for themselves if they want to see historical data? Is there a risk that if patients choose to write down the data themselves that they make mistakes, an unnecessary risk as PICASO actually allows for automatically capturing data directly from the device? Would perhaps the possibility to see a historical overview help the patient to understand that fluctuations are inevitable thereby diminishing the overall anxiety concerning fluctuations? Are patients empowered if they are denied access to historical data? Are they denied a basic right if they are denied access to historical data? Is the clinician providing appropriate care of the patient's health if they knowingly give access to data that risk making the patient anxious? These and other questions will be considered in the forthcoming deliverables based on empirical knowledge from the trials (we will be able to compare feedback from patients in the two trial as the UDUS trial does allow access to historical data in the Patient Dashboard).

3.2 Stigma and stigmatisation

An important issue to consider in the context of surveillance – whether used in the context of crime or epidemics – is that of stereotyping and stigmatisation. In the context of surveillance, especially targeted surveillance, the concepts of stereotypes and stigma may be reinforced. The extent to which surveillance practices are if not controlled by then at least a reflection of dominant notions of stereotypes, stigmas and prejudices is linked to the context of use and also the purpose of the surveillance.

The notion of stigma as a sociological phenomenon owes much to Émile Durkheim and Erving Goffman. They have contributed to the understanding of stigma as a social construct and a social fact used to identify and devalue "others". Goffman (1963) defined stigma as an attribute, behaviour or reputation, and he described three types of stigma:

- associated with physical deformities
- weakness or character deficiencies
- belonging to different social groups (ethnic, religious or racial).

Stigma and stigmatization have received interest in several disciplines which tend to agree that stigmatisation is rooted in a perceived threat, whether individual, social, economic, cultural, moral, or physical (see Stangor

& Crandall 2000). Stigmatisation can occur when, for example, (1) there appears to be a perceived threat that might entail loss of power or economic disadvantage or (2) a norm deviance is constructed, which is then perceived as a threat for social order and hegemony (see Phelan et al., 2008).

Goffman (1963) has shown how the (unwanted) characteristic that stigmatises a person or group tends to overshadow all other characteristics, thus giving it a defining power. However, Goffman argued that it is not the characteristic itself that is stigmatising, but the context in which it is attributed a negative meaning: "*The term stigma, then, will be used to refer to an attribute that is deeply discrediting, but it should be seen that a language of relationships, not attributes, is really needed. An attribute that stigmatizes one type of possessor can confirm the usualness of another, and therefore is neither creditable nor discreditable as a thing in itself*. (Goffman, 1963:13). Understanding stereotyping and stigmatising as embedded in social structures and therefore as a part of their social context is crucial; the underlying power structures cannot be ignored and it becomes possible to see how (and why) stereotypes can be constructed and deconstructed.

The practice of surveillance, especially targeted surveillance, may reinforce concepts of – and reinforcements of – stereotypes and stigma. The extent to which surveillance practices are if not controlled by then at least a reflection of dominant notions of stereotypes, stigmas and prejudices or discrimination is linked to the context of use and also the purpose of the surveillance.

In the context of health, stereotyping and stigmatisation is most evident in cases of public health surveillance used to e.g. discover and monitor epidemic outbreaks, to map disease, target intervention, and determine patterns. While effective and ethical surveillance of public health is an important tool for monitoring and containing an epidemic, it also risks stigmatising entire groups of people or communities. The risk of stigmatisation, and its level of severity, will depend on the context, on the type of disease pandemic. Diseases with severe risk and levels of stigmatisation which were evident on a global would include HIV/AIDS, Ebola, and SARS. A non-virus example would be obesity. The public surveillance of the diseases mentioned here have caused it sufferers to be stigmatised, discriminated against, excluded and to be violently attacked.

The above examples have been used to highlight the most severe risks associated with public health surveillance and monitoring and to emphasise that ethics and ethical frameworks are essential, including for how to publicly disseminate public health surveillance data in the attempt to contain and prevent the spread of disease. Moving from a community and global context to a more individual context, the use of personal health monitoring technologies represent another example of surveillance and monitoring. It is also more closely related to PICASO and the following section will analyse the ethical aspects of monitoring as used in PICASO.

Moving beyond public health monitoring, surveillance technology is also central to the concept of eHealth and m-health. For example, surveillance technologies support and facilitate public health monitoring, home-hospitalisation, self-management, and home-monitoring. The use of surveillance technology for monitoring health, whether that of an individual or "the public" as a whole, rely on the transmittance of personal medical data and on a certain degree of surveillance of individuals.

Surveillance technology allows chronically ill people to monitor important health parameters, thereby facilitating a better self-management of their condition, potentially reducing or minimising complications that require hospitalisation. It may simply also reduce the number of visits to either the GP or a specialist because a health parameter is measured and monitored at home, thereby also giving the patient more autonomy, independence and flexibility in living with their condition as life become less controlled by (organised around) "a doctor's appointment".

With respect to stigma and the stigmatisation of patients, the contribution and quote from Goffman above still apply; the context of use of personal health monitoring technologies will affect how the individual using or wearing such technologies is perceived by others. Take the simple activity tracker such as Fitbit which is used by patients in the PICASO trials. When used by a healthy sportive active person, it will hardly have any negative stigmatising risk; it is used to measure performance in an already well-performing person. However, when used by a chronically ill patient who must be more active as part of managing their chronic condition, the focus may initially be more on the passiveness of the person (you are not active enough) and on the fact that activity is tracked to prevent their condition to deteriorate or to manage it, rather than to measure high performance levels. The difference is fundamental; the first example is used on the (more than average) healthy and active person, it is a self-motivated choice spurred by ambition and for the self-imposed monitoring of that ambition. The second example is used on the (more than average, in the meaning of "chronically") ill and less active person, it has been prescribed by doctors spurred by deterioration of health, by the chronic condition suffered, and to motivate (and help) the person to take more responsibility for their own health and physical activity. This dichotomy in itself reinforces the stereotyping it exemplifies.

Design and standardisation can also have a stigmatising effect notably in relation to frail, disabled, senior citizens and people with low e-skills. Mainstream design generally excludes *per se* this group of users. Vision and hearing impairment, physical limitations (e.g., arthritis) and complexity automatically excludes a large percentage of this group from using the technology. On the other hand, special design, particularly if the aesthetic aspect is neglected, may have a stigmatising effect because it signals that the user has some form of disability or low ICT skills (SENIOR 2008a).

3.2.1 Stigma and personal health monitoring – The PICASO context

The PICASO Patient Self-monitoring Platform integrates three types of monitoring schemes – scheduled vital signs measurements with medical devices, continuous activity and behaviour monitoring using wearable sensors and patient self-assessment using established clinical questionnaires. The Patient Self-monitoring framework ensures that all patient measurements are transferred in secure way into the designated storage facility. This helps patients and clinicians to establish a complete view of the patient health status compared with existing solutions that only supports one of these three monitoring schemes. It also allows care organisations to take advantage of standardised off-the-self products for health to improve therapy of patients with multi-morbidities.

From an ethical perspective, PICASO have taken the necessary precautions to avoid that the surveillance used in the project reinforces negative stereotyping and stigmatising. The devices used in PICASO are therefore standard off-the shelf devices. This means that we avoid using special design that can label and stigmatise. PICASO includes one wearable device, the Fitbit, and while its design does not signal special needs it is of course clear that to really understand the signal this wearable device transmits one must look at the wearer and the context. Hence, there is a risk that PICASO users feel different, feel labelled, feel stigmatised as their physical appearance and condition can indicate that the use of Fitbit is in a health rather than an exercise context. On the other hand, precisely because of their condition, users may feel that the Fitbit reinforces a positive message; that they are actively engaged in their health and in managing their condition. As such, there is a possibility that it can help to reinforce a positive feeling of being more in control and empowered. Notions of empowerment will be investigated in detail in a forthcoming deliverable *D3.6 Practical Implementation of Patient Empowerment and Joint Care* and it will here be interesting to analyse the effect of using wearables on experiences of empowerment and stigmatisation.

3.3 Dignity

The very first article in the Charter of Fundamental Rights of the European Union (2000/C 364/01) concerns human dignity: "*Human dignity is inviolable. It must be respected and protected.*" However, the meaning of dignity remains complex because it is a multidimensional concept; human dignity is at risk when any one of its dimensions is threatened or violated. Overall, human dignity is closely related to the human right to privacy and protection of personal data. A right, and issue, which has become even more important and pressing in the digital society of today and the future. The GDPR is a clear example of the pressing need to ensure that right.

The principle of dignity affirms that any human being is priceless, literally invaluable, independent of their age, gender, socio-economic condition, ethnicity, religion, etc. According to the Charter, dignity includes i) the right to life and ii) the right to the integrity of the person, which also implies the right to the free and informed consent of the person concerned. These two aspects are very relevant in the context of healthcare and healthcare technologies. First of all, healthcare technologies (including assisted living technologies) may offer a way to improve the quality of life for chronic patients and enable them to live better and longer as technology can help them to manage their condition. Secondly, the right to the integrity means that an individual's physical and psychological conditions should be respected and no one has the right to infringe upon them without explicit and informed permission. This principle of dignity is vital and reminds us that the implementation of healthcare and assisted living technologies should always consider the needs and capabilities of the patient.

In this respect, it is vital that patients, as end-users, are properly consulted so that their needs and requirements are met; so that solutions become individualised. In addition, the end-user should be able to control the system or the devices in some way to prevent a complete erosion of autonomy and privacy. This includes the option of opting completely out (at any time) in relation to the use of healthcare technologies. It is important though to ensure that the end-user really understands what the technology offers, its risks and benefits as this is a prerequisite for an informed choice, and for informed consent. Involving the end-user to identify the needs and requirements of an ICT based system or service is a first step in the right direction.

With specific reference to e-inclusion and ageing, the Communication on Ageing well in the Information Society stated: "*Solutions can only bring benefits if users have access to basic ICT facilities, have the appropriate education and motivation, and ethical and psychological issues are properly addressed. There is no specific reference point for ethics in ICT for ageing, for example, in safeguarding human dignity and autonomy where solutions require a degree of monitoring and intervention*." (EC 2007).

The notion of Inclusion was included in PICASO's ethical guidelines and checklist with specific reference to "ease of use" and "usability" of ICT-based solutions that are aimed at frail and/or senior citizens. More precisely, what is at stake here is the notion of e-inclusion and e-literacy or digital literacy. This includes access to appropriate training, user-friendly design and support.

In the context of e-inclusion, e-literacy refers the capacity to use ICT as a tool for communication, whether that's using email or social media platforms, and the use of devices such as smart phones, tablets and PCs. As digitalisation spreads, issues of e-Inclusion also become more acute and invites us to look beyond "traditional" usability issues of digital solutions, particularly when such solutions are aimed at the elderly and frail citizens, and particularly in the context of ICT based healthcare and assistive living solutions and services. Compared to younger generations, many elderly citizens require more time to pick up ICT skills and perform simple computer tasks. Research conducted in the SENIOR project suggested how "feeling too old to learn" is often a perception moulded by dominant social perception about ageing, rather than by seniors themselves (SENIOR, 2008b).

More than 10 years after the Communication on Ageing well in the Information Society mentioned above, the European Data Protection Supervisor (EDPS) published an Opinion, 'Towards a new digital ethics', which (also) emphasises the importance of safeguarding human dignity as the continuous development of technologies, and in particular surveillance technologies, sets new challenges for the protection of (data) privacy and hence human dignity. The threat surveillance technologies and continuously increasing collection of personal data (and big data) pose to human dignity is emphasised in the Opinion: "*The EDPS considers that better respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics […] Privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing.*" (EDPS 2015).[3]

The notion of dignity is here emphasised as fundamental, as embracing all other issues at stake; if dignity is protected and preserved the threat to autonomy, privacy, protection of data, stigmatisation etc. can be evaded. By emphasising human dignity as an entity of its own that must be safeguarded and protected, it also becomes apparent that there is more at stake than the illegal sharing, leaking or selling of personal data. It is clear that as surveillance technologies continues to develop and become more sophisticated and more widely applied (e.g. used also for profiling for commercial purposes), the protection of personal data against misuse (including covert use) becomes more crucial. The threat to our personal data and hence our privacy is simultaneously a threat to our human dignity, to our very personal identity. Individuals' awareness and understanding of such risks and how to protect themselves differ immensely, as does the knowledge of personal rights concerning privacy and data protection. In fact, the potential misuse and abuse of our personal data may often go beyond our wildest imagination and have consequence we did not see coming.

With the increasing digitalisation of our societies, and all that entails, digital footprints (or "breadcrumbs" as EDPS refers to) are constantly traced and often used to profile individuals which can be used for multiple purposes. Profiling activities in general, and particularly when used to predict people's behaviour, can be used to reinforce existing stereotypes and support discriminatory practises and stigmatisation.

In the context of healthcare (specifically nursing), the article 'An analysis of the concept dignity' (Griffin-Heslin 2005) considers four defining attributes of dignity: respect, autonomy, empowerment and communication which each consists of several dimensions. Respect includes self-respect, respect for others, respect for peoples' privacy, confidentiality and self-belief and belief in others. Autonomy includes having choice, giving choice, making decisions, being able to make decisions, competence, rights, needs, and independence. Empowerment includes a feeling of being important and valuable, self-esteem, self-worth, modesty and pride. Communication might be verbal or nonverbal and also includes explaining and understanding information, feeling comfort and giving time to the audience (Griffin-Heslin 2005, Adib-Hajbaghery & Aghajani 2015). By recognising that human dignity has multiple attributes and aspects, the gravity of any threat to it cannot be

[3] A privacy impact assessment will be presented in section 4.

ignored and when looking at the attributes described above, it is clear that threats are of both external and internal nature.

Although dignity in the work cited above is not considered in relation to technological solutions for healthcare in general, or monitoring and surveillance technologies for healthcare in particular, the multidimensionality of the concept of dignity still applies. Healthcare technologies and monitoring and surveillance technologies in particular do not make it any less complex, in fact, it is possible to see these technologies are both supporting and threatening the four attributes of dignity, and so of dignity itself. What is clear though, is that the human dignity in our digital age is as complex and crucial to safeguard as ever. Consider also that observing dignity and privacy is essential for establishing a good rapport between the healthcare professionals and patients.

Another aspect to consider is that patients should not be subjected to care activities that undermines their dignity. In the context of healthcare technology, an example would be to request that patients wear a device that can be seen as degrading or stigmatising, or it could be to demand that patients use a complex technological/digital solution (thereby also neglecting to take users' ICT literacy into account which then become an exclusion factor), or a solution/system with inadequate data protection measures in place, and so on.

3.3.1 Dignity for PICASO users

The issue of dignity is included in the PICASO ethical checklist precisely to safeguard respect for their person and personal decisions. 'Respect' is key and used to indicate the project's obligation to uphold confidentiality of personal data, respect for the participants' person and autonomy, and to fair and non-discriminatory treatment of all potential participants.

Confidential treatment of personal data is of course closely linked to the right to privacy and protection of personal data – which the first section of the Ethical Checklist deals with. When confidentiality is mentioned in connection with dignity it is precisely to stress that data protection issues can affect human dignity. Careless handling of personal data (i.e. not treating it with confidentiality) could be an example of (simple) disregard and indifference for that person and his/her privacy, or it could be a purposeful act to use the data for personal or other gains. When a person (and their personal data) is treated with disregard, disrespect and/or as a means for personal gain, their value and rights as human beings is diminished, if not completely dismissed, and their ownership personal data is not respected.

Dignity as respect for the person and their autonomy is in PICASO is mainly related ensuring that the any wearables or other devices used in the trials will not curtail participants' freedom or openly stigmatise them. It takes the notion of respect exemplified above a little further to also include respecting the person's life, movements and choices. It should remind us to be aware of the risk to (directly or indirectly) use data from the trial's home-monitoring system to limit the person's autonomy or otherwise threaten their dignity as decision-making and independent persons. For example, when a patient uses the PICASO home-monitoring solution the doctor can now continuously monitor if a patient follows the care plan. For instance, the patient has to actively confirm medication intake (using the Patient Dashboard) and the doctor will now have a digital record of how well a patient adheres to the care plan. This data can be discussed with the patient and/or his/her informal caregivers and the patient will be expected to explain the data, to explain his/her non-adherence. The patient can be held responsible in a whole new way and forging adherence suddenly becomes tricky; of course, the patient can lie and confirm medication intake even if he/she didn't take it, but the fact even this requires an action illustrates the sense of control and monitoring a patient is subject to with such a system.[4]

In D3.3 The PICASO Ethical Guidelines, the link between dignity and integrity is mentioned which will be further explained here. First of all, by linking dignity with integrity we put focus on the interaction, on the relationship between patient and physician: the integrity of the treater will help protect and uphold the dignity of the person be treated. By associating integrity and dignity, the focus is thus on the interaction between two and what happens to that interaction and relationship with the use of PICASO to implement a home-monitoring system and as a way for physicians to share patient data. When dignity is an ethical requirement in PICASO it is therefore not intended to indicate that the trial physicians need general reminding to treat their patients with dignity and integrity. Instead it is intended to create awareness of how a system like PICASO can potentially put patients' dignity at risk if for instance appropriate data security measures are not in place and their personal data is misused. It is not simply the physician who is required to treat patients with dignity and integrity; the technological solution itself must have integrity, meaning that it must be designed to uphold and safeguard

[4] Of course, home monitoring data will always "only" be supplementary or support the clinical records, not replacing it.

human dignity which as we have shown includes fulfilling the legal and ethical requirements with respect to privacy and protection of personal data.

Finally, in addition to emphasising usability and user acceptance requirement in the development work, the project has taken care to provide adequate instruction and training in using PICASO so as to best way possible prevent encouraging feelings of related to incompetence, low self-esteem, or low self-respect caused by difficulties in using PICASO. Therefore, patients (and when relevant their informal carers) who participate in PICASO have been carefully selected by the trial owners who have also provided detailed information about the project as part of the recruitment and informed consent process. Patients have been selected on basis of health-related criteria as well as also on their ability to fully understand what the trial (including the technologies and applications) involves and requires from them. Informed consent forms have been obtained from all end-users, including information on how to opt out of at any stage.

4 Privacy/Data Protection Impact Assessment

D3.5 Privacy Compliance Laws Associated with Surveillance identified and discussed the main privacy and data protection requirements applying to the project. They will not be repeated in depth here as they are beyond the cope of this deliverable, but will instead be summarised to provide the reader, as well as project partners, with a more condensed overview of the requirement. In addition, and according to the project review, this document will also identify the steps taken to comply with the requirements related to privacy and data protection (GDPR requirements). The requirements can be grouped into several areas. These are:

- The need to conduct an Impact Assessment
- The need to identify data controllers and data processors
- The need to ensure that consent meets the standards of the GDPR
- The need to comply with data protection principles as outlines in the GDPR
- The need to facilitate data subject rights.

4.1 Data Protection Impact Assessment:

Article 35 of the GDPR requires a data protection impact assessment be performed when it is likely that processing will give rise to a significant risk for the rights and freedoms of individuals. Given that Article 35 identifies the processing of significant amounts of sensitive data and the advice provided by the Article 35, the consortium deemed it necessary to conduct an impact assessment in this project. In this context the deliverables *D3.3 The PICASO Ethical Guidelines*, *D3.5 Privacy Compliance Laws Associated with Surveillance* and the internal document(s), *ID3.7 Annual Compliance Monitoring Report 1* (and 2) are considered collectively to meet the needs of such an assessment.[5]

4.2 Identify Data/controllers and processors

In 'PICASO as a research project'[6], it was necessary to define whether both data controllers and processors exist and who they are. In doing so it will be important to remember that a data controller is not necessarily the party collecting the data in question but the party that decides on what is done with it, how and by whom. In doing so, it was necessary that the precise arrangement decided upon whether the respective hospital partners retain total possession over patient data or whether it is passed to other partners for further processing. Where this is the case other partners may be classed as data processors, and in such circumstances, it will be necessary to conclude a contract between the hospital partners and the other partners that are concerned in order to ensure that data is processed correctly. This will also be the case where the services of local cloud providers are used. In such cases it should be ensured that the binding contact is created between data controller (i.e. the local hospital) and data processor. Such a contract should include the specified requirements as described in the GDPR pertaining to Data Processing Contracts.

The analysis conducted in the project has identified that there are two controllers, more precisely the two hospital partners (UNITOV and UDUS). It is these two partners alone that can determine the aims and the means of the processing that will occur. These partners are aware of this status and have implemented all necessary requirements as outlines in the GDPR and national law. As large hospitals they already have appointed data protections officers that will monitor compliance on an ongoing basis. In addition, data sharing and processing agreements have been created between the controller partners and those partners who may constitute partners within the project (CNET, TUK, FRAUNHOFER, IN-JET)

4.3 Data Protection Principles

The GDPR outlines six principles for processing of personal data. The following subsections will take a closer look at the project requirements related to these principles.

[5] *ID3.8 Annual Compliance Monitoring Report 2* will be submitted in M38 (March 2019). It will be closely linked to the legal requirements in D3.5.
[6] As D3.5 explains, it is necessary to distinguish between 'PICASO as a research project' and 'PICASO as an exploitable product'. This deliverable is concerned with the former unless otherwise stated.

4.3.1 Fairness, lawfulness and transparency of processing

Data subjects (i.e. patients in the context of PICASO) should be able to know what information has been collected about them, the purpose of its use, who can access and use it. Users should also be informed about: how to gain access to information collected about them and how they may control who has access to it. To achieve this the transparency of data processing has been ensured. Data controllers should be clearly identified and be able to respond to requests of e.g. data subjects. Controllers must therefore inform data subjects before the processing of their personal data about the main components of the processing (e.g. purpose of processing, identity and address of the controller, etc.).

In order to fulfil the requisite requirements of transparency, it was necessary to fully explain to potential data subjects in an understandable way, why their data it is being collected, what will happen with it. In the context of the trials in the PICASO project, this will entail ensuring that such processes are fully disclosed on the consent form that all participants must sign. In doing so it must be ensured that information is tailored to be understandable to the relevant audience taking into account their age, level of education, cognitive capacity and their respective language.[7] The two data controllers identified above (i.e. UNITOV and UDUS) are responsible for this. They have drafted consent forms so as to comply with all requirements listed in D3.5, including those outlined in Article 3.5 of the Data Protection Directive. The consent forms were checked by each partners' respective DPO and gained approval from local ethics boards and the PICASO Ethical Board. They were also checked by VUB which forms part of the PICASO Ethical Board.

4.3.2 'Data minimisation' and 'purpose limitation'

This fundamental principle of data protection is an expression coined by legal doctrine to refer to two key data protection principles, namely, the purpose limitation and the data minimisation principles. The purpose of use limitation, or purpose binding principle[8] prohibits further processing which is incompatible with the original purpose(s) of the collection. The data minimisation principle must act as a general principle policy for any technological development: information systems and software shall be configured by minimising the processing of personal data. In simple terms this means that no more data is collected and processed than is strictly necessary. The purposes for which personal data are collected should be specified at the time of collection. In addition, the use of those data should be limited to those previously defined purposes.

For the PICASO project**,** 'data minimisation' and 'purpose limitation' are actually two separate but closely linked principles. In most instances however, it is not possible to fulfil one without fulfilling the other. The most important element for the PICASO project is to be aware of its goals as a project so as to know what data is required. Once the ultimate goals of the project are known it quickly becomes apparent which types of data are needed and which are not (relevant to data minimisation). They are also relevant in understanding what constitutes acceptable use of individual data and what goes beyond (relevant to purpose limitation). Essentially PICASO as a project must not collect data that is not needed and must not subsequently use data for purposes that went beyond the original reasons for collection. This most notably will apply to the medical institutions involved in data processing in PICASO, who will need to ensure that patient data is not kept for any longer than is strictly necessary. This will however need to be decided taking into account national data protection laws on the use of medical data.[9]

4.3.3 Accuracy of Data

This principle implies that data must be adequate, up to date, relevant and not excessive for the purposes for which it is collected. Irrelevant data must not be collected and if it has been collected it must be discarded[10]. These key principles have been codified at constitutional level by art. 8 of the EU Charter, which states that personal data "*must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*".[11]

For both 'PICASO as a research project' and 'PICASO as an exploitable product' it will be necessary to ensure that best procedures and devices are used to ensure that data is correct. This will involve where necessary

[7] As PICASO deliverable 3.3 discusses all consent forms have been translated into the local language i.e. Italian or German. They have also been created in line with local ethics requirements.
[8] Art. 6 (1) b) Directive
[9] Discussed with important examples in D3.5 Annex
[10] Art. 6 (1) c) Directive
[11] As the travaux préparatoires indicate, art. 8 codifies and must be read in the light of Council of Europe and European Union legislation, in particular Directive 95/46/EC.

using trained staff so as to ensure that data is stored correctly. In addition, it will be essential to ensure that any devices used will be of sufficient quality in order to ensure that data is accurate to the required level of sensitivity (section 6 in D3.5 discussed that this may often mean that it is necessary to use devices that have been correctly certified with the CE mark).[12] In order to achieve this both hospital partners have ensured that all staff are fully trained to use all equipment envisaged for use within the PICASO project.

4.3.4 Storage limitation

In principle data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data were collected or for which they are further processed. This requirement may however be subject to certain requirements relating to national law that require the retention of medical data used in clinical practice or research for defined periods.[13] Where possible data should be anonymised.

It will be necessary to ensure that all precautions are taken to ensure that data is kept for no longer than is necessary. As data in 'PICASO as a research project' is stored with online cloud providers, a specific clause in the data processing contract between data controller and data processor.

Specifically, the two hospital partners have instigated procedures to ensure that data is not kept longer than necessary after the completion of the project. The sole exception is that some copies must be kept of file afterwards to comply with local laws on the retention of medical and trial records (see annex of D3.5). In addition to this the data sharing and processing agreements that are made between the hospital partners and the partners in the project that act as processors will demand that all personal data is deleted when the project is finished.

4.3.5 Data security

Appropriate technical and organisational measures should be taken into consideration when personal data is processed in order to ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

For 'PICASO as a research project' it will be necessary to consider all relevant threats to security and take appropriate technical measures. This includes threats that arise through malevolent action or otherwise. All contracts between the data controller(s) and data processor(s) (including a cloud service provider) will have to ensure a legally binding requirement exists to ensure that the principle of data security is met.

4.3.6 Data Protection by Design

The GDPR confirmed 'data protection by design' as a data protection principle in its own right. This principle demands that data processing systems must be designed in a way from the outset that ensures data protection requirements are carried out. This includes ensuring that the data protection principles described here are implemented, that data is only processed where there is a correct legal base, and that the rights of any data subject will be respected. Of crucial importance is that data protection and its requirements are considered throughout the project including in the conceptualization, design and implementation stages of any project.

For PICASO it is necessary to ensure therefore that at each stage of design the requirements of data protection are considered. This means that all design partners must consider these requirements both when designing the PICASO trial infrastructure and when implementing it. This includes the legal requirements as described within this document. In this spirit, the legal requirement incumbent upon all hospital and technical partner have been identified early in the project at regular meetings, thoroughly analysed in D3.5 (concerning privacy and data protection) and checked for compliance in the internal document(s) *ID3.7/8 Annual Compliance Monitoring Report 1/2*. The aim was to ensure that such requirements were born in mind from the outset of the project and built into the design of the systems used in the PICASO trials. The aim of the compliance report was to ensure that this occurred and where necessary make adjustments.

[12] See discussion on medical devices in D3.5.
[13] Discussed with important examples in Annex of D3.5.

4.3.7 Privacy by Default

This is another principle that has been introduced by the GDPR.[14] It essentially demands that any system designed to process personal data should be designed to use the least intrusive basis as a starting point. Only with the approval of the data subject (preferably on a step-by-step and granular basis) should the processing of personal data be broadened to include further forms of processing.

For 'PICASO as a research project' this principle has a lesser relevance. This is because the envisaged forms of processing are fixed from the outset. The possibility for granularity in the trial phase of the project is thus in reality limited. As a consequence, consent has been sought at the beginning of the project from the data subjects for all forms of processing that are likely to occur (through signed consent forms – see deliverables D3.3, D8.4 and D8.7). Implementing granularity at this stage of the project would not be practical given that consent will be paper based – meaning that it would be very burdensome for both the patient and from an administrative point of view to be constantly signed new consent forms for each new data processing operation.

4.3.8 Accountability[15]

The final principle under the GDPR states that data controllers must be able to demonstrate compliance with the other principles. This is a short sentence with major implications. One of the notable changes under the GDPR compared with the former directive, is the increased compliance burden, much of which is sparked by the accountability principle. It is not enough to comply, you have to be seen to be complying. The type of effort needed to demonstrate compliance will vary according to the complexity of the operation but may include:

- assessing current practice and developing a data privacy governance structure which may include appointing a Data Protection Officer;
- creating a personal data inventory;
- implementing appropriate privacy notices;
- obtaining appropriate consents;
- using appropriate organisation and technical measures to ensure compliance with the data protection principles;
- using Privacy Impact Assessments; and
- creating a breach reporting mechanism.
- the use of legally binding data processing agreements where applicable.

For PICASO it was necessary to implement practices associated with accountability. In this regard D3.5 (Privacy and Data protection Requirements), together with some of the more ethical themed documents in Work Package 3 (including for *D3.3 The PICASO Ethical Guidelines* and *ID3.7/ID3.7 Annual Compliance Monitoring Report 1/2*) can be considered as an impact assessment.[16]Their aim was to ensure the aspects of accountability described above were met. In their entirety these deliverables consider the range of legal and ethical issues that are mandated by article 35 GDPR. These deliverables will also help to ensure that the relevant requirements are met given that in order to produce it, it was necessary to carry out an audit of many of these elements. In other regards the data controllers (and in particular their respective DPOs) involved in the project must ensure that efforts are made at addressing the relative accountancy mechanisms described here.

4.4 Consent Requirements

During the PICASO project, the legal basis relied upon for the processing of personal data has been informed consent. This has been secured through the use of signed consent forms to be issued to patients at each of the hospital sites.[17] In general, the data protection regulation makes a number of points about what is required for consent to occur. These notably include:[18]

[14] See article 25 of the GDPR.
[15] *The description of this principle has been taken directly from Law Firm TaylorWessing. The authors would like to convey their thanks to the this firm for its concise yet, accurate description. Available at: https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html*
[16] *This is also required under art 35 GDPR*
[17] For more information see deliverable D3.3 which describes how to obtain informed consent in an ethically sound manner.
[18] Details are described in article 6 of the GDPR.

- Data subject must give his consent freely, without undue pressure. The consent is freely given „if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent".
- Data subject must be duly informed about the consequences of giving consent. To have sufficient information before giving consent data controller must provide easily accessible information in an easily understandable language.
- The consent must be specific, reasonably concrete, which relates to the reasonable expectations of an average data subject.
- The data subject must be able to revoke consent.
- The data subject must be provided with the requisite information as described in articles 13-14 of the GDPR.

Given however that PIASO will be handling sensitive data the requirements for consent are stricter. Article 9(1) states: "*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.*"[19]

The key word here is 'explicit', which denotes a higher and more formal standard for consent. However, it has not been defined what exactly this may require for various forms of electronic consent. There is however little doubt the use of signed consent forms as proposed by PICASO would meat such a requirement if it meets certain conditions. The consent form in PICASO has been designed with these conditions in mind, including:

- The person giving consent must clearly state that his actions specifically constitute an act of consent.
- The consent should be revocable
- It must be informed, i.e. the individual must be provided with the requisite information to make a decision.
- The individual must be provided with the additional information as demanded by data protection law.[20]

It should be noted that further principles relating to national law (i.e. in the case of the PICASO trials, Germany and Italy) may apply to formalities concerning consent. Relevant laws in this area are described in the annex to D3.5. The consent forms used in the PICASO trials have been checked by the DPOs of the hospital partners, the ethics bodies of each hospital and VUB (in its role on the PICASO Ethical Board).

4.5 Data Subject Rights

A data subject is a living, identifiable individual to whom particular personal data relates. In PICASO, patients participating the trials are the data subjects and as such the PICASO project is required to respect their rights as defined in the GDPR. The following subsections presents an overview of the main rights and their associated requirements for PICASO.

4.5.1 A Right to basic information and information required for the purposes of consent[21]

The GDPR demands that data subjects are furnished with sufficient information to be able to properly understand the means of and the purpose for the processing in question. The GDPR presents a list of items that are needed and which must be described to the data subject in order inter alia for consent to be gathered. In PICASO is necessary to ensure that the information required is presented on the relevant consent forms (also discussed above). These include:[22]

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of the data protection officer, where applicable
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- The recipients or categories of recipients of the personal data, if any

[19] Emphasis added by author.
[20] The relevant provisions describing the informational requirements upon the data controller are described in article 12-14 of the GDPR.
[21] See GDPR Recitals 58, 60 and Articles 13 – 14.
[22] Further rights in terms of information apply where the personal data is not gathered directly from the data subject but is taken from an intermediate party.

- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with a supervisory authority.

The consent forms used in the PICASO trials have been checked by the DPOs of the hospital partners, the ethics bodies of each hospital and VUB (in its role on the PICASO Ethical Board). This includes an analysis to ensure that the requirements of article 13 of the GDPR were correctly included.

4.5.2 The Right of Access[23]

Data subjects are entitled to access their personal data (confirmed in Article 15 f the GDPR). Such access is important for the data subject in order to discern whether his or her rights are being complied with. Data subjects have the right to receive not only access to their data but also to information concerning their data (as described above). Data controllers may charge a reasonable fee for such access (in order to deter vexatious claims for access). In order to comply with such a right the hospital partners have instigated procedures to comply with such requests where they be made.

4.5.3 A Right to Rectification.

Data subjects have a right to rectify their data where it is incorrect. Such a right is closely related to and dependent on the right to access.[24] . In order to comply with such a right the hospital partners have instigated procedures to comply with such requests where they be made.

4.5.4 A Right of Erasure

This right allows data subjects to demand the detention of their data when its retention is no longer justified. Where the legal base for the processing of such data was consent, data subjects are entitled to withdraw their consent. This article does however make allowance for instances where the Data Controller must maintain data in order to comply with other EU or national laws. This may be important within the context of PICASO where national laws may demand that clinical or research data be kept for a longer period.[25] Similarly as with the rights described above, it will be necessary to ensure (using a data processing contract) that any third party data processors comply with such a right. Accordingly, the hospital partners of PICASO are committed to facilitating this right in ways that are compatible with any requirements under national law (i.e. deleting excess copies at the end of the project).

4.5.5 Data Portability

Data subjects are also provided with a right of data portability. More specifically this relates to a "right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format".[26] This right seemingly is limited by the use of words "which he or she has provided" which seems limit the extent of the right to the data that has been provided by the data subject and therefore not further data that has been created from subsequent processing. In a project such as PICASO this would seemingly relate to the raw data that is gathered from the patient concerned and not any specialist analysis that has been performed on top of it. According to the GDPR such data should be provided in a way that is transferable to a third party or even transferred directly to another controller where that is possible. The hospital partners have thus instigated procedures to comply with such requests should they be made.

[23] *Article 15 GDPR*
[24] *See articles 5 and 16 of the GDPR.*
[25] *For more GDPR article 17. Article 18 also describes circumstances where processing may be restricted upon demand of the data subject (these may apply were for instance national law demands deletion.*
[26] *See GDPR Article 20*

5 Concluding remarks

An ethical analysis of monitoring must always be placed in context; it is necessary to understand the purpose for the monitoring, the type of technologies and devices used, and the level of control the observed party (data subject) has and is put under (a control often reinforced by the technology used). In PICASO as a research project this analysis has hopefully helped to understand the issues at stake and how to handle them, a knowledge that should be included (disseminated) in 'PICASO as an exploitable product'. Due to the timing of this deliverable, empirical knowledge and actual instances of ethical problems or raised concerns is still very limited. As the trial progresses, all issues related to ethics will be noted and analysed in forthcoming deliverables, notably *ID3.8 Annual Compliance Monitoring Report 2* and *D8.9 Third Annual Trial Progress and Ethical Report.* Moreover, *D3.6 Practical Implementation of Patient Empowerment and Joint Care* may discuss some experiences of patient empowerment from an ethical perspective.

These mentioned deliverables will also consider the recommendations and requirements from the analysis of the data protection and privacy requirements and the impact assessment presented in this deliverable. With the implementation of the GDPR in May 2018, the rights of the data subjects have become more emphasised and, in many ways, more tangible (and hard to take lightly or even ignore!). As PICASO deals with patient data, privacy and data protection is all the more important – both to protect the individual patient and to make sure that 'PICASO as an exploitable product' can be realised from a legal perspective.

6 References

Adib-Hajbaghery & Aghajani (2015) — Adib-Hajbaghery M, Aghajani M. (2015), Patients dignity in nursing. Nurs Midwifery. Stud. 2015 Mar;4(1):e22809. Epub 2015 Mar 20

EC (2007) — European Commission. (2007). Ageing well in the information society, action plan on information and communication technologies and ageing, an i2010 initiative. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2007) 332 final. Brussels, 14 June 2007.

Griffin-Heslin (2005) — Griffin-Heslin VL (2005). An analysis of the concept dignity. Accid Emerg Nurs. 2005;13(4):251–7

Moran (2015) — Moran, S. (2015). Surveillance Ethics, in Philosophy Now, online version: https://philosophynow.org/issues/110/Surveillance_Ethics

SENIOR (2008a) — SENIOR Project (2008a), D1.4 Socio-Anthropological Workshop Report

SENIOR (2008b) — SENIOR Project (2008b), D2.3 Document on Intelligent User Interface

Wright, D. (2011) — Wright, D (2012). An Ethical Impact Assessment Framework for Information Technology, *Ethics and Information Technology*, Vol. 13, no. 3, September 2011, pp.199-266