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

Project acronym: MyHealthAvatar

Deliverable No. D11.1
The ethical and legal framework of MyHealthAvatar

Grant agreement no: 600929

Dissemination Level		
PU	Public	**X**
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)	

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:	The ethical and legal framework of MyHealthAvatar
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	PU
Version:	1
Actual Submission Date:	28.02.2015
Editor: Institution: E-Mail:	Prof. Dr. Nikolaus Forgó LUH forgo@iri.uni-hannover.de

ABSTRACT:
This deliverable provides an overview of the applicable European data protection framework and relevant ethical guidelines. In addition, guidelines for patient-specific computer-based models will be presented.

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

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

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**
0.1	15.01.2015	Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen
0.2	22.01.2015	Draft	Ass.-iur. Alan Dahi
0.3	29.01.2015	Draft	Dr. Marc Stauch
0.4	06.01.2015	Draft	Dipl.-Jur. Sarah Jensen
0.5.	20.02.2015	PreFinal Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen
0.6	24.02.2015	Review Draft	Prof. Dr. Norbert Graf (USAAR), Prof. Dr. Feng Dong (BED)
0.7	27.02.2015	Final Draft	Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.-iur. Alan Dahi

List of LUH contributors

- Prof. Dr. Nikolaus Forgó
- Dipl.-Jur. Sarah Jensen
- Dr. Marc Stauch
- Ass.-iur. Alan Dahi

Contents

1 Executive Summary

The MyHealthAvatar (MHA) project is a research and demonstration-oriented iterative study. It will examine the feasibility of creating personal health records configured as digital patients. The vision is to set up a 4D avatar representing the health status of patients over time and encouraging the engagement of both medical professionals and patients. Since the 4D avatar will allow health and other data collection, sharing, access 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.

Some of the data that is going to be used will be anonymous, other will not, which means that personal data will be processed to some extent and that the Data Protection Directive (and its relevant national transposition) will be applicable. Thus, data protection issues will have to be considered from a legal perspective as well from an ethical point of view. Therefore, we will not only analyse European rules, but also national rules concerning security and privacy protection.

2 Introduction

The primary focus of MyHealthAvatar is to present a platform for citizens and patients that enables them to organise and access their own health and lifestyle data in a clear and useful manner and thereby take greater control over health risks and therapies, through following sound preventive strategies to reduce the chance of a condition arising, and in the self-management of existing conditions. In the process the system will offer tools and applications to empower the patient in following and understanding their health needs, and allowing them to share data within e.g. patient support groups, and with relevant treating physicians in a genuinely collaborative approach.

In addition the patient-specific computer-based models and tools offered by the MyHealthAvatar infrastructure are becoming increasingly significant in medical research because it is hoped that they can improve diagnosis and optimise clinical treatment by predicting outcomes of therapies and surgical interventions.[3] The purpose of these models is mostly to facilitate access to patient data and to offer analysis tools that run on that data to underpin the clinical decision making process and to improve treatment of diseases.[4]

Although there are already projects funded by the European Union such as Discipulus[5] and Computational Horizons in Cancer (CHIC)[6], there has been – compared to the research in the technical and medical field – little research into the required legal and ethical requirements in this context. But especially privacy and data protection issues can arise in the context of patient-specific computer-based models when sensitive health data are used. Furthermore, there is a potential risk that patients could follow poor advice because the model does not provide an accurate forecast or that doctors rely on the information stored in the model. Thus, liability issues could arise as well.

Against this background, this deliverable is composed with the intention to clarify the ethical and legal requirements, which have to be followed within the parameters of the MHA project.

The following Chapter 3 constitutes an overview of what the MHA project is aiming to do. Afterwards, in Chapter 4, we will offer an abstract introduction to the key legal principles that will be applicable in the MHA project. Here the Data Protection Directive (95/46/EC)[7] 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 dwell on the different legal bases that must be complied with when sensitive data is processed. Afterwards the need for a fair data processing will be pointed out, including the need for de-identification so far as compatible with the purpose of use, data minimisation and limited retention.

[3] Neal, Kerckhoffs, p. 111.

[4] Zasada, Wang, Haidar, Liu, Graf, Clapworthy, Manos, Coveney, pp. 314–327.

[5] See the DISCIPULUS project roadmap for the digital patient, http://www.digital-patient.net/files/DP-Roadmap_FINAL_N.pdf

[6] See http://chic-vph.eu/.

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

Also other duties on the data controller will be outlined such as information, access, correction and data security. Beyond that, in Chapter 5, key ethical requirements will be analysed. The main focus will be the issue of the user's consent highlighted also from a legal perspective, but also aspects such as respect for autonomy, feedback for research info and the need for avoiding harm will be pointed out.

Thereafter Chapter 6 will apply the legal and ethical principles discussed to the development and piloting of the MHA platform in concreto. The course that should be followed by each project partner to comply with the rules and principles, which have been outlined in the part beforehand will be indicated. In this regard, an analysis will be performed of the application of the salient rules to the high end use scenarios, data linkage and architecture (including proposed use of cloud computing).

In terms of future exploitation following the development and piloting of the platform, the key legal requirements of security, privacy and autonomy will also be addressed. In this context, potential threats to informed consent will be examined, as well as the question of how user control can be achieved and how active consent can be protected through computer security measures.

3 Overview of MHA

MyHealthAvatar will offer access, collection and sharing of long term, longitudinal personal health status data through a digital representation, a so-called avatar.[8] It will help deliver clinical analysis, prediction, prevention and treatment tailored to the individual citizen, all while giving the citizen full control over her own personal health data.[9]

The architectural platform will be designed as an integrated facility that allows numerous functionalities rather than just storing data.[10] Besides internal data repositories that need to be built to allow the individual to store data in the avatars ICT utilities shall be used to support data collection with minimal user input; an ICT toolbox shall support clinical decisions by using simulation models and visual analytics and a local cloud solution shall support quick data transfer.[11]

3.1 Repositories

There are two sets of repositories existing, emanating from WP5 and WP6, respectively: WP 5 "Models and repositories" (Task Leader ICCS) deals with the development of clinical oriented repositories,[12] which will be used to support the execution of the simulation models of the project.[13] Here there are two repositories being developed: a data repository of multiscale data and a repository of special biomechanics and tumour growth and response to treatment.[14] The latter was previously deployed in the TUMOR[15] (Translantic Tumor Model Repositories) project.[16]

ICCS is analyzing the integration of MHA with ObTiMA, a clinical trial support system.[17] In order to facilitate the presentation of this data, and optimize utility for platform users, FORTH has been developing state of the art visualization technologies and methodologies for the envisaged 4D health avatar implementation.[18] A visual data analysis suite to support data analysis in an avatar centric view around the avatar models is going to be built.[19] Moreover, a software toolbox is going to be developed to analyze multiscale images.[20]

For its part, the WP 6 repository (Task Leader BED) is the central repository of the project, and aims at storing health related data of individual citizens such as lifestyle data, diet, geographical

[8] DoW, Part A, p. 3 of 5.

[9] DoW, Part B, p. 2 of 56.

[10] D3.2, p. 5.

[11] D3.2, p. 5.

[12] D1.3, p. 12.

[13] D1.3, p. 12.

[14] D1.1, p. 14.

[15] See http://www.tumor-project.eu/.

[16] D1.3, p. 12.

[17] D1.3, p. 13.

[18] D3.1, p. 8.

[19] D1.1, p. 19.

[20] D1.1, p. 19.

environment, but also family histories and other risk factors[21] collected from the web and mobile apps.[22] Currently volunteers – who signed an informed consent form developed by WP 11 – are already uploading their data collected by devices such as Fitbit.

As part of the development phase, the consortium has registered accounts with popular social networks such as Twitter, Facebook and Google[23] that publish status messages and that are created to retrieve easily user information. Moreover the data repository has been established to support the current version of the MHA platform.[24] Moreover, BED is building a semantic data repository based on the Linked Data approach to support data searching and processing.[25]

3.2. Cloud Infrastructure

In the MHA project a cloud infrastructure shall support data processing by utilizing resources with individual institutions.[26] The reason for adopting this solution is the far higher processing capacities that are thereby enabled. At the same time, since the cloud is going to be used in healthcare, specific needs concerning security, privacy and legality must be considered.[27] In this regard, the Project will take full account of the data protection issues raised by cloud-based data processing, as discussed by the Article 29 Working Party (WP29) (set up under the Directive)[28] in its Opinion 2012[29]. The WP29 analysis and recommendations are detailed in section 4.4.3, and include the concern that commercial public clouds do not comply with sound data protection requirements because of their inherent legal and ethical limitations[30], arising from lack of control by the client over data processing operations.

Accordingly a private cloud has been tested; in this context FORTH is deploying a private cloud in order to host the project's chimeric synthetic data (see 3.4 below). Additionally, BED uses a new public cloud server (Linode based in London which is officially rented by ANS to host the MHA platform infrastructure, and the lifestyle data collected by the health tracker (Fitbit, Withings, Moves) pilot studies. Subsequently it is intended that each cloud will contain a copy of the entire MyHealthAvatar system and data. The cloud infrastructure FORTH is using has been designed as privately-deployed and considers both security issues in biomedical research and the possibility to outsource the infrastructure to commercial cloud computing facilities.[31] A local cloud infrastructure

[21] D1.1, p. 15.

[22] D1.3, p. 14.

[23] D6.1, p. 18.

[24] D1.3, p. 14.

[25] D1.1, p. 16.

[26] D1.3, p. 9.

[27] D3.1, p. 52.

[28] The party is made up under Article 29 of Directive 95/46/EC. According to Article 2 of Directive 95/46/EC the European body consists of the head of the data protection authorities of all 28 member states and helps European stakeholders to better understand the European data protection law by issuing so called opinions.

[29] See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[30] D3.1, p. 6.

[31] D1.1, p. 12; D1.3, p. 10.

is being built to support data processing by utilizing resources within individual institutions. MHA will utilize the latest architecture technology on cloud ensuring high information security.[32]

3.3. Data linkage

As discussed above, one aim of MHA is to develop data collection utilities, and to experiment with the Linked Data approach, so patients do not have to undertake large efforts themselves to populate the data repository with health-related data, which instead can be collected mainly by mobile apps such as Fitbit and Moves.[33] FORTH is providing a methodology for the integration of collection with external sources such as existing data and model warehouses, social networks and hospital records.[34] As to the latter, the architecture seeks to support the export of health-related patient's data from linked hospitals, through facilitating a gateway with the EPSOS project[35]. This will make it technically feasible for queries generated in the MHA system to be forwarded to hospital information systems with patient consent to transfer of relevant requested data.

In the meantime, an integrated data collection platform for users has been built to retrieve third-party health information to MHA data repositories.[36] There are not only links between the MHA platform and Facebook and Twitter, but also between the MHA platform and GoogleDrive, Fitbit and Moves, allowing for information exchange between each other. With respect to Twitter, linking has been completed in the direction Twitter to MHA.[37] The other way has not yet been completed, as well as other linkings. The wearable device Fitbit, and the Moves application have been integrated into the MHA platform[38] because they allow collection of large-scale timely personal health information.[39] In the near future, Withings, iHealth and probably other sensors such as Medisana will be integrated.[40] Moreover, an online patient diary has been designed, which would facilitate the collection and presentation of data from such devices and applications, as well as self-inputted user data. Currently, BED is working on Intelligent Textbox to allow smart data input without any huge user effort.[41]

3.4 Synthetic data

A set of Java applications has already been implemented into the data repository and has generated web users and synthetic avatars. A hundred web user accounts were generated according to the synthetic data such as user id and gender.[42] MyHealthAvatar considers user avatars at the scale of

[32] D3.1, p. 6.

[33] D1.3, p. 14.

[34] D1.1, p. 11.

[35] See http://www.epsos.eu/.

[36] D6.1, p. 6.

[37] D1.3, p. 10.

[38] D1.3, p. 14.

[39] D6.1, p. 5.

[40] D1.3, p. 14.

[41] D1.3, p. 14.

[42] D1.1, p. 16.

big data, i.e. as a hub for integrating many disparate kinds of health and lifestyle data to offer an increasingly complete picture of the patient's health and lifestyle activities. The platform will also permit the data to be accessed by patient-specific computer-based models and tools offered by the MyHealthAvatar. Neal and Kerckhoffs define patient-specific modelling as "the development of computational models of human pathophysiology that are individualized to patient-specific data".[43]

From a technical point of view, given the attendant demands on data processing capacity, it is reasonable to investigate NoSQL approaches. Here Cassandra Java client library Astyanax and Cassandra[44] will be used.[45]

As regards the synthetic data, this will simulate virtual persons within so called artificial populations. This is mainly presented in a tabular structure - each virtual individual will have an ID gender, age, his/her life styles (smoking, drinking habits), symptoms, treatment etc. In some cases the project will use anonymized images from real patients who will give consent that FORTH can collect from the involved clinicians. These data will – stripped bare of all original accompanying data – be integrated with new simulated data values (chimeric synthetic data). These synthetic data follow the statistical distributions that have been studied from real data. 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 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.

3.5 Data used for use cases and High End Clinical Demos

In order to show the benefits of MHA use cases and scenarios have been collected within the first 6 months in WP 2, a preliminary "user needs" analysis was presented in D2.2. Subsequently, there has been a reduction to a final set of refined use cases described in WP 7 "Use cases" (based on the initial collection from WP 2) and a demonstration of all the use cases of D7.1 demonstrated through 4 High End Clinical Demos in D9.1.

There are two partners providing clinical data to the MHA project:
FORTH has collected full scale and comprehensive datasets (images) to cover a range of cancer diseases.[46] For this purpose FORTH officially collaborates with clinicians who provide the data. The images take the form of perfusion imaging (T2*/T1) of brain gliomas and diffusion MR imaging in histological classification of soft tissue sarcomas, which will be transformed into chimeric synthetic data (see above).[47] Furthermore, full genome data will be analyzed. This data is based on blood by completing genotyping snp6 (1 million snps). It is also planned to work on genotyping for

[43] Neal, Kerckhoffs, p. 111

[44] See http://cassandra.apache.org.

[45] D1.1, p. 15.

[46] D1.3, p. 15.

[47] D1.3, p. 15.

predisposition regarding drug metabolism and on tissues by generating gene expression profiling-afymetrix and cancer molecular mutation profiling

For its part, partner USAAR is providing de-identified data molecular data from patients with nephroblastoma (utilising synergies with the associated CHIC project in so far as the ethical approval USAAR has received in August 2013 allows data sharing between MHA and CHIC). ObTiMA guarantees data safety and security.[48] So far, no personal (as opposed to synthetic and/or securely de-identified) data have been used, and nor is such data use envisaged for WP5 during the lifetime of the MHA project.

3.6 Data from volunteers

In order to investigate how individuals respond to the MHA platform in WP6, BED has recruited volunteers who have agreed to provide lifestyle data for evaluating the MHA platform and its technology, in particular by transferring such data from the devices Fitbit and Withings and the apps Moves and MyTracks. Two more apps are planned for the high end use scenarios (diabetes and CHF).

[48] D9.1, p. 39.

4 Introduction to key legal principles

The following chapter provides an introduction to the key legal principles concerning data protection that are applicable in general to projects such as MHA that utilize personal health and other data within the EU. In chapter 6 there will then be an analysis applying this concretely to what should be done in order to comply with those rules and principles in the particular context of MHA. At present the legal rules are undergoing reform, with the EU Directive 95/46/EC that currently provides the template for member state rules in this area due to be replaced by a new General Data Protection Regulation[49] in the next few years. The Regulation is currently at an advanced stage in the EU legislative process, with the Council of Ministers considering amendments made by the European Parliament to the original 2012 Commission Proposal. However, it remains uncertain what the outcome will be in terms of the substantive legal rules. For this reason, as well as the fact that the MHA project will most likely conclude prior to the commencement of the Regulation, the focus of analysis in the present Deliverable will remain Directive 95/46/EC (hereafter 'the Data Protection Directive').

4.1 Scope of the Data Protection Directive

The Data Protection Directive[50] aims at protecting the right to privacy individuals enjoy by regulating, amongst others, the "processing of personal data wholly or partly by automatic means".[51] It is the major source for the legal requirements that need to be met when processing personal data throughout the territory of the EU/EEA. In this connection, 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".

Personal data is defined in Article 2 (a) of the Data Protection Directive 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". By contrast, if the data is not to be seen as being personal, the Data Protection Directive does not apply.

Accordingly one should begin by considering further the conditions under which a piece of information will be considered as "personal data". In determining this question, the four parts of the Directive's definition have to be considered cumulatively. The Article 29 Working Party (WP29)

[49] See http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CD0QFjAB&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdata-protection%2Fdocument%2Freview2012%2Fcom_2012_11_en.pdf&ei=6JFyUuTjHcaHtAbP7YDIDQ&usg=AFQjCNGtks6MyKe5X0GWIghrB6xfF3g8wA&bvm=bv.55819444,d.Yms.

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

[51] Article 3 (1) Directive 95/46/EC.

undertook such a cumulative analysis in its Opinion 4/2007,[52] which provides persuasive guidance on the matter.

According to the WP29, the first element of the definition, “any information” requires a broad interpretation regardless of the nature or content of the information and of the format or medium in which the information is presented.[53] It includes any sort of statements about a person irrespective of the correctness of the information.[54]

The second part “relating to” clarifies that the information must relate to the individuals it is about.[55] This element is crucial in order to determine the substantive scope of the concept, especially in relation to new technologies.[56] There are situations where it is not obvious whether the information “relates” to an individual, e.g. when the data concerns material objects in the first instance, but those objects belong to someone.[57] Here, in order to decide when the data “relate” to an individual, the opinion 4/2007 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.[58] 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 evaluated for each specific data item on its own merits and within the particular context.[59]

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,[60] whereas the second component is pertinent when it is possible to distinguish a person from the group although he is not identified yet.[61] “Identifiers”, which permit identification, can be particular pieces of information that hold a particularly privileged and close relationship with the particular individual.[62] Article 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.[63] 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.[64]

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

[53] Opinion 4/2007, p. 6.

[54] Opinion 4/2007, p. 6

[55] Opinion 4/2007, p. 9.

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

[57] Opinion 4/2007, p. 9.

[58] Opinion 4/2007, p. 10

[59] Opinion 4/2007, p. 12.

[60] Opinion 4/2007, p. 12.

[61] Opinion 4/2007, p. 12.

[62] Opinion 4/2007, p. 12.

[63] Opinion 4/2007, p. 13.

[64] Opinion 4/2007, p. 14.

Indirect identification is relevant when a unique combination of several identifiers allows a certain person to be singled out,[65] e.g. the combination of gender, date of birth and address.

The attribute "identifiable" is qualified in Recital 26 of Directive 95/46/EC by the statement that "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." It follows that a person will not count as identifiable when "means likely reasonably to be used" do not exist, and consequently the information here cannot be considered as personal data.[66] 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 organisational dysfunctions (e.g. breaches of confidentiality) and technical failures.[67] The effect of this qualification is to rule out the purely theoretical possibility of data being associated with a given individual from making it personal data.

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.[68] 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.[69] It also has to be taken into account that the assessment of "reasonably likely means" is likely to change over time. Thus any data processing system purporting to make use only of non-identifiable (and hence non-personal) data will need to demonstrate its ability to adapt to new developments as they happen by incorporating the appropriate technical and organisational measures.

The fourth element of the definition of personal data from the Directive is the term "natural person". Here a question arises as to whether this aspect means that only data from living data subjects are eligible for protection. If so, once a subject has died one could argue that this "former" personal data falls outside the ambit of the Directive. On the other hand, it is apparent that such data – e.g. medical information in a patient record – may have implications for other persons than the deceased, such as surviving family members.[70] On this basis, as well as the frequent uncertainty in practice as to whether a given data subject is still living, it may be preferable to regard all persons as putative data-subjects and for the use of their data be treated as subject to data protection rules.

4.2 Need for lawful processing under data protection law

A basic principle in the Data Protection Directive according to Article 7 is that the processing of personal data requires to be justified by reference to a legal basis (enumerated in Article 7 (b) - (f) of the Directive, or the data subject has given consent according to Article 7 (a).

[65] Opinion 4/2007, p. 13.

[66] Opinion 4/2007, p. 15.

[67] Opinion 4/2007, p. 15.

[68] Opinion 4/2007, p. 17.

[69] Opinion 4/2007, p. 17.

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

This basic rule also applies to data concerning health, which belong to the category of sensitive data as stipulated in Article 8 of the Directive. Since sensitive data contains information affecting the privacy interests of a data subject more than other data does[71], Article 8 of Directive 95/46/EC includes a stronger protection for such data. Thus in Article 8 (1) of Directive 95/46/EC it is stated that Member States shall prohibit the processing of this category of personal data, but this is then subject to a number of strictly drawn exemptions, allowing such processing to occur in certain limited circumstances.[72] These exemptions set out in Article 8 paragraph 2 ff of the Directive 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:

“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[73] and according to Article 8 paragraph 6, the Member State has to let the Commission know.

In addition, Article 8 (3) of the Directive 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.” At the same time it remains open how far this provision would provide a more general exemption in relation to the use of personal health records (PHRs) for purposes that go beyond the direct individual treatment and care of the patient. In this regard, its requirement for the data to be

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

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

[73] Working Document on the processing of personal data relating to health in electronic health records, p. 12; see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.

processed by a health professional also limits the scope of application.[74] The question then how far Article 8 (3) might serve to legitimate the types of processing of health data envisaged in the MyHealthAvatar project will be analysed in more detail in Chapter 6 below.

4.3 Need for fair processing

Besides the need to show a lawful processing basis, various legal requirements are also imposed on the data controller that go to the fairness of the processing. Pursuant to Article 2 (d) of the Data Protection Directive the controller is "a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

The Directive 95/46/EC stipulates in Article 6 the need for fair processing which include the need for limited retention, de-identification, and data minimization. According to the principle of limited retention of data, which is stipulated in Article 6 (1) (e) of Directive 95/46/EC data must be kept "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". This means that data should be erased as soon as it is no longer needed for the purposes for which it was collected. If it is planned to continue using the data, data should be anonymized or at least pseudonymized (together with the adoption of necessary technical and organizational data security measures to prevent re-identification) in order to ensure a lawful storage.[75] If data shall be stored for longer periods for scientific use, appropriate safeguards need to be taken pursuant to Article 6 (1) (e) (sentence 2).

A further legal requirement of data protection law is that data so far as compatible with the purpose of use has to be de-identified prior to use according to Article 6 (1) (c) and (e) of Directive 95/46/EC. If there is no way to re-link the data to an individual, it loses its status of personal data. Instead, it is anonymous data then. We have previously considered the definition of the concept of personal data under Art 2 (a) of the Directive, as persuasively interpreted by the WP29 (see 4.1 above); however, given the relevance of the (non-) identifiability of data for the fairness of its processing (including for later secondary purposes not part of the original collecting rationale), the key techniques for de-identifying data are examined further below.

4.3.1 anonymized data

As noted above, pursuant to Recital 26 of Directive 95/46/EC, the protective regime it sets out is not applicable to data rendered anonymous in such a way that the data subject is no longer identifiable, i.e. the link that refers to the data subject is irrecoverably erased. According to the Article 29 Working Party anonymous data is "any information relating to a natural person where the person <u>cannot be identified</u>, whether by the data controller or by any other person, <u>taking into account all</u>

[74] Pöttgen, p. 55.

[75] Handbook on European data protection law, p. 73; see http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.

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."[76] So the major criterion for determining what efforts can be used for verification of de-identification is the question how likely it is to identify the individual. According to the opinion 4/2007 by the Article 29 Working Party the criterion of "all means likely reasonably to be used either by the controller or by any other person" should take into account all factors at stake such as 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 organisational dysfunctions (e.g. breaches of confidentiality) and technical failures.[77]

In this connection, though, it should be underlined that the Directive is very likely applicable with regard to the process of anonymizing personal data itself, as this would count as data processing. Furthermore, in terms of sensitive health data, it has to be considered that parties such as insurances and employers could have high interests in health data and could have the opportunity and motivation to re-identify this data indirectly, through data-matching, even where direct identifiers that refer to the patient on the face of the data have been removed.

4.3.2 pseudonymized data

In practice, anonymizing data is sometimes more or less impossible or might not be compatible with the purpose of use. This will often be true, for example, in the context of personalised health care environment (in which the services aimed for by the MHA project will operate): here the provision of individually targeted advice information requires the system to distinguish accurately between users and associate the right data with the relevant user. In this context, a more practical approach could be the use of "pseudonymous data". The Data Protection Directive does not mention this term but it is legislatively recognised in the Draft General Data Protection Regulation. The current draft of the General Data Protection Regulation defines pseudonymous data in Article 4 (2a) as "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution".

Similarly, the Article 29 Working Party refers to pseudonymous data in its opinion 4/2007 on the concept of personal data and defines pseudonymization as "the process of disguising identities"[78] and gives some examples how pseudonymization 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 anonymized data).[79] The Working Party points out that retraceable 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.[80]

[76] Opinion 4/2007, p. 21.

[77] Opinion 4/2007, p. 15.

[78] Opinion 4/2007, p. 18.

[79] Opinion 4/2007, p. 18.

[80] Opinion 4/2007, p. 18.

So in conclusion it can be said that the common understanding of pseudonymized data is that there are reversibly coded data and that an official channel for re-linking the data remains. Thus, pseudonymous data is in the Working Party's view personal data, subject to the terms of the Directive. However pseudonymization can be viewed as a good solution for protecting the privacy of the data subject if organisational and technical safeguards prevent them from being re-identified.

4.3.3 Principle of purpose limitation

The European data protection regulation relies upon the principles of purpose limitation and the minimization of personal data collection.[81]

The principle of data minimization derives from Article 6 (1) (b) and (c) of Directive 95/46/EC and states that data controllers shall collect only the personal data they really need and keep it only for as long as they need it.[82] The data controller should limit the collection of personal data to what is directly relevant to accomplish a specified and legitimate purpose.[83] Moreover the personal data should be kept not longer than necessary for the purposes the data has been collected for cf. Article 6 (1) (c) of Directive 95/46/EC.

The principle of purpose limitation is in the same direction and means that once the data is collected for specified, explicit and legitimate purposes it must not be further processed in a way incompatible with the purposes at collection according to Article 6 (1b) of the Data Protection Directive. Article 6 (1) (b) (sentence 2) of Directive 95/46/EC states that further processing of data for scientific purposes shall not be considered as incompatible as long as the controller compensates for this change by implementing appropriate safeguards. However pursuant to opinion 03/2013[84] of the Article 29 Working Party the provision should not be read as a general authorization to further process because all relevant circumstances and factors need to be included and furthermore it must be ensured that the processing has a legal basis in one of the grounds listed in Article 7 and complies with other important requirements stipulated in Directive 95/46/EC.[85]

Among the appropriate safeguards one should consider taking specific additional security measures such as encryption and restricting access to personal data only on a need-to-know basis.[86] The more easily the data subject can be identified, the more additional safeguards may be required[87] and the more sensitive the data are, the more should be done to limit the possibilities of re-identification in addition to the need for additional safeguards.[88]
In terms of further processing of personal data concerning health, the Article 29 Working Party

[81] De Andrade, Monteleone, p. 131.

[82] De Andrade, Monteleone, p. 131.

[83] De Andrade, Monteleone, p. 131.

[84] See Opinion 03/2013 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[85] Opinion 03/2013, p. 28.

[86] Opinion 03/2013, p. 32.

[87] Opinion 03/2013, p. 32.

[88] Opinion 03/2013, p. 32.

states that consent of the data subject is required.[89] Any exceptions to this requirement for consent should be specified in law, with appropriate safeguards, including technical and organizational measures to prevent undue impact on the data subjects.[90] In case of doubt, the processing should be subject to prior authorization of the competent data protection authority. Exceptions should only apply with regard to research that serves an important public interest, and only if that research cannot possibly be carried out otherwise.[91] Here it should be stressed that it is highly relevant to implement appropriate safeguards to reduce the risk of identification to a minimum. If the research purpose demands that data cannot be anonymized, the personal data should be pseudonymized (using reversibly coded data) and the data controller needs to guarantee that the data is secure.

These principles will be relevant in the context of MyHealthAvatar, where the information residing in the platform is constituted of diverse sources of data collected in different ways and at different points in time. This raises questions of the compatibility of data reuse, in order for such reuse for additional purposes still to amount to fair processing under Article 6 (1) (b) of the Data Protection Directive. The application to the project of the relevant principles, which have been implemented with some local variations at member state, will be examined more fully in Chapter 6.

4.4 Other Duties on the Data Controller

In addition to the duties of fair and lawful processing that are enumerated in Articles 6, 7, and 8 of Directive 95/46/EC, its subsequent provisions impose a number of further and independent obligations upon the data controller.

4.4.1 Information to be given to the data subject

One such further obligation is the duty to provide the data subject with information at the time of collecting data from him. Pursuant to Article 10 of Directive 95/46/EC the data controller has to inform the data subject about the identity of the controller and of his potential representative, the purposes of processing and further information the data subject could need for a fair processing such as who will receive the data and that the data subject has the right of access to and rectify the data concerning them.

Article 11 of Directive 95/46/EC enumerates the information the data controller has to give the data subject when he did not receive the data from the data subject. The information is again the identity of the controller, the purposes of processing and further information, e.g. categories of data concerned, recipients and the existence of the right of access to and the right to rectify the data concerning the data subject. Article 11 also states that the controller has to inform the data subject at the latest when the data is first disclosed, better when personal data is recorded or its disclosure to a third party is envisaged.

[89] Opinion 03/2013, p.32.

[90] Opinion 03/2013, pp. 32 f.

[91] Opinion 03/2013, pp. 32 f.

4.4.2 Data subject's right of access to data and rectification, erasure and blocking

Article 12 (a) refers to the data subject's right of access, which includes obtaining confirmation from the controller as to whether data concerning the subject are being processed and what the purposes are. Here the latter is entitled to know the categories of data concerned and the recipients of data, which data is being processed and what the data source is. Further he should be informed if there is an automated data processing intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability and conduct, the knowledge of the logic involved. The data controller is required to inform the data subject without constraint at reasonable intervals and without excessive delay or expense.

Furthermore the data subject can demand from the data controller the rectification, erasure or blocking of data, if the data processing does not comply with the rules stipulated in Directive 95/46/EC, cf. Article 12 (b) and notification to third parties to whom the data has been disclosed of any rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort, cf. Article 12 (c).

4.4.3 Security of data processing, including in the cloud 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 pseudoymized) data consistent with the achievement of the project outcomes. In this regard privacy enhancing technologies (PETs) should be applied as much as possible.[92] Moreover Article 17 (1) of Directive 95/46/EC must be considered that states that the Member States must provide that all technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access are undertaken. Also the opinion 03/2013 of the Article 29 Working Party states that the data controller has to adopt appropriate safeguards to ensure that the privacy interests of the data subject are protected so far as reasonably possible.[93] The measures have to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, but also considering state of the art and the cost of implementation. Sensitive medical data deserve high protection as third parties might have high interest in the data. In similar vein, the (non-binding) Council of Europe Recommendation on the Protection of Medical Data[94] R(97)5, recommends appropriate technical and organizational measures to protect personal data against accidental or illegal destruction, accidental loss, as well as against unauthorized access, alteration, communication or any other form of processing.[95] These measures shall ensure an appropriate level of security taking into account the technical state

[92] WP131, p. 19.

[93] Opinion 03/2013, p. 3.

[94] See http://www1.umn.edu/humanrts/instree/coerecr97-5.html.

[95] Recommendation No. R (97) 5 on the Protection of Medical Data; at 9.1 ff.

of the art and also of the sensitive nature of medical data and the evaluation of potential risks.[96] Such appropriate measures are access control, transmission control, authorization control, input control, job control, and availability control.[97]

Given that, as discussed in Chapter 3, the MyHealthAvatar platform plans to utilize a cloud computing infrastructure, it is germane to conclude this Chapter by anticipating some specific issues of security arising in that context. Here it is important to distinguish between the data controller and the data processor. Whereas the data controller is the person who determines the purposes of processing, cf. Article 2 (d) of Directive 95/46/EC, the cloud provider, who processes the personal data on behalf of the controller, fulfils the definition of a processor, which is stipulated in Article 2 (e) of the Data Protection Directive. Since the onus is upon the data controller to comply with the rules stipulated in the Directive 95/46/EC there are relevant aspects the data controller should consider.

Firstly, it is important to know what national law is applicable. Article 4 (1) (a) of the Data Protection Directive stipulates that the law applicable is defined by reference to the place of establishment of the data controller. Secondly, Article 17 (3) of Directive 95/46/EC must be taken into account as it is stated there that the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller. Moreover, the processor (cloud provider) must implement technical and organizational measures to adequately safeguard personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The Article 29 Working Party Opinion 05/2012 on cloud computing[98] states that a contract between the cloud client and the cloud provider should also include, inter alia, details on the security measures the cloud provider has to comply with.[99] Here it is important to stress that this depends on the risks that occur when processing and the nature of data.[100] As already referred to the level of security measures has to be a high one when sensitive medical data is processed. The technical and organizational measures have to be concretized.[101] Moreover the client's instructions have to be issued to the provider, and purpose of data processing and the nature of personal data processed have to be provided by the cloud provider. Furthermore it must be ensured that personal data are erased when the cloud client requests this.[102] This is in particular important if the data subject withdraws consent to continued data storage and use. Then the host must be sure that the cloud provider deletes the data for sure. In addition it should be regulated that only authorized persons of

[96] Recommendation No. R (97) 5 on the Protection of Medical Data; at 9.1.

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

[98] See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[99] Opinion 05/2012, p. 12.

[100] Opinion 05/2012, pp. 12 f.

[101] Opinion 05/2012, p. 13.

[102] Opinion 05/2012, p. 13.

the cloud provider may have access to the data and that the provider supports the data controller in facilitating exercise of data subject's rights to access, rectify or erase the data.[103] Another important aspect is that there should be a clause guaranteeing that the cloud provider does not disclose the data to third parties.[104] It is also critical that the cloud provider provides a list of locations where the data may be processed.[105] With respect to MHA this is important because it is recommendable to store the data in the EU only.

Concerning technical and organizational measures, Article 17 (2) of the Data Protection Directive should also be mentioned, which covers the delegation of some processing activities by the controller to other parties and states that "the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures."

[103] Opinion 05/2012, p. 13.

[104] Opinion 05/2012, p. 13.

[105] Opinion 05/2012, p. 13.

5 Ethical aspects

5.1 The doctrine of informed consent

The MyHealthAvatar platform aims to attract citizens and patients to contribute their data and make use of the offered tools and services in an empowered and autonomous manner. This implies that users must have trust and confidence in the workings of the system and the benignity of its aims and objectives. In this regard it is of fundamental importance not only to comply with legal requirements, but also architect the platform infrastructure so as to comply with ethical requirements in a transparent and demonstrable fashion. The most important aspect of ethical requirements is the doctrine of informed consent.[106]

Already the common decency and the minimal respect we owe to other persons provide a justification for obtaining wherever possible informed consent from the patient.[107] 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.[108] 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 right of self-determination.[109] At the core of the doctrine stands the principle that any preventive, diagnostic or therapeutic medical intervention as well as scientific research may only be achieved by accepting a prior, free and informed consent.[110] 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.[111]

5.2 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 interventions on capable patients, aimed at diagnosis, treatment, care and medical research. As regards non-physical operations that touch upon the patient's autonomy and privacy by involving use of his data, then, as discussed in Chapter 4, this too requires a legal basis, either in the form of explicit consent (under Article 8 (2) (a) of the Data Protection) or as a necessary ancillary aspect of professional medical care under Article 8 (3). Similarly, non-interventional research using data alone, may as we have seen be permitted in the public interest, subject to appropriate safeguards at member state level, pursuant to Article 8 (4) of Directive 95/46/EC. However, even if – given the existence of such alternative processing bases – an informed consent by the patient is thus not legally required for the data processing in question, 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 build trust, as well as protecting physicians and technicians against later accusations and possible litigation.

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

[107] Forgó, Kollek, Arning, Kruegel, Petersen, p. 10.

[108] Forgó, Kollek, Arning, Kruegel, Petersen, p. 10.

[109] Forgó, Kollek, Arning, Kruegel, Petersen, p. 10.

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

[111] Hansson, Dillner, Bartram, Carlson, Helgesson, p. 267.

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 user must be aware of the scope of consent.

Voluntariness 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[112]. There must be no external pressure on the patient to make a certain decision,[113] and the patient must not suffer disadvantages if consent is refused or withheld. This would be the case if consent were given under external influences like coercion, duress, pressure, manipulation or undue influence.[114] External pressure could also bear on the needed voluntariness if the patient is in a relationship of dependence with the person seeking consent.[115]

The consent attains the requisite specificity if the data subject knows to which sort of personal data and to which activities the consent refers.[116] The more rights and freedoms of the patient are borne upon, the higher the requirements concerning the degree of specification.[117] In this context, the Declaration of Helsinki emphasises that it is not only important to obtain consent as a matter of form, but also of crucial significance what methods are used to deliver attendant information to the data subject, and that it should be ensured that the latter has understood the information.[118]

5.3 Scope of consent

The data subject is aware of the scope of consent if he grants 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 (as discussed above at 4.4.1).

The consent is invalid if wrong or incomplete information has tempted the person to consent. Moreover, in relation to the research use of health data, the Declaration of Helsinki notes that the data subject must be "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".[119]

[112] The "Ethical Principles for Medical Research Involving Human Subjects" in Helsinki, briefly called the Declaration of Helsinki, was adopted by the General Assembly of the World Medical Association in 1964 and stresses the need to obtain informed consent in medical treatment and research; see http://www.wma.net/en/30publications/10policies/b3/.

[113] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.

[114] Brock, p. 43.

[115] Dammann, Simitis, pp. 116 f.

[116] Forgó, Kollek, Arning, Kruegel, Petersen, p. 114.

[117] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.

[118] Declaration of Helsinki, sec. 26.

[119] Declaration of Helsinki, sec. 26.

To know the scope of consent is particularly important to determine whether a patient is happy for a secondary use of data to take place (as opposed to its original use in respect of the patient's own treatment and care). Thus, in the context of MyHealthAvatar, it could be that controllers of the infrastructure would like to process data to produce generalised advice for other patients with similar conditions, or to develop models for future research purposes, but cannot define clearly these purposes when asking for consent.[120] In this regard there are three different models of consent on which debate within the professional healthcare and research ethics community is focused: specified consent, broad or blanket consent, and tiered consent. [121] As presented further in the following subsections, the first type of consent aims at informing the patient of concrete research and other contemplated data uses at the point of data collection. By contrast, the broad consent seeks a 'once and for all' authorisation by the patient of future use, and contains no restrictions in respects of future uses. The tiered consent offers a hybrid approach, by allowing different levels of authorisation in the consent process.[122]

5.3.1 Specified consent

The doctrine of a specified consent is similar to the original doctrine of consent which stipulates that persons concerned be informed of the primary and also secondary aims of a specific processing purpose.[123] This model has the advantage that the individual's autonomy and self-determination is fully respected. But nevertheless many scholars are of the opinion that specific consent could harm the quality of secondary data use, as consent would be needed for every new projected usage. Accordingly, in a context such as non-interventional medical research, 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[124] as requests for re-consent are usually characterised by low response rates.[125] Moreover, a specific consent could overstrain volunteers because of the amount of information.[126]

5.3.2 Broad consent

A broad consent means that individuals agree to data collection and processing for future projects, which are not yet defined.[127] Groups such as TMF[128] argue for broad consent as the only way to make sure that the fullest and most beneficial use of medical data (including, increasingly, those facilitated by 'big data' applications) occurs, thereby enabling both better care for the individual patient and the advancement of medical science in general.[129] This is also indicated by the

[120] Forgó, Kollek, Arning, Kruegel, Petersen, p. 12.

[121] Forgó, Kollek, Arning, Kruegel, Petersen, p. 13.

[122] Forgó, Kollek, Arning, Kruegel, Petersen, pp. 12 f.

[123] Forgó, Kollek, Arning, Kruegel, Petersen, p. 13.

[124] Buchanan, McPherson, Brody, Califano, Kahn, McCullough, Robertson, p. 12.

[125] Hansson, Dillner, Bartram, Carlson, Helgesson, pp. 266 f.

[126] Fernandez, Kodish, Taweel, Shurin, Weijer, p. 2906.

[127] Forgó, Kollek, Arning, Kruegel, Petersen, pp. 12 f.

[128] See http://www.tmf-ev.de/

[129] Comment on the draft by the European Parliament regarding A regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, p. 7; see

Declaration of Helsinki, which does not exclude broad consent.[130] Some scholars argue that blanket consent cannot be considered true consent, because individuals do not know exactly what they are agreeing to.[131] Others regard this kind of consent acceptable as long as individuals know that they have the right to withdraw the consent.[132]

In terms of the draft of the General Data Protection Regulation it is not yet clear if broad consent will be accepted legally.[133] However, this matter will be kept under review as the legislation moves forward, and any necessary changes to the MHA consent processes flagged accordingly. In this regard, a possible approach, combining broad and specific consent in a manner attuned to the individual patient's informational needs could also be offered by 'tiered consent', considered next.

5.3.3 Tiered consent

To overcome the above mentioned problems of consent to unforeseen secondary data uses, including future research, a third type of consent, the tiered consent, has been recommended by some legal scholars and bioethicists. The tiered consent model allows the opportunity to choose between several alternatives on different levels[134], e.g.

1. consent for the collection, processing and use of data only for an immediate contemplated purpose;
2. consent for the current purpose and in addition for other related purposes and studies (where these may be regarded as compatible with the original use);
3. consent also for unrelated purposes and studies (including ones potentially raising new implications for the data subject and/or others).[135]

Another possibility would be to allow the individuals to pre-specify their consent for different uses.[136] 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 subjects change their addresses without informing the data controller.

5.4 Additional requirements in respect of secondary (research) data usage

There are a number of further ethical requirements listed in the Declaration of Helsinki that, while directed in the first instance at participation in medical research projects, may be regarded as

http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDMQFjAC&url=http%3A%2F%2Fwww.tmf-ev.de%2FDesktopmodules%2FBring2Mind%2FDMX%2FDownload.aspx%3FEntryId%3D25101%26PortalId%3D0&ei=sJ_PVLikLs2u7AbMm4D4DA&usg=AFQjCNEs8ilUrMk57MXqc8CdQmk20-j5LQ&bvm=bv.85076809,d.ZGU

[130] Declaration of Helsinki, sec. 25 ff.

[131] Caulfield, Upshur, Daar, p. 3.

[132] O'Neill, p. 6.

[133] See http://www.ukbiobank.ac.uk/ethics/.

[134] Forgó, Kollek, Arning, Kruegel, Petersen, p. 17.

[135] Williams, p. 454.

[136] Caulfield, Upshur, Daar, pp. 1 ff.

exemplary for secondary uses of patient data more generally. Thus, “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”.[137] Also from a legal point of view each data subject must have the right to withdraw his consent as it is referred to Article 12 lit. b) of Directive 95/46/EC. Furthermore 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.

Generally, the Declaration of Helsinki advises that the consent should be obtained in written form.[138] This is consistent with Article 2 lit. j) of the Clinical Trials Regulation (2001(20/EC)[139] and Article 29 of Regulation No 536/2014[140] (that repeals the Clinical Trials Regulation; applicable not before May 2016). Also § 4a of the German Federal Data Protection Action (BDSG)[141] demands the written form for every informed consent. This form is apposite not only for reasons of proof, but also in order to formally signify the importance attached to the dignity and integrity of all research subjects when agreeing to participate in research. A further advantage is that the patient can refer back to the written record, reminding himself of the scope and implications of his or her decision. However, there are situations that may involve consent in non-written form, e.g. an online registration (albeit here the possibility to print out a hardcopy should be given). In either case, consent must be formally documented and witnessed according to the Declaration of Helsinki.[142]

5.5 Minors and mentally incompetent research subjects

A further requirement for the validity of the consent is that the patient in question is mentally capable to take decisions.[143] This is no problem when persons concerned have attained legal age and are contractually capable. In other cases, where the research subject is mentally incompetent, the Declaration of Helsinki stipulates that the physician must seek informed consent from the legally authorized representative.[144] In addition, the Declaration of Helsinki stipulates that incompetent 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.”[145]

[137] Declaration of Helsinki, sec. 26.

[138] Declaration of Helsinki, sec. 26.

[139] See http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&url=http%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2001%3A121%3A0034%3A0044%3Aen%3APDF&ei=RlnrVLDgCM_taMrageAG&usg=AFQjCNF6kgDk1WznU2zCQzjiv8dv4MCKbQ&bvm=bv.86475890,d.d2s&cad=rja

[140] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.158.01.0001.01.ENG.

[141] See http://www.gesetze-im-internet.de/bdsg_1990/__4a.html.

[142] Declaration of Helsinki, sec. 26.

[143] Pedroni, Pimple, p. 6.

[144] Declaration of Helsinki, sec. 28.

[145] Declaration of Helsinki, sec. 28.

As regards minors, an authorised representative is not necessary anymore 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 understand the implications of his or her decision, especially which result his or her consent has for the data collection, processing and its use. Nevertheless it may generally be assumed that a 14-year- old person can be considered responsible and mature enough to make this decision. As to persons under disability it can be noted that their capability will be subject to assessment by the physician.

5.6 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.[146] 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 concreto. 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.[147] 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.[148]

If data rendered anonymous (which means that it is only with an unreasonable effort possible or to find a connection between the data and the person concerned) are used, the sovereignty and the right of self-determination of the person concerned are arguably not violated because it is very unlikely that his or her identity is retraceable, and thus risks of harm or other personal implications from such data use will not arise. Therefore the conclusion could 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, this is not entirely incontrovertible: after all the data processing involves exploiting a resource deriving from the patient. Accordingly, so far as reasonably practical, it is recommended to seek the patient's consent even if his or her data shall be used in anonymized 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, then – as a second-best option – it corresponds to the respect for the patient's interests (in particular in minimizing any risk of harm from the data processing), that his or her data is rendered anonymous.

5.7 When consent may be insufficient: the need for avoiding harm

Another ethical commitment of the data controller is to avoid harm of the data subject. This is an aspect of the principle of non-maleficence ('primum non nocere') – a further basic rule of medical ethics. The idea behind this is that the person behind the data may not be harmed because he has agreed to the data processing. In this regard de-identification of data to reduce risks of potential

[146] Declaration of Helsinki, sec. 32.

[147] Declaration of Helsinki, sec. 32.

[148] Declaration of Helsinki, sec. 32.

harm to the subject is desirable even where the patient consents to the relevant data use. By using the data in anonymized, or at least strongly pseudonymized, form only this danger can be minimized. Since the data controller will benefit from the data subjects' data, it seems appropriate to ensure as far as possible as the data controller that harm to the privacy and other fundamental interests of the data subjects will be avoided as much as possible.

In addition to the initial de-identification of the data so far as possible (consistently with the purpose for which its use is required) it will be essential to maintain protection against later misuse and/or loss/unauthorized disclosure. This can only be achieved by implementing appropriate safeguards and technical measures. A further important ethical issue also concerns the need for proper management of feedback of potentially distressing individual information to the patient. As already shown in terms of Article 10 of Directive 95/46/EC the data controller must inform the data subject about his identity, the purposes of processing and further information such as recipients of data and the existence of the right of access to the data and the right to rectify the data. Also the respect and decency the data controller owes to the data subject argues for the ethical and moral obligation to inform the data subject about context-relevant content and to explain relevant aspects of the data processing.

However, it will also be relevant to consider matters from the other direction in terms of a given data subject's 'right not to know'.[149] This implies the need for approaches in which the data subject is gently and gradually made aware of the fact that information exists that could be relevant to his condition, and available care and treatment, while still having the opportunity to decline to receive the information. It seems very likely, given the sensitivity of such a dialogue, plus the potential need for counseling and professional advice, that this is not a matter that could be discharged by automated electronic communications. Rather a professional human agent, preferably the physician in charge of the patient's care, should be involved. We shall consider this point further in the concrete case of the MyhealthAvatar platform in Chapter 6. However, briefly anticipating that discussion, it will be important to design interactions between the system and patient/citizen, at least where more significant feedback is provided, in such a way that direct professional health care involvement is secured by default. By these means frustration, possible distress/anxiety and misunderstandings on the part of the citizen can be minimized.

[149] Graeme Laurie, Genetic Privacy: A Challenge to Medico-Legal Norms.

6 Application of the legal and ethical rules to MHA

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 is developed and tested[150] by using not only synthetic data that create virtual persons, but also by processing real data from volunteers who upload lifestyle data collected by the apps such as Fitbit. In terms of the high end clinical demos FORTH is providing full scale and comprehensive datasets (images) which will be transformed into chimeric synthetic data and USAAR is providing securely de-identified molecular data and imaging data from patients with nephroblastoma.
Another disincentive for MHA to overcome could be privacy concerns since many physicians and patients fear that medical records may not be secure[151]. Therefore legal aspects and security related to the storing and processing of sensitive medical data in terms of the MHA project are at the core of the first key stage.

Once the platform and all the planned functions are built, the exploitation stage will aim at finally using the platform. Decision-support systems based on patient-specific simulation can also be done with data that do not identify and can generally not identify the single patient (i.e. using anonymous or pseudonymous data, as these terms were explained in Chapter 4 above). But insofar as single patients shall upload their data and allow their doctor access to this information and/or the patient shall use different tools to analyse his lifestyle or to better understand diagnoses and treatments, the uploaded information cannot be anonymized or pseudonymized without becoming useless.

This deliverable will focus mainly on the currently relevant development and testing stage of the project whereas D11.4 (due in PM [36]) will cover the needs for a legal framework for the subsequent exploitation of MyHealthAvatar. However we will also provide a short outlook regarding the exploitation stage.

6.1 The high end use scenarios

In order to demonstrate the benefits of MHA and to show the specific user needs of the MyHealthAvatar platform use cases and scenarios have been collected within the first 6 months in WP 2 “User needs” (presented in D2.2). So far, no real (as opposed to synthetic) data have been used so the Data Protection Directive has not been applicable in terms of this task. Subsequently, there has been a reduction to final set of refined use cases described in WP 7 “Use cases” (based on the initial collection from WP 2) and a demonstration of all the use cases of D7.1 demonstrated through 4 High End Clinical Demos in D9.1.

The four high end use demos are being evolved by relevant partners, as follows:

(1) diabetes and emergency demo (BED)
(2) congestive heart failure demo (FORTH)

[150] DoW, Part B, p. 11 of 56.
[151] Anderson, p. 481.

(3) osteoarthritis demo (FORTH)
(4) nephroblastoma demo (ICCS/USAAR)[152]

To the extent that the processing of personal data from patients may be required in these demos, then – as discussed in Chapter 4 – the relevant project partner, as the data controller under Directive 95/46/EC will need to show a lawful basis for this. As discussed in Chapters 4 and 5, the preferable option would be to rely upon the patients' explicit informed consent under Article 8 (2) (a); however, where the data constitutes retrospective records that relate to many past patients, this may present obstacles for the controller, in terms of costs and logistical effort required to contact each patient. As noted also in Chapter 5, the question of what exactly will amount to valid consent in this context (in terms of its required degree of specificity) remains uncertain too.

In this regard, it will be pertinent to consider the domestic law of each above partner in relation to consent for data use, as well as other legal bases under the Directive that would legitimate the processing. Here, Article 8 (3), which is specifically directed at health data processing, appears relevant. However, as discussed in Chapter 4, the scope of this Article is limited to processing carried out by medical professionals or those under an equivalent duty of confidentiality. Arguably this could apply to some of the nephroblastoma demo activities carried out by partner USAAR, but not to those of the other, technical partners' demos. Moreover, the purpose of the data processing at issue would likely be classified as scientific research, as it aims at exploring potential project applications. In this regard it is noteworthy that "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 Article 8 (3).[153] Of course, this assessment would cause difficulties in demarcation.

According to the exemption in Article 8 (3) the relevant processing must be for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature.[154] In contrast, further processing, which is not required for the direct provision of such services, such as medical research, is not covered.[155] 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 the Directive can apply, if sensitive data for purposes of medical research is processed and no consent has been obtained. As noted earlier, this provision grants member states the power to introduce provisions at domestic level that permit processing of sensitive personal data in the public interest, subject to adequate safeguards to protect the rights of the data subject.

It follows that the analysis of how and under what conditions the relevant MyHealthAvatar partners may process personal data in realising the respective high end scenarios will need to be investigated separately for each by reference to applicable domestic rules: UK law for BED; Greek law for FORTH

[152] D9.1, p. 5.
[153] Pöttgen, p. 54.
[154] Working Document EHR, p. 10.
[155] Working Document EHR, p. 10.

and ICCS, and German law (more specifically Saarland state law) for USAAR. The relevant analyses are presented below when considering each high end use scenario in turn.

6.1.1 Diabetes scenario

The diabetes demo targets the promotion of self-management of chronic health conditions.[156] As currently envisaged, not only synthetic data will be used for the demonstration purposes, but also healthy participants shall be involved in order to show how a self-management service with focus on a risk assessment for diabetes can improve their lives.[157] Therefore, a "considerable number of participants will be recruited to test the platform and they will contribute a significant amount of data to the platform."[158] In this regard, participants will be normal citizens from the MHA consortium, students from participating universities, citizens from linked projects such as MyLifeHub and Carrer, medical professionals from the MHA consortium and other linked projects such as MyLifeHub and Carrer and other volunteers.[159] After having tested the diabetes demo, the participants will be asked about their experiences in a survey and interview.[160]

Here BED as the project coordinator of the demo fulfils the definition of the data controller, British rules needs to be taken into account. Schedule 1, Part 1 of the UK Data Protection Act 1998[161] sets out the key data protection principles. The first of these 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. 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 1998 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 caused. 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.

[156] D9.1, p. 11.

[157] D9.1, p. 14.

[158] D9.1, p. 13.

[159] D9.1, p. 17.

[160] D9.1, pp. 17 f.

[161] See http://www.legislation.gov.uk/ukpga/1998/29/contents.

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 only", 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 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.

Although the legal exemption as foreseen by Article 8 (4) of Directive 95/46/EC (or with a view to the draft of the General Data Protection Regulation Article 9 (2g)) could be applicable, it is strongly recommended to ask the participants for consent in order to respect the individual's right of autonomy and self-determination. This approach emphasises that the volunteer is regarded as an autonomously participating subject. At this point it should be noted for the whole MHA project that whenever possible, consent should be sought by the partners providing or collecting personal data. Similarly from an ethical point of view it is crucial that the consent is given freely. As discussed in Chapter 5, this requires that consent must be given by way of a self-determined act without any external influences.[162] This extends also to pressure that might occur through an internal relation of dependence with the physician, for example.[163]

The Declaration of Helsinki states that "participation by individuals capable of giving informed consent as subjects in medical research must be voluntary. Although it may be appropriate to consult family members or community leaders, no individual capable of giving consent may be enrolled in a research study unless he freely agrees"[164]. 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."[165]
So to sum up, great importance must be attached to guarantee the freedom of decision-making while seeking consent.

[162] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.

[163] Forgó, Kollek, Arning, Kruegel, Petersen, p. 113.

[164] Declaration of Helsinki, sec. 25.

[165] Declaration of Helsinki, sec. 12.

To comply with the requirement of a consent given for a specific case it is important to inform the potential volunteer of the sort of personal data that is going to be processed and to refer to the functionalities of the diabetes scenario, which will include a personal diary for the storage and management of the health status, sensors and mobiles for uploading the data into the platform, a risk assessment model, a mobile app for accessing the MHA platform and “MyEmergencyIdentifier” for granting limited access to the stored data in case of an emergency.[166] Regarding “MyEmergencyIdentifier” it should be stressed that this aspect of the Diabetes demo goes beyond the existing legal requirements. According to Article 8 (c) of Directive 95/46/EC data processing is permitted without consent in the patient’s vital interests. In terms of MHA this means that a doctor could be permitted to access the data stored in the MHA platform in an emergency case. However from the legal perspective this scenario represents an exception and does not change the recommendation to our partners providing or collecting data that whenever possible patient consent should be sought.

A consent form should also inform the patient about the identity of the data controller, the purposes of the data processing and further information in terms of the specific circumstances to meet the requirements of Article 10 of Directive 95/46/EC. As to ethical considerations, the Declaration of Helsinki provides that the volunteer needs to be informed about the aims, methods, benefits and risks and the right to refuse to participate and the right to withdraw consent at any time without reprisal.[167] Since the Declaration of Helsinki advises to seek consent in written form[168] and also for purposes of proof, the volunteers should sign a consent form. In this way, the volunteer will also be warned about the importance of their decision. A relevant patient information sheet and consent form for this demo will be drafted in due course.

6.1.2 CHF scenario

The congestive heart failure (CHF) demo, being run by FORTH, includes two types of services: a real-time patient/doctor alarming and a risk assessment.[169] For the monitoring alarm scenario FORTH needs to collect real data in real time from medical devices that take real measurement data. A MHA Smartphone mobile application has been planned in this context. Secondly, for the risk assessment FORTH will retrieve data from the users’ profiles from the MHA platform through related services concerning the health and clinical status of the patient. MHA will obtain the information from a Clinical Information System using the “Link with External Clinical Sources” service FORTH has (using EPSOS “patient summary” interface).[170]

The data that shall be collected is demographic such as gender, age, BMI, genetic, physiology-pathology, clinical and protocols/references regarding disease diagnosis/treatment.[171] Furthermore, FORTH is planning to present what other of a patient’s health-related data could be

[166] D9.1, p. 13.

[167] Declaration of Helsinki , sec. 26

[168] Declaration of Helsinki sec. 26.

[169] D9.1, p. 20.

[170] D9.1, pp. 22, 26.

[171] D9.1, pp. 24 f.

embedded into the platform.[172] For the evaluation phase FORTH will seek to maximize patient variation and responses by recruiting people from different ages, genders, geographical locations, disease duration and ethnic groups.[173] Participants that will be recruited are citizens from the MHA consortium, students from the participated universities, medical professionals from the MHA consortium and from the university hospital of Heraklion and other volunteers.[174] For purposes of evaluation a survey and interview is planned and in addition a focus group and a workshop.[175]

In terms of the real data that is going to be used a consent-driven approach is needed if data from volunteers shall be recruited. Here we refer to the requirements stipulated for the “diabetes demo”. Since the functionalities differ from the diabetes demo and other data is going to be collected, a separate specific consent form will be drafted in due course.

Both here and in respect of the proposed reuse of data from clinical information system for the risk assessment tool, FORTH will have full regard to the relevant Greek rules governing use of sensitive data. Here Article 4 (1a) of the “Protection of Individuals with regard to the Processing of Personal Data”[176] stipulates that personal data, in order to be lawfully processed must be collected fairly and lawfully for specific, explicit and legitimate purposes and fairly and lawfully processed in view of such purposes. Moreover, according to Article 4 (1b) the personal data must not be excessive in relation to the purposes for which they are processed at any given time. Paragraph 1d notes that the data must be kept in a form, which permits identification of data subjects for no longer than the period required, according to the Authority, for the purposes for which such data were collected or processed. Once this period of time is lapsed, the Authority may, by means of a reasoned decision, allow the maintenance of personal data for historical, scientific or statistical purposes, provided that it considers that the rights of the data subjects or even third parties are not violated in any given case. Paragraph 2 stipulates that the controller has to ensure compliance with the above mentioned rules. Otherwise the data has to be destroyed.

6.1.3 Osteoarthritis scenario

The objective of this demo is to empower both patients and medical professionals by providing a supportive environment for the long-term management of osteoarthritis condition. In this context relevant data will be visualized so medical professionals and patients can review a plethora of clinical and personal health information through the MHA platform.[177]

For this purpose multi-scale data will be made available (MRI, Micro CT and sequencing) from a small number of patients.[178] This data will be anonymized by the hospital FORTH is collaborating with and

[172] D9.1, p. 23.
[173] D9.1, p. 27.
[174] D9.1, pp. 27 f.
[175] D9.1, p. 28.
[176] See http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL.
[177] D9.1, p. 30.
[178] D9.1, p. 31.

then synthetic (chimeric) patients will be created for the demonstration purpose by FORTH.[179] Here, as discussed above, real image data will be de-identified (removal of metadata, leaving bare images only) and then synthetic data will be added to it to create a profile for a fictive patient who is the image subject (chimeric data). It is arguable, in terms of the definition of personal data in Directive 95/46/EC that such data falls outside the said definition. As discussed in Chapter 4, recital 26 of the Directive classifies data as anonymous (and hence outside the scope of data protection rules) where it cannot be re-associated with the data subject using "reasonably likely means": this may well appear to cover bare fracture images divested of all labels or other surrounding data. However, for the sake of both legal certainty and professional best practice FORTH is on the way to get ethics approval for using the de-identified image data. Other project parties who need access to the chimeric data will be required to sign a written undertaking in which they agree not to use the data purely for necessary project work, to fully secure it, and not disclose it to any other party.

From the legal point of view, to the extent that personal data is processed, then – as discussed above for the CHF scenario –, FORTH will have full regard to the relevant Greek rules governing use of sensitive data, as set out in the "Protection of Individuals with regard to the Processing of Personal Data"[180]. Given that, as discussed in Chapter 4, distinguishing anonymous from personal data is often context-dependent – depending on the surrounding circumstances in which the data is processed, there is an underlying requirement for responsible data governance. Here by implementing sufficient safeguards such as access controls and privacy impact assessments, the anonymity of project data can be ensured to a high degree. Especially important is that it is guaranteed that a patient will not re-identified from the patient's data.

Secondly, and this also applies to the other demos in which data is anonymized, the data controller must consider the rules stipulated in the Data Protection Directive when s/he anonymizes personal data. Insofar as FORTH would undertake the anonymization itself, and does not use multi-scale data that has already been anonymized by someone else, consent should be prima facie sought from the patients. However, as noted in Chapter 5, it should be reiterated that the Declaration of Helsinki states that in situations where consent is impossible or impractical to obtain for research, the research may be done also without consent[181]. But in this situation the Declaration of Helsinki asks for consideration and approval of a research ethics committee.[182] As already mentioned FORTH has applied for ethics approval for using the de-identified multiscale data.

Later on, for the evaluation of the developed platform a set of volunteers is needed and FORTH is already trying to engage volunteers.[183] Again participants that will be recruited are citizens from the MHA consortium, individuals from the participated universities, citizens from linked projects such as MyLifeHub and Carrer and medical professionals from the MHA consortium other volunteers.

[179] D9.1, p. 31.

[180] See http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL.

[181] Declaration of Helsinki, sec. 32.

[182] Declaration of Helsinki, sec. 32.

[183] D9.1, p. 34.

Also this demo will create a survey and do an interview and implement a focus group and a workshop.[184]

6.1.4 Nephroblastoma demo (ICCS/USAAR)

This demo aims at providing a harmonized platform that is going to test therapeutic preoperative approaches for nephroblastoma.[185] The outcome will be to demonstrate to patients or parents of patients how a tumour responds to preoperative chemotherapy.[186] This demonstration will be of a general, indicative character rather than predicting individual patient response. For demonstration purposes, there will be no real patients involved. [187] Anonymized multiscale data that have been collected by USAAR from the previous projects p-medicine[188] and TUMOR will be used so ICCS and USAAR can generate synthetic data populations. USAAR has ethical approval for this (see appendix 6).

As discussed above in Chapter 5, physicians usually are obliged to seek consent for the collection, analysis, storage and/or reuse of health data for medical research already because of ethical aspects.[189] 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.[190] In this regard, the patient must be informed of the project, which plans to process his data and due to this information the patient must be able to understand which consequences his 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.

Here, though the data is anonymized, it could still potentially be problematic that the patient who gave consent for the data processing for the projects p-medicine and TUMOR could not know exactly what would happen to his data in the MyHealthAvatar project. Here it is unclear if the allusion to the fact that the patient's data could be used for future research projects would be sufficient to comply with the ethical requirements. In the ethical discourse, as discussed in Chapter 5, different models of consent have been designed for which reason the scope of consent is controversial.

Similarly, the German Federal Data Protection Act (BDSG)[191] 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.

[184] D9.1, p. 35.

[185] D9.1, p. 38.

[186] D9.1, p. 43.

[187] D9.1, p. 43.

[188] See http://p-medicine.eu/.

[189] Declaration of Helsinki, sec. 32.

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

[191] See http://www.gesetze-im-internet.de/bdsg_1990/.

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.[192] 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 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 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.

Related to USAAR, which is located in Saarland, Section 13 of the Data Protection Act of Saarland[193] would be relevant as well. Section 13 (1) provides that storing, modifying or using personal data is permitted if it is necessary for the fulfillment of its tasks. The data may only be processed for the purposes for which they have been collected. If the body has gained knowledge without collecting the data, the data may only be processed for the purposes they have been stored for the first time before. If personal data shall be processed for purposes for which they have not been collected or stored for the first time, it is only permitted if the data subject has given consent, or if it is not possible or only possible with an unreasonable amount of effort to ask for consent, but obvious that it is in the data subject's interest and he would give consent if he knew this other purpose, or a provision allows the data processing for other purposes, or it is necessary to protect against serious disadvantages for the common welfare or imminent danger of life or health, cf. section 13 (2).

[192] Kühn, p. 130.

[193] See http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCkQFjAB&url=http%3A%2F%2Fwww.saarland.de%2Fdokumente%2Fthema_justiz%2F205-4.pdf&ei=e0e-VK66HMb4UMSlg9AH&usg=AFQjCNHM7g-g8JHBrnPQcmXMHoSMJCtckA&bvm=bv.83829542,d.d24

As previously pointed out, though, the Declaration of Helsinki allows that "there may be exceptional situations where consent would be impossible or impractical to obtain for such research. In such situations the research may be done only after consideration and approval of a research ethics committee."[194] 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.
In this regards, USAAR applied for ethical approval from its ethics committee, which was achieved from the local hospital in August 2013 for the MHA project and the CHIC project, and permits data-sharing with the project CHIC. Accordingly data can be shared with the rest of the consortium.

USAAR has planned besides 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 has approval of an ethics committee 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 is 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.

The validation of the developed demonstration will be done through a set of volunteers.[195] Here it is necessary to recruit as many patients as possible.[196] D9.1 includes a description of how the data can help in using the planned simulation model. After pre-processing available data of nephroblastoma patients, the data will be implemented into the nephroblastoma simulation model.[197] Numerical parameter studies and further information from experimental and theoretical biology literature, semi-automatic adaption of the model parameters can be conducted when integrating insights from personalized multiscale clinical patient profiles.[198] The determined model parameter values can form the 'in-silico profile' of the patient.[199]

USAAR is going to "record data regarding radiology, histology, biological markers on blood and urine tests and genetic counselling."[200] Moreover biomaterial by many molecular and proteomic technologies from patients that are enrolled in the new nephroblastoma protocol will be analyzed to make biomaterial for molecular and genetic research be available in order to find new biomarkers

[194] Declaration of Helsinki, sec. 32.
[195] D9.1, p. 65.
[196] D9.1, p. 37.
[197] D9.1, p. 43.
[198] D9.1, p. 43.
[199] D9.1, p. 43.
[200] D9.1, p. 62.

and targets for new compound.[201] The patients will have given consent before for this research.[202] The data will be preprocessed by the VPH modelling partner (ICCS) and transformed appropriately into Wilms Oncosimulator input.[203]

As to the validation of the nephroblastoma demo, consent by the volunteers is needed. Moreover, security aspects need to be considered to avoid unauthorized access. Data security in MHA is discussed in more detail in section 6.3 below. However, as regards the nephroblastoma data in particular, it appears that the ObTiMA system utilized by USAAR can, as an ontology-based clinical trial management system, provide the required data safety and security: all GCP criteria, including an Audit Trail, can be fulfilled.[204] Personal data is going to be encrypted and pseudonymized and will be stored in a central database that is located in a controlled zone at the Saarland University Hospital to ensure data safety and data protection".[205] Treating physicians only will be able to see the real names and have access to their patients.[206]
Data entry will be possible remotely via the internet, but subject to strong authentication, access, and encryption safeguards. "To get access to ObTiMA and the eCRFs each participating centre needs to register for getting member of the SIOP-RTSG and the SIOP nephroblastoma study. After registration and signing a contract for participation in the UMBRELLA or any other study or trial credentials to use ObTiMA will be provided."[207]

So as far as can be judged at the present stage, the validation scenario complies with appropriate security standards. However the legal issues will be examined further when more details are available in D11.4.

6.2 Validating the platform by data linkage

When the MyHealthAvatar platform is operational, a key presupposition for its successful deployment is that data gathered in a variety of contexts can be linked in a rapid and seamless way so as to produce a realistic complete overview of each citizen user, in terms of their health condition and lifestyle activities across time. It is this completeness that allows optimal decision-making by the patient; for the patient (where the patient elects to share the data with a physician, with whom he collaborates in managing and receiving care; and for the community (where the patient agrees to allow his data to be used in de-identified form for wider health research). Here, the key control mechanism for protecting the patient's privacy and autonomy interests will be the need for informed consent (see the discussion in part 4.3).

One key point that is likely to be essential in practical terms for succeeding is that the user can upload their data easily and comfortably. Of course, this uploading needs to be secure, not only for

[201] D9.1, p. 62.
[202] D9.1, p. 62.
[203] D9.1, p. 62.
[204] D9.1, p. 39.
[205] D9.1 pp. 39 f.
[206] D9.1, p.40.
[207] D9.1, p. 39.

legal reasons (see Article 17 of the Directive, discussed in Chapter 4), but also to retain confidence. The MHA consortium is aware of these aspects and is therefore testing the modalities for convenient and secure linkage with external sources. In WP 2 FORTH analyzed user needs and requirements for the linkage to social networks from PM1 to PM9 in order to identify end user needs and requirements for the linkage to external sources. The results are described in D2.3 and depict other EU funded projects that could be relevant for MyHealthAvatar (such as p-medicine, Chic, Discipulus) and online social networking platforms (such as Facebook, LinkedIn, Google+and Twitter).

Similarly, an aim of WP 6 has been to develop data collection utilities, and to experiment with the Linked Data approach, so patients do not have to undertake big efforts themselves to populate the data repository with health-related data, which instead can be collected mainly by mobile apps such as Fitbit and Moves.[208] Therefore FORTH provides a methodology for the integration of collection with external sources such as existing data and model warehouses, social networks and hospital records.[209] As to the latter, the architecture seeks to support the export of health-related patient's data from linked hospitals. D6.1 reviewed existing data collection utilities, amongst others information extraction from social networks and health data extractions from social media.[210] Here, data storage and security aspects were also considered.[211] In this regard D6.1 states that there are some concerns about user data protection and legal consideration with respect to health data from social media.[212] This is why linking to Twitter and Facebook was designed in year 1[213] but has not been practically released yet.[214]

As noted in Chapter 3, in the meantime an integrated data collection platform for users has been built to retrieve third-party health information to MHA data repositories.[215] There are not only links between the MHA platform and Facebook and Twitter, but also between the MHA platform and GoogleDrive, Fitbit and Moves allowing for information exchange between each other. The wearable device Fitbit and Moves application have been integrated into the MHA platform[216] because they allow collection of large-scale timely personal health information.[217] With respect to Twitter, linking has been completed in the direction Twitter to MHA.[218] The other direction will be completed in due course pending further ethical and legal examination, as well as other linkings.
In the near future, Withings, iHealth and probably other sensors such as Medisana will be integrated.[219] Moreover, an online patient diary has been designed, which would facilitate the collection of data from it. Currently, BED is working on Intelligent Textbox to allow smart data input

[208] D1.1, p. 14; D1.3, p. 14.

[209] D1.1, p. 11.

[210] D6.1, pp. 2,5.

[211] D6.1, p. 6.

[212] D6.1, p. 15.

[213] D1.2, p. 4.

[214] D6.1, p. 15.

[215] D6.1, p. 6.

[216] D1.3, p. 14.

[217] D6.1, p. 5.

[218] D1.3, p. 10.

[219] D1.3, p. 14.

without any huge user effort.[220] The next step, which will be the subject of further analysis as part of Task 11.3, will be to link data from MHA to a hospital system.

In order to test the MHA platform the consortium has recruited (among consortium members) several volunteers testing the MHA platform by uploading data collected with the device Fitbit. In this context USAAR has contacted participants involved in the first round of the MHA survey and participants from the external projects MyLifeHub (UK EPSRC project) and CARRE (fp7 project). This testing phase is a middle stage before the platform will be completely opened to the public.

LUH has recommended a consent-driven approach to comply with Article 8 (2) (a) of Directive 95/46/EC and the ethical requirements (examined in Chapter 5) and drafted consent forms to make sure that the consent given by the participants complies with the legal and ethical requirements explained above, in particular that they are made aware of how their data will be used and protected within the project. In this regard THREE different forms of consent have been developed: one for the consortium member employees who are participating directly in the MHA project, one for participants from the external projects MyLifeHub and CARRE and one for general volunteers (the relevant consent forms are attached in appendices 2, 3 and 4).
Firstly, the drafts state that personal health data will be processed on the MHA private demo platform by transferring data from devices and apps such as Fitbit and Moves. Then the project is explained and it is guaranteed that all necessary state-of-the-art security measures are incorporated in the platform to hinder accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse. The latter is crucial in order to meet the requirements of Article 17 (1) of Directive 95/46/EC.

As to matters of cloud computing the volunteer is warned that their data may be stored and used in a public cloud that may use servers located outside the EU/EEA and that these servers may provide a level of privacy protection that is lower than that offered by the EU data protection legislation. BED uses a new public cloud server (Linode based in London which is rented by ANS) to host the uploaded lifestyle data. Moreover the volunteers need to know that the devices and apps they use to collect their data are subject to their own third party rules and that the MHA project is not able to control the data processing by such parties. The consent forms provide that the project will ask the volunteer for additional consent if it is planned to make the demo platform public or use the data for other purposes or if the functions of MHA will change or additional apps, devices and services will be linked to the MHA platform. In this context it should be pointed out that, if the additional mobile apps for the diabetes and the CHF scenarios will be linked with the MHA platform the volunteers will be contacted to ask for a new consent.

Since it is important for a valid consent that the patient understands what s/he gives his/her consent to[221] the volunteers have been given the opportunity to ask questions about the data processing. Moreover they have been informed that they will not suffer adverse consequences if they refuse to grant consent or withdraw consent. In this regard the consent forms comply with the requirements

[220] D1.3, p. 14.

[221] Declaration of Helsinki, sec. 26.

stipulated in the Declaration of Helsinki[222] and Article 12 lit. b and Article 7 (3) of the current draft of the General Data Protection Regulation.

In terms of the high end clinical demos, CHF linkage with external clinical information hospital systems should make it possible to acquire specific EHR patient related data.[223] Also the OST demo plans interactions between MHA platform, external resources and the users.[224] Whenever volunteers are recruited it is critical that they grant consent for this data linkage as well. Here the details of the data linkage should be explained so the volunteers can understand how their data will be processed. Furthermore the data linkage needs to be secure. Since the details are not yet finalised, LUH will give legal guidance on this aspect in due course.

6.3 Security aspects

6.3.1 Architecture

As discussed in Chapter 4 above it is the controller's duty to make sure that the system's architecture complies with security aspects that are stipulated in Article 17 of Directive 95/46/EC. In this regard the security framework deployed by the controller should ensure that only authorized persons have access to the data stored in the repositories and that the data are secured against unauthorized access.

FORTH is primarily concerned with standard specifications, practices and guidelines such as software, guidelines, protocols, formats and laws and is concerned with IT and non IT standards that might influence MyHealthAvatar's project architectural design.[225] Security standards have been taken account of from beginning of the project. In D3.1 it is stipulated that "high security and privacy are necessary in modern medical applications. Strict policies are defined by official medical instances to ensure that the confidential medical data can be accessed and manipulated in a secure way. For this the data is protected by different security and privacy mechanisms like authentication, identification, authorization, anonymization, protected data transport and storage."[226] It is clear that MyHealthAvatar must use these mechanisms so as to guarantee a high level of security. As examples, SAML, Liberty-Alliance, WS-, OpenID, PKIX and XACML and Cassandra are mentioned.

As outlined in D3.2 security aspects are also being taken into full consideration for the MHA architecture.[227] Thus the structure of the architecture platform has been built by bearing in mind all the security aspects of the technological platform, ranging from user authentication, authorization, auditing, to data integrity and privacy to pseudonymization and (potential) re-identification of

[222] Declaration of Helsinki, sec. 26.

[223] D9.1, p. 22.

[224] D9.1, pp. 32 f.

[225] D3.1, p. 8.

[226] D3.1, p. 72.

[227] D3.2, p. 7.

patient data.[228] Further, appropriate authentication and authorization mechanisms have been implemented pursuant to the directives of WP3[229] in which the system's architecture seeks to be realized. 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.

By these means, it is ensured that only authorized persons can access the content of the data and the models repositories.[230] BED has investigated API Security with OAuth 2.0 to make sure that issues concerning grant access will be solved such as resource owner password grant, used by demo platform user authentication, implicit grant (used by demo platform JavaScript request), authorization code grant (under implementation and testing used by 3rd server-side request).[231] Here not only will the OAuth 2.0 standard for authorization of users be used; but initial actions towards implementing the corresponding service provider and service client have been investigated in order to enable the secure identification of the different users of the MHA platform such as citizens and clinicians.[232] For the integration of WP 5 and WP 6 three options for the integration have been considered which are via Message Queue, via APIs and via iFrames.[233] Taken together, these state of the art technical measures aim to ensure protection of personal data in the MHA infrastructure against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access to the high level commensurate with the sensitivity of the data in question. Through these means the requirements stipulated in Article 17 of 95/46/EC are complied with as well as the relevant provisions in the CoE Recommendation on the Protection of Medical Data of the Committee of Ministers to Member States, R(97)5.

6.3.2 Cloud computing

As discussed previously, MyHealthAvatar relies upon a private and public cloud infrastructure, which is used by FORTH on Crete (private-based) and BED in the UK (public-based). The privately-deployed cloud infrastructure takes full account of both security issues in biomedical research and the possibility to outsource the infrastructure to commercial cloud computing facilities.[234] Generally, a privately-deployed public is be regarded as safer, as the data controller retains fullest technical control, and this set up should be used preferably when the platform is up and running, and health data is stored inside it. At present during validation only lifestyle data is stored in the public cloud as permitted by the consent forms; as discussed in 4.4.3, it is here important for appropriate data security measures by the cloud provider to be regulated by contract.

[228] D1.1, p. 11; D1.3, p. 9.
[229] D1.1, p. 17.
[230] D1.3, p. 13.
[231] D1.3, p. 15.
[232] D1.3, p. 13.
[233] D1.3, p. 13.
[234] D1.1, p. 12; D1.3, p. 10.

As depicted above Article 4 (1) (a) of Directive 95/46/EC states that the law applicable is defined by reference to the place of establishment of the data controller.
The person or organization, who hosts the MyHealthAvatar platform fulfils the definition of a "data controller" stated in Article 2 (d) of Directive 95/46/EC. Contrary, the cloud provider, who processes the personal data on behalf of the controller, fulfils the definition of a processor, which is stipulated in Article 2 (e) of the Data Protection Directive. There might also be situations in which a provider of cloud services may be considered as a joint controller or a controller in their own right, e.g. when the provider processes data for his own purposes.[235] This depends on the concrete circumstances.[236]

As noted earlier, the cloud-based approach has been adopted in order to handle the high volume of sophisticated processing operations within the avatar infrastructure. At the same time, the partners utilizing such data processing facilities and repositories will need to remain mindful of any additional risk that accrues through choosing such an option over more traditional methods of on-site processing. As discussed in Chapter 4, this has been the subject of recent guidance from the Article 29 Working Party. At the same time, gains in some aspects of data protection (in particular the safeguards to data integrity enabled by multi-site replication) may also be mentioned. In addition it recommendable that the data is stored in clouds that use servers located inside the EU/EEA only. This remains the best way to ensure that the processing of the data happens in a secure manner and that the requirements of the Data Protection Directive and the WP29 Opinion 05/2012 are met.

6.4 Outlook for the "Exploitation stage"

In the exploitation stage the MyHealthAvatar platform will be set up and opened to users from the general public. Although strictly beyond the parameters of the MHA project, it is clearly important, as part of a feasibility study, already to anticipate and address the key issues that will need to be taken care of so as to ensure the effective, legally-and-ethically compliant operation of the platform. In particular it will be essential for the avatar-service provider to demonstrate that it is a trustworthy and reliable operator that guarantees security and integrity of the data. In this regard there will be the need to ensure at a technical level, where the patient wants to use the MHA platform as a storage for his personal data, that patient data will not be lost. The users need to be confident that great importance is attached to the meeting of legal and ethical requirements. In this context not only questions of how the requirements of the data controller can be complied with need to be thought through, but also of how informed consent of end-users will be achieved, security aspects, and how privacy can be ensured. It will also be crucial to manage the feedback of health information (which may include potentially alarming or distressing content) from the system to patients and citizens in a sensitive and controlled way, backed up by safeguards (e.g. physician involvement, opportunities for counseling) as required.

The document "Proposed legal framework for MyHealthAvatar" (drafted by Manolis Tsiknakis from FORTH and Norbert Graf from USAAR, and approved by LUH) that has been circulated amongst the consortium (this is attached as appendix 5) is an important point of reference for the exploitation stage. It takes into account the conclusions of the eHealth Task Force Report – Redesigning health in

[235] Opinion 05/2012, p. 8.

[236] Opinion 05/2012, p. 8.

Europe for 2020[237] and describes different data sources such as EHR, hospital information system (HIS) and citizens that are using MHA and devices that can be linked with MHA. Moreover, the possibility of linking the MHA platform to different social networks is mentioned.

It is also stated that the citizens must give consent for linking the data and uploading the data, e.g. in terms of specific data or all data if wished. It is planned that the users can at any time without giving a reason ask to have their data deleted. Moreover a table shall show information such as which data are stored at what time and which data have been deleted again. The same goes for the linkage of data. With respect to devices an API will be provided in due course so data can be uploaded by using devices. It must be agreed in a contract with the device provider that it is prohibited to use the data, necessary to implement technical and organizational security safeguards, and that the data will only be stored in the MHA platform if the citizen/patient allows this.

6.4.1. Complying with requirements of the data controller

The first issue which should be taken notice of is that the person or organisation who hosts the MyHealthAvatar platform fulfils the definition of a "data controller" which is stipulated in Article 2d of Directive 95/46/EC. As discussed above the controller will need to ensure fair processing including the need for de-identification so far as compatible with purpose of use, data minimization, limited retention and the principle of purpose limitation. According to the opinion 03/2013 of the Article 29 Working Party, one aspect of this relates to the need for the controller to adopt appropriate safeguards to ensure that the privacy interests of the data subject are protected so far as reasonably possible.[238] This is important because third parties such as insurances and employers might have a huge interest in the data. Also, as Bainbridge has pointed out, an inherent danger of systems (such as MHA) is that the stored information might fall into the wrong hands.[239] In order to avoid implementing a transparent patient security measures are crucial. Furthermore citizens tend to be over panic concerning data security. As a general starting point, it is important that MyHealthAvatar makes use of all appropriate state of the art privacy enhancing technologies, such as contained in the ISO/IEC 27001:2013.

This argument 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)[240] that "privacy enhancing technologies (PETs) should be applied as much as anyway possible in order to promote personal data protection."[241] The legal framework concerning security measures should foresee the necessity of a reliable and effective system of electronic identification and

[237] See http://www.epractice.eu/en/library/5362646.

[238] Opinion 03/2013, p. 3.

[239] Brainbridge, pp. 635 f.

[240] See http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCYQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fpolicies%2Fprivacy%2Fdocs%2Fwpdocs%2F2007%2Fwp131_en.pdf&ei=hsnQVO_wI4rwULSZhLAM&usg=AFQjCNHHJ54fZ0VkucJxcX1SO1E605htwA&bvm=bv.85076809,d.ZGU&cad=rja.

[241] WP131, p. 19.

authentication.[242] Moreover it would be desirable to have a constantly up-dated register for checking on the accurate authorization of persons having or requesting access to the EHR system.[243] Processing steps such as access requests for reading or writing and internal checks and follow up on correct authorisation should be documented comprehensively.[244] The content of the system needs to be secured by backup and recovery mechanisms and unauthorised access to the data has to be prevented, e.g. by cryptographic algorithms.[245] Furthermore should the authorised persons be instructed on how to use EHR systems properly and how to avoid security risks and breaches.[246] Finally there should be regular internal and external data protection auditing, backed up by data logging as part of a sound data management system.[247] These aspects are acknowledged in the MHA “Proposed legal framework” document, which states that it is important that the entire platform infrastructure meets the requirements of Article 17 of Directive 95/46/EC. By building the security system as is described there, MHA will 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.

6.4.2 Informed consent

The approach for the MHA exploitation stage is a consent-driven one, which puts patient empowerment and informed participation in his/her own health care at the centre of the project agenda. Consistent with this aspiration the document “Proposed legal framework for MyHealthAvatar” recognises in “Lever for change #1: My data, my decisions” that the individual users must give consent according to Article 8 (2) (a) of Directive 95/46/EC for data access and that they will be informed about how the data will be used. The users shall have the possibility to allow the health system to use pseudonymized data for epidemiological purpose. In addition e-consent mechanisms shall be explored to enable users to give consent to certain categories of data without requiring additional consent to each sub-use, e.g.

Since informed consent needs to be granted explicitly pursuant to Article 8 (2) (a) of Directive 95/46/EC, the user will be asked to consent by registering himself on the MyHealthAvatar platform taking into account the need for an “opt in”-solution. At this stage full and appropriate new user information sheets and consent forms will be prepared and implemented (i.e. distinct from those contained in appendices 2 - 4, which are limited to data processing for validation during the project lifetime). These consents will also require translating into other languages as required according to the platform target population. The user will be able to release his data without indicating a reason and solely for use in a given project. The information as to which data were released to whom at what time will be stored in the platform as well as the informed consent in order to ensure data security and transparency. The user will grant consent for a further use and the purposes will be explained in layman language in the General Terms and Conditions. This approach is very welcome

[242] WP131, p. 20.

[243] WP131, p. 20.

[244] WP131, p. 20.

[245] WP131, p. 20.

[246] WP131, p. 20.

[247] WP131, p. 20.

because the platform will comply with Article 7 lit. a and Article 8 (2a) of the Data Protection Directive. It is important that the citizen voluntarily takes the decision to become a user of MHA. Hence it must be analyzed how it can be ensured that consent is given freely and that there are no external influences like coercion, duress, pressure, manipulation or undue influence. As already mentioned, health insurances and employers might be very interested in the stored data and could exert pressure to register with the MHA platform and to threaten the citizens that otherwise the insurance will not insure or hire the person in question. But also physicians to whom the patient has a very dependent relationship or family members could try to influence the citizen. Another threat patients might fear is disadvantage from a physician at a clinic where they are treated. This raises the question of how the data controller could check that the potential users have the free choice of refusing to be part of MyHealthAvatar.

One preventive measure would be to teach physicians not to actively encourage joining, but just to inform patients about the platform in an objective way.
A second preventive measure could be to guarantee that the data will never be transferred to third parties such as employers and insurances in order to reduce the risk that such third parties could put pressure on the citizen to register. In similar vein, sufficient computer security measures should be implemented to prevent relatives from gaining unauthorized access, or coercing the user to log in and divulge their information. In this context, consideration could be given to some kind of 'panic button' that would deny access to the system or bring up only redacted information. Finally, it would be helpful to offer the user an easy solution to delete his avatar and to withdraw his or her consent at any time.

As far as minors may be involved it must be taken into consideration that they deserve specific protection of their personal data because they may be less aware of the risks and consequences of a granted consent and of their rights in respect of the processing of personal data. As depicted above, a 14-year-old is usually considered responsible and mature enough to make decisions. One option to address the problem that persons aged under 14 years could be not mature enough to grant consent would be not to allow persons aged under 14 years to register with the platform. This is why a section in the General Terms and Conditions could clarify that users of the platform warrant to be aged over 14 years. Another option might be that the legal representative grants consent. In this context, Article 8 (1) of the current draft of the General Data Protection Regulation (GDPR) could serve as a guideline as it states that "for the purposes of this Regulation, in relation to the offering of goods or services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or legal guardian. The controller shall make reasonable efforts to verify such consent, taking into consideration available technology without causing otherwise unnecessary processing of personal data."

It will also be important to take account of the increasing autonomy of the child as it matures and make provision for obtaining re-consent by the child to continued participation in the platform as and when appropriate. It is suggested that this requirement should operate as soon as the child acquires sufficient understanding and competence to make the decision for itself: this may putatively be considered to occur at 14. Indeed, at the latest when the child attains majority there will also be a legal requirement for it to consent to the ongoing data storage and processing, as the previous consents provided by the parents will lose any residual validity. Since, though it is not yet finally determined how the MHA consortium proposes to handle these issues, LUH will keep this matter under review and provide further consultation and advice in due course.

6.4.3 Health and disease prediction

MyHealthAvatar is a species of personal health record. But contrary to passive systems such as HealthVault where the user is simply able to store health-related data, the purpose of MHA goes beyond this: as well as serving as a data repository only, it will incentivize citizens to use tools to analyze their data and to encourage individuals to change their lifestyle and to look after their health. At the same time, in this context ethical concerns about health and disease prediction may also arise, and will need to be thought through in respect of the piloting/validation, but particularly in the exploitation stage.

The question is if citizens really wish to be subjects of prediction and to learn, for example that their lifestyle increases the risk of certain chronic diseases. Since it is very difficult to change one's lifestyle, citizens might thereby suffer feelings of frustration, embarrassment or distress. In terms of informed consent it is therefore important to alert citizens to the risk of having such emotions when using disease prediction tools: here, especially the less obvious risks should be clearly communicated in advance. Moreover, it will be important to design the system in a way that citizens – at least when utilizing these applications outside a clinical setting – see general trends rather than specific predictions or diagnoses. One option could be to ensure that such tools may only be deployed 'collaboratively' by the patient and doctor together in a clinical setting, also ensuring professional oversight of data input by the citizen and interpretation of and recommendations concerning the tool's 'prediction'. At the very least (if that is felt to be too paternalistic in some cases) the user should receive clear information and advice on the use of the tool and that they should consult with a physician to have the results interpreted and for recommended life-style changes where appropriate.

Similarly, patients should be diagnosed by physicians because they can estimate how they should inform the patient about potentially bad or distressing news and what words they should use. Moreover a disease prediction tool cannot counsel a patient in the way a doctor can do and from the special relationship between physician and doctor follows that the patient should discuss questions of how the patient should handle a disease etc. As already noted, it is particularly important to ensure that patients are not exposed without counseling support to actual or perceived bad news that might be contained in the data. Here care also needs to be given to designing the information provision in such a way so as not to suggest bad news 'by implication' (e.g. by telling the patient to see his doctor). Here a solution could be to ensure the patient is instructed (and is aware that he will be) to see his doctor whenever certain health results are available - whether they be good or bad.

6.4.4 Liability

A related threat to the MHA platform's success and viability could be that the linked data are not accurate and that a physician or the MHA user who uses prognosis tools trusts this information.

Technically the inaccuracy and uncertainty of health data from diverse devices can be improved through advanced data aggregation algorithms, which are very time-consuming.[248] From a legal point of view especially liability issues could arise, which need to be thought through intensively. For instance, a citizen might follow poor advice and fall ill (or conversely be falsely reassured), or a clinician might follow a recommended procedure[249] after using the MHA platform and might consequently harm his or her patient. Equally, the loss of data through system malfunction, especially where its contribution required user investment over an extended time period, may lead significant distress, even if no other harm occurs, and might lead to legal action. Another issue is that the physician (when the user shares his information with a doctor) could be led to trust uploaded or linked data that are wrong or incomplete.

There is no European legislation, which is specifically applicable for the liability for products and services composing eHealth applications or supplied through them.[250] The Directive 2001/95 on General Product Safety[251] applies for products in general only and not for services, whereas the Directive 93/42 on Medical Devices[252] applies for devices only, but not for services. The Directive 2006/123/EC on Services in the Internal Market[253] expressly excludes services provided by health professionals to patients to assess and restore their state of health.[254] The Directive 2011/24/EU on Patients Rights in Cross-Border Care[255] places eHealth in a legal context for the first time.[256] It requires Member States to cooperate on interoperability standards to allow full use of eHealth services across EU borders. But this Directive does not mention the liability for harm, which may arise as a result of providing care across borders by means of eHealth solutions.[257]

It can be concluded by this that at present the liability arising from harm caused by the supply of MyHealthAvatar would be governed by the ordinary rules of law applicable in the different European Union Member States. This presents a major challenge since there could be the necessity of analysing every legal framework of those Member States in which the MHA platform would be opened. To bypass this problem, it is crucial to decide on who will host the platform. If BED will host the platform and therefore will fulfil the definition of the data controller, UK law would be applicable. At present, without having full details as to how the platform might operate and be used

[248] D6.1, p. 29.

[249] Andoulsi, Wilson, p. 174.

[250] Andoulsi, Wilson, p. 177.

[251] See http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/general-product-safety/index_en.htm.

[252] See http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC8QFjAA&url=http%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DCONSLEG%3A1993L0042%3A20071011%3Aen%3APDF&ei=qM3QVIrxFM-R7AaN94HACA&usg=AFQjCNF3-X3wKvasTARcxpKcPuzQG2HI9g&bvm=bv.85076809,d.ZGU.

[253] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0123

[254] Andoulsi, Wilson, p. 174.

[255] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF.

[256] Andoulsi, Wilson, p. 174.

[257] Andoulsi, Wilson, p. 174.

or relied upon by participants in practice, it is somewhat speculative to construct concrete scenarios in which liability might be in issue. This applies also to the possible impact of certification (so far as applicable) of individual elements under medical devices legislation. However, in order to pre-empt potential claims so far as possible in a general manner, we would propose creating and including a liability disclaimer as part of the General Terms and Conditions.

6.4.5 e-Privacy Directive

A final matter that is relevant to consider briefly is the potential impact (in overlap with data protection rules) of the e-Privacy Directive 2002/58/EC.[258] The latter instrument particularises and complements the Data Protection Directive with regards to the processing of personal data in the electronic communication sector. First of all, the e-Privacy Directive seeks to ensure an equivalent level of protection of fundamental rights and freedoms, especially the right to privacy, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community, cf. Article 1.

Pursuant to Article 3 of the e-Privacy Directive, the Directive is applicable to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community. Therefore it is essential to know if MHA is an electronic communications service in order to know if the platform will have to fulfil the requirements, especially the one stated in Article 4 of the e-Privacy Directive: the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. The measures shall ensure a level of security appropriate to the risk presented considering the state of the art and the cost of their implementation. Paragraph 2 stipulates that in case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk.

The e-Privacy Directive does not provide for a definition of “electronic communications service”, but according to Article 2 of the e-Privacy Directive the definitions of the Directive 2002/21/EC concerning a common regulatory framework for electronic communications networks and services shall apply regarding the e-Privacy Directive. Article 2 (c) of Directive 2002/21/EC[259] defines an electronic communication service as “a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.”

[258] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

[259] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:HTML.

Although the detailed functions of MyHealthAvatar are not yet determined and it is possible that a function could be created to contact other persons suffering from the same disease, the platform will not exist mainly to covey signals on electronic communications networks. Instead, the key functionalities will be the lifetime collection of the user’s health status data, a tool to engage the user in his or her own healthcare, the ability to access a rich set of data from various sources, an interface to access hospital data and healthcare resources, a toolbox for data analysis, fusion and visualization for both clinicians and patients, easy data collection from patients, the admission to prediction to risk assessment as well as the admission to data sharing and multiple platforms. But nevertheless, it is recommendable to meet these requirements, firstly to show the MHA users that ethical standards are met and secondly to comply with Article 17 of Directive 95/46/EC. Hence, MHA should ensure confidentiality of communications and security of their platform and notify personal data breaches to the competent authority at national level.

7 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 legal and ethical concerns.

As can be seen from Chapter 4 the processing of sensitive personal data is prohibited, except if there is a legal basis such as Article 8 (4) of Directive 95/46/EC or the data subject has given informed consent.
Moreover the Data Protection Directive sets the onus upon the data controller to meet the requirements of the need for a fair processing, which includes the need for limited retention, de-identifaction of data and data minimization. Another duty is to ensure data security. In Chapter 5, key ethical requirements, which subsist in overlap with the legal norms, were examined, including the doctrine of the informed consent.

In terms of the application of these legal and ethical principles to the MHA project we started in Chapter 6 with a legal and ethical analysis of the high end use scenarios. For data that is going to be processed by partners following collection from volunteers' appropriate consent forms and information sheets will be drafted. As to the reuse of anonymized data that have been collected from other projects ethics approvals are available.

In terms of recruiting volunteers for validating the demo platform by linking data collected by devices such as Fitbit the use of a well-drafted and informative consent form is crucial. The relevant forms have already been drafted and can be found in the appendices. In both the high end scenarios and in other aspects of the overall infrastructure, the MHA project shall place security aspects at the forefront and implement appropriate and proportionate security architecture, including state of the art authentication and authorization mechanisms. By these means the potential risk of an unauthorized access is kept to a minimum and the architecture complies with Article 17 of the Data Protection Directive and the Recommendation on the Protection of Medical Data.

Finally a preliminary presentation of important issues that need to be considered when exploiting the MHA platform has been given. This includes not only duties of the data controller and issues around consent, but also how health and disease prediction can be performed without harming the user and how liability risks can be preempted in the best way.

References

- Anderson J G (2007): Social, ethical and legal barriers to E-health; *International Journal of Medical Informatics 76*, 480-483.
- Andoulsi I, Wilson P (2013): Understanding Liability in eHealth: Towards Greater Clarity at European Union Level, *eHealth: Legal, Ethical and Governance*, 165-180
- Brainbridge DI (2008): Introduction to information technology law, 6th edn. Pearson, Harlow.
- Brock D W (1993): Life and death, Cambridge: Cambridge University Press
- 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
- 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
- Dammann Ulrich, Simitis, Spiros (1997): EG-Datenschutzrichtlinie, Baden-Baden: Nomos-Verlagsgesellschaft
- De Andrade N G, Monteleone S (2012): Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications, *European Data Protection: Coming of Age,* 119-144.
- 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
- Forgó N, Kollek R, Arning M, Kruegel T, Petersen I (2010): Ethical and Legal Requirements for Transnational Genetic Research, München: C.H.Beck Verlag
- 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.
- Kühn H C (2004): The Implementation of the Data Protection Directive 95/46/EC in Germany, *Beyleveld et al., Implementation of the Data Protection Directive in Relation to Medical Research in Europe*, 121-140
- Laurie, Graeme (2002): Genetic Privacy: A Challenge to Medico-Legal Norms, Cambridge University Press.
- Neal M L, Kerckhoffs R, (2009): Current progress in patient-specific modeling, *BRIEFINGS IN BIOINFORMATICS. VOL 11 No 1*, 111-126.
- O’Neill O (2003): Some limits of informed consent, *Journal of Medical Ethics*, 29, 4-7
- 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.

- Pöttgen, N (2009): Medizinische Forschung und Datenschutz, Frankfurt am Main: Peter Lang GmbH
- Williams (2001): Informed consent in genetic research, Croatian Medical Journal, 42 (4), 451-457
- Zasada S J, Wang T, Haidar, Liu E, Graf N, Clapworthy G, Manos S, Coveney P V, (2012): IMENSE An e-infrastructure environment for patient-specific multiscale data integration, modelling and clinical treatment, *Journal of Computational Science, Volume 3, Issue 5*, 314 – 327.

• Appendix 1 – Abbreviations and acronyms

ANS	AnSmart
BED	University of Bedforshire
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
CHIC	Computational Horizons in Cancer
EC	European Community
EEA	European Economic Area
e.g.	exempli gratia/for example
EHR	Electronic Health Records
EPSOS	European Patients Smart Open Services
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 Universität Hannover
MHA	MyHealthAvatar

MRI	magnetic resonance imaging
no.	Number
p.	page/pages
PETs	Privacy enhancing technologies
PHR	Personal Health Records
p-medicine	From data sharing and integration via VPH models to personalized medicine
sec	Section
TMF	Technology, Methods, and Infrastructure for Networked Medical Research
TUMOR	Transatlantic Tumour Model Repositories
UK	United Kingdom
USAAR	Universität des Saarlandes
WMA	World Medical Association
WP	Work Package

Appendix 2 - Consent form for processing of lifestyle and health data for MHA

I, the undersigned ____, born on

the_____________________, in____________________________ and resident at

_____________________ / ________________________________ (address),

reachable via ____ (e-mail-address), employee of
____, declare by the present consent form my agreement to the processing of my personal health data on the MyHealthAvatar private demo platform in particular by transferring data from the device Fitbit / the device Withings/ the app Moves / the app MyTracks / the social networking service Twitter [please delete those which do not apply] for the purposes of scientific development and validation of the European project MyHealthAvatar (Grant agreement no: 600929) [http://www.myhealthavatar.eu/].

I understand and agree that all data that I collect and provide to the project by using the above mentioned services may for the project duration be stored and used by the institutions participating in the project [as listed on the project website] in a public cloud that may use servers located outside the EU/EEA (and may provide a level of privacy protection lower than that offered by EU data protection legislation).

Furthermore, I am aware of the fact that the above mentioned devices, apps and the service Twitter are subject to their own third party privacy rules and that the project has no control over data processing by such parties.

I understand that at the moment, unless I opt to share my data with other users of the demo platform, the institutions participating in the project are the only entities, which have access to the data, which I have uploaded to the platform. In case of any change to this position, and in particular if it is planned to make the demo platform public or use the data for non-project purposes, the project will inform me by using my address or e-mail-address (as specified by me) for additional consent.

I have been given the opportunity to ask questions about the processing of my data and I have had these answered satisfactorily. I am also aware that my participation is voluntary and that I will not suffer adverse consequences for refusing to grant consent. I understand that I have the right at any time to withdraw my consent to the processing of my data on the platform without giving any reason. In the event of wishing to do so or having other concerns I may contact the project coordinator Prof. Feng Dong (feng.dong@beds.ac.uk) at University of Bedfordshire.

A copy of this agreement will be sent to my address/e-mail-address (as specified by me) and another copy will be retained for record-keeping by the project.

____

Date, Name

Appendix 3 - Consent form for participating data for use in evaluating the MHA platform

I, the undersigned ____, born on

the______________________, in_____________________________ and resident at

______________________ / _________________________________ (address),

reachable via ____ (e-mail-address), declare by the present consent form my agreement to the processing of my personal health data on the MyHealthAvatar private demo platform in particular by transferring data from the device 'Fitbit' / the device 'Withings' / the app

'Moves' / the app 'MyTracks' / the social networking service 'Twitter' [please delete those which do not apply] for the purposes of scientific development and validation of the European research project MyHealthAvatar (Grant agreement no: 600929) (http://www.myhealthavatar.eu/). In addition, users have the option, if they wish, directly to input further health-related information into the platform via a textbox: any such text data would be processed only by the institutions participating in the project (as listed on the project website) and not disclosed to any third parties.

The MyHealthAvatar project is a feasibility study that aims in the future to propose a solution for access, collection and sharing of long-term and consistent personal health status data through an integrated environment, which will allow more sophisticated clinical data analysis, prediction, prevention and treatment simulations tailored to the individual citizen. At the present time, as part of the technical development of this environment, the MyHealthAvatar project wishes to use the data in exploring different options for presenting it in an efficient and user-friendly manner. The intention is to allow the data collected by the above mentioned apps, devices, services, and text-input, to be linked within the MyHealthAvatar platform only, and accessible to each user in a timeline.

I am aware that all necessary state-of-the-art security measures are incorporated in the platform to protect my data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse.

I understand and agree that all data that I collect and provide to the project by using the above mentioned services may for the project duration be stored and used by the institutions participating in the project in a public cloud that may use servers located outside the EU/EEA (and may provide a level of privacy protection lower than that offered by EU data protection legislation).

Furthermore, I am aware of the fact that the above mentioned devices, apps and services are subject to their own third party privacy rules (from the device-manufacturers, e.g. FitBit) and that the project has no control over data processing by such parties.

I understand that at the moment, unless I opt to share my data with other users of the demo platform, the institutions participating in the project are the only entities, which have access to the data which I have uploaded to the platform.

In case of any change to the above position, and in particular if the functions of MyHealthAvatar will change, if additional apps, devices and other services will be linked to the MyHealthAvatar platform, or if it is planned to make the demo platform public or use the data for any other purposes than those mentioned, the project will inform me by using my address or e-mail-address (as specified by me) for additional consent.

I have been given the opportunity to ask questions about the processing of my data and I have had these answered satisfactorily.

I am aware that my participation is voluntary and that I will not suffer adverse consequences for refusing to grant consent. I understand that I have the right at any time to withdraw my consent to the processing of my data on the platform without giving any reason. In the event of wishing to do so or having other concerns I may contact the coordinator Prof. Feng Dong (feng.dong@beds.ac.uk) at University of Bedfordshire.

In this case, my uploaded data will be permanently deleted from the MHA platform.

A copy of this agreement will be sent to my address/e-mail-address (as specified by me) and another copy will be retained for record-keeping by the project.

____

Date, Name

Appendix 4 - Appendix Consent form for the external projects MyLifeHub and CARRE

I, the undersigned ____, born on

the______________________, in______________________________ and resident at

______________________ / _________________________________ (address),

reachable via ____ (e-mail-address), declare by the present consent form my agreement to the processing of my personal health data on the MyHealthAvatar (MHA) private demo platform in particular by transferring data from the device Fitbit / the app Moves / the app MyTracks / the social networking service Twitter [please delete those which do not apply] for the purposes of scientific development and validation of the European research project MyHealthAvatar (Grant agreement no: 600929) (http://www.myhealthavatar.eu/).

The MyHealthAvatar project is a feasibility study, which aims in the future to propose a solution for access, collection and sharing of long-term and consistent personal health status data through an integrated environment. This will allow more sophisticated clinical data analysis, prediction, prevention and treatment simulations tailored to the individual citizen. Presently, as part of the technical development of this environment the MyHealthAvatar project wishes to use the data in exploring different options for presenting it in an efficient and user-friendly manner. The intention is to allow the data collected by the above mentioned apps, device and service to be linked within the MyHealthAvatar platform only, and accessible to each user in a timeline.

I am aware that all necessary state-of-the-art security measures are incorporated in the platform to protect my data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse.

I understand and agree that all data that I collect and provide to the project by using the above mentioned services may for the project duration be stored and used by the institutions participating in the project (as listed on the project website) in a public cloud that may use servers located outside the EU/EEA (and may provide a level of privacy protection lower than that offered by EU data protection legislation).

Furthermore, I am aware of the fact that the above mentioned device, apps and the Twitter service are subject to their own third party privacy rules (from the device-manufacturers, e.g. FitBit) and that the project has no control over data processing by such parties.

I understand that at the moment, unless I opt to share my data with other users of the demo platform, the institutions participating in the project are the only entities, which have access to the data which I have uploaded to the platform.

In case of any change to the above position, and in particular if the functions of MyHealthAvatar will change, if additional apps, devices and other services will be linked to the MyHealthAvatar platform, or if it is planned to make the demo platform public or use the data for any other purposes than those mentioned, the project will inform me by using my address or e-mail-address (as specified by me) for additional consent.

I have been given the opportunity to ask questions about the processing of my data and I have had these answered satisfactorily.

I am aware that my participation is completely voluntary and that I will not suffer adverse consequences for refusing to grant consent. I understand that I have the right at any time to withdraw my consent to the processing of my data on the platform without giving any reason. In the event of wishing to do so or having other concerns I may contact the coordinator Prof. Feng Dong (feng.dong@beds.ac.uk) at The University of Bedfordshire.

In this case, my uploaded data will be permanently deleted from the MHA platform.

A copy of this agreement will be sent to my address/e-mail-address (as specified by me) and another copy will be retained for record-keeping by the project.

____

Date, Name

Appendix 5 – Proposed legal framework for MyHealthAvatar

Proposed legal framework for MyHealthAvatar

Manolis Tsiknakis and Norbert Graf

Context

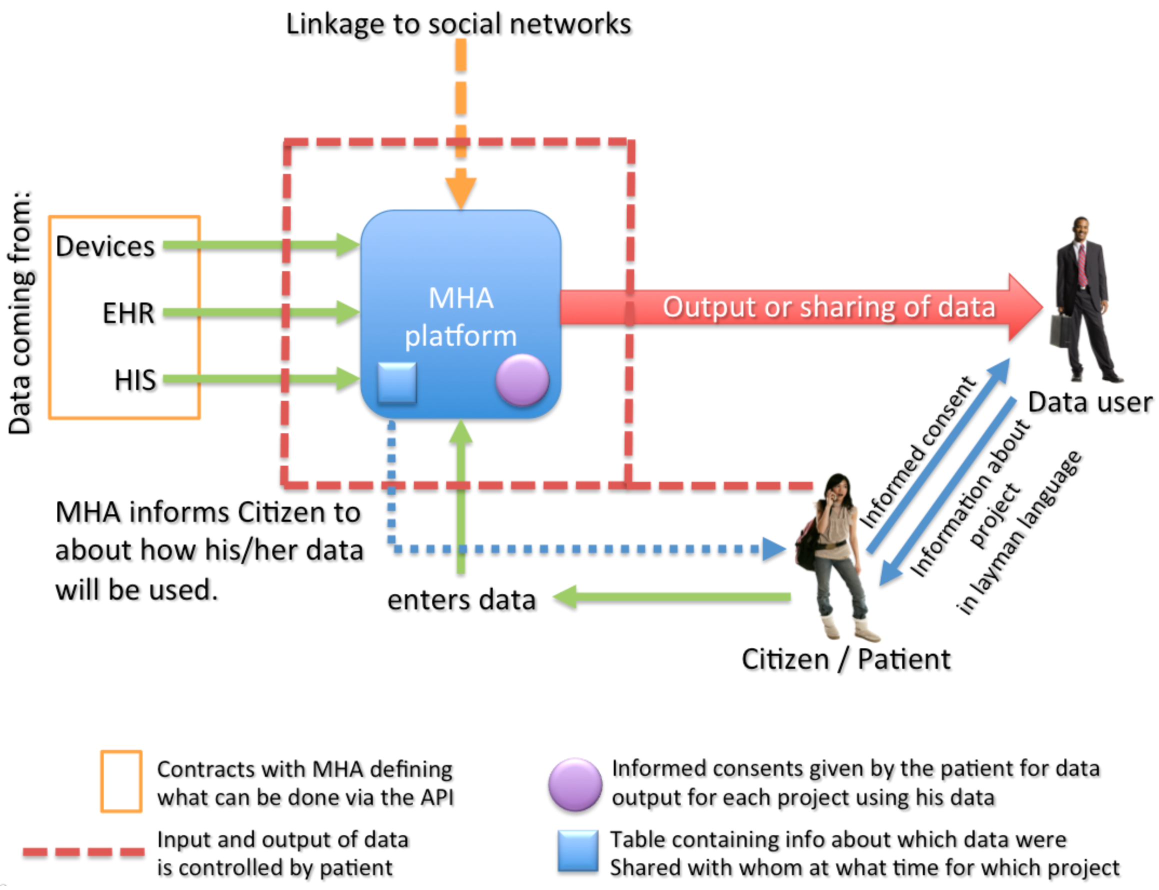
- We take into consideration the conclusions of the *eHealth Task Force Report* - Redesigning health in Europe for 2020 (http://www.epractice.eu/en/library/5362646) for the project stages that involve the use of patient/citizen data (validation and exploitation stage).

Lever for change #1: **My data, my decisions**

- Individuals are the 'owners' and controllers of their own health data, with the right to make decisions over access to the data (by giving consent according to Article 8 (2a) of Directive 95/46/EC) and to be informed about how it will be used. This principle is outlined in EU law, especially in the Data Protection Directive, and European human rights jurisprudence but is rarely fully implemented in health systems.
- This represents a shift in the power relationships within healthcare; away from the unrestrained authority of the medical professional and towards a more collaborative partnership with patients taking on a greater responsibility and more active role in managing their own wellbeing.
- There are different ways of dealing with these new scenarios of individuals as primary controllers of their own data.
- One possibility is the shared control between the patient and the health system depending on the use; i.e. patients as owners of personal health information but allowing the health system to use depersonalised or 'pseudonymised' data for epidemiological purpose; e-consent mechanisms could be explored to allow patient to make differentiated choices based on finely grained information as to implications of different uses; potentially, if he/she wished, a patient could give consent to a given category of use (where the relevant implications across the category are stable) without requiring additional consent to each sub-use.

Lever for change #2: **Liberate the data**

- Taking these "guidelines" into consideration and also the fact that MyHealthAvatar is a demonstration (a feasibility) project, we propose the following legal framework as graphically described in the subsequent figure.
- The principles of the framework are reported in subsequent text


Linkage to social networks
Data coming from:
Devices
EHR
HIS
MHA platform
Output or sharing of data
Data user
Informed consent
Information about project in layman language
MHA informs Citizen to about how his/her data will be used.
enters data
Citizen / Patient
Contracts with MHA defining what can be done via the API
Input and output of data is controlled by patient
Informed consents given by the patient for data output for each project using his data
Table containing info about which data were Shared with whom at what time for which project

The MHA platform can receive data from different sources during the validation and exploitation stage. These sources are:

1. Data from devices citizens or patients are using
2. Data from EHR
3. Data from the hospital information system (HIS)
4. Data directly entered by the citizen/patient

The MHA platform can be linked to different social networks.

For all data stored in the MHA platform or linked to the MHA platform the citizen/patient needs to allow an upload of his/her data or linkage of his/her data He can give permission in respect of specific data or to all data, as well as for linkage.

Without the consent of the patient no data can be uploaded or linked. The patient can at any time without giving a reason ask to have his/her data deleted-A table needs to be stored within the platform that contains the information, which data are stored at what time and also which data were deleted again. The same applies for the linkage of data.

As devices needs to be connected with the MHA platform an API is provided so that data can be uploaded. There needs to be a contract with the provider of the device that he will not use the data, will implement necessary technical and organisational security safeguards, and the data will only be stored in the MHA platform if the citizen/patient allows this.

If someone wants to use data, the patient needs to give his consent for that usage because Article 2 (h) of Directive 95/46/EC requires that consent has to be given not only voluntarily, but also for a specific purpose. In this regard, prior to consenting, the purpose of using the data should be explained to the patient in layman language.

An informed consent needs to be expressly provided by the citizen/patient.

Especially, concerning the exploitation stage, but probably also during the validation stage, the user will be asked to consent by registering himself or herself on the MyHealthAvatar platform. Here, in line with Article 8 (2a) of Directive 95/46/EC it the consent needs to be explicit. This means that consent cannot be obtained by the presence of a pre-ticked box, but that the data subject must take some positive action (‘opt in’).

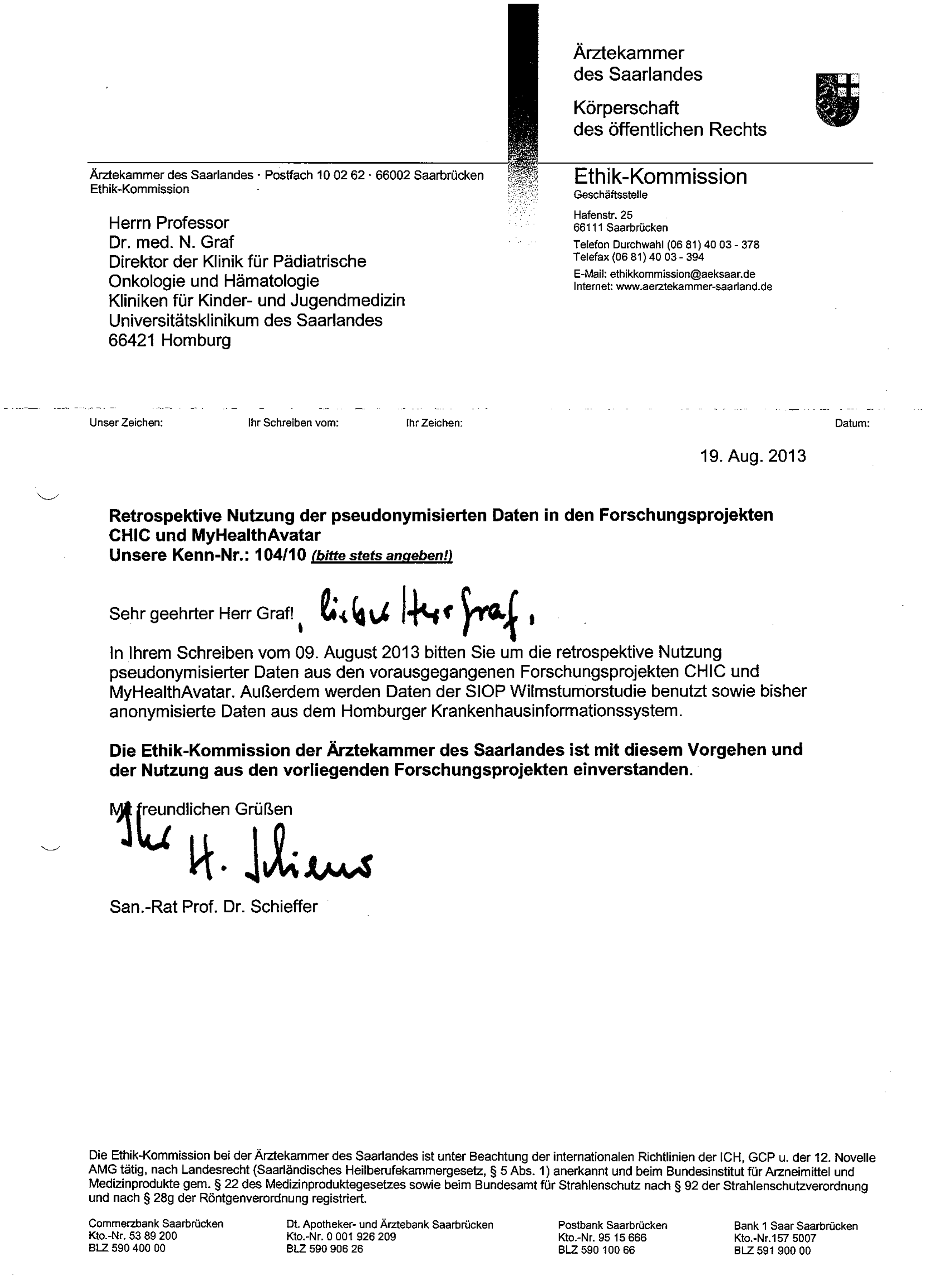
Thereafter the patient can release the data or not without telling why and solely for use in a given project (or category of projects), as the patient wishes. In the interests of ensuring data security and transparency, the information as to which data were released to whom at what time will be stored in the platform as well as the informed consent.

It will also be important to build a security system in order to meet the requirements of Article 17 of Directive 95/46/EC. The latter 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[260] 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.

By building the security system, MHA will 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.

[260] See http://www1.umn.edu/humanrts/instree/coerecr97-5.html.

Appendix 6 – Ethical Approval for data use from USAAR



Ärztekammer
des Saarlandes

Körperschaft
des öffentlichen Rechts

Ärztekammer des Saarlandes · Postfach 10 02 62 · 66002 Saarbrücken
Ethik-Kommission

Herrn Professor
Dr. med. N. Graf
Direktor der Klinik für Pädiatrische
Onkologie und Hämatologie
Kliniken für Kinder- und Jugendmedizin
Universitätsklinikum des Saarlandes
66421 Homburg

Ethik-Kommission
Geschäftsstelle

Hafenstr. 25
66111 Saarbrücken
Telefon Durchwahl (06 81) 40 03 - 378
Telefax (06 81) 40 03 - 394
E-Mail: ethikkommission@aeksaar.de
Internet: www.aerztekammer-saarland.de

Unser Zeichen:	Ihr Schreiben vom:	Ihr Zeichen:	Datum:
			19. Aug. 2013

Retrospektive Nutzung der pseudonymisierten Daten in den Forschungsprojekten CHIC und MyHealthAvatar
Unsere Kenn-Nr.: 104/10 ***(bitte stets angeben!)***

~~Sehr geehrter Herr Graf!~~ Lieber Herr Graf,

In Ihrem Schreiben vom 09. August 2013 bitten Sie um die retrospektive Nutzung pseudonymisierter Daten aus den vorausgegangenen Forschungsprojekten CHIC und MyHealthAvatar. Außerdem werden Daten der SIOP Wilmstumorstudie benutzt sowie bisher anonymisierte Daten aus dem Homburger Krankenhausinformationssystem.

Die Ethik-Kommission der Ärztekammer des Saarlandes ist mit diesem Vorgehen und der Nutzung aus den vorliegenden Forschungsprojekten einverstanden.

Mit freundlichen Grüßen

Ihr H. Schieffer

San.-Rat Prof. Dr. Schieffer

Die Ethik-Kommission bei der Ärztekammer des Saarlandes ist unter Beachtung der internationalen Richtlinien der ICH, GCP u. der 12. Novelle AMG tätig, nach Landesrecht (Saarländisches Heilberufekammergesetz, § 5 Abs. 1) anerkannt und beim Bundesinstitut für Arzneimittel und Medizinprodukte gem. § 22 des Medizinproduktegesetzes sowie beim Bundesamt für Strahlenschutz nach § 92 der Strahlenschutzverordnung und nach § 28g der Röntgenverordnung registriert.

Commerzbank Saarbrücken	Dt. Apotheker- und Ärztebank Saarbrücken	Postbank Saarbrücken	Bank 1 Saar Saarbrücken
Kto.-Nr. 53 89 200	Kto.-Nr. 0 001 926 209	Kto.-Nr. 95 15 666	Kto.-Nr.157 5007
BLZ 590 400 00	BLZ 590 906 26	BLZ 590 100 66	BLZ 591 900 00