A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information

Project acronym: MyHealthAvatar

Deliverable No. D11.1
Ethical clearance

Grant agreement no: 600929

Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	**X**

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	MyHealthAvatar
Project Full Name:	A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information
Deliverable No.:	D11.1
Document name:	Ethical clearance
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	CO
Version:	1
Actual Submission Date:	31.05.2013
Editor: Institution: E-Mail:	

ABSTRACT:
This deliverable provides an overview of the applicable European data protection framework and relevant ethical guidelines. In addition, a provisional analysis of the proposed data use in the MyHealthAvatar project will be presented in order to provide a sound starting point for ensuring legal and ethical compliance.

KEYWORD LIST:
Legal and ethical framework, Data Protection Directive, Declaration of Helsinki

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 600929.

[1] **R**=Report, **P**=Prototype, **D**=Demonstrator, **O**=Other

[2] **PU**=Public, **PP**=Restricted to other programme participants (including the Commission Services), **RE**=Restricted to a group specified by the consortium (including the Commission Services), **CO**=Confidential, only for members of the consortium (including the Commission Services)

The author is solely responsible for its content, it does not represent the opinion of the European Community and the Community is not responsible for any use that might be made of data appearing therein.

MODIFICATION CONTROL			
Version	**Date**	**Status**	**Author**
1.0	29.05.2013	Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen
2.0		Draft	
3.0		Draft	

List of contributors

- Prof. Dr. Nikolaus Forgó, LUH
- Dr. Marc Stauch, LUH
- Dipl.-Jur. Sarah Jensen, LUH
- Ass.-Jur. Dania Kobeissi, LUH

Contents

1 Executive Summary

The MyHealthAvatar project is a research and demonstration-oriented iterative process, through which the feasibility of creating personal health records configured as digital patients shall be studied. The vision is to set up a 4D avatar representing the health status of patients and encouraging the engagement of both medical professionals and patients.
Since the 4D avatar will allow health and other data access, collection, sharing and analysis, the presence of a sound, privacy-compliant legal and ethical framework must be assured.
In particular, great importance should be attached to the safeguarding of patient rights, especially their right of privacy concerning medical data.
At this early stage of the project, a number of the specific details are not yet clarified, for example whether all data which will be processed within the MyHealthAvatar platform is to be rendered anonymous (as defined by EU data protection law), and if so what form such anonymisation could take.
However, it is most likely that personal data will be processed to some extent, so the Data Protection Directive will be applicable and data protection issues will have to be considered from a legal perspective as well from an ethical point of view.
To this end, this deliverable will offer an introduction and overview of the applicable European data protection framework and relevant ethical guidelines as well as a provisional analysis of the proposed data use in the MyHealthAvatar project in order to provide a sound starting point for ensuring legal and ethical compliance.

2 Introduction

As long as patients participate in medical research, there will be always a debate on ethical and legal requirements. Against this background the MHA - MyHealthAvatar's description of work presents several ethical requirements, which will be further elucidated to make sure that the objectives of the project will respect the rights and fundamental interests of patients. This deliverable is composed of two sections with the intention to clarify the ethical and legal requirements which have to be followed when using patient data in the context both of medical research generally, and within the parameters of the MHA project.

The first section constitutes of giving a general overview of the relevant legislation that must be kept in mind throughout MHA project. The Data Protection Directive (95/46/EC)[3] will be used as a legal starting point because it has been implemented into national law by all EU member states and therefore offers a clear basis for depicting the most relevant legal concepts. First, it will be outlined when the Data Protection Directive will apply. In this respect we shall proceed to consider the different categories of data, which the Data Protection Directive distinguishes. These include personal data, anonymous data and special categories of data as sensitive data. Beyond that, several Member States have implemented pseudonymous data[4] that makes a fourth category of data. In order to describe these categories of data we will mainly focus on the opinion 4/2007[5] by the Article 29 Working Party[6] in which the Working Party has provided guidance on the way in which the concept of personal data in Directive 95/46/EC should be understood.[7]Afterwards data security issues will be presented and then ethical requirements will be analysed. The main focus will be the issue of patient consent highlighted also from a legal perspective.

The second section will indicate the course that should be followed by each project partner dealing with potential ethical issues, by drawing up a preliminary legal framework for MHA. In this regard, a provisional analysis will be performed of the application of the salient rules to likely factual scenario of MHA, with reference to ethical and legal issues which have been outlined in the first section of this deliverable. This concludes seeking to concretise key measures to be taken at various stages of proposed data use within the MHA project.

[3] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[4] For example the German Data Protection Act in § 3 Nr. 6a BDSG.

[5] See Opinion 4/2007 at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[6] The party is made up under Article 29 of Directive 95/46/EC. According to Article 2 of Directive 95/46/EC it is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. The independent European advisory body aims at the protection of individuals with regard to the processing of personal data.

[7] Opinion 4/2007, p. 25.

3 Overview of legal and ethical requirements

3.1 Legal requirements

3.1.1 Scope of the Data Protection Directive

Pursuant to Article 3 (1) Directive 95/46/EC, the Data Protection Directive applies only to personal data. If the data is not to be seen as being personal, the Data Protection Directive does not apply. This is especially the case when data is rendered anonymous.
Furthermore, the Data Protection Directive only applies within the EU/EEA territory.

3.1.1.1 Personal data

The term of "Personal data" is defined in Article 2 lit. a) of Directive 95/46/EC as "*any information relating to an identified or identifiable natural person, ('data subject')*". In this regard, an "identifiable person" is defined as "*one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".
As mentioned above we will refer to the leading opinion on the concept of personal data (Opinion 4/2007) by the Article 29 Data Protection Working Party in order to elaborate further on the meaning of personal data. As a general consideration it can be noted that the European lawmaker intended to adopt a broad notion of personal data in order to pursue the objective of a wide protection of the right to privacy with regard to the processing of personal data.[8] To analysis the term „personal data" in concrete, its definition can be divided into four parts, which are:

- Any information
- Relating to
- An identified or identifiable
- Natural person

In order to determine whether a piece of information should be consider as "personal data" the four parts have to be considered cumulatively. The first component" any information" requires a broad interpretation regardless of nature, content of the information and format or medium in which the information is presented.[9] It includes any sort of statements about a person irrespective of the correctness of the information.[10] Moreover it is immaterial whether the information is "objective" in nature, such as the presence of a certain substance in a person's blood, or takes the form of a "subjective" opinion or assessment.

The second part "relating to" clarifies that the information must relate to the individuals it is about.[11] This element is crucial in order to determine the substantive scope of the concept, especially in

[8] Opinion 4/2007, p. 25.
[9] Opinion 4/2007, p. 6.
[10] Opinion4/2007, p. 6
[11] Opinion 4/2007, p. 9.

relation to new technologies.[12] Of course this relationship can be easily established in many situations, e.g. when the results of a patient's medical test are contained in his or her medical records.[13] But there are also situations where it is not so obvious whether the information "relates" to an Individual, e.g. when the data concerns objects in the first instance, but those objects belong to someone.[14] In order to decide when the data "relate" to an individual, the opinion proposes three alternative (and independently sufficient) tests that may be used, which ask in turn whether a "content" element, a "purpose" element or a "result" element is present in the relation between the information and individual.[15] At the same time, as the Working Party acknowledges, it is not possible to lay down an exhaustive and conclusive rule which makes clear when information is related to a person because the question of whether data relate to a certain person has to be valued for each specific data item on its own merits and within the particular context.[16] The third element consists of the two limbs "identified or identifiable" The first term "identified" is relevant, when a natural person is distinguished from all other members of a certain group of people[17] whereas the second component is pertinent when it is possible to distinguish a person from the group although he or she is not identified yet.[18] "Identifiers", which permit identification, can be particular pieces of information that hold a particularly privileged and close relationship with the particular individual.[19] Art. 2 (a) of Directive 95/46/EC states that persons can be identified directly or indirectly. Relative to direct identification the name of a person is the most common identifier.[20] But there are also unique identifiers like numbers, which are assigned to the persons registered in a file so two persons cannot be confused with each other in the file. This unique identifier, i.e. the number, then refers to an identified natural person.[21]
Indirect identification is relevant when a unique combination of several identifiers allows a certain person to be singled out,[22] e.g. the combination of gender, date of birth and address.

The third part "identifiable" is defined in Recital 26 of Directive 95/46/EC as "*whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify said person.*" So a person is not identifiable when *"all the means likely reasonably to be used"* do not exist and consequently the information cannot be considered as personal data.[23] The relevant factors for assessing the question of means likely reasonably to be used are cost, intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals as well as the risk of

[12] Opinion 4/2007, p. 25.
[13] Opinion 4/2007, p. 9.
[14] Opinion 4/2007, p. 9.
[15] Opinion 4/2007, p. 10
[16] Opinion 4/2007, p. 12.
[17] Opinion 4/2007, p. 12.
[18] Opinion 4/2007, p. 12.
[19] Opinion 4/2007, p. 12.
[20] Opinion 4/2007, p. 13.
[21] Opinion 4/2007, p. 14.
[22] Opinion 4/2007, p. 13.
[23] Opinion 4/2007, p. 15.

organisational dysfunctions (e.g. breaches of confidentiality) and technical failures.[24] It has to be taken into account that the assessment of these factors is likely to change over time and therefore the system should be able to adapt to new developments as they happen by incorporating the appropriate technical and organisational measures.[25] In this context the Working Party gives an example of pharmaceutical research data where it is not very likely that the data subject will be identified:

"Hospitals or individual physicians transfer data from medical records of their patients to a company for the purpose of medical research. No names of the patients are used but only serial numbers attributed randomly to each clinical case, in order to ensure coherence and to avoid confusion with information on different patients. The names of patients stay exclusively in possession of the respective doctors bound by medical secrecy. The data do not contain any additional information, which make identification of the patients possible by combining it. In addition, all other measures have been taken to prevent the data subjects from being identified or becoming identifiable, be it legal, technical or organisational. Under these circumstances, a Data Protection Authority may consider that no means are present in the processing performed by the pharmaceutical company, which make it likely reasonably to be used to identify the data subjects."[26]

Nevertheless the Working Party makes clear that: "*where the purpose of the processing implies the identification of individuals, it can be assumed that the data controller or any other person involved have or will have the means likely reasonably to be used to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms.*"[27] Where identification of the data subject is not included in the purpose of the process the technical measures to prevent identification are very important for deciding if there are personal data or not.[28] If appropriate state-of-the-art technical and organizational measures shall protect the data against identification, the persons are not identifiable considering all the means likely reasonably to be used by the controller or by any other person to identify the individuals. [29]

The fourth element of the definition of personal data is the term "natural person".
The main idea of that part is that the protection afforded by the rules of the Data Protection Directive applies to all human beings without any restrictions considering nationals or residents in a certain country.[30] Hence recital 2 of the Directive points out that "*data processing systems are designed to serve man*" and that they "*must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms*".

[24] Opinion 4/2007, p. 15.
[25] Opinion 4/2007, p. 15.
[26] Opinion 4/2007, p. 15 f.
[27] Opinion 4/2007, p. 16.
[28] Opinion 4/2007, p. 17.
[29] Opinion 4/2007, p. 17.
[30] Opinion 4/2007, p. 21.

This idea is also referred to in Article 6 of the Universal Declaration of Human Rights, according to which "*Everyone has the right to recognition everywhere as a person before the law*". Basically, information relating to dead individuals is not considered as personal data subject to the rules of the Directive, since the dead are no longer natural persons in civil law.[31] Despite that, these data may indirectly receive some protection, e.g. when the information on the dead individual refers to a living person. This can be the case when the dead person suffered from a certain disease where the conclusion can be drawn that his or her progeny suffers from the same disease. Apart from this fact, nothing prevents a Member States from extending the scope of the national legislation to areas not included in the scope of the directive.[32] The extent to which data protection rules may apply before birth depends on the national legal systems.[33] Whereas some Member States acknowledge the general principle that children conceived but not yet born are considered as if they were born as far as benefits are concerned, in other Member States particular legal provisions exist to confer the specific protection.

3.1.1.2 Anonymous data

A further data category is the one of anonymous data. Pursuant to Recital 26 of Directive 95/46/EC, the Data Protection Directive is not applicable to data rendered anonymous in such a way that the data subject is no longer identifiable. Relating to the MyHealthAvatar project it is crucial to know whether the data processed within the project are rendered anonymous. If this is the case, data protection legislation would not apply to the processing within MyHealthAvatar. In this connection it has to be underlined that the Directive is of course applicable for the anonymisation of personal data. In the first draft of Directive 95/46/EC, Article 2 lit. b) defined anonymisation as personal data modified "*in such a way that the information they contain can no longer be associated with a specific individual or an individual capable of being determined except at the price of an excessive effort in terms of staff, expenditure and time*"[34]. But the final version failed to draw up a definition.[35] The difference between both definitions is the fact that the proposal takes "*an excessive effort in terms of staff, expenditure and time*" into consideration whereas the valid definition considers data as anonymous only if the data subject is no longer identifiable, i.e. the link that refers to the data subject is irrecoverably erased. However, the European perception regarding "anonymous data" seems to have changed as one can illustrate with the "First report on the implementation of the Data Protection Directive"[36] the European Commission published in 2003.[37]

In this report it is stated that "*it is necessary to find an interpretation consistent both with the reinforced protection foreseen for this category of data by the Directive and the realities of daily*

[31] Opinion 4/2007, p. 22.

[32] Judgment of the European Court of Justice C-101/2001 of 06/11/2003 (Lindqvist), § 98.

[33] Opinion 4/2007, p. 23.

[34] Proposal for a council directive concerning the protection of individuals in relation to the processing of personal data COM (90) 314; available here http://aei.pitt.edu/3768/1/3768.pdf.

[35] Forgó, Kollek, Arning, Kruegel, Petersen, p.69.

[36] See http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf.

[37] Forgó, Kollek, Arning, Kruegel, Petersen, p.69.

business, routine processing operations and the effective risks that certain operations pose for the protection of the fundamental rights and freedoms of individuals."[38] Alluding to a document of the European Privacy Officers Forum (EPOF) the Commission stresses that the interpretation of certain provisions of Directive 95/46/EC had to be reasonable and flexible, giving "sensitive data" as an example.[39] In the document, the EPOF stated that the definition of anonymisation should be pragmatic and highlighted that the capability of identification must be subject to the reasonableness standard.[40] According to this, the Working Party defines anonymous data *"as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking into account all of the means likely reasonably to be used either by the controller or by any other person to identify that individual. Anonymized data would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible. "*[41] In conclusion one can presume that the European Commission approves a definition of "anonymous data" with an "excessive effort" as a component.[42]
Consequently, information concerning personal or material circumstances which can only be attributed to an identified or identifiable person with a disproportionate expenditure of time, costs and effort should be classified as anonymous data.[43]

3.1.1.3 Pseudonymous data

The next category of data is "pseudonymous data". The Data Protection Directive does not mention this term but nevertheless, some member states legislations provide a definition of pseudonymised data; e.g. the German Federal Data Protection Act ("BDSG") defines in section 3 paragraph (6a) pseudonymising as "*replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult"*. And also the Art 29 Working Party refers to pseudonymous data in its opinion on the concept of personal data and defines pseudonymisation as "*the process of disguising identities*"[44] and gives some examples how pseudonymisation can be done, e.g. by using correspondence lists for identities and their pseudonyms or by using two-way cryptography algorithms (whereas the use of one-way cryptography usually creates anonymised data).[45] The Working Party points out that retraceably pseudonymous data is data where it is possible to backtrack to the individual, so that the individual's identity can be discovered, but then only under predefined circumstances. [46] So in conclusion it can be said that the common understanding of pseudonymous data is that there are

[38] Report from the Commission - First report on the implementation of the Data Protection Directive (95/46/EC) /* COM/2003/0265 final */, sec. 4.2 The need for a reasonable and flexible interpretation; available here http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:HTML.
[39] Forgó, Kollek, Arning, Kruegel, Petersen, p.69.
[40] Forgó, Kollek, Arning, Kruegel, Petersen, p.69.
[41] Opinion 4/2007, p. 21.
[42] Forgó, Kollek, Arning, Kruegel, Petersen, p.69.
[43] Forgó, Kollek, Arning, Kruegel, Petersen, p.70.
[44] Opinion 4/2007, p. 18.
[45] Opinion 4/2007, p. 18.
[46] Opinion 4/2007, p. 18.

reversibly coded data and that an official channel for re-linking the data remains. Thus, pseudonymous data is personal data and so the data protection legislation applies. The Working Party states that when one wants to determine whether a person is identifiable, account should be taken of "*all the means likely reasonably to be used either by the controller or by any other person to identify a person".* [47] This means that personal data can be considered to be anonymous for one data controller, whereas it has to be considered pseudonymous for another data controller. However, if one party is able to re-identify the patient concerned in a research project, this data set can arguably not be anonymous for the other parties. Therefore the data would be personal for all if it is personal for one project partner.

3.1.1.4 Sensitive data

Since certain information is more important for the privacy of a person than other kinds of information, the Data Protection Directive provides special categories of personal data in its section III (which includes Article 8 and Article 9 of Directive 95/46/EC). Article 8 (1) of Directive 95/46/EC enumerates these categories which are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. All these categories have in common that they are sensitive data. Recital 34 mentions the term of "sensitive categories of data".

The basic principle in the Data Protection Directive is according to Article 6 (1) and Article 7 of Directive 95/46/EC that the processing of personal data is forbidden, except if there is a legal basis or the data subject has given informed consent. This basic rule also applies to sensitive data. But since this kind of data contains information affecting the privacy of a data subject more than other data does[48], Article 8 of Directive 95/46/EC includes a stronger protection for sensitive data. In Article 8 (I) of Directive 95/46/EC it is stated that Member States shall prohibit the processing of this category of personal data.

Article 8 (2), (3), (5) of 95/46/EC include very strict exemptions which constitute a legal permission for the processing of sensitive data.[49] The exemptions given in Article 8 paragraph 2 of Directive 95/46/EC include, in simplified terms, the explicit consent of the data subject (lit. a), processing that is necessary for purposes in the field of employment law (lit. b), processing that is necessary to protect the vital interests of the data subjects (lit. c), processing that is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, an association or any other non-profit-seeking body (lit. d) as well as the processing of data which are manifestly made public by the data subject or necessary for the establishment, exercise or defence of legal of claims (lit. e). Furthermore, Member States may introduce exemptions in addition to those laid down in paragraph 2 **for reasons of substantial public interest** according to Article 8 (4) of Directive 95/46/EC. What public interest includes is mentioned in Recital (34) of the Directive:

[47] Opinion 4/2007, p. 19.

[48] Forgó, Kollek, Arning, Kruegel, Petersen, p.72.

[49] Forgó, Kollek, Arning, Kruegel, Petersen, p.73.

"Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in ***areas such as public health and social protection*** *- especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system -* ***scientific research and government statistics.****"* As is made clear, though, Member States here have to "*provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals"* according to Recital (34) when they lay down a further exemption. So if a Member State wants to use this exemption, it must be contained in a legal provision or a decision of the supervisory authority[50] and according to Article 8 paragraph 6, the Member State has to let the Commission know.

Article 8 (3) of Directive 95/46/EC allows the processing of sensitive data where it "*is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national laws or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.*" The term "medical research" is not mentioned in Article 8 (3) of Directive 95/46/EC. As a result, it is generally agreed that paragraph 3 does not apply to medical research in general which raises the question if an application to sub-areas of medical research is possible. Nicole Pöttgen suggests that this can be only the case if medical research relates to the purposes otherwise mentioned in Art 8(3).[51] Of course, this assessment would cause difficulties in demarcation. Besides, it must be pointed out that Article 8 (3) of Directive 95/46/EC requires that the data has to be processed by a health professional. This requirement would already minimize the scope of application.[52]Similarly it remains open how far Article 8 (3) would provide a more general exemption in relation to the use of electronic health records (EHRs) for purposes that go beyond the direct individual treatment and care of the patient. The MHA Description of Work states on page 3, 39 of 56 and 8 of 40 that within the MyHealthAvatar project a system shall be set up which will provide access to external sources like EHRs.

In 2007 the Article 29 Working Party published a Working Document on the processing of personal data relating to health in electronic health records (EHR)[53] (Working Document EHR) in which it defines electronic health records as "*a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes".*[54] Moreover the Article 29 Working Party notes that in their view all data contained in medical documentation, electronic health records and EHR systems should be considered to be

[50] Working Document EHR, p. 12; available here http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.
[51] Pöttgen, p. 54.

[52] Pöttgen, p. 55.
[53] See Working Document EHR at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.
[54] Working Document EHR, p. 4.

sensitive personal data[55] which means that all EHRs contain sensitive data. However, the exemption in Article 8 (3) does not apply because for it to do so the relevant processing must be for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature.[56] In contrast, further processing, which is not required for the direct provision of such services, such as medical research, is not covered.[57] Therefore, probably Article 8 (3) cannot serve as a legal basis for the processing of sensitive data for purposes of medical research.
Instead, only the exemption of Article 8 (4) of Directive 95/46/EC can apply, if sensitive data for purposes of medical research is processed and no consent has been obtained.

3.1.2 Data security

Data security can be achieved by technical and organisational but also by accompanying legal measures. Due to the increased specialization of healthcare providers and healthcare researches, it is not unusual that the team dealing with one patient consists of 10 to 50 people.[58] Therefore it is important to establish technical and legal rules concerning the handling of data.
Article 17 of 95/46/EC states that the Member States must provide that all technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access are undertaken. Also the Recommendation on the Protection of Medical Data[59] of the Committee of Ministers to Member States, R(97)5, recommends appropriate technical and organisational measures to protect personal data against accidental or illegal destruction, accidental loss, as well as against unauthorised access, alteration, communication or any other form of processing.[60]
These measures shall ensure an appropriate level of security taking account of the technical state of the art and also of the sensitive nature of medical data and the evaluation of potential risks.[61]
Such appropriate measures are

- access control,
- transmission control,
- authorisation control,
- input control,
- job control and
- availability control.

All these measures aim at the guarantee of confidentiality integrity and accuracy of processed data.[62]

[55] Working Document EHR, p. 7.
[56] Working Document EHR, p. 10.
[57] Working Document EHR, p. 10.
[58] Forgó, Kollek, Arning, Kruegel, Petersen, p. 71.
[59] See http://www1.umn.edu/humanrts/instree/coerecr97-5.html.
[60] http://www1.umn.edu/humanrts/instree/coerecr97-5.html; at 9.1 ff.
[61] http://www1.umn.edu/humanrts/instree/coerecr97-5.html; at 9.1.
[62] http://www1.umn.edu/humanrts/instree/coerecr97-5.html, at 9.2.

Access control is crucial to prevent unauthorised persons from gaining access to data repositories. Otherwise persons without authorisation could misuse them.
By making sure that persons entitled to use the data repository have access only to the data personal data will not be read, copied, modified or removed without authorisation.[63]
Transmission control ensures that this will not happen during electronic transmission or transport and that one can comprehend to which bodies the transfer of personal data is envisaged.[64]
Authorisation control guarantees that data processing systems are prevented from being used without authorisation.
Another danger could be that unauthorised persons can check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.[65] By setting up an input control, this risk can eliminated.
Job control ensures that the data is processed strictly in accordance with the instructions of the principal and availability control ensures that personal data is protected from accidental destruction or loss. [66]
Finally, it is important to ensure that data collected for different purposes can be processed separately.[67]

3.2 Ethical requirements

3.2.1 The doctrine of informed consent

3.2.1.1 General

It is of fundamental importance to comply not only with legal requirements, but also with ethical requirements during the whole project. The most important aspect of ethical requirements is the doctrine of informed consent.[68]
Already the common decency and the minimal respect we owe to other persons provide a justification for obtaining wherever possible an informed consent of the patient.[69]
In general, the doctrine of informed consent aims to achieve the protection of the patient's fundamental rights to autonomy and self-determination in medical interventions.[70] A human being must not be used merely as a means. Instead, one should act in accordance with the patient's wishes and respect his or her autonomy. [71]
At the core of the doctrine stands the principle that any preventive, diagnostic or therapeutic

[63] Forgó, Kollek, Arning, Kruegel, Petersen, p. 72.
[64] Forgó, Kollek, Arning, Kruegel, Petersen, p. 72.
[65] Forgó, Kollek, Arning, Kruegel, Petersen, p. 72.
[66] Forgó, Kollek, Arning, Kruegel, Petersen, p. 72.
[67] Forgó, Kollek, Arning, Kruegel, Petersen, p. 72.
[68] Forgó, Kollek, Arning, Kruegel, Petersen, p. 8.
[69] Forgó, Kollek, Arning, Kruegel, Petersen, p. 10.
[70] Forgó, Kollek, Arning, Kruegel, Petersen, p. 10.
[71] Forgó, Kollek, Arning, Kruegel, Petersen, p. 8.

medical intervention as well as scientific research may only be achieved by accepting a prior, free and informed consent.[72] Moreover, consent should be explicitly expressed and the patient shall have the right to withdraw his or her consent at any time and for any reason without any disadvantages.[73] As already referred to above, the processing of personal data is generally prohibited unless the concerned person has given consent or unless there is a legal basic which allows the processing. Since the depicted exemptions of Article 8 (3) and (4) of Directive 95/46/EC are very strict, the doctrine of informed consent with its different models plays a key role in data protection law as well as in the MyHealthAvatar project.

3.2.1.2 Historical background

The doctrine of informed consent is one of the most well known key principles in ethics.[74] But from a historical point of view for a long time patients did not have the right to decide whether his or her medical data shall be used for any medical intervention or not.[75]
Although the idea of informed consent was already developed in the sixth or fifth century A.C. in ancient Greece, it remained common not to tell the patient the truth about his or her state of health in order to not to harm the patient. This paternalistic approach prevailed until the second half of the 20th century in western countries until the social emancipation movement of the 1960th and 1970th changed this approach.[76]
Today the conception of the relationships between patient and physician is characterised by individualism, integrity and self-determination and the physicians must accept that it is the patient who has the right to decide about medical interventions. The rights to integrity and self-determination, which *form the basis for modern medical ethics*, have been affirmed as human rights by the majority of the countries in the world at the Conference on Human Rights in Vienna in 1933.[77] In 1964, the General Assembly of the World Medical Association adopted the "Ethical Principles for Medical Research Involving Human Subjects" in Helsinki, briefly called Declaration of Helsinki[78]. In that document, the General Assembly of the World Medical Association stresses the need to obtain informed consent in medical treatment and research.[79] But nevertheless it is often not clear precisely how the doctrine should be applied in different medical contexts.

[72] Forgó, Kollek, Arning, Kruegel, Petersen,p. 8.
[73] Hansson, Dillner, Bartram, Carlson, Helgesson, p. 267.
[74] Forgó, Kollek, Arning, Kruegel, Petersen, p. 8.
[75] Forgó, Kollek, Arning, Kruegel, Petersen, p. 9.
[76] Forgó, Kollek, Arning, Kruegel, Petersenp. 9.
[77] See http://www.unhchr.ch/Huridocda/Huridoca.nsf/(Symbol)/A.CONF.157.24+(Part+I).En?Opendocument.
[78] World Medical Association (1964): Declaration of Helsinki (Ethical Principles for Medical Research Involving Human Subjects) adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964, as amended by various Assemblies, last in Note of Clarification on Paragraph 30 added by the WMA General Assembly, Tokyo 2004.
[79] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24;
available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

3.2.1.3 Legal Aspects of the Doctrine of Informed Consent

The doctrine of informed consent represents not only a crucial ethical but also a legal requirement for medical research. Hence, the informed consent for ethical reasons has to meet the same standards as those for legal reasons. Even if an informed consent by the patient is not required for the processing of personal data, it is nevertheless recommendable to do it with the patient's consent in order to show respect to the patient's integrity and self-determination and besides to protect physicians against accusations and possible litigation. However it is also necessary to be able to prove the informed consent of each affected patient because Article 7 (1) of the draft of an EU data protection regulation (that is expected to supersede Directive 95/46/EC in the next couple of years)[80] provides that the controller has to bear the burden of proof for the data subject's consent. In order to meet this requirement this chapter will examine the legal aspects of the informed consent and clarify the questions, which could arise in different contexts of application.

3.2.1.3.1 General Framework

Pursuant to Article 2 (h) of Directive 95/46/EC the data subject's consent is defined as *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".
The definition shows that the patient's

- consent has to be given voluntarily,
- for a specific case and that
- the patient must be aware of the scope of consent.

Article 8 (2a) of Directive 95/46/EC stipulates that for sensitive data additionally to the above mentioned requirements the data subject must have given his or her explicit consent to the processing of those data.
Moreover the research subject has to be capable to take decisions and in many cases consent must be (in particular when it comes to clinical trials) in written form.

3.2.1.3.2 Voluntariness

Above all, consent must be given voluntarily and freely which means that the person concerned has to be self-determined while giving the consent. This requirement corresponds to the ethical requirements of the Declaration of Helsinki. The wording "*freely given […] indication*" shows that there must be no external pressure on the patient to make a certain decision.[81] This would be the case if consent would be given under external influences like coercion, duress, pressure,

[80] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art.7 para.1, available here http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.
[81] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.

manipulation or undue influence.[82] External pressure could also bear on the needed voluntariness if the patient is in a relationship of dependence with the person seeking consent.[83] This problem could also arise when the individual is in a dependent relationship relative to his or her physician. In such a situation, the Declaration of Helsinki advises to seek the informed consent by an appropriately qualified person who is completely independent of this relationship.[84]
Furthermore, the patient is able to give consent only, when he or she is has understood what will happen with his or her data when giving consent.[85] In addition, it is not relevant if the person concerned acts in his or her own interest or for the benefit of somebody else.[86]

3.2.1.3.3 For a specific case

A further requirement is that the consent must relate to a specific case. The more rights and freedoms of the patient are touched, the higher requirements concerning the degree of specification.[87]
The data subject has to know to which sort of personal data and to which activities the consent refers.[88] Besides, the Declaration of Helsinki emphasises that it is not only important to receive the consent but also of crucial significance how methods used to deliver the information are used and that it should be ensured that the data subject has understood the information.[89]

3.2.1.3.4 Awareness of the scope of consent

The data subject must be aware of the scope of consent. This means that the consent is valid only if the patient gave his or her consent in awareness of the factual situation.
By way of analogy, it is useful to consider Article 10 of Direction 95/46/EC, which enumerates the information which subsequently has to be given to the patient.

Those are:

- *the identity of the controller and of his representative, if any;*
- *the purposes of the processing for which the data are intended;*

and any further information such as

- *the recipients or categories of recipients of the data,*

[82] Brock, p. 43.
[83] Dammann, Simitis, p. 116 f.
[84] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 26, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.
[85] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.
[86] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.
[87] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.
[88] Forgó, Kollek, Arning, Kruegel, Petersen, p. 114.
[89] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24.

- *whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,*
- *the existence of the right of access to and the right to rectify the data concerning him and*
- *further information if necessary with regard to the specific circumstances in which the data are collected*

The consent is invalid if wrong or incomplete information has tempted the person to consent.

Moreover the Declaration of Helsinki notes that "*each potential subject of medical research must be adequately informed of*

- *the aims,*
- *methods,*
- *sources of funding,*
- *any possible conflicts of interest,*
- *institutional affiliations of the researcher,*
- *the anticipated benefits and potential risks of the study,*
- *the discomfort it may entail and*
- *any other relevant aspects".*[90]

Furthermore, "*the potential subject must be informed of*

- *the right to refuse to participate in the study and*
- *the right to withdraw consent to participate at any time without reprisal*".[91]

3.2.1.3.5 Capability to Take Decisions

A further requirement for the validity of the consent is that the patient in question must be capable to take decisions.[92] This is no problem when persons concerned have the legal age and are contractually capable. Then the person must agree in person and his or her consent must comply with the data processing. But there could arise some difficulties when MyHealthAvatar deals with minors or persons under disability. Then the right of self-determination is harmed. To avoid difficulties, one has to reflect under which circumstances these persons can give consent though. The Declaration of Helsinki stipulates that the patient must be able to make a decision or, when the research subject is incompetent, the

[90] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

[91] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

[92] Pedroni, Pimple, p.4; available here http://mypage.iu.edu/~pimple/sas/res/ic.pdf p.6.

physician must seek informed consent from the legally authorized representative.[93] Besides, the Declaration of Helsinki states that these persons *"must not be included in a research study that has no likelihood of benefit for them unless it is intended to promote the health of the population represented by the potential subject, the research cannot instead be performed with competent persons, and the research entails only minimal risk and minimal burden."*[94]

An authorised representative is not necessary any more when the minor is capable of insight. There is no general rule for finding out whether this is the case. Instead, it must be examined for every specific case, if the minor is able to realise the scope of his or her decision, especially if he or she is capable to understand which result his or her consent has for the data collection, processing and its use. Nevertheless we assume that a 14-years old person can be considered responsible and mature enough make this decision. As to persons under disability it can be noted that their capability will be subject to assessment by the physician.[95]

3.2.1.3.6 Written Form Consent

Generally, the Declaration of Helsinki advises to seek the person's consent in written form.[96] This is consistent with Article 4a of the German Federal Data Protection Action (BDSG)[97] that also demands the written form for every informed consent.

If the consent cannot be expressed in writing, the Declaration of Helsinki states that the non-written consent must be formally documented and witnessed.[98]As a general recommendation the written form should always be taken not only for reasons of proof, but also in order to show that the MyHealthAvatar project attaches importance to the dignity and integrity of all research subjects. A further advantage of the written form is that the patient can become aware of the importance and reach of his or her decision.

3.2.1.3.7 Right to withdraw

The Declaration of Helsinki also makes clear that the potential subject must be informed of the right to refuse to participate in the study or to withdraw consent to participate at any time without

[93] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 27, available here http://www.wma.net/en/30publications/10policies/b3/.

[94] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 27, available here http://www.wma.net/en/30publications/10policies/b3/.

[95] Forgó, Kollek, Arning, Kruegel, Petersen, p. 119.

[96] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

[97] Available here http://www.gesetze-im-internet.de/bdsg_1990/__4a.html.

[98] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

reprisal.[99] In section 6 the Declaration of Helsinki points out why the right to withdraw is so important:

"In medical research involving human subjects, the well-being of the individual research subject must take precedence over all other interests."[100]

Also from a legal point of view each data subject must have the right to withdraw his or her consent as it is referred to Art. 12 lit b) of Directive 95/46/EC. And also the draft of an EU Data Protection Regulation stipulates that the person concerned can withdraw its consent at any time:

"The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal".[101]

In conclusion it can be recommended to give the participants the possibility to revoke their consent with future effect, but that the participant must be informed that, as regards data already collected and used, it may not be possible for the consent to be withdrawn with retroactive effect.

3.2.1.4 Process of Informed Consent

Although the requirement of an informed consent in medical research projects is widely recognized, there is a significant lack of clarity as to the implementation of the process of informed consent. The procedure of giving consent contains more than just obtaining a signature of the patient.[102] It also serves the interests of the researcher to reduce the risk that a legal subject will pursue legal actions because of misunderstandings.[103] Controllers should see the need of consent as an opportunity to reduce the possibility of unhappiness and/or litigation by revealing their purposes and advising the patient of the possibility to refuse.[104] The process of informed consent is not only a formality but also the chance to reduce existing uncertainties on the part of patients and thus increase the number of participants.[105]

Most important is to make sure that the patient understands what he or she gives his consent to. The person educating the patient should create a comfortable atmosphere in which the patient is encouraged to ask questions.

The information given to the patient must not be too complex or incomprehensible in order not to

[99] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

[100] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 6, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.

[101] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art.7 para.3, available here http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[102] Clayton, Steinberg, Khoury, Thomson, Andrews, Kahn, Kopelman, Weiss, p. 1787.

[103] Clayton, Steinberg, Khoury, Thomson, Andrews, Kahn, Kopelman, Weiss, p. 1787.

[104] Clayton, Steinberg, Khoury, Thomson, Andrews, Kahn, Kopelman, Weiss, p. 1787.

[105] Geißler, Informed consent in clinical trials, available here http://www.krebsgesellschaft.de/download/forum_3.10_geisler-patientenperspektive.pdf.

overburden the patient. Therefore it is crucial that the person seeking consent is well trained in this area and that this person makes clear that the patient has the right to refuse his or her consent.

Consent can be only valid, if the patient has understood the information given by the educating person.[106] But of course, it can never be guaranteed, if the patient has fully understood the information. Therefore, it is only required that the patient must have understood the information which allows him to come to a responsible decision.[107]
If the information is comprehensible and the patient has the chance to ask the person seeking his or her consent remaining questions, the requirements for informed consent to participate in a medical research project are fulfilled.

3.2.1.5 Scope of Consent

3.2.1.5.1 General

MyHealthAvatar provides for the development of an 'avatar' that individuals will be able to use for storing health data. At the same time, data shall be used, which have been collected from clinical partners for former research projects. Hence, it is very important to clarify the scope of the consent. Although it is indisputable that law and ethics require consent, the exact scope is not clear.
This applies above all to the consent for future research purposes, which cannot be clearly defined when consent is sought.[108]
At stake are three different models of consent on which debate within the research ethics community is continuing:
- specified consent;
- broad or blanket consent; and
- tiered consent. [109]

3.2.1.5.2 Specified consent

The specified consent aims at concrete research projects whereas the broad or blanket consent contains no restrictions in respects of future projects. The tiered consent provides for different levels of authorisation in the consent process.[110]

The doctrine of a specified consent is similar to the original doctrine of consent which stipulates that patients be informed of the primary and also secondary aims of a specific research project. [111]

[106] Pedroni,Pimple, p.4, available here: http://mypage.iu.edu/~pimple/sas/res/ic.pdf.
[107] Pedroni, Pimple, p.4, available here: http://mypage.iu.edu/~pimple/sas/res/ic.pdf.
[108] Forgó, Kollek, Arning, Kruegel, Petersen, p. 12.
[109] Forgó, Kollek, Arning, Kruegel, Petersen, p. 12.
[110] Forgó, Kollek, Arning, Kruegel, Petersen, p. 12 f.
[111] Forgó, Kollek, Arning, Kruegel, Petersen, p. 13.

Moreover, patients shall be informed about the risks and benefits of their participation in the research project and must be aware of the fact that they can withdraw consent to participate at any time without reprisal.[112]
This model has the advantage that the patient's autonomy and self-determination is fully respected. But nevertheless many scholars are of the opinion that specific consent could harm the quality of research because consent would be needed for every new research project. The results of requiring a specified consent would be contrary to the interest not only of society, but also to the interest of the individual research subject as well[113] as request for re-consent are usually characterised by low response rates.[114]
Hansson et al show that it is not unlikely that many volunteers lose their interest and do not agree again.[115] A further problem arises when the volunteers have changed their contact data or are deceased.[116] As a result, these data could be lost whereby the quality of research projects would decrease extremely.
Fernandez et al point out that the model of specified consent could even weaken the idea of informed consent which is the respect for the patient's autonomy and self-determination because the amount of issues regularly listed could overstrain the patients.[117]
When datasets are to be collected and processed for several future research projects which are not yet clearly outlined, the specific consent would require that the patient must have been informed as to any special purpose for the collection, processing and use of his or her health data while giving the consent in the previous situation.
It is highly questionable if the consent given in the previous situation, could comply with these requirements

3.2.1.5.3 Broad or blanket consent

A broad or blanket consent means that patients agree to data collection and processing which is not limited to a current research project. Instead, they also agree to have their data stored and used by researchers in future projects which are not yet defined.[118]
The question arises if this model of consent neglects the patient's right of autonomy and self-determination since participants only know to a certain extent what they are agreeing to.[119] Hence, Caulfield et al argue that broad consent cannot have much legal weight because it is too vague[120].
Furthermore, the British Medical Research Council notes that this type of model could overstrain

[112] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.
[113] Buchanan, McPherson, Brody, Califano, Kahn, McCullough, Robertson, p. 12.
[114] Hansson, Dillner, Bartram, Carlson, Helgesson, p. 266 f.
[115] Hansson, Dillner, Bartram, Carlson, Helgesson, p. 266.
[116] De Montgolfier, Moutel, Duchange, Theodorou, Herve, Leport, p. 668.
[117] Fernandez, Kodish, Taweel, Shurin, Weijer, p. 2906.
[118] Forgó, Kollek, Arning, Kruegel, Petersen, p. 12 f.
[119] Hansson, Dillner, Bartram, Carlson, Helgesson, p. 267.
[120] Forgó, Kollek, Arning, Kruegel, Petersen, p. 16.

people.[121] In contrast, Wertz regards the blanket consent as acceptable as long as it is limited to diagnosis and treatment of diseases[122] and O'Neill is of the opinion that broad consent complies with the ethical requirements as long as patients know that they have the right to withdraw the consent.[123]
While the concept of a broad consent is highly debated in scholarship, a practical approach offers another view: Public opinion surveys have proven that most people accept future research with already collected data.[124] Therefore some scholars recommend this model of consent because it is not only very efficient, but also allows for the interests of patients and investigators. Moreover, the broad or blanket consent would be more cost and time efficient than a procedure which seeks to apply a specified consent.[125]
However, as long as the broad blanket is controversial, then broad consent does not offer an adequate risk-free solution.

3.2.1.5.4 Tiered consent

To overcome the above mentioned problems of consent to future research, a third type of consent, **the tiered consent**, is recommended by several scholars.
The tiered consent model allows the opportunity to choose between several alternatives on different levels which can be:

1. refusing the consent,
2. giving consent only to unidentified or unlinked use,
3. giving consent to coded or identified use for one specified research project with no further contact permitted (so further studies would be impossible),
4. giving consent to coded or identified use for one specified research with further contact permitted (so further studies would be possible),
5. giving consent to coded or identified use for future research related to the current study and
6. giving consent to coded use for any future research.[126]

The third possibility is consistent with the specified consent; and so it is with the last mentioned level as regards the broad consent.
The details are disputed in scholarship.
For example, Williams proposes to choose only between three levels which are:
1. consent for the collection, processing and use of data only for the current study,
2. consent for the current study and in addition for other related studies and
3. consent also for unrelated studies.[127]

---

[121] MRC 2004, 3.
[122] Wertz, p.58.
[123] O'Neill, p. 6.
[124] Chen, Rosenstein, Muthappan, Hilsenbeck, Miller, Emanuel, Wendler, p. 652-655.
[125] Forgó, Kollek, Arning, Kruegel, Petersen, p. 14.
[126] Forgó, Kollek, Arning, Kruegel, Petersen, p. 17.
[127] Williams, p. 454.

In contrast, Caulfield et al suggest a "step-by-step model" in which the patients have to pre-specify their consent for different uses.[128]
It is obvious that the advantages and disadvantages are congruent with those arising in respect of specified consent. This scope of consent complies with the ethical requirements, but there are practical difficulties which have to be kept in mind, e.g. high costs for obtaining re-consent and difficulties when participants change their addresses without informing the researcher.
From an ethical point of view the tiered consent should comply with the ethical requirements. This is also indicated by the Declaration of Helsinki, which does not exclude the broad consent.[129] Probably the world's biggest biomedical database UK Biobank also stipulates that patients can give permission to long-term storage and use of medical information for health-related purposes.

3.2.2 When consent cannot be achieved

The Declaration of Helsinki takes the view that physicians must normally seek consent for the collection, analysis, storage and/or reuse when they use identifiable data for medical research.[130] This is due to the fact that the doctrine of informed consent requires respecting human dignity in general as well as the patient's autonomy and self-determination in concrete.
However, situations exist where it is impossible or impractical to obtain consent for such research or situations where consent would threaten the validity of the research.[131] The Declaration of Helsinki states that in such situations the research may be done without consent, but subject to the consideration and approval of a research ethics committee.[132]
Also the Central Ethics Commission of the German Medical Association[133] argues for the need of a detailed ethical justification by the researcher when the consent of a patient does not exist.
MyHealthAvatar plans to use data rendered anonymous which means that it is only with an unreasonable effort possible or even not possible to find a connection between the data and the person concerned. In this case, the sovereignty and the right of self-determination of the person concerned are not violated because it is very unlikely that his or her identity is retraceable.

---

[128] Caulfield, Upshur, Daar, p. 1 ff.

[129] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art. 7; available here http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[130] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 25, available here http://www.wma.net/en/30publications/10policies/b3/index.html.

[131] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 25, available here http://www.wma.net/en/30publications/10policies/b3/index.html.

[132] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 25, available here http://www.wma.net/en/30publications/10policies/b3/index.html.

[133] Available here http://www.zentrale-ethikkommission.de/downloads/Patientenbezogen1.pdf.

Therefore the conclusion can be drawn that the ethical requirements of human dignity and mutual respect are observed even without consent and that anonymous data protect individual dignity and respect the patient as a person. But nevertheless it is recommended to seek the patient's consent even if his or her data shall be used in anonymised form only, because from an ethical point of view it is respectful to the patient, as well as importantly furthering public trust in medical research as a whole.
If it is not possible to obtain the consent of the patient, it corresponds to the respect for the patient, that his or her data is rendered anonymous.
Also Article 3a of the German Federal Data Protection Act (BDSG)[134] provides that personal data shall be rendered anonymous if possible and as far as the effort required is not disproportionate to the desired purpose of protection.
The principle to avoid damage to a patient is a further basic rule which has to be followed.
The idea behind this is that the person behind the data may not be harmed because he or she has agreed to the data processing. By using the data in anonymised form only this danger can be averted.

3.2.3 Summary of the ethical requirements

The Declaration of Helsinki stipulates several ethical requirements which have to be complied with.
It is crucial to achieve the informed consent of patients in medical research whenever possible in order to show respect to the patient's integrity and self-determination.
At the same time, problems may occur when the person seeking consent has given insufficient or overly-complicated information to the patient concerned.
Then the patient cannot take the decision after having traded the advantages and disadvantages of his or her consent to the collection, processing and use of health data.
Therefore it is important to provide adequate training to the person who is tasked with obtaining informed consent.
Even if a patient has not given his or her consent the ethical requirements of human dignity and mutual respect can be observed when it is very unlikely that the patient's identity is retraceable because the right of self-determination will not be violated.
Moreover, the processing of anonymous data within medical research projects targets the creation of new knowledge which will inure to the benefit of the patient.
So to sum up one can say that there are strong arguments for the ethical justifiability of the anonymisation and further use of personal data.

[134] Available here http://www.gesetze-im-internet.de/bdsg_1990/__3a.html.

4 Legal, Ethical and Security Requirements of MyHealthAvatar

4.1 General

According to the Description of Work MyHealthAvatar is the attempt to build a 4D avatar in order to represent the health status of citizens for future healthcare.[135] The 4D avatar can be helpful to support individualized prediction and treatment of patients.[136] Therefore information relating to individual citizen's health status must be collected and processed.
The MyHealthAvatar project contains two keys stage:

- The "Development Stage"
- The "Exploitation Stage"

In this chapter a provisional application to likely factual scenarios of MHA shall be shown.
It is important to note that the legal requirements can differ depending on which forms of data will be provided and who will use it for what reason. The first key stage in which data protection issues have to be illuminated is the building of the MyHealthAvatar platform.
In this phase the vision of a digital patient shall be set and tested.[137] Therefore data will be provided by USAAR , FORTH and BED.[138] BED and ICCS will store the health related data in a data repository they are building.[139] Once the platform is built up, the second key stage will be to test and finally to use the platform by setting up a clinical trial.

4.2 The "Development Stage"

The clinical partners USAAR and FORTH will provide clinical data.
Whereas USAAR will provide clinical data from patients with nephroblastoma[140], lung cancer and glioblastoma[141], FORTH will provide multi-scale data.[142]
The data for lung cancer and glioblastoma, which will be provided by USAAR, has been collected from the EC project ContraCancrum[143].
According to USAAR, USAAR has already provided this data in ContraCancrum and Tumor and is on the way to get ethical approval as well for MyHealthAvatar and CHIC from the Ethics Committee "Ethikkommission der Ärztekammer des Saarlandes". At the moment it is not clear when the ethical approval will be achieved.
The only link to personal data is kept at the USAAR and USAAR has already offered to eliminate this

[135] DoW, Part A, p. 3 of 5.
[136] DoW, Part B, p. 2 of 56.
[137] DoW, Part B, p. 11 of 56.
[138] DoW, Workplan Tables, p. 16, 18 and 19 of 40.
[139] DoW, Workplan Tables, p. 16 of 40.
[140] DoW, Workplan Tables, p. 16 of 40.
[141] DoW, Part B, p. 48 of 56.
[142] DoW, Workplan Tables, p. 19 of 40.
[143] DoW, Part B, p. 48 of 56.

link if this would be helpful.
FORTH informed us via e-mail that it will provide medical imaging data (normally MRI) either or molecular analysis data (e.g. microarray data) high resolution genotyping, or even extended genome sequence data (exome or personal genome) for a small number of patients or volunteers. At the moment, it is not yet clear if the multi-scale data is anonymised or pseudonymised.
ICCS will develop a repository of models and data repository of multi-scale data exploitable by the models in order to support the multi-scale cancer models stored in the model repository.[144]
The repository will contain data provided by USAAR from other projects, such as ACGT, p-medicine, ContraCancrum, Tumor, etc.[145] According to the Kick off Meeting minutes the data will include image and histological data for a number of selected clinical cases, such as nephroblastoma and can be used to predict tumor growth and response to drug. The data have passed though de-identification and pseudo-anonymisation processes.[146] Only authorised persons will have access to the content of the data and the model repositories. [147]
BED will collect data from online patient diary which will be used by volunteers.[148] The intention is to use them to demonstrate the functions of visual data analysis.[149] Additionally, it is planned to create two websites in order to collect citizen's life style, environment, and activities related data and to use mobile phones to collect data such as blood pressure, temperate and heart beat.[150] Moreover, it is planned to purchase data from social networks.[151] At a later stage, BED will build a data repository to store health related data of citizens collected from the web and mobile apps such as information as to patient's life style, diet, and other clinical related information.[152] Therefore a number of tailored information extraction tools for the web and mobile apps shall be developed.[153]
BED informed us via e-mail that synthetic data will form a key resource at the first stage of the project. The collected data will be used to create a synthetic data layer. The public would not have access to the collected data. They will only have access to the synthetic data.
The synthetic data will create virtual persons or so called artificial populations. It will be mainly in a tabular structure - each virtual individual will have an ID gender, age, his/her life styles (smoking, drink), symptoms, treatment etc. All of them will be simulated. These synthetic data will follow the statistical distributions that have been studied from real data. Therefore, BED will use medical and health datasets. In addition, it will also have recourse to social network data like tweets and emails datasets, which shall be used as sample data to support the development of toolkits. It should be emphasized that there is a rationale behind the data for example, for a certain age and certain gender; the artificial population will show a correct distribution of a certain disease. Hence, there

[144] DoW, Workplan Tables, p. 16 of 40.
[145] DoW, Workplan Tables, p. 16 of 40.
[146] DoW, Workplan Tables, p. 16 of 40.
[147] DoW, Workplan Tables, p. 16 of 40.
[148] DoW, Workplan Tables, p. 18 of 40.
[149] DoW, Workplan Tables, p. 18 of 40.
[150] DoW, Workplan Tables, p. 18 of 40.
[151] DoW, Workplan Tables, p. 18 of 40.
[152] DoW, Workplan Tables, p. 18 of 40.
[153] DoW, Workplan Tables, p. 18 of 40.

will be value to users to log into the avatar system, and to see these cases. From the research point of view, the synthetic data provides population data on which it is possible to perform research in data storage (data base) and data analysis.

4.2.1 Ethical and Legal Considerations

4.2.1.1 National Data Protection Law

Legal starting point is the Data Protection Directive that is transposed into national law of each project partner.
Concerning USAAR, the implementing law is the German Federal Data Protection Act (BDSG)[154], in the case of FORTH the relevant law is the Greek Law on Protection of individuals with regard to the processing of personal data[155] and in the case of BED the implementing law is the Data Protection Act of 16th July 1998[156]

4.2.1.2 USAAR

As already mentioned USAAR will provide data that has been collected from the EC project ContraCancrum. The German Federal Data Protection Act is restrictive on the question of reuse of data for secondary research purposes. Pursuant to § 39 (1) of BDSG personal data subject to professional or special official secrecy and provided by the body obligated to secrecy in the performance of its professional or official duties may be processed or used by the controller only for the purpose for which they were received. The body obligated to secrecy must give its consent to any transfer to a private body. This rule is due to the principle of frugal use of sensitive data. According to § 39 (2) BDSG the data may be processed or used for another purpose only if the change of purpose is permitted by special legislation. § 14 (2) No. 9 stipulates the rule for public bodies that recording, alteration or use for other purposes shall be lawful only if necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.
This requirement shows the importance of balancing interests between research and patient privacy and self-determination.[157] Section 40 (1) of BDSG states in Part IV "Special provision" of the Act that personal data collected or recorded for purposes of scientific research may be processed or used only for purposes of scientific research.
Moreover, personal data shall be rendered anonymous as soon as the research purpose allows pursuant to Section 40 (2) of BDSG. Until then, the features enabling the attribution of information

[154] Available here http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf.
[155] Available here http://www.privireal.org/content/dp/greece.php.
[156] Available here http://www.legislation.gov.uk/ukpga/1998/29/contents.
[157] Kühn, p.130.

concerning personal or material circumstances to an identified or identifiable person shall be kept separately. They may be combined with the information only to the extent required by the research purpose. Concerning data processing by public bodies Section 19a (1) of BDSG notes that the data subject shall be notified of such, recording the identity of the controller and the purposes of collection, processing or use, if the data is collected without his or her knowledge. The data subject shall also be notified of recipients or categories of recipients except where he or she must expect transfer to such recipients. If a transfer is planned, notification shall be provided no later than the first transfer. An exemption is made in Section 19a (2) of BDSG. There it is stated that a notification is not necessary if the data subject already has this information, notifying the data subject would involve a disproportionate effort, or recording or transfer of personal data is expressly laid down by law. The controller shall stipulate in writing the conditions under which notification shall not be provided in accordance with no. 2 or 3.
As to data processing by private bodies and commercial enterprises Section 33 of BDSG stipulates that the data subject shall be notified of such recording, if personal data are recorded for own purposes for the first time without the data subject's knowledge. According to Section 33 (2) of BDSG notification shall not be required if the data subject has become aware of the recording or transfer by other means, recording or transfer is expressly laid down by law or recording or transfer is necessary for the purposes of scientific research and notification would require a disproportionate effort. At state level, similar provisions prohibit data processing for secondary purposes. Related to USAAR, which is located in Saarland, Section 13 of the Data Protection Act of Saarland would be relevant as well.

4.2.1.3 FORTH

As to FORTH, the relevant law is the Greek Law on Protection of individuals with regard to the processing of personal data.[158] There it is stated that processing of sensitive data is generally prohibited, unless one of the exceptions provided in it is applicable. Pursuant to Article 7(2)(a) the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, will be permitted by the Authority, when the data subject has given his or her written consent, unless such consent has been extracted in a manner contrary to the law or bonos mores, or if law provides that any consent given may not lift the relevant prohibition. Article 7 (1) notes that in general, the collection and processing of sensitive data is prohibited. But Article 7 (2) (f) makes an exemption for the case that processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken.
To summarize, data processing is allowed when there is consent of the data subject.
In the case that the data subject has not given consent, the data can be used nevertheless for the purposes of scientific research as long as all necessary measures are taken for the protection of the data subjects. It is not clear what the lawmaker means by "necessary measures" and if "anonymity is maintained" means that the data must be anonymised or if it is enough to protect the data by pseudonymisation.

[158] Available here http://www.privireal.org/content/dp/greece.php.

4.2.1.4 BED

BED will collect data from online patient diary which will be used by volunteers and build a data repository to store health related data of citizens collected from the web and mobile apps at a later stage. In the UK, the reuse of data for research purposes is governed by the Data Protection Act of 16th July 1998[159].

Schedule 1, Part 1 sets out the data protection principles.

No. 1 states that "*personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—(a)at least one of the conditions in Schedule 2 is met, and(b)in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met*."

The most important condition which is met in Schedule 2 is mentioned in no. 1: *"The data subject has given his consent to the processing."* And also Schedule 3 stresses the importance of an explicit consent to the processing of the personal data of the data subject.

From this legal implementation the conclusion can be drawn that it is crucial to obtain consent from the volunteers.[160]

In addition, Schedule 1, Part 1, no.2 stipulates that "*personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*".

Section 33 of the Act sets some legal requirements re the processing of personal data for research purposes. So Section 33 (1a) and (1b) of the Act set "relevant conditions", which include that data may not be processed to support measures or decisions with respect to particular individuals and that the data may not processed in such a way that substantial damage or substantial distress is, or is likely to be.

Pursuant to Section 33 (2) of the Act data processing may not be regarded as incompatible with the purposes for which they were obtained, if this data is processed for research purposes in compliance with the relevant conditions ensuring patient privacy.

According to Section 33 (3) of the Act, personal data may be kept indefinitely, if the personal data which are processed only for research purposes are in compliance with the relevant conditions.

Section 33 (4) of the Act states that, if the personal data is processed in compliance with the relevant conditions and the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them, personal data which are processed only for research purposes are exempt from section 7. Section 7 of the Act is about the right of access to personal data. This means that data subjects are prevented from having the right to access processed information, if the research results are not made public in such a way that individual data subjects can be identified from this information.

According to Section 33 (5d) of the Act, personal data shall not be treated as processed for other than research purposes, if they are disclosed *"to any person, for research purposes onl*y", Section 33 (5a), *"to the data subject or a person acting on his behalf",* Section 33 (5b), *"at the request, or with the consent, of the data subject or a person acting on his behalf"* ,Section 35 (5c), *"or in circumstances in which the person making the disclosure has reasonable grounds for believing that*

[159] Available here http://www.legislation.gov.uk/ukpga/1998/29/contents.

[160] See also 4.2.3.2 "Freely given consent".

the disclosure falls within paragraph (a), (b) or (c").
Lastly, it should be pointed out that personal data must not be processed unless an entry in respect of the data controller is included in the register maintained by the Commissioner, Section 17 (1) of the Act.

4.2.2 Scope of the Data Protection Directive

First of all, it is crucial to find out, if the processing of the data provided by USAAR and FORTH falls within the scope of the Data Protection Directive.
According to Article 2 lit. a) Directive 95/46/EC "personal data" is defined as "*any information relating to an identified or identifiable natural person, ('data subject')*". An "**identifiable person**" is "*one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".
If the data provided were non-personal data no further requirements would be need to be adhered to be proceed.
According to recital 26 a person is not identified or an identifiable person, if the data concerned is rendered anonymous, means that the information cannot be linked to an identifiable person using reasonably likely means. The Working Party defines anonymous data "*as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking into account all of the means likely reasonably to be used either by the controller or by any other person to identify that individual. Anonymized data would therefore be anonymous data that previously referred to an identifiable person, but where that identification is no longer possible*. "[161]
It depends on the surrounding circumstances in which data is processed, whether data can be regarded as being anonymous. By implementing sufficient safeguards such as access controls and privacy impact assessments, the anonymity of project data can be ensured.
Especially important is that it is guaranteed that a patient will not re-identified from the patient's data.

4.2.2.1 Data provided by USAAR

According to the Description of Work, USAAR will provide anonymised data concerning glioblastoma and lung cancer.[162] This would mean that the data protection Directive is not applicable.
As far as LUH is presently advised, there is still a link to the personal data kept at the USAAR.
This shows that, at the moment, these data is probably not irreversibly coded, but that there is a key for re-identifying the data when required. As a result, the Data Protection Directive would be

[161] Opinion 4/2007, p. 21.
[162] DoW, Part B, p. 48 of 56.

applicable.
USAAR informed us via mail that it is in the process of obtaining an ethical approval for using data concerning lung cancer and glioblastoma in MyHealthAvatar and CHIC.
This fact could also indicate that the data is not anonymised, but pseudonymised.
If the data is pseudonymised, a legal basis would therefore be needed which can be an informed consent or a legal exemption. As referred above, the legal exemption of Article 8 (4) of Directive 95/46/EC could apply when no consent has been obtained and sensitive data shall be processed.
Concerning the molecular data, it appears that these data cannot be linked to a specific patient. Assuming this is correct, and that secure access control is in operation these data may properly be regarded as anonymised, so that the Data Protection Directive is not applicable.

4.2.2.2 Data provided by FORTH

At the moment, it is not yet clear if the multiscale data being collected is anonymous or pseudonymous. It will need to be further ascertained if the data will contain information with the reasonable possibility of re-establishing a link between the multiscale data and the patient. From an ethical point of view it is preferable to remove retraceable information because by this the patient's privacy can be fully protected.

4.2.2.3 Data collected by BED

BED is collecting data which will be used to create a synthetic data layer (fake data) in order to create virtual persons or so called fake populations. Therefore BED uses medical and health datasets, but also social network data like tweets and email datasets which shall be used as sample data to support BED to develop toolkits attract some health related information from them.
The twitter and email data will not be directly stored in MHA data repository. They are going to be used in order to investigate the possibility of automatic extracting useful information (health related) from the twitter and email of the citizens. To develop these techniques, BED will need some experimental data. That is the purpose of having these data.
The medical and health datasets are in anonymous form since it is not reasonably possible to identify the concerned patients individually and hence the datasets are not personal data for the purposes of the data protection rules.
By contrast, the tweets and e-mails probably are not rendered anonymous, and will thus fall within the terms of Directive 95/46/EC, and the UK Data Protection Act.[163]
Admittedly, with respect to the tweets it depends on the context and if the tweets contain any information relating to an identified or identifiable person. Anyhow it is at least probable that there will be some tweets that disclose such information.
The e-mails definitely are personal data because though they are stripped of their contents, they reveal the names of senders and recipients and as LUH presently understands one can also comprehend when the transmission took place.

[163] Available at http://www.legislation.gov.uk/ukpga/1998/29/contents.

4.2.2.4 Summary

It is likely that some of the envisaged data processing within MHA, with particular respect to the tweets and e-mail data to be used by BED and the multiscale data provided by FORTH, will need to be considered and justified under the data protection legal framework.
To ensure certainty, LUH encourages BED and FORTH to obtain ethical approvals from the responsible authorities in their respective jurisdictions to them. In the case of FORTH, this should pertain to the proposed transfer and use of its multiscale data for the purposes of the project. In respect of BED, an important issue relates also to the need for ethical approval to establish an on-site data repository, which will later contain some personal data. As the manager of this repository, BED will fulfil the definition of "data controller" under the EU Directive, with responsibility for safeguarding and securing the data from misuse.
Throughout, the onus will also be upon BED and FORTH and the project consortium to show a good reason for needing to use these data.
As to the clinical data provided by USAAR, there could also be personal data since there is still a link kept at the USAAR. But USAAR has already offered to destroy the link. If no consent has been obtained, we suggest as a minimum essential requirement the need to anonymise the data.
Furthermore, USAAR is on the way to obtaining ethical approval as well for MyHealthAvatar.
Sometimes the research purpose demands that data cannot be anonymised.
If this is the case, personal data should be pseudonymised prior to the processing operation which means using a reversibly coded data and that an official channel for re-linking the data remains.
If the data cannot be anonymised, one should guarantee that the data is secure.
Therefore it is important to think about how the risk of identification can be reduced to a minimum.

4.2.3 Consent

As has been discussed in part 3 of this deliverable, in order to respect the individual's right of autonomy and self-determination the patient's consent should be sought wherever reasonably possible. Moreover, this behaviour emphasises that the patient is regarded as an autonomously participating subject. Also the Declaration of Helsinki classifies the search for consent as good ethical practice.[164] So whenever possible, consent should be sought by the partners providing or collecting personal data.
Besides legal and ethical considerations, practical reasons argue for the patient's consent as well because the fact of the patient's approval of the data processing constitutes very important information about him or her. The fact, if the patient agrees in further data processing can serve as an indicator, that when later approached as an eligible potential participant, the patient will more likely consent to participate.

[164] See http://www.wma.net/en/30publications/10policies/d1/], principles 9 and 10.

4.2.3.1 Data provided by USAAR

Even if the data offered by USAAR is anonymised the data use in MHA must be compatible with the original consents at time data collected. Otherwise there could problems occur relating to the ethical requirements.

Physicians usually are obliged to seek consent for the collection, analysis, storage and/or reuse of health data for medical research.[165] This is due to the fact that common decency and the minimal respect we owe to other persons require making sure that the patient's rights as autonomy and self-determination are not infringed.[166]

So in general, it can be said that, as far as possible, the patient's consent should be sought in order to respect the patient's right of autonomy.

As previously discussed, the doctrine of informed consent stresses that "*any preventive, diagnostic, or therapeutic medical intervention is only acceptable with prior, free and informed consent of the person concerned, based on adequate information*".[167]

Also the Declaration of Helsinki stipulates that "*in medical research involving competent human subjects, each potential subject must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, and any other relevant aspects of the study*."[168] In addition, the patient must be informed of the right to refuse to participate in the study or to withdraw consent to participate at any time without reprisal and it is crucial to ensure that the patient has understood the information. [169]

To sum up, the patient must be informed of the project which plans to process his or her data and due to this information the patient must be able to understand which consequences his or her consent can have.

According to the data provided by USAAR patients should have understood that their data also will be used in future research projects.

Problematical could be the fact that in the situation when giving consent for the EC project ContraCancrum the patient could not know exactly what would happen to his or her data in the MyHealthAvatar project.

It is controversial if the allusion to the fact that the patient's data could be used for future research projects is sufficient to comply with the ethical requirements.

In the ethical discourse, as discussed in part 3, different models of consent have been designed for which reason the scope of consent is controversial.

However, notwithstanding the question which type of consent USAAR has used for seeking consent

---

[165] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 25, available here http://www.wma.net/en/30publications/10policies/b3/index.html.

[166] Forgó, Kollek, Arning, Kruegel, Petersen, p.8.

[167] Forgó, Kollek, Arning, Kruegel, Petersen, p.8.

[168] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/30publications/10policies/b3/index.html.

[169] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 24, available here http://www.wma.net/en/30publications/10policies/b3/index.html.

for the EC project ContraCancrum, it should be pointed out that the Declaration of Helsinki notes that "*there may be situations where consent would be impossible or impractical to obtain for such research or would pose a threat to the validity of the research. In such situations the research may be done only after consideration and approval of a research ethics committee*."[170]
For example, the public interest in improving public health could outbalance the individual's interests to give consent when it is impossible or impractical to seek consent due to the sample size of the research cohort or the use of retrospective data.
USAAR informed us via mail that it plans to create new data for lung cancer and glioblastoma for the research project CHIC and plans to re-use these data in MyHealthAvatar. Since USAAR endeavours an approval of an ethics committee as well there should be no difficulties with the compliance of legal requirements. Moreover, the research exemption of Article 8 (4) of the Directive 95(46/EC could apply if no consent has been obtained. Therefore the data processing must take place for reasons of substantial public interest. Recital (34) of the Directive stipulates that public interest includes areas such as public health and social protection and scientific research and government statistics.
But in addition to compliance with legal requirements, it should be also guaranteed that the project respects ethical requirements. The WMA suggests the need for ethics committee approval if there are any doubts concerning patient consent to inclusion in the database. Due to this fact, it is always recommendable to seek and obtain the approval of its ethics committee to the data processing in question.

4.2.3.2 Freely given consent

WP6 will need some volunteer participants who will be involved in the data collection through their use of social media and from mobile apps.
Therefore BED plans to build some social network to get some followers, e.g. MyHealthAvatar Facebook or MyHealthAvatar Twitter.
Concerning the volunteers it is crucial to stress that the volunteers' consent must be given freely. This is pursuant to Article 2 (h) of Directive 95/46(EC where it is stated that consent is *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".
But also from an ethical point of view it is crucial that the consent is given freely which means that consent must be given in a self-determined action without any external influences.[171] It does not suffice that there are no external forces because pressure can be also achieved by an internal relation of dependence with the physician, for example.[172]
The Declaration of Helsinki states that "*participation by competent individuals as subjects in medical research must be voluntary. Although it may be appropriate to consult family members or*

[170] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 25, available here http://www.wma.net/en/30publications/10policies/b3/index.html.
[171] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.
[172] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.

community leaders, no competent individual may be enrolled in a research study unless he or she freely agrees."[173]
In addition, the Declaration stipulates that "*research on patients or healthy volunteers requires the supervision of a competent and appropriately qualified physician or other health care professional."*[174]
So to sum up, LUH recommends attaching great importance to guarantee the freedom of decision-making while seeking consent during WP6.

4.2.4 Security requirements

As already mentioned ICCS will build a data repository to support the model repository. The data will have passed though the necessary de-identification and (pseudo)-anonymisation processes.
In addition, BED will build a data repository to hold health related information which has been collected from web and mobile apps.
In the MHA Description of Work, it is stressed that only authorized persons shall have access to the content of the data and the model repositories. Appropriate authentication and authorization mechanisms will be implemented according to the directives of WP3.
These mechanisms are required for the secure storage of data and models and their associated information into the MyHealthAvatar repositories and also for the secure retrieval of this information by the MyHealthAvatar platform.
Since all individuals have the right to privacy and may thus expect that confidentiality and protection of their personal information will be rigorously upheld[175], it is crucial to safeguard the security of the data in the repository during the whole MyHealthAvatar process and especially when the data layer is built up.
According to Article 16 of 95/46/EC "*any person acting under the authority of the [data] controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.*"
Article 17 of 95/46/EC states that the Member States must provide that all technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access are undertaken.
In addition, "*having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected*", Article 17 no. 1 of 95/46/EC.
Concerning MyHealthAvatar it can be stated that clear guidelines should be set as to the data processing and that the data transfer should permit access and processing only as long as is

[173] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 11, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.
[174] World Medical Association, Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 1964, sec. 16, available here http://www.wma.net/en/20activities/10ethics/10helsinki/.
[175] WP131, see: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, page 21.

absolutely necessary.
Also the Recommendation on the Protection of Medical Data[176] of the Committee of Ministers to Member States, R(97)5, recommends appropriate technical and organisational measures to protect personal data against accidental or illegal destruction, accidental loss, as well as against unauthorised access, alteration, communication or any other form of processing.[177] Such appropriate measures are access control, transmission control, authorisation control, input control, job control and availability control.[178]
Although it is not yet clear how the data layer will be built exactly, it can be already pointed out that the authorised persons have to comply with appropriate state of the art security safeguards at any time while dealing with the data.
Not only in reference to the data layer, but also while developing the MyHealthAvatar platform, security guidance policies must always be respected.
Therefore Privacy enhancing technologies (PETs) should be applied as much as possible in order to protect personal data. This opinion is also supported by the Article 29 Working Party, which stresses in its Working Document on the processing of personal data relating to health in electronic health records (EHR) that "*privacy enhancing technologies (PETs) should be applied as much as anyway possible in order to promote personal data protection*."[179]
Particularly, the legal framework concerning security measures should foresee the necessity of

"*• the development of a reliable and effective system of electronic identification and authentication as well as constantly up-dated registers for checking on the accurate authorization of persons having or requesting access to the EHR system;*
• comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorization;
• effective back up and recovery mechanisms in order to secure the content of the system;
• preventing unauthorized access to or alteration of EHR data at the time of transfer or of back up storage, e.g. by using cryptographic algorithms;
• clear and documented instructions to all authorized personnel on how to properly use EHR systems and how to avoid security risks and breaches;
• a clear distinction of functions and competences concerning the categories of persons in charge of the system or at least involved in the system with a view to liability for shortcomings;
• regular internal and external data protection auditing."[180]

In order to ensure compliance with these provided guidelines, it should be guaranteed that security features will be analysed in every project phase and that recognised state of the art standards will be complied with.

[176] See http://www1.umn.edu/humanrts/instree/coerecr97-5.html.
[177] http://www1.umn.edu/humanrts/instree/coerecr97-5.html, at 9.1 ff.
[178] Forgó, Kollek, Arning, Kruegel, Petersen, p. 72.
[179] WP131, see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.
[180] WP131, see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf at 19-20; see also the Commission's Communication on Promoting Data Protection by PETs (COM(2007) 228 final, at http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf.

One example could be the ISO/IEC 27001:2005[181], which also contains appropriate state of the art privacy enhancing technologies.
Furthermore, the EHR systems must be established in full compliance with the principles of protection of personal data, as enshrined in Directive 95/46/EC.[182]

4.3 The "Exploitation stage"

In the exploitation stage the MyHealthAvatar platform will be set up.
The detailed implications of this stage of the project, which is still well in the future, will be fully analysed in good time in the future relevant WP 11 deliverables. However, an aspect already worth highlighting is the possibility at that stage that some of the patients, who provided data for the validation of the project, may decline to take part further in any research. If this is the case, their wish must be respected and their data may not be transferred to the MyHealthAvatar avatar. From a legal angle, data processing can be done without consent if the data is rendered anonymous because in this case, the Data Protection Directive does not apply.
But from an ethical point of view it is recommended not to use the data even in anonymised form in order to respect the patient's right of self-determination.
Data from other patients, who are happy to participate in the continuing medical research and provide their medical data, can be used and stored without any concerns.

[181] http://www.iso.org/iso/catalogue_detail?csnumber=42103.
[182] WP131, see: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf, p. 21 f.

5 Conclusion

MyHealthAvatar is an interface that will give access to new and existing integrative models and data to support clinical applications. Another application of MyHealthAvatar is to offer tools and useful clinical data through the avatar to encourage the engagement of both medical professionals and patients. Nevertheless, the setting up of a sound legal framework must be ensured so as to allow clinical and other data to be transferred, accessed, and maintained under a secure virtualization application. By doing so it will provide an important reference for medical professionals to make personalized clinical decisions without compromise ethical and legal issues that might be raised or come to pass throughout the development of the models or in the treatment of patients.
The possibilities to find, retrieve, and reuse all of the data; information and knowledge of patients and their physiological attributes have a clear potential to engage ethical and legal concerns. Therefore, in order to show respect to the patient's integrity and self-determination, it is crucial to achieve the patient's consent, whenever possible. In this regard, when organizing volunteers to participate the research in this task, great importance should be attached to the fact that the consent is given freely.
However, situations exist where it is impossible or impractical to obtain consent.
The Declaration of Helsinki states that a consideration and approval of a research ethics committee could help to make the research still possible.
But nevertheless legal requirements must also be considered in such a case. As referred above, the legal exemption of Article 8 (4) of Directive 95/46/EC could apply when no consent has been obtained and sensitive data shall be processed. Therefore the data processing must take place for reasons of substantial public interest.
The legal exemption of Article 8 (3) of Directive 95/46/EC cannot serve as a legal basis for the processing of sensitive data for purposes of medical research because the term "medical research" is not mentioned in Article 8 (3) of Directive 95/46/EC and the relevant processing must be for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature.

In addition, ethical standards require that data should render anonymous in order to respect the sovereignty and the right of self-determination of the person concerned.
Moreover, and independently of the issue of consent, the patient's privacy must always be protected. In this context it is important to think about how the risk of identification can be reduced to a minimum, by the use wherever possible of anonymous (or at least securely pseudoymised) data consistent with the achievement of the project outcomes. Therefore Privacy enhancing technologies (PETs) should be applied as much as possible.

6 References

[1] Brock D W (1993): Life and death, Cambridge: Cambridge University Press

[2] Buchanan A, McPherson E, Brody B A, Califano A, Kahn J, McCullough N, Robertson JA (2002): Pharmacogenetics: ethical and regulatory issues in research and clinical practice, Consortium on Pharmacogenetics. Report on the Consortium on Pharmacogenetics: Finding and Recommendations

[3] Caulfield T, Upshur R E G, Daar A (2003): DNA databanks and consent: a suggested policy option involving an authorization model, *BMC Medical Ethics,* 4, 1-4

[4] Chen D T, Rosenstein D L, Muthappan P, Hilsenbeck S G, Miller F G, Emanuel E J; Wendler D (2005): Research with stored biological samples. What do research participants want? *Archives of Internal Medicine,* 165, 652-655.

[5] Clayton E W, Steinberg K, Khoury M J, Thomson E, Andrews L, Kahn M J E, Kopelman L, Weiss J O (1995): Informed consent for genetic research on stored tissue samples, *Journal of the American Medical Association*, 1786-1792

[6] Dammann Ulrich, Simitis, Spiros (1997): EG-Datenschutzrichtlinie, Baden-Baden: Nomos-Verlagsgesellschaft

[7] De Montgolfier S, Moutel G, Duchange N, Theororou I, Herve C, Leport C, APROCO Study Group (2002): Ethical reflections on pharmacogenetics and DNA banking in a cohort of HIV-infected patients, *Pharmacogenetics,* 12 (9), 667-675

[8] Fernandez C V, Kodish E, Taweel S, Shurin S, Weijer C, Children's Oncology Group (2003a): Disclosure of the right of research participants to receive research results: an analysis of consent forms in the Children's Oncology Group, *Cancer*, 97 (11), 2904-2909

[9] Forgó N, Kollek R, Arning M, Kruegel T, Petersen I (2010): Ethical and Legal Requirements for Transnational Genetic Research, München: C.H.Beck Verlag

[10] Geißler J (2010) : Informed consent in clinical trials, *FORUM,3,* 56-59

[11] Hansson M G, Dillner J, Bartram C R, Carlson J A, Helgesson G (2006): Should donors be allowed to give broad consent to future biobank research? *Lancet Oncology,* 7, 266-269.

[12] Kühn H C (2004): The Implementation of the Data Protection Directive 95/46/EC in Germany, in: Beyleveld et al., Implementation of the Data Protection Directive in Relation to Medical Research in Europe, 121-140

[13] O'Neill O (2003): Some limits of informed consent, *Journal of Medical Ethics*, 29, 4-7

[14] Pedroni J A, Pimple K D (2001): A Brief Introduction to Informed Consent in Research with Human Subjects, The Trustees of Indiana University
available here http://mypage.iu.edu/~pimple/sas/res/ic.pdf

[15] Pöttgen, N (2009): Medizinische Forschung und Datenschutz, Frankfurt am Main: Peter Lang GmbH

[16] Wertz D C (1999): Archived specimen: A platform of discussion, *Community Genetics,* 2, 51-60

[17] Williams (2001): Informed consent in genetic research, Croatian Medical Journal, 42 (4), 451-457

Appendix 1 – Abbreviations and acronyms

ACGT	Advancing Clinico-Genomic Trials on Cancer
Art.	Article
BED	University of Bedforshire
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
CHIC	Computational Horizons in Cancer
ContraCancrum	Clinically oriented translational cancer multilevel modelling
EC	European Community
EEA	European Economic Area
e.g	exempli gratia/for example
EHR	Electronic Health Records
EPOF	European Privacy Officers Forum
etc.	et cetera
EU	European Union
f.	following page
ff.	following pages
FORTH	Foundation for Research and Technology Hellas
ICCS	Institute of Communication and Computer Systems
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
lit.	litera/letter
LUH	Leibniz Universitaet Hannover

miRNA	micro-ribonucleic acid
MRC	Medical Research Council (UK)
MRI	magnetic resonance imaging
no.	number
p.	page/pages
PETs	Privacy enhancing technologies
p-medicine	From data sharing and integration via VPH models to personalized medicine
sec	Section
TUMOR	Transatlantic Tumour Model Repositories
UK	United Kingdom
USAAR	Universitaet des Saarlandes
WMA	World Medical Association
WP	Work Package