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

Project acronym: MyHealthAvatar

Deliverable No. 11.3
Understanding the Legal and IPR regime in MyHealthAvatars

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.:	D11.3
Document name:	Understanding the Legal and IPR regime in MyHealthAvatars
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	PU
Version:	1
Actual Submission Date:	31/08/2015
Editor: Institution: E-Mail:	Prof. Dr. Nikolaus Forgó LUH forgo@iri.uni-hannover.de

ABSTRACT: This deliverable provides an overview of the most important legal issues that need to be considered in the context of digital avatars. In particular data protection issues, including e-consent systems, data collection by hospital information systems and apps, data sharing and liability are under review. But also intellectual property rights are crucial.

KEYWORD LIST: e-consent system, hospital information system (HIS), data sharing, apps, liability, data ownership, Intellectual Property Rights (IPR)

[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^{o} 600929.

MODIFICATION CONTROL			
Version	**Date**	**Status**	**Author**
0.1	15.07.2015	Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.iur Alan Dahi, Iryna Lishchuk
0.2	11.08.2015	Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass. iur Alan Dahi, Iryna Lishchuk
0.3	16.08.2015	Draft	Dipl.-Jur. Sarah Jensen, Ass.iur Alan Dahi, Iryna Lishchuk
0.4	20.08.2015	Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.iur Alan Dahi, Iryna Lishchuk
0.5	22.08.2015	Pre-final draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.iur Alan Dahi, Iryna Lishchuk
0.6	27.08.2015	Review draft	Prof. Feng Dong (BED), Prof. Dr. Norbert Graf (USAAR), Dr. Emmanouil G. Spanakis (FORTH)
1.0	31.08.2015	Final	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.iur Alan Dahi, Iryna Lishchuk

List of LUH contributors

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

Contents

1. Executive Summary

This deliverable gives an overview and analysis of the main legal issues that can arise in the context of digital avatars. It consists of two main parts. The first part focuses on data protection issues including data ownership, electronically given consent, data collection and sharing, and liability for the correctness of data. The second part analyses intellectual property implications of digital avatars and depicts the IP rights that could arise if medical data is processed in avatars. It also analyses the protection of software and algorithms by IP rights, and provides an overview of IPR issues that need to be taken into account when sharing data with third parties. The overall analysis shows that data protection is just one aspect of the legal framework of MyHealthAvatar and that IPR issues are crucial as well.

Specifically, the deliverable shows that the European data protection regime does not address the question of data ownership, but sets up a rights and control regime for data that balances the data subject's rights with the interests of data controllers and processors. Regarding electronic consent, the deliverable shows that there are no insurmountable hurdles, and that consent can in principle be sought and granted electronically. The situation may be further clarified once the General Data Protection Regulation enters force (insofar as this provides for harmonised rules on the conditions for explicit consent). However, the European policy maker should consider legislating clearer rules on the certification of software-based health and life-style tools and apps, and governing redress in cases of harm resulting from use. These rules should also clarify the responsibilities of the eco-systems, including platforms like MyHealthAvatar, which act as intermediaries in presenting such tools and apps to users. Concerning intellectual property, the deliverable shows that software components of MHA are protectable by copyright, and that user-submitted data could in some circumstances also enjoy copyright protection.

2. Introduction

This deliverable is the outcome of task 11.3. The task calls for a general analysis of legal issues surrounding the use of digital patient-centered health avatars. In particular, the task raises the questions of data ownership and control, of responsibility and liability for the correctness of the data, as well as of collecting and sharing data, for example with hospitals, data warehouses, and social networks such as Twitter and Facebook. This is a more abstract analysis than deliverable 11.1, where LUH provided a concrete analysis of the MHA legal framework and the high-end use scenarios, data linkage and architecture (including proposed use of cloud computing).

Thus, the aim of this deliverable is to give the reader the necessary overview of the data protection and the intellectual property regimes as they apply to the MyHealthAvatar project, and to highlight some of the major legal issues. Consequently, the deliverable is structured in two parts.

The first addresses data protection and related aspects such as the question of data ownership and questions of granting consent electronically. Data ownership, broadly understood, is at the core of MyHealthAvatar, because the project is essentially a tool to organize sensitive health data that ultimately originates from the user herself. It is also an important issue to focus on because the sensitive data will be "handled" by a number of actors. How can the MyHealthAvatar user ensure that the data she releases will not end up in the wrong hands or be used to her detriment? Another issue that is explored is that of electronically granted consent: How does this differ from consent granted offline? How should MyHealthAvatar approach the matter? Following consent the question of how data is collected, both by MyHealthAvatar and by external apps that will connect to the MyHealthAvatar platform. This leads us to the sharing of data with third parties such as social networks and hospitals and of how to address the risks of sharing data, which is an inherent and essential element of the platform, without compromising its functionality. Arising out of the collection and sharing of data is the issue of liability for the factual correctness of the data. Correct data is an absolute requirement when it comes to health, as the data is the basis for recommendations regarding lifestyle changes and treatment of conditions. Incorrect data can lead to the user suffering harm.

The second part of the deliverable is equally important. It addresses questions of intellectual property rights that need to be considered – both with regards to the development of the platform, as well as concerning its use. Examples are the protection that underlying algorithms and software are awarded by the law, and the intellectual property implications of sharing data with third party networks such as Withings and Twitter.

We conclude the deliverable by summarizing the results and providing policy recommendations, where available.

3. Data protection and privacy implications of digital health avatars

3.1. Whose data is it? The issue of ownership in personal data

3.1.1. Background – why this issue poses a challenge in MyHealthAvatar

At the heart of MyHealthAvatar (MHA) is personal data, which ultimately is always derived from the user herself. It is envisaged that, when the platform is operational, the data will be collected by the hospital and then inputted by the user or the hospital into MyHealthAvatar,[3] or that it might be collected by the user herself and then entered into the system.[4] Either way, the source is always the user. A user might consequently feel that it is *her* data that is being processed, and that she should be able to do with it as she pleases – including, perhaps, prohibiting others, such as the data collector, from doing with the data as they please. In contrast, the entity that collected the data might argue that it should have extensive rights over the data because of the effort made in collecting and curating it. By way of example, should the "ownership" of an x-ray image of a fractured fifth metacarpal made by a hospital to treat a patient's injury rest with the hospital or with the patient? What about the fact, the piece of information, that the patient injured herself? And even more basic: What is ownership exactly?

As already indicated by our patient who wishes to do with her data as she pleases, including denying others its enjoyment, the law typically understands (in simplified terms)[5] ownership as the societally recognized right of a person (legal or natural) to exert exclusive control over a thing.[6] However, things typically do not emanate their state of ownership. Simply looking at an object will not tell you who the owner is. In order to facilitate legal transactions, both the common law[7] and the civil law[8] have variations of the idea that possession, ie physical control, is generally indicative of ownership.

However, possession of data is not as clearly definable as is possession of chattels. Indeed, the intangible nature of personal data means that traditional approaches to ownership

[3] D3.2 v2.0, pp. 40 et seqq.

[4] D9.1, p. 75 et seq.

[5] This simplification ignores that society does not recognize any absolute property right, as becomes clear for example during a criminal investigation, where the state can seize property. See also article 14 paras 1 and 2 of the German Basic Law (*Grundgesetz*): "(1) Property and the right of inheritance shall be guaranteed. Their content and limits shall be defined by the laws. (2) Property entails obligations. Its use shall also serve the public good." See also Barbara J Evans, 'Much ado about data ownership', (2011) 25 Harv. J. L. & Tech. 79 et seqq, p. 69-130.

[6] See the following description of how people imagine property to be: "There is nothing which fo generally ftrikes the imagination, and engages the affections of mankind, as the right of property; or that fole and defpotic dominion which one man claims and exercifes over the external things of the world, in total exclufion of the right of any other individual in the univerfe." William Blackstone, *Blackstone's Commentaries on the Laws of England* (first printed in 1765), .P 2 *The* Rights *of* Things. Book II. Ch. i. Accessible at http://avalon.law.yale.edu/18th_century/blackstone_bk2ch1.asp.

[7] Carol M. Rose, 'Possession as the Origin of Property', (1985) Faculty Scholarship Series, Paper 1830, see http://digitalcommons.law.yale.edu/fss_papers/1830, p. 74 et seqq.

[8] Eg section 1006 of the German Civil Code (*Bürgerliches Gesetzbuch*).

cannot be easily applied to it. A tangible asset, for example a hammer, is fully rivalrous – it can only be used in a zero-sum fashion. This is in contrast to intangible assets such as data, which can be replicated without limit and are non-rivalrous, ie which can principally be used by more than one person simultaneously without their usefulness being affected.[9] This can be particularly seen where data is stored in the cloud, as is also the case in MyHealthAvatar, as described in deliverable D3.2 v2.0. pp. 8, 17. A multitude of parties may have (simultaneous) access to data stored in the cloud.

Even though basically all jurisdictions have adopted[10] so-called intellectual property rights (IPR)[11] such as copyright, patents, and trademark, which grant a type of control over certain intangibles, information *per se* such as facts – and that is generally what personal data is, namely facts relating to an individual – do not fall under the IPR regime.[12] Even if personal data is not "property", though, it is apparent that there are other forms of rights and duties governing and limiting its use. This part will consider these issues further against the backdrop of European data protection law.[13]

3.1.2. European data protection law and "data ownership"

As illustrated, property rights are the legal recognition that the owner shall have (exclusive) control over a thing's use. However, ownership is not the only vehicle the law can use to convey such control. Control regimes and rights can have a very similar effect to property/ownership.[14] To a certain extent, this is what the current European data protection framework seeks to achieve. It is in effect a control regime that grants certain rights over personal data, however without addressing the ownership of the data. The only explicit reference to property/ownership is the statement in Directive 95/46/EC (the Data Protection Directive)[15] that the access rights a data subject enjoys "must not adversely affect trade secrets or intellectual property".[16] The Data Protection Directive distributes its control regime across three main actors: the data subject, the data controller, and the data processor. Each of these actors has a certain set of rights that, at least in part, speak for an element of control over the data.

[9] Barbara J Evans, 'Much ado about data ownership', (2011) 25 Harv. J. L. & Tech. 78, p. 69-130.

[10] See as a proxy for this statement the list of member states of the World Intellectual Property Organization, available at http://www.wipo.int/members/en/.

[11] The application of IPR to MyHealthAvatar is looked at in detail in part 4 of this Deliverable below.

[12] Gilad Rosner, 'Who owns your data?' in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (UbiComp '14 Adjunct). ACM, New York, NY, USA (2014), 623-628, 625. DOI=10.1145/2638728.2641679, see http://doi.acm.org/10.1145/2638728.2641679.

[13] The United States has similar problems in figuring out ownership of personal (patient) data. See for example Barbara J Evans, 'Much ado about data ownership', (2011) 25 Harv. J. L. & Tech, p. 69-130.

[14] Gilad Rosner, 'Who owns your data?' in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (UbiComp '14 Adjunct). ACM, New York, NY, USA (2014), 623-628, 627. DOI=10.1145/2638728.2641679, see http://doi.acm.org/10.1145/2638728.2641679.

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

[16] Recital 41 Data Protection Directive.

3.1.2.1. The data subject

The data subject is the individual to whom a piece of personal data relates; the data subject is the source of the personal data. In recognition of the data subject being the origin of "her" personal data, and in acknowledgment of the fact that the data subject will generally want to control her data the Data Protection Directive grants the data subject a number of rights that she can exercise in regard to her data. These are mainly rights of information,[17] of access,[18] and of rectification, erasure and blocking of data.[19] These rights give the data subject a toolset with which she can control to a certain extent her personal data: She can access it, and she can have it rectified, erased and blocked. By way of these rights, the data subject has a certain amount of 'ownership' of, in the sense of effective control over, her data.

3.1.2.2. The data controller

The term "data controller" already suggests control over the data. The data controller is the party who "alone or jointly with others determines the purposes and means of the processing of personal data"[20]. The control can stem from explicit legal competence (ie by legislative act), from implicit competence (ie by legal practice, for example for an employer in relation to its employees), and from factual influence (such as by virtue of a contract between the data subject and the data controller; or simply by virtue of the factual circumstances, regardless of the legality of the processing).[21] Flowing from this aspect of control, the Data Protection Directive places a number of legal obligations on the data controller, which are the mirror image of the data subject's rights.

3.1.2.3. The data processor

A data controller can engage a "data processor", which is a party who processes the data on the controller's behalf.[22] The defining elements in the controller-processor relationship are that the controller assumes overall responsibility for the processing occurring,[23] and also that the data controller determines the purpose of the processing.[24] As soon as the data processor processes for purposes not assigned by the controller, the processor becomes in respect to the extra-contractual processing a data controller. The data processor, consequently, while having a certain level of potential control over the data, is the furthest removed from the class of data owner because the processor only acts subject to instructions from the data controller. This situation can be compared to the so-called "Besitzdiener" (*servant of possession*) recognised in German law[25]. Even though the *Besitzdiener* has factual possession (control) of a chattel, the law denies recognition of any

[17] Articles 10, 11 Data Protection Directive.

[18] Article 12 Data Protection Directive.

[19] Recital 41, Art 12 (b) Data Protection Directive.

[20] Article 2 (d) Data Protection Directive.

[21] Opinion 1/2010, p. 10 et seqq.

[22] Article 2 (e) Data Protection Directive.

[23] European Union Agency for Fundamental Rights, Council of Europe – European Court of Human Rights, *Handbook on European data protection law* (2014), p. 88 et seq.

[24] Opinion 1/2010, p. 15.

[25] See section 855 of the German Civil Code (*Bürgerliches Gesetzbuch*).

legally recognised possession on grounds that the *Besitzdiener* only acts subject to instructions by the legal possessor.

3.1.3. Summary

Summarising the above, personal data in the European Union is subject to a data protection framework that grants certain rights to its use to a number of actors. In response, then, to the question posed in the task on the ownership of the data processed in MyHealthAvatar, there is no single "owner" of the personal data (with the exclusive right to determine what is done with it) – the law does not directly address the issue of ownership of the data. Rather, the law creates a rights and control regime under which the use of the data is regulated. One of the most powerful elements of the control regime put in place by the Data Protection Directive is the principle of consent. In this regard, a key issue in MyHealthAvatar is ensuring the validity of user consent to the processing of their health data in a context, where – rather than communicating directly with health care personnel - they interact with the system remotely. This raises the question of how consent may be granted digitally, which will be addressed next.

3.2. The challenges of granting consent digitally – electronic informed consent

Asking volunteers and potential users of the MyHealthAvatar platform for consent is an important element of the MyHealthAvatar legal framework[26] in showing that the project respects the doctrine of informed consent that aims to achieve the protection of the fundamental rights to autonomy and self-determination of individuals whose sensitive health data is going to be processed.[27] The consent-driven approach shows that MyHealthAvatar does not only comply with legal norms, but also with ethical requirements – the common decency and minimal respect we owe to other persons demand that wherever possible informed consent should be obtained.[28] Since the typical individual user will wish to join the MyHealthAvatar platform from home rather than in a clinical environment (where the user interacts face-to-face with a relevant clinician), electronic informed consent (e-consent) will play a key role.

3.2.1. The added value of e-consent compared to paper-based consent

E-consent is frequently not only delivered electronically, but is also interactive with multi-media such as videos, audio files[29], interactive graphics, podcasts and embedded comments in the consent forms[30], as well as diagrams, images and graphics.[31] Moreover, some e-

[26] See MyHealthAvatar Deliverable 11.1, The Ethical and Legal Framework of MyHealthAvatar, part 5.

[27] Forgó, Kollek, Arning, Kruegel, Petersen, 'Ethical and Legal Requirements for Transnational Genetic Research' (2010), p. 10.

[28] Ibid.

[29] Hudziak, Lilly, 'Session IV: Use of E-Consent Technology in the Informed Consent Process' (2015).

[30] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011), see http://www.quorumreview.com/blog/2011/12/08/recording-slides-quorums-webinar-electronic-consent-technologies-facilitate-improve-research-process/.

[31] FDA, p. 5.

consent systems allow one to click on a link for further information on a particular part, to click on terms to get connected to an online dictionary in order to understand a special term[32], or to tag unclear sections in order to ask clinical staff later.[33] By supplementing text information in such a fashion, information can be presented in a more user-friendly and digestible fashion, allowing the user to better understand what she is asked to sign.[34] This should result in improved satisfaction and decision-making by the individual.[35] Of course, the interactive measures that are used must be appropriate for the comprehension level of the targeted individuals.[36] E-consent systems have the added advantage of being able to check if the user has understood what she is asked to give consent to, for example by asking multiple-choice questions at the end of each section of the e-consent that are automatically evaluated.[37] In contrast, paper-based consent forms are linear and may overburden the data subject with too much information.[38]

Moreover, the risk of being pressured into consenting could be lower than it is with traditional paper-based consent forms because the user can better analyse the consent form in an informal atmosphere and ask family members and friends before signing it.[39] It is likely that a user will inform herself in a more detailed manner at home[40] than if asked in a hospital setting. Later, in case of any proposed modification of the scope of processing, the MyHealthAvatar user can be asked for new e-consent to cover this, easily by email or another electronic notification, which again links to clear explanations of the changes and their implications. As discussed later, in part 3.5.3 below, this may also provide a useful and beneficial mechanism for obtaining consent for research uses of the data.

Finally, electronic consent has the advantage that withdrawal of consent is easier, as the grantor can do so electronically without having to go back to the grantee.

3.2.2. Challenges of e-consent systems

Despite their benefits, e-consent systems also have disadvantages. For example, users will have fewer possibilities to directly ask staff questions.[41] Assuming the necessary resources, MyHealthAvatar should be organised to alleviate this disadvantage by permitting interested citizens to contact MyHealthAvatar staff who can answer questions adequately. Contact could be in-person or via (video-) chats, telephone and email. This mirrors the draft

[32] McNair, Costello, Crowder 'Electronic Informed Consent: A New Industry Standard' (2014), p. 1.

[33] McNair, Costello, Crowder, 'Electronic Informed Consent: A New Industry Standard' (2014), p. 1.

[34] Parrish , 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011); Gossen 'Electronic Informed Consent: Possibilities, Benefits, and Challenges' (2012), see http://rebarinteractive.com/electronic-informed-consent-introduction/.

[35] Hudziak, Lilly, 'Session IV: Use of E-Consent Technology in the Informed Consent Process' (2015).

[36] FDA, p. 5.

[37] FDA, p. 5.

[38] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011).

[39] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011).

[40] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011).

[41] Coiera, Clarke 'The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment' (2004), Journal of the American Medical Informatics Associatin, Voll 11 No 2, p. 130.

guidance by the US Food and Drug Administration (FDA) "Use of Electronic Informed Consent in Clinical Investigations – Questions and Answers – Guidance for Industry"[42], which similarly recommends offering intra-person discussions with study personnel or electronic messaging, telephone calls, videoconferencing and live chats.[43]

Further challenges are ensuring that the e-consent system is secured against unauthorised access and that the person signing is properly authenticated. We will investigate these issues in part 3.2.4. First, though, we will consider how MyHealthAvatar could manage the e-consent process from a legal and ethical viewpoint.

3.2.3. The legal and ethical requirements of e-consent

At the outset one may note that Data Protection Directive itself does not specifically mention e-consent, but only consent in general. As can be found in article 7 (a) and especially in article 8 (2a) Data Protection Directive, the processing of sensitive personal data such as health data is forbidden except if there is a legal basis or the data subject has given informed and explicit consent. The same principle is restated in the Council's draft of the planned General Data Protection Regulation[44] (GDPR). Recital 31 GDPR states: "In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law". Article 2 (h) Data Protection Directive defines the "data subject's consent" 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 GDPR defines consent similarly.[45]

Thus, there is the formal need to ensure that consent is given "explicitly" under article 8 (2a) Data Protection Directive. According to the Article 29 Working Party[46], explicit consent means that consent must be expressed by the data subject.[47]Here, it should be stressed that only an "opt-in-solution" should be considered, and not an "opt-out-solution" where the individual would have to delete an already ticked box.[48] Moreover, it must also be ensured that the data subject consents without any undue external pressure, eg exerted by a physician, employer, health insurance company, or pharmaceutical company. Consent must also be specifically informed in line with article 2 (h) Data Protection Directive [and article 4 (8) GDPR]. We next consider each of these requirements in more detail.

---

[42] See http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM436811.pdf.

[43] FDA, p.4.

[44] See http://statewatch.org/news/2015/jun/eu-council-dp-reg-9398-15.pdf.

[45] Article 4 (8) GDPR.

[46] 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.

[47] Opinion 15/2011, p. 25.

[48] Article 29 Working Party's Opinion 15/2011, p. 25 et seq.

3.2.3.1. Achieving explicit consent electronically?

The Data Protection Directive does not state that explicit consent must necessarily be given in a written form. According to the Article 29 Working Party's Opinion 15/2011 on the definition of consent[49], explicit consent may also be given by using electronic or digital signatures.[50] Depending on the context, clickable buttons, sending confirmation emails, clicking on icons, etc are also valid measures to signify explicit consent.[51] These two methods are illustrative of the two types of electronic consent that exist: the "full signature" consent, signified by electronic or digital signature, and the "not-full signature"[52] consent, signified eg by ticks of a box or answers to questions.

However, in practice, such consent is typically given with a hand-written signature.[53] Moreover, some member states require in their domestic data protection law that consent has to be in writing. This is possible because the Data Protection Directive only sets the minimum standards to be applied at national law and member states are free to apply stricter rules as long as the latter do not conflict with free movement and free market rules. For instance, article 27 (2) (1) Polish Data Protection Act states that consent has to be given in written form for the processing of sensitive data. And § 4a (1) German Federal Data Protection Act (FDPA)[54] stipulates that "[c]onsent shall be given in writing unless special circumstances warrant any other form". According to paragraph 2 sentence 1, in the field of scientific research, a special circumstance shall be deemed to exist if the defined purpose of research would be seriously affected if consent were obtained in writing. Also the Greek Data Protection Act[55] requires a written consent form for the processing of sensitive health data pursuant to article 7 (2a) Greek Data Protection Act[56].

Here electronic signature software can be used on computers, tablets and with PDF documents.[57] According to article 5 (1) E-Signature-Directive 1999/93/EC[58] electronic signatures are also to be regarded as equivalent to written signatures. However, this directive is in the process of being repealed and will be replaced by regulation 910/2014[59] from July 2016.[60] The aim of the new regulation is to strengthen the EU Single Market by

[49] See http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[50] Opinion 15/2011, p. 26.

[51] Opinion 15/2011, p. 26.

[52] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011).

[53] Opinion 15/2011, p. 25.

[54] See http://www.gesetze-im-internet.de/englisch_bdsg/index.html.

[55] http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF.

[56] See http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF.

[57] See http://bio-optronics.com/advancing-clinical-research-understanding-econsent/.

[58] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML.

[59] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[60] See http://certifiedsignature.eu/.

building trust and convenience in secure cross-border electronic transactions, but does not change significantly the area of electronic signatures.

In terms of the current draft of the GDPR, which is expected to replace the Data Protection Directive in the next few years, this would not require an electronic signature for e-consent: Recital 25 stipulates that consent can be given by a

> "written, including electronic, oral statement or, if required by specific circumstances, by any other clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed".

This

> "could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data".

Since a regulation is self-executing and does not require any implementing measures, it actually leads to a harmonized level of protection which means that – on the basis of recital 41, articles 4(8) and 9 – explicit consent will not require a written expression in the member states anymore.

However, since the GDPR is still only a draft, there is no definitive answer yet whether there will be a uniform approach to the requirements for an 'explicit consent'. So MHA should at any rate allow for the possibility that in some member states written consent will be needed. As noted, the use of qualified electronic signatures would be one option because they count as written consent and provide strongest proof of the individual having consented. However, such signatures are not used widely. Therefore it may create difficulties for the acceptance of MyHealthAvatar to build an e-consent system asking for electronic signatures.

For now (pending the adoption of the GDPR), another option would be to provide for traditional hardcopy consent forms as an alternative for users based in those member states that require formal written consent. In this regard, the system could be initially configured in such a way that MHA offers different forms of consent (e-consent, written consent) according to the user's member state of domicile.

3.2.3.2 The need for voluntary consent

As stated in article 2 (h) Data Protection Directive [and in article 4 (8) GDPR], consent must be given voluntarily. This requires that the consent system is non-intrusive and that doctors, researchers, employers, health insurers and pharmaceutical companies are prevented from exerting pressure on the individual to register with MyHealthAvatar and/or to share stored data with them. For example, health insurance companies might try to coerce an individual to sign up to MyHealthAvatar in order to evaluate her health data before deciding on whether/how to insure her. Although this risk cannot be avoided completely, the

consortium must think about appropriate measures to ensure that this risk is as minimal as possible.

Once the platform is up and running it will also be important to consider that subsequently (during their on-going use of the platform) many individuals will wish to transfer their data to third parties and/or make the data available for processing by tools and apps developed by third parties. Here, one option would be to ask third parties to sign a contract with MyHealthAvatar before the MyHealthAvatar user can share the data with them and to include article provision stating that exerting pressure, duress and coercion is prohibited and leads to exclusion from the whole MyHealthAvatar sharing system. This requires that the platform administrator implements a centre where users can notify the latter of third parties having exerted pressure. There may also be the risk of domestic pressure (eg one spouse demanding access to the other's data): a possible solution at the practical level could be to install a panic button that can be pressed in the case of exerted pressure and coercion. By using this panic button, access to the stored data can be declined by simulating a technical problem, for instance.

3.2.3.3. The need for informing the individual

Interested citizens should be informed of the intent and purpose of MyHealthAvatar, its functionalities, risks, etc. by full and appropriate information and consent forms that must be read before it is possible to sign up to MyHealthAvatar. As suggested, in the context of e-consent, this information would be provided in a structured and layered way on-line. Such information and the user consent forms must be offered in different languages according to the platform target population. In order to build trust, the documents should show the user that MyHealthAvatar complies with legal requirements and secondly should guarantee that personal data will not be misused. Multi-media functions and clickable links should be included to make the information as user-friendly as possible.

In Annex 2, a draft model information sheet (adaptable for electronic presentation) and consent form is presented that could be used for the (planned) MyHealthAvatar user interface to upload personal data. The information included, and consent, is designed to cover the initial signing up by the user and provision of data by the user to the platform. Subsequently, further consents would be sought electronically to additional processing purposes (including where the data would be shared with other parties, eg the patient's physician, or accessed by third party apps. A further, special situation, involving the need for further consent as well as other safeguards, relates to the potential processing of user health data in the platform for secondary purposes (as opposed to for the direct care or treatment of the user). The key scenario here, of usage of such data for general scientific research purposes, is addressed in part 3.5.3 below.

3.2.4. The duty of the controller to implement necessary technical measures

Since the platform administrator fulfils the definition of the data controller according to article 2 (d) Data Protection Directive [and article 4 (5) GDPR], she needs to implement technical mechanisms that ensure that the above-mentioned requirements are met from a technical point of view. Firstly, the data controller must take measures to check that the

person giving consent is the person to whom the data relate.[61] In this regard, the recommendations of the FDA are instructive in the manner they deal with the issue of identity and state that the system should include a method to ensure that the person signing the consent form is the subject concerned.[62]

Secondly, it is crucial to maintain the individual's freedom to give consent. Article 12 (b) Data Protection Directive and article 7 (3) GDPR stipulate that the data subject must be able to withdraw her consent at any time without needing to indicate any reason. The data subject's right to withdraw her consent is also relevant in terms of situations where parents have given consent for their minors. It is recommendable to include an alert system for notification of the adult user that new consent is sought. Moreover, the platform administrator should observe the legal age of maturity; in this regard, mechanisms will need to be explored for verifying that the user has sufficient capacity to grant consent and access and review relevant information.

The e-consent system must also offer an easy solution for the user to delete her avatar and to withdraw her consent at any time, as data subjects have the right to withdraw their consent. The user should also always be able to access the consent form in the avatar system. To store the consent form in the MyHealthAvatar platform is also important for the platform administrator, because this allows him to easily prove that consent was given. It is also necessary to comply with the recommendation of the (non-binding) recital 32 GDPR that states that

> "[w]here processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given the consent to the processing operation [...]. A declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and its content should not be unusual within the overall context".

In addition to the need for recording whether the user has adequately been informed of all choices and consequences, the data controller should enable the MyHealthAvatar user to change her consent and privacy preferences. This is especially relevant for data sharing, eg with treating physicians. It implies that the MyHealthAvatar user is able to give and withhold e-consent to the data processing in general and the data sharing in particular.

Furthermore, the MyHealthAvatar user must be able to manage the access rights to her data: she must be able to decide who should have access to the data and she must be able to follow the data flow. Only then will the requirements of article 12 Data Protection Directive and articles 14, 15 GDPR be met and data transparency ensured. For this goal an audit trail needs to be implemented. An audit trail, including via a document versioning system, is important to understand if there were revisions of the consent form.[63] This

[61] Coiera, Clarke, 'The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment', *Journal of the American Medical Informatics Association,* Vol. 11 No. 2 (2004), p. 135.

[62] FDA, p. 4.

[63] FDA, p. 8.

should include the identity of the person who revised the consent form, why the changes were necessary and when the changes took place.[64]
Moreover, access control mechanisms have to be adopted. Common methodologies in this context are the Discretionary Access Control (DAC), the Mandatory Access Control (MAC) and the Role Based Access Control (RBAC). All these methodologies are analysed in D3.2 v2.0.[65]

The DAC means that the authorisation originates from the owner or creator of an object and is passed on to other projects. In MAC permissions are managed centrally and ordinary users of the system cannot change the permissions. In RBAC permissions are granted by the system not with focus on the subject itself but rather on the task or purpose a subject has. The subjects are categorised into roles according to their tasks and each role is then assigned to a corresponding set of permissions.[66]

The analysis of all three types of access control mechanisms leads to the result that neither DAC nor MAC are suitable for MyHealthAvatar. DAC does not permit the user to change permissions.[67] MAC is not appropriate because of the difficulties and costs to manage a huge amount of objects and users centrally.[68] RBAC seems to be suitable as it permits users to easily manage their own permissions. The reason for this is that the system is characterised by organisational structures of institutions that can be mapped to roles in a straightforward manner.[69] However, RBAC can only be implemented after having clarified uncertainties and undecided details, such as different tasks and permission rights.
Apart from this, the data controller needs to ensure that the mechanisms and channels through which the individual can view her private information are safeguarded.[70] Otherwise unauthorised third parties could access patient information by circumventing the consent checking mechanism.[71] Therefore the e-consent system must be supported by security functions that minimise the likelihood of unauthorised access.[72] In accordance with article 17 Data Protection Directive, these should ensure a level of security appropriate to the risks represented by the processing and the (in this case, highly sensitive) nature of the data to be protected. Restricted access and methods to ensure confidentiality regarding the subject's identity and encryption of the data subject's information are appropriate measures

[64] FDA, p. 9.
[65] D3.2 v2.0, p. 58 f.
[66] D3.2 v2.0, p. 58.
[67] D3.2 v2.0, p. 58.
[68] D3.2 v2.0, p. 58.
[69] D3.2 v2.0, p. 58 f.
[70] Coiera, Clarke, 'The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment', *Journal of the American Medical Informatics Association,* Vol. 11 No. 2, p. 129 f.
[71] Coiera, Clarke, 'The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment', *Journal of the American Medical Informatics Association,* Vol. 11 No. 2, p. 131.
[72] Coiera, Clarke, 'The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment', *Journal of the American Medical Informatics Association,* Vol. 11 No. 2, p. 135.

to make the system secure, as a minimum.[73] Support services, personnel training and user education should be considered as well.

The system should equally be sensitive to user behaviour in practice, such as the possibility some users, at least initially, may not include their real ID in their profile to sign up. This could be addressed by providing for credential checks to ensure that the user logging in is the person who created the account in the first place. The verification of user ID will also be a crucial element in relation to the proposed linkage with hospital HIS systems (considered in 3.3): here it must be controlled that an MHA user requesting transfer of HIS data to the platform really is the relevant hospital patient. A further risk identified by the MHA consortium is that personal health records may inadvertently be inaccurate. This risk can be reduced by using data from hospital information systems (collected according to recognised technical standards). However, as discussed in part 3.3, below, this – at least where a direct transfer of data is aimed at – poses some practical and legal challenges. In other cases, where data is inserted by the user, a secure user ID should be used for logging in the system to avoid that fake data are uploaded by unauthorised third parties.

3.3 Collecting data by linkage with Hospital Information Systems and other external data warehouses

As discussed in deliverable D11.1, a key assumption for the successful deployment of the MyHealthAvatar platform is that health and lifestyle data gathered in a variety of contexts can be linked in a rapid and seamless way to allow a realistic complete overview of each user with regards to their health and lifestyle. Consequently, data should be as complete and accurate as possible in order for correct decision-making by the patient (regarding strategies for reducing future health-risks, or self-management of existing conditions). The same goes for decisions made by other actors with whom the user has opted to share the data, such as the patient's physician. Here, work has been ongoing in WP 6 to develop data collection utilities, and to experiment with the Linked Data approach, so patients do not have to undertake excessive efforts themselves to populate the data repository with health-related data, which instead can be collected, eg, by mobile apps such as Fitbit and Moves.[74]

Besides such lifestyle data, another essential source of patient health data – of particular value in terms of potential quality and relevance – is data collected on the user by health professionals in the course of clinical care and treatment provided to the user, and then stored in the hospital information system (HIS) of the relevant clinical provider.[75] Similarly, in the case of data approved for research use, this may reside in a relevant data-bank or warehouse. Accordingly, the WP6 architecture (mainly being implemented by BED) seeks to support the export of health-related patient data from linked hospitals, and provide a methodology for the linking, as well as taking account of data storage and security aspects.[76] Nevertheless, a challenge of a non-technical nature that remains with regard to sourcing

[73] FDA, p. 7.

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

[75] See D3.2 v2.0 p. 41.

[76] D6.1, p. 6.

and use of HIS data stems from institutional inertia and risk adversity: hospitals holding valuable data are often unwilling to share it for various reasons, some more cogent than others, including patient confidentiality concerns, proprietary motives and resource implications. These problems were noted by the EU eHealth Task Force in its Report 'Redesigning health in Europe for 2020', where it commented on the current tendency for health data to be 'siloed' within many discrete hospital repositories, and the need for data release for its potential (to improve the level of health care and efficiency of health care systems) to be realized.[77]

Against this background, the MHA project will utilize an approach driven by user demand, in which the process of instigating the transfer of HIS data is led by the patient (the term used hereafter for a platform user who has relevant data stored in an HIS) by entering a formal data transfer request to the clinic/hospital or other data warehouse/repository to ask for transfer to the MHA infrastructure. This approach accords with the overall patient-centered ethos that informs the project, with its goal of empowering citizens/users to take responsibility where practical for their own health care and lifestyle choices. In this context, bearing in mind also that the hospital, in transferring the data, would be processing it within the definition Data Protection Directive, the rules of the Directive serve to concretize the nature and form of the consent required.

A draft model 'patient data transfer request', which aims to demonstrate, in line with these requirements, the form the patient's request to the hospital could take, so as to mandate the transfer to MHA, is presented as Annex 4 of this Deliverable. This is also coupled with a waiver by the patient, through which the latter agrees to release the hospital from potential liability arising from the transfer. (For clarity, although reference is hereafter to a 'transfer' of the data, what is generally involved is the hospital copying the relevant data to send to MHA, while retaining the original data in its system.)

In addition, from the perspective of the clinic/hospital, it will, apart from requiring the patient's consent, reasonably wish to be assured that the highly sensitive data at issue will be properly safeguarded and processed by the transfer recipient (ie the MHA platform). Admittedly, the patient has provided the hospital with a waiver, but in this developing area of the law questions may remain as to its effectiveness in some circumstances. This follows from the fiduciary element of the professional medical relationship between the hospital and its patients: thus even where the patient (through the request to transfer the data) releases it from its *prima facie* confidentiality duty, the transfer should arguably be independently justified in the patient's interests. In terms of data protection law, too, the hospital as data controller is obliged not merely to process the data lawfully (as mandated here by the patient's consent), but also in accord with the principles of fair data processing in article 6 Data Protection Directive. At least in the context of transfers of highly sensitive data to third parties, this could imply a positive duty on the transferor to verify the *bona fides* of the transferee and its competence to handle the data.

[77] See 'Redesigning health in Europe for 2020', European Union, 2012, at p. 9 ('5 levers for change').

In order to address these issues in MyHealthAvatar, a model contractual data transfer agreement has been developed for hospitals that propose (following receipt of a request from the patient) to transfer the patient's data to the MHA Platform. This draft model agreement is appended to the Deliverable as Annex 5, and its key provisions and intent will be discussed shortly. However, it is also important to take account of the possibility that a particular hospital may simply not be prepared to act upon a patient's data transfer request. In that case, there will need to be an alternative mechanism in place for getting the patient's data into the MHA infrastructure. We shall consider this alternative under point 3.3.2 below. Next, though, under 3.3.1, we consider the 'direct' way for patients to effect transfer of HIS data to the MHA repository.

3.3.1. Direct HIS data transfer approach

The first alternative by which data for a MHA user currently contained in a hospital (or similar) information system is transferred to the MHA platform envisages (i) a transfer request by the MHA platform user/hospital patient to the hospital; (ii) the hospital entering into a relevant data transfer agreement with MHA; followed then by the actual transfer. These documents enjoy a symbiotic relationship, each cross-referencing the other, and with both needed for a valid transfer to go ahead. We begin by discussing the patient data transfer request (and waiver).

3.3.1.1. Patient request and waiver

In and through this request, the patient/user does three main things: she confirms her identity and status as a current or former patient of the hospital and as a member/user of the MHA Platform; she requests the hospital to transfer her health data from its HIS to the Platform; and she agrees to release (by a waiver of potential rights of redress) the hospital from liability for harm arising from the transfer. As previously noted, a prerequisite is that the hospital can check the ID-correspondence between the patient/requester and the designated MHA user account for data transfer. Here MHA should offer the same verification standards as required by hospitals when they release health records pursuant to direct patient access requests. This may include using security questions or sending extra keywords to the user's mobile phone or by checking the IP and location where they are trying to log in.

In addition it is fundamental that the request reflects the requirements for a valid consent to the processing by the hospital in the transfer of sensitive health data, ie the need for the consent to be explicit and specifically informed as discussed in 3.2. In this regard, there is reference to the purpose of the MHA Platform as a secure data-holding infrastructure that allows the user to control access and use of her data, and that this was explained to the patient when she registered with the Platform. The document also delineates the scope of the health data for transfer: *prima facie* this will comprise health data in the HIS that relates to the patient, but the patient is also given the option to exclude some data from transfer, ie relating to relevant conditions specified by the patient.

The purpose of the waiver is to make explicit that the patient, when requesting the hospital to transfer the health data also releases the hospital from any liability for privacy-based

harm arising out of this act. Although the patient will have consented to the relevant transfer (and hence the disclosure of the data to MHA), it may be uncertain how far this would be conclusive against a subsequent claim for harm stemming from the disclosure. It is also apparent that the mere threat of a claim may have negative costs from the hospital's point of view. The waiver thus makes the parties' positions more legally certain, also by linking the effectiveness of the waiver to the fact the hospital acted not just with the patient's consent, but also in accordance with the terms of the relevant data transfer agreement with MHA. As will be discussed under 3.2.2, the latter agreement offers assurances to the hospital that MHA will deal with the data and the patient in a lawful, fair, and secure manner, thereby pre-empting an argument that the hospital (even with the patient's consent) was possibly negligent in transferring the data.[78] At the same time the agreement makes clear the hospital would remain liable for the consequences of a direct privacy-breach by itself, such as by using a known unsafe transmission method or disclosing data outside the patient's request. In such a case the patient waiver would not apply, as the transfer would not be "in accordance with the terms of the relevant…agreement" (point 3).

3.3.1.2. Data transfer agreement

The Data Transfer Agreement aims to formalize the legal position of the hospital, providing its HIS data, and the MHA Platform, as recipient, by setting out the respective rights and duties of the parties in processing the data. In particular it requires that the processing occurs consistently with ethical and legal principles of medical confidentiality, and of European data protection law. The agreement consists of a preamble (explaining the background to it), six operative clauses, and two annexes. As clause 1 explains, the agreement presupposes that the hospital has received a written data transfer request from the patient (in the form set out in Annex A of that agreement[79]) to transfer health data of the patient in the hospital's HIS to the MHA Platform. The key obligations of the hospital and of the MHA Platform are then set out in clauses 2 and 3, respectively.

3.3.1.2.1. Obligations on Hospital

Under clause 2, the hospital agrees to transfer the HIS health data of the relevant patient (who is specifically referred to in the clause) to MHA. In some cases, where the patient is no longer treated at the hospital and is not likely to visit it again (eg she has relocated to a different city), there can be a single transfer of all the data collected by the hospital during the patient's past episodes of treatment at the hospital. In other cases, where the patient remains a present or future patient of the hospital, the latter also agrees to transfer updated data within a reasonable time (left subject to further agreement by the parties) of this arriving in the hospital HIS. The hospital further agrees to only transfer data of the patient lawfully obtained and held, not to exceed the scope of the patient's request, and to observe appropriate data transit security. It acknowledges that it shall be liable for harm arising out of a breach of these obligations.

[78] Admittedly, in several member state legal systems, the consent of the victim to an act will (in line with the Latin maxim, 'volenti non fit injuria') defeat a subsequent claim for harm arising from that act; however, in this context there is the risk then of protracted debate as to the validity of the patient's consent.

[79] Presented in Annex 4 below of the present Deliverable.

3.3.1.2.2. Obligations on MHA

As noted, the obligations on MHA are contained in clause 3 of the agreement. The first of these is to ensure patient data is processed in accord with applicable data protection and confidentiality rules, and within the scope of the patient's consent. Initially, the relevant purposes and scope of data processing, with regard to the data's storage and presentation on the platform will be set by the user terms and conditions that the relevant patient signed when she registered with MHA. However, consent may also be given dynamically in the future by the user to permit further processing activities, including through making the data available via the platform to specific processing tools and services (including ones offered by third party developers). Here, as clause 3 states, MHA as the mediator of such further tools and services needs to adhere to appropriate ethical standards in its dealings with the user, including by offering a transparent environment for the user to understand, weigh up and decide on the services to use. In this regard, MHA must also ensure that the user is aware of and in a position to exercise her statutory rights as a data subject. This includes, particularly where the user has agreed to allow her data to be processed by third party tools and apps, the provision of a means for him to revoke consent and secure deletion of the relevant data.

> "A further obligation on MHA is to implement adequate technical and organizational measures, in line with article 17 Data Protection Directive, "to protect 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".

These duties are also concretized in Annex B of the agreement. In addition, the MHA platform administrator should ensure that any of its employees who will have access to the data are made aware of the terms of the agreement. There is also a special provision where it is proposed (subject to the user's consent) to process the data for secondary purposes of medical research as opposed to the user's care and treatment. Here, where the identity of the user is presumptively not integral to the processing purpose, it is provided that MHA shall ensure no more personal information than necessary is included in the data: this is consistent with the data minimization principle in article 6 (e) Data Protection Directive. Lastly MHA shall if required deposit the agreement with the relevant data protection supervisory authorities.

3.3.2. Alternative two-step transfer approach

As previously noted, there remains the possibility in some cases that a hospital, despite receiving a data transfer request from one of its patients, will not be willing to comply by initiating a direct transfer of the data to MHA. This may be for reasons connected to the local data governance policies it operates, or concerns about resources expended on the transfer (especially where the hospital plans to have no other interaction with the MHA platform and hence sees no scope for return benefits). A second issue that will in any case need to be solved is of a technical nature, namely the requirement for the platform, when receiving data in the different structures used by different HISs, to structure it into a format usable by MHA. It is thus important, pending the resolution of these issues, to consider an

alternative two-step mechanism to manage the transfer: under this approach the user will first invoke her rights under data protection law and/or applicable domestic law on accessing medical records to require the hospital to disclose the data to her; in a second step she will then upload the data herself to the MHA platform.

This alternative approach, while securing the objective of populating the platform with HIS data relating to users, is arguably not as sustainable as the first option 'direct transfer' approach for several reasons. First, more effort will be required of users, which they may find onerous: this is particularly so where the user is a current patient of the hospital, whose data is being regularly added to and updated in the HIS. Here, the user will be burdened with having to make regular repeat access requests in order to obtain the data. Secondly, there are greater risks, given the longer line of communication, to data security; this stems also from the need for intermediate storage of the data (presumably on the user's own computer) before the user uploads it to the platform. There may also be risks to the integrity of the data (eg that the user may inadvertently contaminate or corrupt the data, so that it is no longer accurate when it reaches the platform. This risk is highest if the data is provided by the hospital in non-digital format, requiring manual entry and upload by the user. Some forms of data (eg certain image data) may also simply be unsuited to this two-step approach. For these reasons, it would be preferable over time for the direct transfer approach discussed under 3.3.1 to be recognised as the default health data transfer norm.

3.4. Collecting data by apps

According to the European Commission's Green Paper on mobile health (mHealth),[80] there were approximately 97,000 mHealth apps on the market in April 2014, whereby 70% target the consumer wellness and fitness segments and 30% health professionals.[81] The Article 29 Working Party also dealt with apps on smart devices in its opinion paper 02/2013[82]. This shows that legal stakeholders are aware of the legal issues that apps can raise. Especially the lack of transparency and of free and informed consents from end users increase data protection risks, but also poor security measures and the disregard for the principle of purpose limitation are relevant factors.[83] The main reason for this is that only few app developers are aware of possible data protection risks for app users.[84] Moreover, data security can only be achieved by the collaboration of all the different stakeholders, including app developers, owners, stores, operating systems and device manufacturers.[85]

Apps are defined by the Article 29 Working Party's opinion paper 02/2013 as "software applications often designed for a specific task and targeted at a particular set of smart devices such as smartphones, tablet computers and internet connected televisions".[86] In

[80] See http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth.

[81] Green paper on mobile health, p. 7.

[82] See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

[83] Opinion 02/2013, p. 5 f.

[84] Opinion 02/2013, p. 5.

[85] Opinion 02/2013, p. 2.

[86] Opinion 02/2013, p. 4.

terms of MyHealthAvatar, apps on smartphones and tablets play an important role for two reasons: firstly because MyHealthAvatar volunteers can already collect lifestyle data by the use of external apps such as Fitbit and Moves and upload the collected data to the MyHealthAvatar platform (cf. D11.1, p. 13); secondly because FORTH and BED are developing apps for specific high end use scenarios, demonstrating the potential for the platform, and user data it holds, in the future to host selected third party apps and services. According to D3.2 v2.0, MyHealthAvatar aims for an integration of mobile devices, external mobile applications and web access applications because these items can improve the user's flexibility and mobility.[87] If MyHealthAvatar served as an overall data-sharing infrastructure for users, the platform administrator could be responsible for ensuring that Third Party apps are appropriate.

App developers are defined as persons who create apps and/or make them available to end users.[88] The platform administrator – in sharing the data with third party app developers – would likely come under the legal duty of care to check the respectability of such developers. Thus it should institute measures, in the form of ex ante and ex post controls on app and tool developers and other data users to allow it to monitor fair usage by the developers, and to remove non-compliant users from the infrastructure.[89] Moreover, it would be recommendable if MyHealthAvatar served as a gatekeeper for third party apps and vetted them before supporting them by the MyHealthAvatar platform. For instance, the administrator could require the app developer to show that her app has been properly certified by a trusted independent agency (eg NHS health apps library[90]). However, the MyHealthAvatar administrator should still advise the MyHealthAvatar user to not rely on apps alone in situations where this may put her health at risk (including example situations and guidance on when the user should seek independent medical advice) coupled with a clear disclaimer of platform responsibility. These issues are further discussed in part 3.6.

To ensure an informed consent and to bypass the risk of a lack of transparency, it is important to have a privacy policy and an information sheet that meets the requirements of article 10 (a) Data Protection Directive which is applicable when data of a data subject are collected. The privacy policy must be easy to read and understand[91] and should include explanations how the app meets European legal requirements[92]; the information sheet should let the end-user know who the data controller is and how she can be contacted, what data is going to be processed for what purposes[93], in what form and if the data will be revealed to and used by third parties. Finally the user must also be informed about how she can exercise her rights, how she can withdraw her consent and delete her data. The latter is especially important to help to avoid a transparent patient. Here a menu approach would be desirable, where implications for the functionality of results are presented to the end-user.

[87] D3.2 v2.0, p. 64.

[88] Opinion 02/2013, p. 9.

[89] Opinion 02/2013, p. 18.

[90] See: [http://apps.nhs.uk/]; as well as safety, the service claims to check apps' data protection compliance.

[91] Opinion 02/2013, p. 23.

[92] Opinion 02/2013, p. 23.

[93] Opinion 02/2013, p. 6, 22.

Moreover it is crucial that the end user can read the information before installing the app and before any data processing[94], but also after installation. The information should therefore not only be stored within the app, but also on the websites of the app developer.[95]

As already depicted in part 3.2.3.3 of this deliverable, the end-user should be informed about the data processing in a user-friendly way, eg by offering clickable links for more information. Especially with regard to a smartphone and its small screen, it is recommendable to summarise the key information[96] so the end-user can see them at first glance. Of course, this does not mean that the app developer shall not reveal all relevant information. The summary of the most relevant information should be more seen as an additional function of the e-consent system, and the same requirements (in terms of the explicitness, voluntariness, and specificity) met as discussed there. Furthermore, the end users should be informed about their rights before installing the app, especially about the right to withdraw consent at any time without any reprisal.

Finally, the end-user must be able to access her stored data easily.[97] Here, the issue of how to ensure that the one who is claiming to be the user is really the user arises.[98] Only if the identity of the inquirer is clear and there is no danger of a data leakage to third parties, access can be allowed.[99] However, to verify the correct identity of the user, the Article 29 Working Party recommends abandoning excessive personal data collection of the end-users, but relying on authentication instead of full identification, which should be sufficient in most scenarios.[100] In order to enable the user to withdraw consent and to delete the data, it would be desirable further if the data were stored on the mobile device because this would allow them to be deleted easily by the data subject, for example by un-installing the app. If the user has un-installed the app, the app developer is not allowed to process the data anymore and must delete them from her server.[101]

In addition to the need for a lawful data processing, the app developer also needs to meet the requirements for a fair data processing. This requires that she considers the principles of purpose limitation and data minimisation.[102] The principle of purpose limitation means that 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 pursuant to article 6 (1b) Data Protection Directive. From this derives the requirement that the data collected by the app must not be further processed for undefined purposes. The principle of data minimization derives from article 6 (1) (b) and (c) Data Protection Directive and states that

[94] Opinion 02/2013, p. 15, 22.
[95] Opinion 02/2013, p. 23.
[96] Opinion 02/2013, p. 24.
[97] Opinion 02/2013, p. 24.
[98] Cf. part 3.2.3.1.4 of this deliverable.
[99] Opinion 02/2013, p. 24 f.
[100] Opinion 02/2013, p. 25.
[101] Opinion 02/2013, p. 25.
[102] Opinion 02/2013, p. 6.

data controllers shall collect only the personal data which are strictly necessary and keep it only for as long as they need it.[103] The data controller should limit the collection of personal data to what is directly relevant to accomplish a specified and legitimate purpose.[104] 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) Data Protection Directive. According to the Article 29 Working Party, the above-mentioned principles can be ensured well by information and user controls.[105]

Pursuant to article 17 Data Protection Directive, app developers must take appropriate security measures, inter alia to prevent data breaches. In case of a data breach, the data controller must inform the end-user. The GDPR[106] stipulates this legal obligation in article 32. Moreover, the GDPR will regulate the principles of privacy by design explicitly in article 23 (1). These principles are already stipulated in recital 46 and article 17 Data Protection Directive and mean for the app developer that she must consider the data protection rules from the beginning of the app's design.[107] Article 23 (1) of the current version states that

> "[h]aving regard to available technology and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (...) technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation, in such a way that the processing will meet the requirements of this Regulation and protect the rights of (...) data subjects" [emphasis added].

Often, third parties are also involved in the development and running of apps, and as noted in MyHealthAvatar a likely development in the future would see the platform opened up in this way, which – provided the process is managed so as to optimise user safeguards and choice – may bring substantial benefits in breadth and depth of functionality. If third party involvement is envisaged for the development of the CHF and/or diabetes apps, it should be stressed that this third party can be a processor as defined in article 2 (e) Data Protection Directive or a controller, article 2 (d). This depends on the task the third party has: if a third party acts exclusively on behalf of the app developer and does not process data for its own purposes, it is likely a data processor.[108]. [109] Here, it is important for the app developer to

[103] De Andrade, Monteleone, 'Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications' (2012), p. 131.

[104] De Andrade, Monteleone, 'Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications' (2012), p. 131.

[105] Opinion 02/2013, p. 17.

[106] See https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCEQFjAAahUKEwju55SA8_rGAhXis3IKHbP8DZQ&url=http%3A%2F%2Fdata.consilium.europa.eu%2Fdoc%2Fdocument%2FST-9565-2015-INIT%2Fen%2Fpdf&ei=gey1Va6jB-LnygOz-begCQ&usg=AFQjCNF2WQF-y6I69l8vSN1B5d13f6O5-w&bvm=bv.98717601,d.bGQ&cad=rja for the current version.

[107] Opinion 02/2013, p.11.

[108] Opinion 02/2013, p.13.

pay heed to meeting the requirements of the data processor. It is proposed that an appropriate interface will be developed shortly, in which the technical work of BED and FORTH will be supplemented by a SOP prepared in consultation with LUH, with instructions for potential external developers.

Already, within the project, BED is developing a demo app for the high end use scenario diabetes and FORTH is doing so for the congestive heart-failure (CHF) scenario[110]. The former app will enable the existing functionalities in MHA to be used for the needs of pre-diabetic care. Here tailored services, such as diabetes risk assessment models for pre-diabetic care will be incorporated, allowing users to better understand their personal risk of developing diabetes. The aim is to empower citizens by providing a supportive environment for the self-management of lifestyles for general health and wellbeing. A particular focus will be to enable more effective pre-diabetic care in terms of risk reduction through improving compliance with healthy lifestyle recommendations. The demonstration will allow the users to play a key role in monitoring and managing their own health. The aim is to have the app tested by relevant stakeholders, including the diabetic care professionals and even real patients. BED has two potential medical (healthcare) contacts, one in Greece and the other one in the UK. However, the details of the testing are yet to be arranged.

As regards the CHF app, it is envisaged to create a congestive-heart-failure Real Time monitoring app and a risk management app to allow for easy access to the MyHealthAvatar platform via smartphones, mobile devices and tablets.[111] Since both partners determine the purposes and means of the processing of personal data on smartphones, they each fulfil the definition of the data controller as defined in article 2 (d) Data Protection Directive[112] and must therefore comply with the above duties imposed by the Data Protection Directive. Here LUH will provide ongoing advice and assistance as required.

3.5. Sharing data

The privacy implications of sharing of data (insofar as desired and consented to by MHA users), for example among digital avatars, with third party social networks, and for biomedical research, are further issues that need to be analysed in preparation for when the platform will be open to the public.

3.5.1. Sharing data among digital avatars

3.5.1.1. Internal data sharing

Sharing data within MyHealthAvatar, ie from user to user, means the data will stay within the MyHealthAvatar ecosystem. This has the advantage from a privacy viewpoint that the user sharing the data will not be confronted with a new technical and legal security framework that might not meet the user's expectations, but that all data remains within the

[109] Opinion 02/2013, p.10.

[110] D3.2 v2.0, p. 20, 25, 27.

[111] D3.2 v2.0, p. 25, 27.

[112] Opinion 02/2013, p. 9.

secure and trusted MyHealthAvatar ecosystem. However, the recipient of the data could always pass on the data to third parties, potentially even against the will of the user sharing the data. The most flexible but still secure approach to address such concerns would be to implement a technical solution that would permit the sharing of data, but subject to certain permissions and restrictions that would ensure that data is not shared further than originally intended. The following is an idea of a possible technical implementation that would be flexible enough to accommodate a possible wish to share data while still being very privacy-minded. It should be noted that this remains for now a purely hypothetical implementation scenario. The current MHA design does not permit the onward-sharing of the data of one user by another.

First, if the recipient of the data wishes to share it on, the original avatar user should be provided with information about the new intended recipient, for example their MyHealthAvatar profile, and asked whether she consents to the (read-only) sharing of her data. The avatar user could then also indicate whether data may in the future always be shared with this new recipient or whether she would like to be asked each time for consent. The consent to share data on must be easily revocable. Finally, the user should be able to delete shared data, so that any recipient no longer has access to it. This could be achieved by a read-only approach to data sharing where the shared data is only mirrored from the source. 'Deleting' shared data would effectively mean cutting the link that allows the data to be mirrored and remotely wiping it from the recipient's account.

The MyHealthAvatar ecosystem will permit users to share their own data with others. Sharing data with other avatar users is a useful feature. For example, family members might wish to share data amongst one other in order to keep themselves apprised of their respective health status (weight, blood sugar readings, etc.) or to motivate each other to adopt positive lifestyle measures (daily steps, other exercise goals, healthy diets). The platforms patientslikeme[113] and I HAD CANCER[114] are examples of platforms for patients that allow users to share data with each other. The nature of sharing information digitally requires, however, awareness of the potential privacy implications. These depend on whether data will be shared internally within the MyHealthAvatar ecosystem or externally with other digital avatar systems. At present consideration is being given to creating user groups, allowing the persons within a group to see eachothers' performance, for example running distance.

3.5.1.2 External data sharing

Sharing data externally with other ecosystems would be possible via the APIs (eg the APIs for sharing and the APIs for general health data) that MyHealthAvatar provides.[115] Such functionality is important because an open ecosystem that can connect with other systems is more attractive to potential and current users. An issue to consider is that while a MyHealthAvatar user will (hopefully) have reviewed and thus trust the platform's security framework and privacy policy, this will not be the case with third-party platforms the user is

[113] See https://www.patientslikeme.com/.

[114] See http://www.ihadcancer.com/.

[115] See D3.2 v2.0, p.44 et seq, p. 88; D3.6.

not part of. However, a MyHealthAvatar user will likely have some sort of trust in a third-party platform. This trust-by-extension needs to be respected. Consequently, MyHealthAvatar should preferably only permit security and privacy-policy vetted third-party systems to connect via MyHealthAvatar's APIs. Where possible, the license agreements between the third party system and MyHealthAvatar should prohibit any use and sharing of the data without the user's explicit consent. An alternative to permitting only vetted third-party systems from connecting would be to warn users that third-party systems might not have as robust security and privacy measures as MyHealthAvatar, and that data should only be shared with such external platforms the user has reviewed and trusts.

3.5.2 Sharing data with third-party social networks

Sharing data with third-party social networks raises the same issues as sharing data with third-party avatar systems. However, MyHealthAvatar will unlikely have any influence over the privacy policies and security frameworks of major social networks such as Twitter and Facebook. Also, there is a high probability that users will already be on these networks and that they will want to share their (lifestyle) data within their respective social circles. For illustrative purposes, this section will look at the privacy policies of Facebook[116] and Twitter[117], the two leading social networks and the two networks explicitly named in task 11.3, and assess the privacy implications of sharing data with them.[118] Twitter is the only social network that MyHealthAvatar currently permits the sharing of data with.[119]

3.5.2.1 Facebook

Facebook collects all type of content provided to them, be it directly from the data subject or from a third party about the data subject. Amongst other things, the data is used to provide, improve and develop its services and show ads. The information is shared in a variety of ways: with people the user shares and communicates with (which can be the public), with people that see content that others share about the user, with any apps, websites and third-party integrations on Facebook or using Facebook's services, as well as with companies within the Facebook group. Information is also shared with vendors, service providers and other partners who support Facebook's business. Facebook states that it stores data as long as it is necessary to provide the user and all the other recipients listed above with its products and services. Upon deletion of one's Facebook account, Facebook will also delete all information associated with the account, except for such information about the user that has been shared by others. Facebook explicitly explains that such information is not part of the user's account and will therefore not be deleted along with the user's account.

3.5.2.2 Twitter

Twitter similarly collects all type of information provided to them. In contrast to Facebook, where the user typically selects with which groups she would like to share her status

[116] See https://www.facebook.com/about/privacy, date of last revision January 30, 2015.

[117] See https://twitter.com/privacy, effective May 18, 2015.

[118] See also the discussion in part 4.3.1 below.

[119] D1.3, p. 10.

updates with (eg with the public, with friends, with colleagues, etc.), the idea behind Twitter is to help the user share information with the world:

> Most of the information you provide us through the Twitter Services is information you are asking us to make public. Your public information includes the messages you Tweet; the metadata provided with Tweets, such as when you Tweeted and the client application you used to Tweet; the language, country, and time zone associated with your account; and the lists you create, people you follow, Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Twitter Services.

Twitter continues by stating that their "default is almost always to make the information you provide through the Twitter Services public for as long as you do not delete it".

The data Twitter collects is used to provide and improve their services. Apart from as directed by the user, the data is shared with service providers. Like with Facebook, other Twitter users may share or disclose information about one, for example by retweeting a tweet. A user can delete their Twitter account. Even though Twitter will then delete the account from their systems, third parties may still keep copies of public tweets.

3.5.3 Sharing data for biomedical research

The sensitive data stored in the MyHealthAvatar platform can be very beneficial for health research. For this reason the data subject might wish to give consent not only for the data processing in terms of storing the data in her personalised avatar and sharing with treating physicians, but also for health research. It therefore becomes clear that not only a MyHealthAvatar e-consent system, but also the whole European research community must consider the aspect of data sharing for biomedical research. Here, it has to be distinguished between e-consent for signing up to the MyHealthAvatar platform as a first step (as was analysed in 3.2), and the wish for "donating" data for clinical research as a second step. Relevant aspects of the latter shall be presented in this part.

3.5.3.1 Benefits for researchers

Researchers can benefit from e-consent systems because they will be able to better meet the ethical and legal requirements of informing the individual. From a practical point of view, e-consent systems can also reach more potential participants, as researchers do not have to actively seek out interested parties. Instead, everybody who has internet access and is familiar with websites can join. Another benefit for researchers using e-consent forms is that they can establish themselves as innovators[120] and store and manage documents electronically[121], which has the advantage that the documents can be retrieved easily.[122] However, some individuals may prefer to sign a paper-based version because they are not familiar with web-based technologies or for other reasons, eg concerns about security and

[120] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011).

[121] Parrish, 'Using Electronic Consent and Technologies to Facilitate and Improve the Research Process' (2011).

[122] FDA, p. 8.

confidentiality.[123] This is why the paper-based version should be offered as well in the MyHealthAvatar system.

3.5.3.2. Consent and the research use of stored data

Admittedly, consent is not always required for medical research. The so-called research exemption of article 8 (4) Data Protection Directive (specifically: its national implementations) could be applicable. Under certain circumstances, personal data may be processed for research purposes, subject to safeguards and a balancing of interests between the data subject and the public interest. For its part the Declaration of Helsinki[124], which provides ethical guidelines for medical research involving human subjects, states that research may be conducted without consent if it is impossible or impracticable to obtain it for the research and if consideration and approval of a research ethics committee have been achieved.[125]

Despite the fact that consent is thus not necessarily required for secondary use of personal data, MyHealthAvatar wishes to emphasise the right to self-determination of each user, and assure trust and confidence among users that their data is processed transparently in accord with their wishes. Therefore, consent should always be sought with regards to research uses of personal data. As already explained in 3.2.3, such consent needs to be specific according to article 2 (h) Data Protection Directive [and article 4 (8) GDPR]. In this regard, it would be desirable for the user to be informed about the specifics of the research. This is also in line with Declaration of Helsinki, which states that the individual must be

> "adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study".[126]

Moreover, the potential subject must be "informed of the right to refuse to participate in the study or to withdraw consent to participate at any time without reprisal", as stated in section 26 of the Declaration of Helsinki.[127] Special attention should be given to the specific information needs of individual potential subjects as well as to the methods used to deliver the information.[128]

In the future, when researchers apply to use data stored in MHA, it is proposed that relevant specific information sheets and consents would be developed and presented to users electronically in the same way as consents for other kinds of further data processing and sharing. Although it is intended that an information sheet will subsequently be stored in the avatar system, the user should be advised to store a copy of it on her computer or to

[123] Hudziak, Lilly, 'Session IV: Use of E-Consent Technology in the Informed Consent Process' (2015).

[124] See http://www.wma.net/en/30publications/10policies/b3/.

[125] Declaration of Helsinki, sec. 32.

[126] Declaration of Helsinki, sec. 26.

[127] Declaration of Helsinki, sec. 26.

[128] Declaration of Helsinki, sec. 26.

print it out and to place it in a folder. As to the latter, the platform administrator should inform the person concerned about the obvious risk that the copy can be seen by other persons when the e-copy is stored or viewed at a device such as mobile phones and tablets.[129] This is especially true in cases in which other persons are using this device or the device gets lost or, in the worst case, hacked.[130]

If a dialogue between physician and patient should take place before giving consent to a specific research, it must be considered that the physician could exert pressure on the MHA user and/or that their relationship could be characterised by a dependent relationship.[131] In such situations an appropriately qualified individual who is completely independent of this relationship must ask the potential subject for informed consent.[132] If the potential research subject is incapable of giving informed consent, eg as is the case for minors, the physician must ask the legally authorised representative for consent.[133]

Besides having the user's properly informed consent, other relevant safeguards required by good research practice and data protection law will also need to be observed. This will include (where there are identifiable risks to the subject's mental or physical well-being) authorization by a responsible ethics committee.[134] In this regard, the MHA should aim to be a leader of good practice in ensuring that requests to users to process their data for research only come from accredited bona fide researchers. In addition, there will be a need to ensure compliance with the data-minimization principle in article 6(e) of the Data Protection Directive: in research the presumption would normally be that the identity of the user is not relevant to the processing purpose, and thus the data should be de-identified. A technical or legal mechanism should be developed to provide for this prior to or immediately upon the transfer of the data to the researcher.

3.6. Liability for the correctness of the data

Besides the need to minimize harms to the user associated with the unauthorized use of their data, it will clearly be important that such avatar systems work safely and properly in delivering accurate and reliable health information to users. Here, there are various risks of other harm such systems create in the context of their use. The clearest stems from the provision of wrong or misleading advice and the harmful consequences of missed or delayed diagnoses that may follow. However, it is also worth considering the risks to patient users that may arise out of the use of the device in a home environment (without access to professional support) where the information itself is accurate. Below we look further at each of these risks, and the applicable legal liability rules that may be triggered in response.

[129] FDA, p. 6.

[130] FDA, p. 6.

[131] Declaration of Helsinki, sec. 27.

[132] Declaration of Helsinki, sec. 27.

[133] Declaration of Helsinki, sec. 27.

[134] Declaration of Helsinki, sec 23.

As previously discussed, the aim of the MyHealthAvatar platform is to offer an infrastructure where multiple sources of user data may be stored, exchanged and combined, and into which apps and tools – developed by third party providers, and which users wish to utilise – may plug seamlessly. In the context of MyHealthAvatar the apps and tools in question address health and/or lifestyle issues that are of interest to the user. Here, in common with any other device designed for the provision of health care in the broad sense, apps and tools may be subject to the EU certification regime for medical devices that aims to ensure their safety and reliability. The relevant provisions, which are set out in the Medical Devices Directive 93/42/EEC, cover devices for the purpose of diagnosing, preventing, monitoring, treatment or alleviation of disease (or injury/disability) or investigating or modifying the anatomy or physiological processes.[135] The Directive provides for a series of pre-marketing certification measures, which vary according to the level of risk to patients should the device malfunction, coupled with post-marketing surveillance aspects. In 2012 the Commission issued detailed guidance explaining when health apps and tools may fall under the relevant rules as 'stand-alone software', i.e. "software which has a medical purpose which at the time of it being placed onto the market is not incorporated into a [separate] medical device".[136]

The EU medical devices regime is currently undergoing reform, with the Directive due to be replaced by a Regulation; nonetheless as yet issues arising specifically from the new proliferation of health apps have not been the focus of change.[137] This is perhaps surprising as – despite the 2012 Commission guidance referred to – the application of the rules in this area remains significantly uncertain. This was highlighted by respondents to the Commission's 2014 mHealth Green Paper, who noted difficulties both in how to draw the line between tools and apps addressing health as opposed to 'life-style' (the latter putatively outside the medical devices regime), and determining which risk class a specific health app falls into for certification purposes.[138] Generally, there appears a wish by policymakers not to risk inhibiting innovation in a nascent growth industry by over-regulation, and a preference for a 'wait and see' approach as to which apps turn out to pose risks in practice.[139] This may also be dictated by practical constraints: given the sheer volume of new apps, it would clearly be difficult to subject every single app to rigorous prior testing. For now, voluntary good practice standards, such as those promulgated by the

[135] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF. If a device works by analyzing bodily material or fluid of the patient, it will be regulated separately under the 'In Vitro Diagnostic Medical Devices Directive' 98/79/EC.

[136] See Medical Devices Guidance Document, MEDDEV 2.1/6 (January 2012), at http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf.

[137] See the EU Council Progress Report 15881/14, on the draft Medical Devices Regulation, at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015881%202014%20INIT.

[138] Summary Report on the Public Consultation on the Green Paper on Mobile Health (January 2015), at: https://ec.europa.eu/digital-agenda/en/news/summary-report-public-consultation-green-paper-mobile-health, at p 11.

[139] See also the approach in recent US guidance from the Food and Drug Agency (Mobile Medical Applications, February 9, 2015) in which it indicates that for most apps it will not seek enforcement compliance.

International Medical Device Regulators Forum,[140] may arguably suffice. Another interesting development has been the emergence of voluntary accreditation systems, including that offered in the UK by the NHS health apps library[141]; these approaches have the potential to significantly build user trust, and are in the interests of developers as well as consumers.

With regard to MyHealthAvatar, several questions arise from the above. In the first place it may be asked how far the platform itself, as a software-operated system, may be subject to the medical devices regime; at present, following the 2012 Commission Guidance, it may be that the overall system, providing a data storage infrastructure linked to a set of generic tools for interoperability and user access, is too diffuse, aiming at lifestyle as much as health (and usable by healthy 'citizens' as well as patients or doctors), to come within the defined medical purposes of the Medical Devices Regime. More likely it is certain of the individual tools and apps that plug into the system that may qualify – depending on their particular purpose; thus it would primarily be the responsibility of the given app developer to satisfy pre-market testing and certification formalities. In the light of such uncertainties, which as argued in part 5, should optimally be addressed by the European policy maker, a present option for MHA will be to explore segregating apps whose functions putatively fall under the medical devices framework, from the life-style-oriented apps (such as those recording the user's exercise), which do not. This matter will impact on subsequent routes to exploitation and accordingly will be addressed further in Deliverable D11.4.

A further, challenging problem is of determining where liability might lie in the event that a user suffers harm through their use of the platform and/or an app or tool used via it, particularly where the app failed to go through relevant pre-market testing. As suggested, the main type of harm in such cases may be where a user relies to their detriment on falsely reassuring advice they receive through the platform/app (eg that their heart condition does not show signs of an imminent acute episode, or that they are in optimal condition to go mountaineering. Here, within a complex platform infrastructure, there will be a need to attribute liability between distinct putative defendants (such as the platform, different app developers, or different data-providers); it will be necessary to disentangle the source of the faulty advice (faulty data input? faulty data analysis – due to software or other failings? misleading result presentation?) and to apportion damages accordingly. The position is made still more complicated by the fragmented nature of private law liability rules in the EU, with each of the 28 members operating distinct personal injury redress rules.[142]

Here, from the perspective of the platform provider/administrator there may be a risk of having to bear responsibility not only for problems caused by the platform itself, but also for errors in third party apps and tools. This could occur if, in presenting an app to users, or simply enabling it to run on the platform, the platform is deemed to have assumed an

[140] '"Software as a Medical Device": Possible framework for Risk Categorisation and Corresponding Considerations', IMDRF (SaMD) Working Group, 18 September 2014.

[141] See http://apps.nhs.uk/ as well as safety, the service claims to check apps' data protection compliance.

[142] See eg the discussion and analysis at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2007/378292/IPOL-JURI_ET%282007%29378292_EN.pdf.

affirmative duty of care to the end-user with respect to the safety of the app;[143] in addition, if the EU product liability regime were found applicable to software apps, then – as regards those apps developed by parties outside the EU, liability may fall upon the platform as the 'importer' of the relevant app.[144] Such issues have so far been little explored either in academic literature or in the courts, making the outcome in different cases very hard to predict. It is submitted that this is a key area that the European policy-maker may look to regulate in a more legally certain manner, so as to promote an environment in which innovative mHealth initiatives like MyHealthAvatar may optimise their potential.

In the meantime, to minimize liability risks, the platform administrator should follow sensible and ethical practice, notably by vetting apps that are to be supported/offered by the platform – such as requiring the developer to show that the app has been properly certified under the Medical Devices Regime (where applicable) or by a trusted independent agency such as NHS health apps library. It is crucial also for this to be supplemented with transparent advice from the platform to the user to not rely on apps alone in situations where this may put their health at risk. This should include example situations and guidance on when the user should seek independent medical advice, and coupled with a clear disclaimer of platform responsibility. In the case of MyHealthAvatar, this approach should be reflected in the terms and conditions that users will sign when they register for the platform, as well as in the form of automatic reminders each time a user signs up for a third party app. At the same time, even where contributory negligence by a user and/or negligence of third parties are established, the platform may still be liable for a portion of the damages; and in many member states a blanket attempt to exclude such liability will not be legally valid.[145] It follows that the platform should in any event seek appropriate liability (and legal costs) insurance cover.

Another area as yet little-explored legally, where liability of the platform could arise, relates to the communication of distressing (accurate) news, which leads to psychological damage or other harm. A tool or platform's degree of 'tact' in the way it presents information has so far escaped any requirement for advance testing prior to marketing.[146] Nonetheless, clearly in ethical terms, tools purporting to offer personalized predictive advice to users should be designed to minimize such potential harms; first, bad news should never be given by a tool, unless the user is aware of the possibility the tool might predict bad news. In this regard, the patient needs to be informed beforehand and actively accept this possibility in consenting to use the tool. In addition, the patient should be advised to discuss the result of the tool

[143] Here, the more a platform applies prior checks to apps and tools allowed to run on it (a service arguably essential for building user trust), the more likely such an assumption of responsibility may be found: on the general issue of platform intermediary liability, see the 2012 Report of the Center for Democracy & Technology, 'Mobile Platforms as Intermediaries': https://cdt.org/files/pdfs/Mobile-Platforms-As-Intermediaries.pdf.

[144] Product Liability Directive 85/374/EEC, article 3. Admittedly, this would require the relevant software app to be seen as a product rather than a service, which may be contentious: see L. Vihul, 'The Liability of Software Manufacturers for Defective Products', Tallin Papers 2014, vol 1(2), at 9.

[145] See eg for the UK, section 2(1) of the Unfair Contract Terms Act 1977, disallowing attempts by contract, or a tortious notice, to exclude liability for personal injury or death.

[146] The issue is not discussed in either the FDA or IMDRF guidance (see notes 38 and 39) on medical apps.

with a physician, and also about the likely limitations in accuracy of prediction by the tool (compared to specialist clinical diagnosis). Second, the manner of disclosure should be designed in a sparing manner; here protocols developed for physicians required to give bad news stress the need for structured dialogue to prepare the person, breaking information into digestible chunks, checking the person's understanding, and offering empathetic responses;[147] practice from the area of professional genetic testing may also serve as a model, including the desirability of ensuring access to counseling. In serious cases it may also be important that the patient is not left alone immediately after receiving the news.

These issues are likely to gain in significance as personalized medical self-care advice outside the clinical setting becomes more common. It is thus to be hoped that the European policy-maker may consider enacting a clear and consistent legal framework as a matter of some importance. For now MyHealthAvatar will aim to lead in terms of best practice by ensuring that apps or tools that carry a risk of producing distressing results are flagged as such to the user; in some cases (eg apps that may reveal the likely or inevitable progression of a serious condition), direct physician involvement in the app use case should be automatically designed in.[148]

[147] See W. Baile et al, 'SPIKES – a Six-Step Protocol for Delivering Bad News' , The Oncologist (2000) Vol 5(4).

[148] Deliverable D11.1, p 62.

4. Intellectual property implications of digital health avatars

This section provides legal analysis of IP-related issues in digital health avatars. The analysis covers, in particular, such issues as: protectability of software and algorithms by IP rights (IPR), what IPR may arise in medical data collected and processed in avatars, ownership of data under perspective of IPR as well as IPR issues which need to be considered by sharing the data with/from third party platforms and projects.

4.1. IPR in software, algorithms and concepts

In this section we analyse protectability of software, algorithms and concepts developed in the project in the system of IPR. Copyright, as a conventional means of protecting software, along with the requirements and scope of protection is considered in the first place. Protection of undisclosed information is then discussed as an alternative means for protecting elements which are precluded from protection by copyright.

The components, which constitute the core of the MHA platform, and the development modes of the components were recently analysed by LUH at the request of the MHA project co-ordinator. The list of MHA software components with recommended licensing solutions is provided in Annex 6 to the present Deliverable: LUH Report MHA Software Licensing. In sum, 17 software components developed by the technical partners: FORTH, BED, ICCS have been identified. The components were analysed from the perspective of license incompatibility issues in upstream licensing and downstream licensing. Legal solutions recommended for avoidance/mitigation of risks following from license incompatibility. In addition licensing solutions recommended for downstream licensing are provided.

The legal analysis and licensing solutions proposed in the above report apply as of the date when the data was provided by the Parties, the analysis was made and the software licensing report, Version 1 of May 2015, was prepared and circulated to the Parties[149] (Insofar as the software developing Parties might wish to substitute some libraries or software dependencies and/or change the mode of communication, the licensing solutions proposed in the report may still be subject to changes. The IPR rules and licensing issues applicable to the exploitation stage will be further examined and provided in Deliverable D11.4, due in M36. The goal of this Deliverable is to examine general issues of IP in software, algorithms and concepts.

4.1.1. Copyright

In the section below we examine copyright as a means of protecting MHA software components. We describe requirements for copyright protection, right holders and their exclusive rights, elements protectable and non-protectable by copyright.

4.1.1.1. Legal framework

Copyright is a conventional means of protecting software, both under International and European law. At the international level, article 10 TRIPS Agreement[150], and article 4 WIPO

[149] Communication from Project Co-ordinator to LUH, 28.05.2015.

[150] Agreement on Trade-Related Aspects of Intellectual Property Rights, the TRIPS Agreement, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, Marrakesh, Morocco, 15 April 1994.

Copyright Treaty[151] grant copyright protection to computer programs as literary works. In the EU, computer programs are protected by copyright by virtue of Directive 2009/24/EC ('the Software Directive').[152] Article 1 of this Directive provides protection to "computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works."[153] More than that, the Software Directive also extends copyright protection which it grants to a program to the preparatory design materials.[154] This extension may be beneficial to protect the software development materials which have been developed at earlier stages of software development and lead to creation of the software codes at a later stage.[155]

4.1.1.2. Requirements for protection

The margin for copyright protection in computer programs in the EU is fairly low. According to article 1 para 3 Software Directive "A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation." Other criteria to determine eligibility for protection do not apply. According to the CJEU's Infopaq Int. Decision[156], originality in the program is expressed if "… through the choice, sequence and combination of those words that the author may express his creativity in an original manner and achieve a result which is an intellectual creation." Consequently, it is the script in which the programmer lays down the program code that is protectable by copyright. On the other hand, symbols, commands, iterations, figures or mathematical concepts, syntax rules, etc. which constitute the alphabet and syntax of the programming language in question (eg C, C++, Python, etc.), considered in isolation, are not protected by copyright[157].

4.1.1.3. Program expression for the purposes of copyright

A key feature of copyright is that, unlike patent law which protects the substance of invention, copyright protects expression.[158] According to the legal provisions, copyright shall apply to a program in any mode or form of expression.[159] However, in the court practice it has been settled that only the source and the object code constitute objects of protection through software copyright. First, this is laid down in article 10 TRIPS Agreement[160], which

[151] WIPO Copyright Treaty, Geneva, 20 December 1996.

[152] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, Official Journal of the European Union, L 111/16, 5 May 2009, see https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCIQFjAAahUKEwjJ4tegqaHHAhUGwxQKHQneDyk&url=http%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2009%3A111%3A0016%3A0022%3AEN%3APDF&ei=qhHKVcnlNoaGU4m8v8gC&usg=AFQjCNFqolVDpaRC9cCewUTyZ035bswssA&bvm=bv.99804247,d.d24&cad=rja

[153] Article 1 para 1 Software Directive.

[154] Ibid.

[155] Ibid, recital 7.

[156] Infopaq International A/S v Danske Dagblades Forening [2009] CJEU, Case C 5/08.

[157] SAS Institute Inc. v World Programming Ltd [2012] CJEU, Case C 406/10.

[158] Andrew M.St. Laurent, Understanding open source and free software licensing, (2004).

[159] Article 1 para 2 Software Directive; Article 4 WIPO Copyright Treaty.

[160] Agreement on Trade-Related Aspects of Intellectual Property Rights, the TRIPS Agreement, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, Marrakesh, Morocco, 15 April 1994.

extends copyright to "Computer programs, whether in source or object code…". Second, it was established by the CJEU in its BSA Decision.[161] The court decided that for software copyright counts only such form of a program expression "which permits reproduction in different computer languages, such as the source code and the object code."[162] In addition, though, besides the program code, the preparatory design materials leading to the development of a program at a later stage may be covered (i.e. provided they meet the originality requirement) by software copyright under the Software Directive[163].

Consequently, MHA software components expressed either in source code or provided as binary executables along with the preparatory design materials are subject to software copyright. However, protection of software codes by copyright does not mean that ideas, principles, mathematical methods, algorithms and concepts which have been used in software development and on which the software codes reside are automatically protected by copyright as well.

4.1.1.4. Non-copyrightability of algorithms and concepts

It is one of the general principles of copyright that copyright protects original expression and does not protect ideas.[164] This principle is reflected in the international and European copyright law. Both WIPO Copyright Treaty and the TRIPS Agreement explicitly exclude "ideas, procedures, methods of operation or mathematical concepts as such" from the scope of copyright.[165] The same principle applies to computer software and is reflected in the Software Directive. By virtue of recital 11 "ideas and principles which underlie any element of a program, including those which underlie its interfaces" both as "logic, algorithms and programming languages" which comprise ideas and principles are removed from the scope of protection under the Directive.

Based on this principle, the CJEU also made clear that "the keywords, syntax, commands and combinations of commands, options, defaults and iterations consist of words, figures or mathematical concepts which, considered in isolation, are not, as such, an intellectual creation of the author of the computer program"[166]and are excluded from copyright as such. The copyright may be achieved only "through the choice, sequence and combination of those words, figures or mathematical concepts that the author may express his creativity in an original manner".[167]

Following this rule and the case law of the CJEU, concepts and algorithms which have been used and/or underlie software development may not be protected by copyright as such.

[161] Bezpečnostní softwarová asociace – Svaz softwarové ochrany v Ministerstvo kultury [2010] CEJU, Case C 393/09.

[162] Ibid, recital 35.

[163] Article 1 para 1, recital 7 Software Directive.

[164] Andrew M.St. Laurent, Understanding open source and free software licensing, (2004).

[165] Article 9 para 2 TRIPS Agreement, Article 2 WIPO Copyright Treaty.

[166] SAS Institute Inc. v World Programming Ltd, supra, 66.

[167] Ibid, 67.

Another alternative of protecting such elements might be the legal regime of undisclosed information, which we will consider below.

4.1.1.5. Identifying the right holder

The question of who owns the rights in software developed for the Project depends on the legal background in the context of which software has been developed. In the MHA Project, there are two potential scenarios of software development. First, software is developed by the Parties themselves; second, software is developed by sub-contractors commissioned by the Parties. The legal outcome and the ownership of rights in these scenarios is regulated differently.

In the case of MHA, software components are normally developed and provided by the Project Parties as their Background and/or Foreground. Software components are usually written by the software developers acting as natural persons. When the programmer develops an MHA component within his employment relations with the Project Party, then according to the work for hire doctrine and article 2 para 3 Software Directive, the economic rights in such a component shall belong to the Party, unless the programmer and the Parties have agreed otherwise. Article 2 para 3 of the Directive provides: "Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract."

When more than one Party develop a component jointly in a way that "their respective share of the work cannot be ascertained"[168], then according to article 8.1 of the MHA CA in conjunction with article II.26 EC-GA, the Parties shall have joint ownership of the component in question and shall exercise their rights as provided for by article 8.1 CA, unless the joint owners agree otherwise.

Insofar as a Project Party commissioned development of software for the Project from a third party (sub-contractor), another ownership regime would apply. In this situation, the work for hire doctrine would not apply and ownership of rights would fall under the general rules of copyright. Here as the default position, the rule of first ownership would apply. According to this rule, the first owner of copyright in a work is the author.[169] This also applies to computer programs, where the Software Directive in first place accords authorship in a program to "the natural person or group of natural persons who has created the program … or the legal person designated as the rightholder…", if the national law so permits.[170] Consequently, under this rule, copyright in software developed upon commission or under the contract for services would normally pass to the software developer, unless the parties explicitly agree otherwise in writing. The fact that the commissioner paid for the work, and even an agreement that the commissioner will own software as a product, does not mean that commissioner owns copyright in software. Copyright and exclusive rights in software remain with the software developer. The

[168] Article II.26 EC-GA.

[169] Chris Reed, John Angel, Computer Law, p.352.

[170] Article 2 para 1 Software Directive.

commissioner may claim an implied license to use the software for the purpose for which it was commissioned, but it will not be sufficient to claim copyright. Copyright in scope of economic rights would pass to the commissioner only if assigned via a (mostly written) agreement.

In such a case, the development by one party of software within the Project has the potential to affect the rights of the other Project Parties as well. However, according to article 4.3 CA, Parties are placed under a duty to ensure that involvement of third parties should not affect such rights. In particular, this relates to the ability of the other Parties to exercise their Access Rights under the Project. In order to comply with its obligations under CA, a Party which engages sub-contractors is thus required to procure such scope of rights in software which would allow it to grant the Access Rights to the other Parties in the scope foreseen by the CA. It follows that a commissioning Party will need to obtain rights in software from a third party developer, either upon assignment in full scope of the rights or via a license with the right to sub-license. Such an assignment or licensing of rights via agreement will need to be evidenced in writing. [171]

4.1.1.6. Scope of rights

The scope of economic rights in software as provided to the right holder under article 4 Software Directive includes the right of reproduction, translation, adaptation, arrangement and any other alteration of a program, any form of distribution to the public, including the rental. These rights are subject to certain exceptions which are foreseen by the Software Directive in article 5 in order to allow the use of the computer programs by the lawful acquirers.

A Party which attains the position of the right holder by virtue of article 2 para 3 Software Directive obtains these economic rights in full. Hence, any reproduction, modification, distribution of software which it developed under the Project would be subject to its authorization. In the alternative, where software for the Project has been developed upon commission, based on the first ownership rule the full scope of rights would pass to the software developer, unless the parties agree otherwise. As described above, there are then two options as to how the relevant Party may procure the rights: either via assignment or licensing with the right of sub-licensing. What the Parties need to consider when they procure the rights from their sub-contractors is that the scope of rights should cover the scope of Access Rights to software, as provided by article 9.8 CA.

Another possibility for protecting the software materials might be the legal regime of undisclosed information.

4.1.2. Protection of software as undisclosed information

In contrast to copyright which protects original expression, the legal regime of undisclosed information may be applied to any kinds of information irrespective whether such information is copyrightable or not. For instance, the software source code or software

[171] Chris Reed, Computer Law , p. 353.

development materials or certain calculations achieved in the process of software development, etc. may be protected, provided they meet the requirements for protection and need to be kept secret. The legal regime of undisclosed information will apply if the information in question is identifiable, has economic value and has been subject to measures to keep it secret.

In so far as the legal protection of undisclosed information is under consideration in the EU[172], article 39 TRIPS Agreement constitutes the legal source of such protection. This provides protection to information which:

> is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
> has commercial value because it is secret; and
> has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[173]

Once the materials which need to be kept secret have been identified, the protective measures need to be taken. The main feature of protected information is the regime of secrecy. Secrecy means that such information should be known to a limited number of persons;[174] moreover, this state of affairs must be achieved "due to the owner's reasonable efforts."[175] A contractual duty to keep the information in question secret can be sufficient to prove the regime of secrecy.[176] (By contrast, allowing publication of the facts would destroy the secrecy and preclude potential protection.[177]) Second, such information should possess economic value. The criteria for measuring the economic value may be different according to the context. The main principle is that information must be "sufficiently secret to have economic value in that such information is not generally known to third parties who could obtain economic value from its use or disclosure."[178]

The main benefit of such protection is that it would allow a person who holds such information in its lawful possession to control sharing of information in question and prevent any disclosure and use of such information without its prior consent. Such information is protected from: "being disclosed to, acquired by, or used by others without

[172] Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Brussels, 28.11.2013, COM(2013) 813 final, 2013/0402 (COD).

[173] Article 39 para 2 TRIPS Agreement.

[174] Klaus Lodigkeit, Intellectual Property Rights in Computer Programs in the USA and Germany (Peter Lang 2006), p. 98.

[175] Hogan Lovells International LLP, Report on Trade Secrets for the European Commission, Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D, LIB02/CM3SET/2743659.17, 2011, 245.

[176] Ibid.

[177] Ibid, p. 100.

[178] Hogan Lovells International LLP, supra, 245 (a).

their consent in a manner contrary to honest commercial practices."[179] In the context of such protection, "a manner contrary to honest commercial practices" includes such actions as: "breach of contract, breach of confidence and inducement to breach, …[as well as] the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition."[180]

In the context of FP7 projects such as MHA, the Project CA provides for some rules relating to non-disclosure of information in article 10. Any information considered as confidential, if brought to the Project, must be subject to the provisions of article 10 CA as well.

The protectable subject matter (but not necessarily in all EU Member States) may be the source code for computer software, research information, prototypes, technical designs, drawings, blue prints, etc.[181] Also, this type of protection may be applied to the concepts and algorithms, which are not protectable by copyright (as discussed above), but may be protected as undisclosed information.

The concepts and algorithms may be covered by protection, either in isolation or embedded into software development materials or R&D information which enjoys such protection. The pre-requisite for this is that such algorithms and/or concepts must be newly developed by the Party concerned (for instance, in result of its research activities or software development process) and must have not been taken from or released into the public domain before. Additionally, the protective measures, as defined above, need to be applied.

4.1.3. Conclusions

As is apparent from the above legal analysis and observations, the typical type of IPR protection which would apply to software components is copyright. Here both the source code and the object code constitute object of protection under the Software Directive. Also, the preparatory design materials, such as plans, flow charts, etc., which have been produced in the process of software development, are covered by software copyright. An alternative option of protecting the software code and/or software development materials would be the legal regime of undisclosed information. Algorithms and concepts, which are precluded from copyright may still be subject to the regime of secrecy, provided such elements have not been disclosed to the public before.

4.2. IP rights of MHA parties

As mentioned above, IPR generally arise through intellectual creation, however, also investing in information may be a sufficient basis for protecting such investment by proprietary rights.[182]

[179] Article 39 para 2 TRIPS Agreement.

[180] Ibid, Footnote 10 to Article 39 para 2.

[181] Ibid, 243.

[182] Herbert Zech, 'Information als Schutzgegenstand' in JUS PRIVATUM, Beiträge zum Privatrecht, Band 166, p. 130 et seq.

4.2.1. Sui generis right in databases

In the case of MHA, such investment is expected to be made in the data repositories. Provided collection of data, their verification and presentation in MHA repositories consumed "investment of considerable human, technical and financial resources", then such repositories may be protected by sui generis right.

A sui generis protected status has been accorded to databases in the EU by the Database Directive.[183] For the purposes of Database Directive "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" constitutes a database.[184] Provided obtaining, verification or presentation of the contents required a substantial investment, evaluated qualitatively and/or quantitatively, such database may be protected by this sui generis right in the EU.[185] The quantitative assessment consists in quantifiable investment in resources, such as deployment of human, financial or technical resources, whereas the qualitative assessment refers to efforts which cannot be quantified, such as intellectual effort or energy.[186]

The holder of the sui generis right would be the person who takes the initiative and the risk of investing into the database.[187] In the context of MHA, the right holder would most likely be the party and/or parties who invested in constructing the repositories and presenting the contents. When several parties collaborated in this task together, then according to article 8.1 CA these parties would own the rights jointly.

The right holder (-s) of the protected repository acquires the right "to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."[188] Protected actions cover extraction and reutilization of the database contents. Extraction includes such actions by which all or a substantial part of the contents is transferred to another medium by any means or in any form permanently or temporary.[189] Reutilization means making the database contents available to the public by the distribution of copies, by renting, by on-line or other forms of transmission.[190] Such extraction and/or reutilization would be covered by the sui generis right, if what was extracted and/or reutilized amounts to the whole or substantial part of the database content. Systematic transfer and/or reutilization of insubstantial pieces which

[183] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, L 77/20, Official Journal of the European Communities, 27.3.96, see http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31996L0009&from=DE.

[184] Ibid, Article 1.

[185] Ibid, Article 7.

[186] Fixtures Marketing Ltd v Organismos prognostikon agonon Podosfairou AE (OPAP) [2004] CJEU, Case C-444/02, recital 44.

[187] Directive 96/9/EC, Article 7 in conjunction with recital 41.

[188] Ibid, Article 7.

[189] Ibid, Article 7 para 2 (a).

[190] Ibid, Article 7 para 2 (b).

if measured cumulatively would result in substantial portion of the database would be subject to authorization as well.[191]

It should be noted that the sui generis right does not apply to software used in making or operating a database.[192] However, intellectual creation in structuring a database may also deserve copyright in its own right.[193] Such protection, though, relates to the database structure, and does not concern the data contents, and accordingly will not be considered further in this deliverable.

4.2.2. Protection of undisclosed information

- The DoW, WP6, T 6.7, p. 19, provides that a number of full scale and comprehensive datasets (images) are to be collected and genomic analysis based "*on blood by completing genotyping snp6 (1 million snps) for predisposition and working on targeted genotyping for predisposition re drug metabolism, and on tissues by generating gene expression profiling- afymetrix and cancer molecular mutation"* is to be made.[194]

The information generated as the result of such processing may also be protected by proprietary rights as undisclosed information.

Technical and non-technical data, R&D information, and genetic material may all constitute protectable subject matter. Protection of undisclosed information is provided for by TRIPS Agreement, article 39. The protection conferred would allow the party or parties who are lawfully in control of such information to prevent such information from unauthorized disclosure, acquisition or use in an unfair manner, such as via breach of contract, breach of confidence, espionage, etc.[195]

The benefits and the scope of protection, the protective measures which need to be taken by the party/parties in control of such information are described in part 4.1.1 above.

4.3. IPR issues following from the sharing of data

In this section IPR issues from collecting, storing and sharing the data from third party social networks and related projects will be analyzed. The legal rights in such data will be clarified, points which need to be observed by the sharing of data will be identified and guidelines for the software developers will be provided.

4.3.1. With third party networks

During the Technical Meeting in Heraklion, in July 2015, linking of the MHA platform to third party networks and sharing of data from such networks was discussed. In continuation of this discussion, the Project Coordinator (BED) has provided a list of such third party

[191] Ibid, Article 7 para 5.

[192] Ibid, Article 1 para 3.

[193] Ibid, Article 3.

[194] DoW, WP6, T.6.7, p.19.

[195] Article 39, Footnote 10 to Article 39 TRIPS Agreement.

networks and services considered for MHA connection[196] According to the data provided, as of July 2015 MHA connects or is going to connect to the following third party platforms and services:

(a) Fitbit – a platform for the users of Fitbit products. Fitbit products allow to track physical activity of the fitbit user, including activity, exercise, food, weight and sleep.[197]

(b) Withings – a platform for the users of Withings devices. Withings devices are smart products and apps that fit into any lifestyle and let the user track his activities in order to improve everyday well-being.[198]

(c) Moves – a platform for the users of Moves. Moves automatically records any walking, cycling, and running of the user and allows to view the distance, duration, steps, and calories burned for each activity.[199]

(d) Twitter – a platform that allows its users to get and provide in-the-moment updates and watch events unfold, in real time, from every angle.[200]

(e) Facebook - a social platform which allows its users to connect to people across the world.[201] The code logic which connects to Facebook- - has been developed, but it is not proposed to connect to Facebook within the lifetime of the Project

(f) CHIC – "Computational Horizons In Cancer (CHIC): Developing Meta- and Hyper-Multiscale Models and Repositories for In Silico Oncology", EU FP 7 Project.[202]

The legal terms and most essential points regarding connecting and sharing of data with these platforms are described below.

4.3.1.1. Fitbit[203]

Fitbit develops and markets devices which allow tracking of the user´s activity, such as step count, sleep, location, calories burnt, etc., and record the collected data into the user´s Fitbit profile.[204]

Fitbit allows the development of applications that would connect to fitbit.com and obtain access to the data of the Fitbit users. This possibility is provided through the Fitbit API. "The Fitbit API allows developers to interact with Fitbit data in their own applications, products and services."[205] The Fitbit API supports the functions to read, write, obtain, modify and follow modifications in the Fitbit user´s data. An application may "read and write data for a

[196] Communication from BED to LUH, 06.07.2015.

[197] Fitbit, http://www.fitbit.com.

[198] Withings, see http://www2.withings.com/us/en/.

[199] Moves, see https://www.moves-app.com/.

[200] Twitter, see https://twitter.com/.

[201] Facebook, see https://www.facebook.com/.

[202] CHIC, see http://chic-vph.eu/project/.

[203] Fitbit, see http://www.fitbit.com/uk.

[204] Fitbit, About Us, see http://www.fitbit.com/uk/about.

[205] Fitbit API Terms, see https://dev.fitbit.com/de/terms.

user's tracker collections, profile data, social resources, fetch status of devices and statistical data."[206]

4.3.1.1.1. Fitbit data and rights in data

Any text, photographs, other data and information which the user submits (is submitted on behalf of the user) to the Fitbit services, including content posted on message board posts, blogs, journals, user comments, food and recipe submissions, etc., constitute User-Generated Content. [207] Two types of data may be distinguished here: personal data, which relates to activity of the user and is transmitted to Fitbit from the tracker devices, geo-positioning, etc.; and data subject to IP rights, such as photographs, posts, recipes etc.

Fitbit receives from the user a license on use of the user´s content, which should allow Fitbit to provide its services. In particular, according to Fitbit Terms of Use, Section User-Generated Content, the user grants Fitbit a fully-fledged

> "perpetual, irrevocable, non-exclusive, worldwide, royalty-free license, with the right to sublicense… to reproduce, distribute, transmit, publicly perform, publicly display, digitally perform, modify, create derivative works of, and otherwise use and commercially exploit ….User Generated Content…. in any media now existing or hereafter developed, including without limitation on websites, in audio format, and in any print media format."[208]

As regards the sharing of data with third parties, so it is again the right of the user to decide with whom to share his Fitbit data.

As regards the IP rights and management of IP rights in the User-Generated Content, so IP rights may subsist in photographs, texts, messages, recipes uploaded or posted by the user. However, in contrast to personal data submitted to Fitbit from the user´s Fitbit devices (which may be tracked to the user wearing the device), the question who owns the rights in data protected by IP rights may not be verified. Due to the technical possibility of free sharing of works, the IPR ownership in the content uploaded by the user may not be verified. Here, the user may upload the content which he created by himself, e.g. photos taken by the user, his personal comments or articles, etc. At the same time, the user is not deprived of the possibility to share third party works, which he received by sharing or got from external sources. In the latter case, if the copyright notice on the work is absent, the copyright ownership in such work and whether the user has the right to share (communicate, distribute, make available to the public, etc.) such work is a legal question.

This issue subjects the use of IP protected items to potential risks, such as infringement of third party rights. Because of this legal uncertainty in IPR ownership, Fitbit releases itself from any liability responsibility for IP clearance of user´s content and shifts the responsibility for non-infringement and compliance with all laws applicable to the user´s content to the user himself.

---

[206] Fitbit Resource Access API https://wiki.fitbit.com/display/API/Fitbit+API;jsessionid=9E7C3354062A9AEE431967930375B920.

[207] Fitbit Terms of Use, User-Generated Content, see http://www.fitbit.com/uk/terms.

[208] Fitbit Terms of Use, supra, User-Generated Content.

According to the Fitbit Terms of Use, Section User-Generated Content[209], the user waives any rights of publicity and privacy in respect of his content, any other legal or moral rights which might preclude Fitbit´s use of such content and agrees not to assert any claims against Fitbit or its sublicensees relating to such use. Also, the user represents that his content does not infringe any IP rights or rights of publicity and privacy of third parties, does not violate any laws, does not contain harmful computer codes, is not defamatory, harmful or otherwise offensive or inappropriate. As regards use of the copyrighted materials, the user agrees that the materials which he posts on Fitbit shall not violate any third party rights and that he has obtained all necessary rights and licenses which would allow posting of such content on Fitbit.[210]

From these provisions it is apparent that use of the user-generated content from Fitbit may be subject to IP claims of third parties. To mitigate this risk it is strongly advisable to include the like provisions that the user bears liability and responsibility for non-violation of third party IP rights and compliance with all laws and legal regulations applicable to such content into the MHA terms of use. The question of IPR ownership, management and responsibility for IP rights in the user generated content will be considered in more detail in Deliverable 11.4, 'Defining the rules for the exploitation of the platform after the project's end'. The legal provision on liability of the user for non-infringement and compliance with all third party rights and laws applicable to such content will be drafted and incorporated into the MHA terms of use which will be prepared in the context of that upcoming Deliverable.

4.3.1.1.2. Data sharing

As regards sharing the Fitbit data with third party services, Fitbit allows this and provides for a technical possibility to exchange data via Fitbit API.

Sharing of Fitbit data with third party services is governed by the Fitbit Terms of Use Section Third Party Services.[211] The agreement states (and deems the user to agree) that Fitbit may provide links or references to websites operated by third parties. In doing so, Fitbit does not assume any responsibility for use of Fitbit data by such third party services and directs the user to the terms of use and privacy settings of such third party services. In this way the user is provided with the possibility to share his data, but has an option to consent or deny such access.

A further technical possibility is the sharing of data from fitbit.com to external websites so that users of other websites might integrate their Fitbit data into such websites. Such synchronization of data is subject to authorization of the Fitbit user.[212] For this, user A who has an account on both an external website A and fitbit.com must allow website A to access and modify his Fitbit data. Data is accessed via HTTP calls. Also, there is a possibility to synchronize updates in the data of user A from fitbit.com to website A. For this, website A must subscribe to changes in a user´s data on fitbit.com.[213] In this case, when user A

[209] Fitbit Terms of Use, supra, User-Generated Content.

[210] Ibid, Copyrighted Materials.

[211] Fitbit Terms of Use, Third Party Services http://www.fitbit.com/uk/terms.

[212] Fitbit API https://wiki.fitbit.com/display/API/Fitbit+API.

[213] Fitbit Subscriptions API https://wiki.fitbit.com/display/API/Fitbit+Subscriptions+API.

updates his data on fitbit.com, fitbit.com makes HTTP call back to website A and website A may fetch updates resources.

To sum up, collection and sharing of data from fitbit.com to MHA platform and MHA applications is allowed and technically possible. In order to connect to fitbit.com an MHA application must be registered at fitbit.com and be authorized by the user to access his data. Once the data will leave Fitbit, the use of such data will be subject to the terms and privacy policy of MHA, if any. For use of the user´s content covered by IP rights by MHA, a license would be required. The issue who of MHA parties will act as a licensee will need to be discussed by the Consortium. Grant of license on use of the user´s content will need to be incorporated into the MHA terms of use. By grant of license, the issue of liability for IP infringement will need to be solved. For this, the MHA terms of use would need to provide that the user ensures that he has a right to grant license on use of the content which he transmits (transmitted on behalf of the user) to MHA platform and/or MHA applications and bears any liability and responsibility for non-infringement and compliance with applicable laws and third party rights.

Insofar as MHA terms of use have not been elaborated and the legal safeguards against liability for IP infringement have not been taken, sharing and use of Fitbit content on MHA might be subject to legal risks and may not be approved from the legal side.

4.3.1.2. Withings[214]

Like Fitbit, Withings invents smart products and apps that let the user track his activity and view his activity progress, like steps gone, calories burnt by swimming, etc.[215]

4.3.1.2.1. Withings data

As follows from the Withings functionality and terms of use, the user´s data on Withings includes data, provided by the user by account registration, data recorded by the tracking devices, the user´s commentaries and hypertext links. The use and sharing of Withings users´ data is subject to the Withings Services Terms and Conditions[216] and Withings Privacy Policy.[217]

Apart from use of the personal data, Withings allows its users to write and submit commentaries and/or opinions on Withings website. Use of such commentaries by Withings is governed by Withings Website Terms of Use.[218] When the user submits his commentary, he grants Withings a non-exclusive, non-personal, royalty free, "transferable, sub licensable, right on a worldwide basis to represent and reproduce the commentary and/or opinion, in whole or in part, in a lineal manner or not on any media, such as the Website, press review

[214] Withings http://www2.withings.com/us/en/.

[215] Withings, About Withings http://www2.withings.com/eu/en/about-withings.

[216] Withings Services Terms and Conditions http://www2.withings.com/eu/en/legal/withings-services-terms-and-conditions .

[217] Withings, Privacy Policy http://www2.withings.com/us/en/legal/privacy-policy-statement#/us/en/legal/privacy.

[218] Withings Website Terms of Use http://www2.withings.com/eu/en/legal/legal-information#/eu/en/legal/website-terms-of-use.

or advertising, presentation or any physical or digital media as long as the rights shall enjoy legal protection."[219] The user´s data on Withings website may also include hypertext links to external webpages.[220] The user is solely responsible for non-violation of IP rights and any content which he posts. Unless required by the applicable law, Withings assumes no liability for non-infringement[221], hence responsibility and liability for the user´s content on Withings lies with the user.

4.3.1.2.2. Data sharing

Through the Withings API Withings allows connecting and exchange data of the Withings users. "Using the Withings API, developers have the ability to access health data measured by Withings products, including weight, body fat, activity, sleep, blood pressure and heart rate, to integrate them into their services or create brand new, innovative user experiences."[222]

Sharing of data via Withings API is regulated by the Withings API Terms of Use.[223] According to Section 6 Intellectual Property, when a developer connects to an API or by using it Withings grants a developer "a worldwide personal, non-transferable, nonassignable, non-sub licensable license, non-exclusive, strictly limited to the purpose of this agreement and to the country from which you connect yourself to the API".[224] The license is limited to the use of an API only and does not give the developer any rights on using the materials from the Withings website, or API or data attached to it. The license explicitly excludes use or sale of the Withings users´ data from the scope of API license. Any use of the data attached to the Withings API requires prior agreement of the user.

Also, sharing of data can occur both from Withings to a partner and from partner to Withings. In both cases, the user must be informed about the purposes of data sharing and must give his prior informed consent to such sharing. The Withings user may see with whom he shared his data, manage data sharing and stop such sharing at any time via a dashboard. When data are shared to Withings, Withings may have to receive the data which the user communicated to a partner, for instance, identity data, body metrics data, activity data, environmental data.[225] From the Withings rules and policy on linking to and sharing data with third party apps and platforms, it follows that , linking of MHA to Withings and sharing of Withings data to and from MHA is technically possible and legally allowed. Such linking is made possible via API exchange. After the implementation of a Withings API, a MHA app in order to be able to access the user´s Withings data and share those data on MHA would need to receive approval by the the user and obtain the user´s informed consent on sharing of his data. By leaving Withings.com, the use of the Withings data on MHA will be governed by MHA terms and policy. Should the user´s data be covered by IP rights (as in the

[219] Ibid, section 9 User's commentary.

[220] Ibid, section 8 Hypertext link.

[221] Ibid, section 11 Warranties.

[222] Ibid.

[223] Withings API Terms of Use, see http://www-media-cdn.withings.com/wysiwyg/legal/2015-Withings-API-Terms-of-Use-VUS.pdf?_ga=1.254361352.1215146296.1418739123.

[224] Ibid, section 6 Intellectual Property.

[225] Withings Privacy Policy, supra.

case with Fitbit, described in Section 4.3.1.1.2 above), a license on use of such IP protected content would be required. Such license will need to be incorporated into the MHA terms of use and the person of a licensee will need to be defined by the Consortium. Givenf the legal uncertainty on IPR ownership in the user´s content, and in order to avoid any legal risks associated with IPR infringement, the user should be made responsible and liable for non-infringement and compliance with all laws and third party rights in the content which he submits (submitted on behalf of the user) to MHA; the user should also ensure that he holds all necessary rights to grant a license to MHA.

As noted, the question of IPR ownership, management and responsibility for IP rights in content which the user will upload or share on the MHA platform, as well as associated legal risks, will subsequently be considered in further detail in Deliverable 11.4.

4.3.1.1.3. Moves[226]

MovesApp is an application which counts any walking, cycling, and running of an app user and shows the distance, duration, steps, and calories burned for each activity. The app is suitable for use on mobile devices and can be downloaded via Google Play and Apple Store.[227]

4.3.1.1.3.1. Moves data

Moves collects data associated with the use of Moves services by the user: e-mail and password by account registration, gender, height, weight and birth, if the user provides such data, location, once the user consents to tracking, information from the user´s device, user´s communication with Moves.[228] Such data is associated with a particular user and use of such data is subject to the Moves Privacy Policy. [229]

4.3.1.1.3.2. Data sharing

Moves also allows building compatible apps and exchange of data with Moves via API. The Moves API enables to access and store data from Moves for providing a service.[230] Use of Moves API is governed by Moves API Terms of Use.[231] Under Section 1 License, the licensor (rightholder of Moves) grants to the software developer a personal, non-transferable, non-exclusive license to use the Moves API for accessing and storing the data from Moves.

By allowing third party services to share the Moves data, Moves requests that such third party should process the Moves data "*lawfully, with due care and in compliance with good processing practice so that the protection of the data subjects´ private life and the other basic rights which safeguard their right to privacy are not restricted without a basis provided*

[226] Moves, see https://www.moves-app.com/.

[227] Ibid.

[228] Moves, Privacy Policy, see https://www.moves-app.com/privacy.

[229] Ibid.

[230] Moves, Summary of Moves API Terms, see https://dev.moves-app.com/docs/terms_summary .

[231] Moves, Moves API Terms of Use, see https://dev.moves-app.com/docs/terms.

by law."[232] Also, organizational and technical measures should be taken to protect the data against accidental loss, destruction, any unauthorized alteration, disclosure or access.[233]

The sharing of Moves data with third parties is regulated by Moves Privacy Policy.[234]The Moves Privacy Policy provides for a possibility that Moves may share the information which Moves collects from its users with third party apps, provided the user chooses to use any of third party apps and/or services and if the user consents to disclosure of his information to those third parties.[235]

Hence, sharing of data from Moves is also technically and legally possible, requires, however, user´s approval of the service and the user´s consent to the data sharing. Also, Moves requires that a third party should provide for adequate protection of the Moves users´ data which they share with that third party service so that the users´ basic rights and the right to privacy are safeguarded. As long as the MHA privacy policy has not been implemented and technical protective measures have not been taken, the MHA will not be able to comply with this Moves license requirement. Also, in case if any of the Moves content should be covered by IP rights, the question of liability for IP infringement would need to be resolved. Considered from this perspective, although sharing of the Moves data is technically possible, it may not be legally justified now.

4.3.1.4. Twitter[236]

In contrast to Fitbit, Withings and Moves, Twitter does not track physical activity of his users. Twitter is a platform for real-time transmission of Tweets: instant messages, photos, reports from the events, etc.[237]

4.3.1.4.1. Twitter Data

Twitter collects and processes data related to the use of Twitter services, such as Twitter websites, SMS, APIs, widgets, applications, etc., by the user. [238] Twitter collects personal information related to use of the Twitter services by the user, such as account information, location, additional personal information, log data, device information, etc.[239] Collection and use of personal information on Twitter is governed by the Twitter Privacy Policy.[240]

Any information, text, graphics, photos or other materials uploaded, downloaded or appearing on the Twitter services constitute Twitter content. [241] Use of the Twitter content is governed by the Twitter Terms of Service.[242]

---

[232] Ibid, Section 3.2.

[233] Ibid.

[234] Moves, Privacy Policy, see https://www.moves-app.com/privacy.

[235] Moves, Privacy Policy, supra, Sharing data with third parties.

[236] Twitter, see https://twitter.com/.

[237] Twitter, About Twitter, see https://about.twitter.com/.

[238] Twitter Privacy Policy, see https://twitter.com/privacy?lang=en.

[239] Ibid.

[240] Ibid.

[241] Twitter Terms of Service, Section 1 Basic Terms, see https://twitter.com/tos?lang=en.

[242] Twitter Terms of Service, see https://twitter.com/tos?lang=en.

The user is responsible for any content that he posts on the Twitter services and any consequences thereof. The originator of such content bears the primary responsibility.[243] Twitter does not guarantee the completeness, accuracy or reliability of any content and communications and is not liable for any content posted, transmitted, broadcasted or made available via Twitter services. [244]

4.3.1.4.2. Rights in data

The user retains the rights in any content that he submits, displays or posts via Twitter services and grants Twitter "a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)." [245]

Such license includes the right of Twitter to make the content submitted to Twitter services available to third parties who partner with Twitter for syndication, broadcast, distribution or publication of Twitter content on other media or services. By this the user remains responsible for his content, the use of his content by other Twitter users and third parties. By submitting the contents to Twitter the user warrants that he has all rights, power and authority to grant the rights in the content which he submits.[246]

Hence, Twitter acts as a service provider, has a license to use the Twitter content for the purpose of providing its services and bears no liability for such content and non-infringement. The user acts as the right holder in the content which he submits and decides on sharing of his content to the others. Most content which the user submits to Twitter is public (available to be viewed by others and third party services) by default, unless the user limits availability of his content via account settings.[247] The user may also reproduce, modify, sell, publicly display, publicly perform, transmit or otherwise use the Twitter content using Twitter API. [248]

4.3.1.4.3. Data sharing

Twitter is constructed in a way (and it is the purpose of Twitter) to make Twitter contents viewable by the public and via third party services.[249] Twitter encourages and permits broad re-use of Twitter content. Exchange of data is enabled by Twitter API.[250] The user is made aware of data sharing and provided with a possibility to make his Tweets visible by approved Twitter followers. [251]

---

[243] Ibid, Section 4 Content on the Services.

[244] Ibid.

[245] Ibid, Section 5 Your Rights.

[246] Twitter Terms of Service, supra, Section 5 Your Rights.

[247] Moves, Privacy Policy, supra, Sharing data with third parties.

[248] Ibid, Section 8 Restrictions on Content and Use of the Services.

[249] Twitter Terms of Service, supra, Section 1 Basic Terms.

[250] Ibid.

[251] Ibid, Section 1 Basic Terms.

Use of Twitter services, incl. API, and use of Twitter content are governed by Twitter Terms of Service[252], Twitter Developer Agreement[253], Twitter Developer Policy[254], Twitter Privacy Policy[255] and supporting documentation[256].

According to the Twitter Developer Agreement, Twitter grants software developer a non-exclusive, royalty free, non-transferrable, non-sublicensable license to use Twitter API to develop Twitter services, copy a reasonable amount and display Twitter content via its services, modify the content to format it for display on its services.[257] By this, software developer obtains a license to use the content to the extent necessary for its services, but Twitter, its licensors and end users retain all worldwide rights in Twitter API, content, including rights in patents, trademarks, copyrights, know-how, data and all proprietary rights.[258]

Also, license on use of Twitter content via API exchange does not allow software developer to collect, cache and store the location data or geographic data contained in the content, except in connection with a Tweet and for identifying the location tagged by the Tweet.[259] Guidelines on using geo data are provided in Geo Guidelines.[260] The main principle is that the user should maintain control of using geo data along with his Tweets. Twitter has elaborated the Developer Policy[261] which forms an integral part of the Software Developer Agreement[262] and provides guidelines which software developers need to comply with when using Twitter API.

4.3.1.4.4. Twitter requirements for data sharing

The MHA Parties who work on connecting MHA to Twitter will need to comply with the Twitter requirements for data sharing. The guiding principles are as follows:

1. Keep API key and other access credentials private.
2. Respect requirements how to display and interact with the user´s content.
3. Maintain the integrity of Twitter products.
4. Respect user´s control and privacy.
5. Clearly identify the service.
6. Keep Twitter Spam Free.

---

[252] Twitter Terms of Service, see https://twitter.com/tos?lang=en.

[253] Twitter Developer Agreement, see https://dev.twitter.com/overview/terms/agreement.

[254] Twitter Developer Policy, see https://dev.twitter.com/overview/terms/policy.

[255] Twitter Privacy Policy, see https://twitter.com/privacy?lang=en.

[256] Twitter, Developers, Documentation, Overview, see https://dev.twitter.com/overview/documentation.

[257] Twitter Developer Agreement, supra, Section I Twitter API and Twitter Content, B. License from Twitter.

[258] Twitter Developer Agreement, Section IV Ownership and Feedback, see https://dev.twitter.com/overview/terms/agreement.

[259] Ibid, II Restrictions on Use of Licensed Materials, C. Geographic Data.

[260] Twitter, Geo Guidelines, see https://dev.twitter.com/overview/terms/geo-developer-guidelines.

[261] Twitter Developer Policy, see https://dev.twitter.com/overview/terms/policy.

[262] Twitter Developer Agreement, supra, I Twitter API and Twitter Content, C Incorporated Terms.

7. Be a good partner to Twitter – follow Twitter guidelines.
8. Avoid replicating the core Twitter experience or features.
9. Engage in appropriate commercial use - advertising.[263]

As regards data sharing via Twitter API, Twitter requires any third party service to display its privacy policy to Twitter users before downloading, signing up or installing an application. The privacy policy of a third party must be compliant will all applicable laws and be no less protective than the Twitter privacy policy.[264]

For sharing the user´s content via API exchange Twitter requires:

1. To get the user's express consent before:
    a. Taking any actions on a user's behalf, including posting content, following/unfollowing other users, modifying profile information, or adding hashtags or other data to the user's Tweets.
    b. Republishing content accessed by means other than via the Twitter API or Twitter other tools.
    c. Using a user's content to promote a commercial product or service, either on a commercial durable good or as part of an advertisement.
    d. Storing non-public content such as direct messages or other private or confidential information.
    e. Sharing or publishing protected content, private or confidential information.
2. To take reasonable efforts to be able to delete Content that Twitter reports as deleted or expired, change treatment of Content that Twitter reports is subject to changed sharing options (eg, become protected) and modify Content that Twitter reports has been modified.
3. To show the user what will be published, including whether any geotags will be added, before posting content to Twitter from web or mobile service.
4. To explain how service will use the content, obtain user´s permission to use the content, use such content in accordance with Twitter Developer Policy, if a service allows posting content to external service and Twitter.
5. To disclose in privacy policy the use of cookies: whether third parties may collect user information on the service and across other websites or online services, information about user options for cookie management and application of Do Not Track setting in supporting web browsers.
6. To disclose when a service adds location information to user´s Tweets, eg a geotag, annotations data, place and specific coordinates, comply with Geo Guidelines.

[263] Twitter Developer Policy, supra.

[264] Ibid, Section 3.s.

7. Not to store Twitter passwords.[265]

By reproducing the Tweets on its services – web or mobile property, software developer needs to follow Display Requirements.[266]

This allows maintaining the integrity and functionality of Twitter services. Twitter encourages using embedded Tweets and embedded Timelines. Reproduced in this way, Tweets and timelines automatically come with all necessary Display Requirements. If using Twitter embeds is not possible, software developer needs to reproduce the Tweets with all attributed prescribed by Twitter. The requisites for re-display of the Tweets are shown in Figure 1.

Figure 1. Examples for rendering details of Individual Tweets on websites and mobile apps.

©Twitter, Twitter Display Requirements

https://dev.twitter.com/overview/terms/display-requirements

Some of the basic display requirements are provided below:

1. The Tweet author's avatar, @username, and name must always be displayed.
2. The Tweet author's @username must always be displayed with the "@" symbol.
3. The Tweet author's name and @username must be displayed on one line horizontally or stacked one above the other vertically.
4. The Tweet author's avatar must be positioned to the left of the author's name and @username
5. The Tweet author's avatar, name, and @username must all link to the user's Twitter profile.
6. Tweet text must be displayed on a line below the author's name and @username, and may not be altered or modified in any way except as outlined in these requirements.
7. Tweet Entities within the Tweet text must be properly linked to their appropriate home on Twitter.
8. Reply, Retweet, and Favorite action icons must always be visible for the user to interact with the Tweet.
9. No other social or 3rd party actions similar to Follow, Reply, Retweet and Favorite may be attached to a Tweet. (eg, subscribe, comment, like).
10. The Tweet timestamp must always be visible and include the date and/or time.

[265] Ibid, section 3 Respect User´s Control and Privacy.

[266] Twitter Display Requirements, see https://dev.twitter.com/overview/terms/display-requirements.

11. The Tweet timestamp must always be linked to the Tweet permalink.
12. The Twitter logo or Follow button for the Tweet author must always be displayed and be reasonably visible.
13. The Twitter logo must link to twitter.com or to an official Twitter client.[267]

The like requirements apply to re-display of Twitter Timelines and Twitter content.[268] Hence, Twitter also provides for a technical possibility and legal basis for sharing Twitter content via Twitter API. When connecting to Twiter, third party services shall abide by the guidelines for using Twitter API and content, as described above and may be found at: https://dev.twitter.com/overview/terms/policy. The key principle in data sharing with Twitter is that a third party service needs to provide the user with information about its service, its terms and privacy policy and ask the user´s permissions before taking any actions with his data. For accessing and using Tweets and content protected by IP rights, a third party service would need to obtain a license to use such information. Liability for non-infringement in such content should remain with the user. Insofar the MHA terms of use and privacy policy have not been elaborated, MHA may not be considered as able to comply with the Twitter requirements for data sharing. Hence, as of now data sharing with Twitter may not be legally justified.

4.3.1.5. Facebook[269]

According to LUH's information,[270] the code logic which connects MHA to Facebook has been developed. The code has not been implemented in the live version of July 2015 because for connecting with Facebook. Facebook requires that third party services inform the users with their privacy policy[271], which is not ready for MHA yet. Indeed, according to the Project Coordinator (BED), MHA will not connect to Facebook during its lifetime. Here, we provide a preliminary analysis of most important legal and IPR issues which would need to be observed if the MHA Platform connects to Facebook during its exploitation stage.

4.3.1.5.1. Facebook data

Facebook is a social network: "People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."[272] The kinds of information which Facebook collects from its users are described in Facebook's Privacy Policy.[273] Such data may subsist in information about the user, which the user submits himself via signing up for an account, the user´s communication data, as well as information in the content which the user posts, such as photos, etc. The other kinds of information identifiable with a particular user may include information which other users

[267] Twitter Display Requirements, supra.

[268] Twitter brand portal, see https://about.twitter.com/company/brand#twitter-content.

[269] Facebook, see https://www.facebook.com.

[270] Communication from BED to LUH, 06.07.2015.

[271] Facebook Platform Policy, see https://developers.facebook.com/policy/#thingstoknow.

[272] Facebook, About, see https://www.facebook.com/facebook/info?tab=page_info.

[273] Facebook, Privacy Policy, see https://www.facebook.com/privacy/explanation.

share about that user, such as when they share a photo, send a message, upload or import the user´s contact information, both as information about payments, device information, etc. Apart from the information circulated by Facebook services internally, Facebook also receives data from websites and apps that use Facebook services, third party partners which offer services jointly with Facebook or Facebook advertisers, or companies owned or operated by Facebook, such as Moves.[274]

4.3.1.5.2. Rights in data

The use of information collected by Facebook is governed by Facebook Privacy Policy and Facebook Terms of Use.[275] According to section 2 of the Facebook Terms of Use, the user owns all content and information which the user posts on Facebook and can manage how such information is shared through the privacy and application settings. For the content protected by IP rights, such as photos or videos (IP content), the user grants Facebook a "non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)."[276] Hence, as might be observed in other platforms, Facebook acts as a service provider, collects and uses data as necessary to provide its services, whereas the user remains the right holder and licenses use of its data to Facebook.

Apart from that, it is the user´s obligation and responsibility not to post any content that infringes third party rights or violates the law.[277] Hence, when transferring Facebook content to another platform it would be reasonable that responsibility for non-infringement should remain with the user.

When connecting to Facebook via API, a software developer grants Facebook all rights necessary to enable his app to work with Facebook. Such rights include: the right to incorporate information which an app provides to Facebook into other parts of Facebook, the right to attribute the source of information using software developer´s name or logos; the right to use his name, logos, content, and information, including screenshots and video captures of an app, to demonstrate or feature use of Facebook, worldwide and royalty-free; right to link to or frame an app, and place content, including ads, around an app, etc.[278]

4.3.1.5.3. Data sharing

Like other platforms, considered above, Facebook also offers its API to third party services for connecting and sharing data with Facebook. Facebook makes its programmatic interfaces available to people for sharing and accessing the information available to them.[279]

Sharing of Facebook data with third party services is also subject to Facebook Terms of Use and Privacy Policy.

---

[274] Moves, Privacy Policy, see https://www.moves-app.com/privacy.

[275] Facebook, Statement of Rights and Responsibilities, see https://www.facebook.com/legal/terms.

[276] Facebook, Statement of Rights and Responsibilities, supra, Section 2.

[277] Ibid, section 5 Protecting Other People´s Rights.

[278] Facebook Platform Policy, see https://developers.facebook.com/policy/#thingstoknow.

[279] Facebook Principles, Open Platforms and Standards, see https://www.facebook.com/principles.php.

Apps, websites and third party integrations on or using Facebook services may receive information about what the Facebook user posts or shares. For example, when a user presses a Facebook Shares button on a website, a website may receive a comment or link which the user shared. Also, third party services may access the user´s public information Public information is the information which the user shares with the public audience, user´s public profile, content shared on a Facebook page.[280] The user´s public profile includes username, age range, country/language, friends list.[281] Public information is available to anyone on and off Facebook and can be seen or accessed via online search engines, API, offline media.[282]

An application wishing to access Facebook user´s data is required to ask the user´s permission to access his content as well as information which other users have shared to the user. Facebook requires external applications to respect its users´ privacy and requires that use of information of Facebook users by an external application be governed by an agreement between the user and such external application.[283] Information collected from Facebook by external apps, websites or integrated services is governed by their own terms and policies.[284]

Developers or operators of applications, websites or social plugins which connect via Facebook API to Facebook must comply with Facebook Platform Policy.[285]

When using Facebook API and sharing data from and to Facebook third party services are asked to do the following:

1. Obtain consent from people before publishing content on their behalf.
2. Use publishing permissions to help people share on Facebook, not to send people messages from the app.
3. Not to prefill captions, comments, messages, or the user message parameter of posts with content a person didn't create, even if the person can edit or remove the content before sharing.
4. Provide a publicly available and easily accessible privacy policy that explains what data the app is collecting and how the data will be used.
5. Use account information in accordance with own privacy policy and other Facebook policies. All other data may only be used outside the app after the user gave his explicit consent.
6. Include privacy policy URL in the App Dashboard.
7. Link to the privacy policy in any app marketplace which allows so.
8. Comply with the own privacy policy.

[280] Facebook Privacy Policy, supra, People you share and communicate with.

[281] Ibid, Apps, websites and third-party integrations on or using our Services.

[282] Ibid, People you share and communicate with.

[283] Facebook, Statement of Rights and Responsibilities, supra, section 2 para 3.

[284] Facebook Privacy Policy, supra, Apps, websites and third-party integrations on or using our Services.

[285] Facebook Platform Policy, see https://developers.facebook.com/policy.

9. Delete all of a person's data received from Facebook (including friend data) if that person asks to, unless retention of such data is required by law, regulation, or separate agreement with Facebook. Aggregated data may be stored only if no information identifying a specific person could be inferred or created from it.
10. Obtain consent from people before using their data in any ad.
11. Obtain adequate consent from people before using any Facebook technology that allows Facebook to collect and process data about them, including for example, Facebook SDKs and browser pixels. When an app uses such technology, disclose to people in the privacy policy that an app is enabling Facebook to collect and process data about them.
12. Obtain consent from people before giving Facebook information that an app independently collected from them.
13. When tracking a person's activity, provide an opt-out from that tracking.
14. Provide meaningful customer support for an app, and make it easy for people to contact for help.
15. If people come to an app from the Facebook app on iOS, give them an option to go back to the Facebook app by using the Back to Facebook banner provided in Facebook SDK.
16. If people come to an app from the Facebook app on Android, it is not allowed to prevent them from going back to Facebook when they press the system back button.[286]

Also, third party services should take measures to protect the Facebook data against unauthorized access and use, protect and use secret keys and access tokens appropriately. It is not allowed to sell, license or purchase any data obtained from Facebook or Facebook services, to transfer any data, incl. anonymous, aggregate or derived data, to any ad network, data broker or advertising or monetization related service. Facebook data may not be put into search engine or directory, incl. web search functionality on Facebook. Only those data and publishing permission may be requested which an app really needs. When a third party uses partner services, it should conclude a written agreement with them to protect Facebook data, limit their use of such information and keep it confidential.[287]

Other requirements for using Facebook API may be found at: https://developers.facebook.com/policy.

Consequently, Facebook provides a technical possibility to share data with Facebook and provides strong guidelines which third party services need to follow when connecting to Facebook. One of the key principles in data sharing with Facebook is giving the user control over his data, asking the user´s permission before taking any action with the user´s data, providing information on the service, its terms and privacy policies. Use of the user´s content protected by IP rights would require license from the user and liability for non-

[286] Facebook Platform Policy, supra, section 2 Give People Control.

[287] Ibid, section 3 Protect data.

infringement in such content should vest with the user. Insofar as MHA terms of use dealing with liability for IP infringement and privacy policy have not been implemented, data sharing with Facebook may not be legally justified. The legal rules on use of the MHA Platform, tailored for the exploitation stage, will deal with the legal and IPR issues arising from connecting to third party platforms, and will be addressed in D.11.4.

4.3.1.6. API licensing issues

From the licensing documentation of third party platforms: Twitter, Facebook, Withings, Fitbbit and Moves analysed above follows that users/licensees are not allowed to transfer or sublicense their rights which they obtained under a license for using the platform services This means that a Project Party which develops an app which connects to a third party platform via third party API does not have a right to grant Access Rights to such APIs to the other Project Parties . According to Article 9.8.3 CA, access to software which is Foreground shall comprise "*Access to the Object Code; and, where normal use of such an Object Code requires an Application Programming Interface (hereafter API), Access to the Object Code and such an API*". Since the third party APIs considered above are licensed into use for free, those Project Parties who might need to access third party APIs, in order to use a Project Party´s app, would need to download the required API from a particular source (e.g. Facebook, Fitbit, Withings, etc.) under the respective license.

4.3.2. Connecting with CHIC and related projects

The possibility to share data from the CHIC repository was discussed at the MHA Technical Meeting, which took place in Heraklion in July 2015. As regards the IP rights, the general rules of IP law and requirement to obtain authorization of the right holder would apply. Provided the information, materials, data or any other works, tools or items from CHIC, which are considered for use in MHA, are protected by IP or other proprietary rights, such as sui generis database right, know-how, confidential information, then the use of such protected items would require license from the respective right holder and the use would be subject to the license rules.

For example, the CHIC models or tools, like Dr.Eye[288], may be protected by software copyright. Any reproduction of these items, such as by loading, displaying, running, transmission or storage in computer, translation, modification, adaptation, distribution of copies would require authorization of the right holder.[289] Also, since the use of third party works may affect the ability of the party to grant Access Rights in MHA and the use of such works is subject to the CA provisions, the rules of MHA in respect of Access Rights must be respected. Provided, the use of protected works by one party poses substantial limitation or restriction on granting the Access Rights, then according to article 9.2.2 CA, such party shall inform the consortium as soon as possible. So that granting of Access Rights is not affected, two options may be considered:

[288] CHIC, Downloads, Public Deliverables, Deliverable No. 5.1.1 The CHIC technical architecture – initial version, Section 5.3.5 Image processing toolkit, see http://chic-vph.eu/uploads/media/D5-1-1_The_CHIC_technical_architecture-initial_version.pdf.

[289] Article 4 Software Directive.

1) a party negotiating a license obtains a license with the right to sublicense;
2) all parties who need to use third party items enter into the license agreement.

Also, if some materials from an external project are provided as “Confidential”, then such materials are protected from unauthorized use and disclosure and may only be used under the rules, as defined by the right holder.

4.3.3. Summary

From the above legal analysis on data sharing with third party platforms and projects the following conclusions can be made.

Third party networks, considered for connecting with MHA, such as: Fitbit, Withings, Moves, Twitter and Facebook provide for a legal and technical possibility to share their data via API exchange. The general requirements for data sharing from the privacy perspective are the following: MHA privacy policy must be displayed to the user before the user signs up for an MHA app or service; the user must be informed about an MHA app or service and purposes of data sharing with MHA; the user must approve an MHA app or service and give his prior informed consent (in some jurisdictions in writing, as discussed in part 3.2.3.1) to such sharing. Insofar as the MHA privacy policy has not been elaborated, MHA may not considered as able to comply with these requirements. Hence, data sharing with third party networks at the current stage may not be legally justified.

As regards IP issues in data sharing with third party networks, the main risk concerns liability for IP infringement in the user generated content. Since origin of such content, ownership and holding of IP rights in it cannot be verified, sharing of IP protected content on MHA may be subject to a legal risk of infringement of third party rights. This risk may be mitigated by the legal provisions that the user bears liability for compliance with the laws and non-infringement in any content which he shares or submits (submitted on behalf of the user) to MHA. Such provisions will need to be incorporated into the MHA terms of use, which will be tailored to the exploitation stage and will be prepared in the context of Deliverable 11.4. Defining the rules for the exploitation of the platform after the project’s end. Before The MHA terms of use and such legal provisions dealing with liability for IP infringement are not in place, sharing of IP protected content from third party networks to MHA may not be legally approved.

With respect to data sharing with the ICCS model repository, ICCS is a Party to MHA Project bound by the provisions of MHA CA. According to the CA rules dealing with Access Rights (Section 9), unless the repository is excluded from granting the Access Rights in MHA. In the latter case, use of the ICCS repository would be subject to the general rules of IP law and authorization of the right holder (-s) will be needed.

Lastly, as regards, data sharing with the CHIC project, the sharing of IP protected content (such as data, research materials, models, etc.) from CHIC is subject to the general rules of IP law and authorization of the right holder (-s) on use of protected data items would be required. By negotiating a license, requirement of the CA dealing with Access Rights would

need to be taken into account and the sublicensing or user rights for the Project Parties would need to be negotiated as well.

5. Conclusion and recommendations

The implementation of digital avatars can raise large privacy and data protection questions, for example concerning the implementation of e-consent systems, but also questions on how to collect data by hospital information systems and apps. Moreover, the MHA user could wish to share her stored data among other avatars, with third-party social networks or for biomedical research purposes. Finally, it has to be clear who is liable for the correctness of the stored data: is it the MHA user, the platform administrator or a treating physician who trusts the correctness of the data and gives wrong advice?

The traditional approaches to ownership cannot be easily applied to personal data because facts do not fall under the IPR regime. Instead, the Data Protection Directive serves as a control regime that protects the data subject's privacy by giving her various rights, such as the rights of information, of access, and of rectification, erasure and blocking of data. Moreover, the central rule of data protection, that personal data must not be processed without a lawful basis, helps to ensure a lawful data processing that takes into account the interests of individuals. In terms of MyHealthAvatar this means that the Data Protection Directive is a key component for the legal framework that the consortium considers.

Regarding the question of electronic consent, the law is in principle open to shifting consent away from paper to the electronic medium. It is to be hoped that the General Data Protection Regulation will put this issue beyond doubt. Thereby, the user will be able to benefit from e-consent systems by using interactive multimedia files to better understand the relevant facts. At the same time, it is acknowledged that various technical difficulties will need to be solved in order to reach an explicit, specific, informed and freely given consent: relevant technical measures should include access control mechanisms, audit trails and easy solutions to withdraw consent. One aspect, with regard to the use of e-consent systems, is the use of qualified electronic signatures – with a provision for hardcopy consents as a fall-back option. These are recommended as long as the Data Protection Directive remains applicable because some Member States currently require that consent has to be given in written form if sensitive health data is processed.

With regard to external data sharing, it is important for users to be aware that they will have less control over their personal data if they share it on social networks like Facebook or Twitter than if they were to keep all data with the MyHealthAvatar ecosystem. Even though a user can in principle delete data from Twitter and Facebook, this right goes only so far. A user has no control over the data as soon as it is shared on by her circle of contacts. In order to protect the MyHealthAvatar user, she should be alerted of the risks behind sharing her MyHealthAvatar data with social networks and be advised to use only those third-party systems that have been security and privacy-policy vetted by MHA before. At least, the MHA user should be warned to share data with third parties whose platform is not as secure and privacy-aware as the MHA Platform is.

With regard to data sharing for research purposes, it will be an aim to seek specific consent from the user, in order to demonstrate maximum respect for the user's autonomy over how their data is used. Measures that need to be taken before asking for consent are to inform

the patient about the specifics of the research and to offer her the possibility to ask a qualified health professional questions. In addition, principles of data minimisation should be observed (requiring de-identification of data if personal data is not necessary for the research); other aspects of ethical good practice should also be designed into the system.

As regards the key liability risks that may face platforms such as MyHealthAvatar, one is that a physician or users may rely on faulty data, resulting in physical harm. A second risk stems from the danger that the platform informs the user of distressing news in an inappropriate way leading to psychological damage. Also important to consider is the potential need for the platform, and/or apps made available through it, to be certified under the Medical Devices Directive. As was analysed, all of the above raise challenging and as yet not fully resolved issues in law. If the European community wishes to promote and take advantage of the considerable potential benefits associated with health avatars it should consider clear legislative action to achieve greater legal certainty in this area.

Moving on to the most important conclusions regarding the intellectual property implications of digital health avatars, the first is that in principle software components of the MHA platform constitute protectable subject matter by software copyright (part 4.1.1). Copyright is the conventional type of protection applicable to software. The margin for copyright protection in software is rather low. Normally, copyright would subsist in the program source code and the object code, and also in the preparatory design materials in the EU. Protection of non-literal program components, such as GUI, structure, sequence and organization, by software copyright is possible in common law countries. In the EU, the ordinary law of copyright would be more plausible. By virtue of work for hire doctrine, the party or parties who developed software for the project would hold the economic rights (the right of reproduction, modification, distribution). Protection of the software source code as undisclosed information is another option. The list of MHA software components and licensing solutions is provided in Annex 6. For their part, algorithms and concepts are excluded from copyright protection, but may be protected as undisclosed information (part 4.1.2).

As regards IP rights in data, both the user and MHA parties may acquire and/or hold proprietary rights in data, which can be seen in part 4.2. On part of the user, the rights may subsist in the content which the user submits to the platform, such as comments or pictures. Such items would normally be covered by copyrights. Use of such content is subject to authorization of the right holder and an IP license for use would be required. The license grant may be incorporated into the MHA terms of use. Since authorship in protected items may not be proven, responsibility for compliance with third party rights and liability for non-infringement should vest with the user who introduces such content. As to the rights held by MHA parties, the party and/or parties who invested financial, technical or human resources into presenting the data in MHA repositories may hold sui generis database right. The sui generis right would allow the right holder(-s) to prevent unauthorized transfer or making the database contents (whole or substantial part of it) available to the public. Also, the MHA parties may protect (if they wish) the results of genomic analysis of medical data as undisclosed information.

The IP issues in data sharing with third party platforms (Withings, Moves, Facebook, Twitter, Fitbit) and related projects (CHIC, ICCS model repository) were analysed in part 4.3. All the platforms allow data sharing through their API subject, however, to their terms and privacy policies. For use of the user generated content protected by IP rights, a license for use would be required. Because of the legal uncertainty in origin of such content, ownership and holding of IP rights, the issue of liability for IPR infringement would need to be resolved. A typical practice for handling liability for IP infringement is incorporation of provisions into the service terms of use which provide that the user ensures that he has all necessary rights to grant an IP license in the content and bears any liability and responsibility for compliance with all applicable laws and non-infringement of third party rights in such content. Use of materials from ICCS model repository is most likely to be managed by Access Rights under CA, unless the repository is excluded from such rights. For use of IP protected items from CHIC, a license with the sublicensing or user rights for the other Project Parties would need to be obtained first.

References

- Blackstone W (1765): Blackstone's Commentaries on the Laws of England
- Coiera E, Clarke R: e-Consent (2004): The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment, *Journal of the American Medical Informatics Association,* Vol. 11 No. 2, 129-140
- 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
- Evans B J (2011): Much ado about data ownership, *Harvard Journal of Law and Technology, Vol. 25, Fall 11*; , 69-130
- Forgó N, Kollek R, Arning M, Kruegel T, Petersen I (2010): Ethical and Legal Requirements for Transnational Genetic Research, München: C.H.Beck Verlag
- Gossen, R (2012): Electronic Informed Consent: Possibilities, Benefits, and Challenges
- Hudziak K, Lilly E (2015): Session IV: Use of E-Consent Technology in the Informed Consent Process
- Laurent A M St (2004): Understanding open source and free software licensing
- Lodigkeit K (2006): Intellectual Property Rights in Computer Programs in the USA and Germany, Peter Lang
- McNair L, Costello A, Crowder C (2014): Electronic Informed Consent: A New Industry Standard
- Parrish M (2011): Using Electronic Consent and Technologies to Facilitate and Improve the Research Process
- Reed C, Angel J (2007): Computer Law, Oxford University Press
- Rose C M (1985): Possession as the Origin of Property, *Faculty Scholarship Series*, *Paper 1830,* 73-88
- Rosner G (2014): Who owns your data?, *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication,* 623-628
- Zech H (2006): Information als Schutzgegenstand, *JUS PRIVATUM, Beiträge zum Privatrecht, Band 166*, Mohr Siebeck

Annexes

Annex 1: Abbreviations and acronyms

API	Application Interface
BED	University of Bedforshire
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
CA	Consortium Agreement
CHF	Congestive Heart Failure
CHIC	Computational Horizons In Cancer
CJEU	Court of Justice
DOW	Description of Work
EC	European Community
EEA	European Economic Area
EU	European Union
FORTH	Foundation for Research and Technology Hellas
FP7	Seventh Framework Programme
GA	Grant Agreement
HIS	Hospital Information System
HTTP	The Hypertext Transfer Protocol
HTTPS	HTTP over Secure Socket Layer
IP	Intellectual Property
IPR	Intellectual Property Right
ICCS	Institute of Communications and Computer Systems
LUH	Leibniz Universität Hannover
MHA	MyHealthAvatar
R&D	Research and Development
SDKs	Software Development Kits
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UK	United Kingdom
URL	Uniform Resource Locator
WIPO	World Intellectual Property Organization
WP	Work Package

Annex 2: Information Sheet

Information Sheet/Privacy Policy

"MyHealthAvatar_User Information Sheet_v0.2_August 2015

I. Need for registration
If you decide to become a user of the MyHealthAvatar platform, you must register at the platform.

Therefore, you have to tick the box by which you confirm that you have read and understood this information sheet/Privacy Policy.

Afterwards, you will still need to complete the consent form. Before doing so, you should also read and familiarise yourself with the MyHealthAvatar General Terms and Conditions.

Thank you for reading this information sheet/Privacy Policy.

II. General information
This information sheet describes the functionalities of MyHealthAvatar, what kind of data you can store in the MyHealthAvatar platform and how your rights are protected. We hope this will allow you to better decide if you want to contribute data to the platform and/or later become a user. Please take your time when you make your decision.

Please read the information provided carefully and discuss it with others if you wish. Feel free to ask us if there is anything that is unclear or if you wish to have more information.

If you decide to contribute your data to the platform and become a user of MyHealthAvatar, you have to give consent to the processing by MyHealthAvatar of the data that you will upload. You can withdraw your consent at any time without any disadvantages. In this case, your uploaded data will be permanently deleted from the MyHealthAvatar platform.

By registering as a user, after confirming that you have read the Information Sheet/ Privacy Policy and the General Terms and Conditions, you will confirm that you were properly informed about this platform.

A copy of the Information Sheet/Privacy Policy and the General Terms and Conditions will be sent to your e-mail-address or postal address (as specified by you) for you to keep.

III. Purpose of MyHealthAvatar
MyHealthAvatar (www.myhealthavatar.eu) proposes a solution for access, collection and sharing of long-term and consistent personal health status and lifestyle data through an integrated environment, which will allow more sophisticated health data analysis, prediction, prevention and treatment simulations tailored to you as an individual citizen.

It is intended that the information provided by the avatar will be valuable for clinical decisions concerning your care, in helping you to best manage your own health and lifestyle. The information generated may also offer a promising resource of population data to support clinical research, leading to strengthened multidisciplinary research excellence in supporting innovative medical care. However, you will retain full control (by giving or declining your consent) over whether you wish your data to be so used.

IV. Functionalities of MyHealthAvatar

Your data is collected for the purposes of allowing more sophisticated clinical and other health data analysis, prediction, prevention and treatment simulations tailored to you as an individual citizen.

This can be achieved by using the functions offered by the avatar as

- a lifetime collection of your health status data,
- a tool to allow you to be active in promoting your own healthcare,
- allowing you to access a rich set of relevant health and other data from various sources,
- an interface to access hospital data and healthcare resources,
- a toolbox for data analysis, fusion and visualization for both you and the clinicians responsible for your care.

As a user, you will thereby have:

- the option to register for predictive risk assessment, and
- the opportunity to share your data on a variety of platforms, either for promoting your own health interests, to help particular other persons, or for general altruistic reasons (such as contributing to current and future medical research).

In order to use MyHealthAvatar to its full extent, you should ideally be prepared to upload data concerning personal information, including gender, age, ethnic, symptoms, diagnosis, treatment and response to drugs; health indicators such as blood pressure, pulses and body temperature; medical data such as images, biological data, multi-scale data; data concerning your life style, eg drinking and smoking habits.

Nevertheless, you should only upload data that you are sure you want to have included in your personalised avatar. The choice is ultimately yours.

V. Security measures to protect your data

We are aware of the fact that the uploaded data are highly sensitive.

All necessary state-of-the-art security measures are incorporated in the platform to protect your data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse. Other users of the MyHealthAvatar

platform will only be able to access your data after you connect with them as “friends” and only after having selected the data you would like to share (eg only lifestyle data or also x-ray images, etc.).

(Please tick here if you would like us to inform you in more technical terms about the planned security measures.)

VI. Your rights

Firstly, we would like to assure you that your data will not be further processed (ie used) without your consent or for other purposes than those you specified in your consent. If you would like to allow us to use your data for a further purpose that you did not initially agree to, such as other health-related projects, you can later give a separate consent for this.

It is your decision whether to disclose your data and information to other parties, such as physicians or added “friends”. Only the persons you want to will have the opportunity to access this data.

Secondly, you retain at all times your full rights as a data subject under the Data Protection Directive, as follows:

Right to information

You have the right to inform yourself about the identity of the controller who hosts this platform and of the controller’s representatives, if any.

When storing data in the platform, this data will be processed. In this context, we point out that you have the right to inform yourself about the purposes of the processing for which the data are intended.

As already mentioned, the purpose of MyHealthAvatar is to access, collect and share long-term and consistent personal health status data in order to analyse, predict, prevent and simulate treatment tailored to you as an individual citizen.

Finally, we would point out to you that you may inform yourself about any further information, eg about the recipients of the data and if you have the right of access to and the right to rectify the data concerning you.

Right of access, rectification, erasure or blocking

At any time, you can apply for information about the personal data stored and request that corrections be made if the data are incorrect or outdated. Furthermore, you can demand to block or delete your data.

Whenever you wish to make use of the above mentioned rights, please feel free to contact MyHealthAvatar [relevant contact details].

Right to object

You have the right to object to the processing of your data at any time.

In this case we will delete your data as soon as reasonably practicable from the MyHealthAvatar platform and/or your avatar. An exception may occasionally have to be made when the data is collected in order to comply with a legal obligation, or when it is necessary for the performance of a contract to which you are a party, or is already being used for a purpose for which you gave your consent, where significant investment has occurred, and the deletion would prejudice the fulfilment of that purpose.

VII. Roles as controller and processor

The host of this platform is [ ]. The host complies with the duties it has as a controller in terms of article 2d Data Protection Directive.

The processors are ..... *(not yet decided)*.

VIII. Applicable national law

The data controller is established on the territory of [ ]. Therefore, our Privacy Policy meets the requirements stipulated in the [relevant domestic law of territory] which implements the requirements of the Data Protection Directive into national law."

Annex 3: Consent form & Registration

Consent sample/Registration

Consent form for registration for the MyHealthAvatar (Version 2; August 2015)

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 register on the MyHealthAvatar platform.

I have read, I understand and I agree to subscribe to the user information sheet/Privacy Policy and the General Terms and Conditions - which form a part of this document (version 02; August 2015).

I understand that one copy of this agreement, the current Privacy Policy and the General Terms and Conditions will be sent to my address/e-mail-address (as specified by me) and another copy will be retained for record-keeping by the operator of the MyHealthAvatar platform. In case of any changes, I will be informed by postal mail or email (as specified by me).

Annex 4: Patient Data Transfer Request to Hospital

Patient Data Transfer Request and Waiver

I, the undersigned ……....., born on the……....., in…….... and resident at…… / ……. (address), reachable via ..... (e-mail-address), am a current/former (delete as appropriate) patient at ..... [name of Hospital], have been a user of the MyHealthAvatar (MHA) Platform since ..... [date].

As set out in the MHA user terms and conditions, of which I was informed at the time of registration, the MHA Platform provides a secure and data protection-compliant infrastructure for the storage and presentation of my health and lifestyle data, where I control the uses made of the data, including who may access it for which purposes.

I hereby make the following request and declaration:

1. I authorise and request the Hospital to transfer the health data that it holds upon me in its record and information systems to the MHA Platform, except for that which is specified in point 2.

2. I do not agree to the transfer of the following categories of data, namely that relating to my: ..... [specified health condition(s)].

3. I agree that where the Hospital acts upon this, my, request and transfers data to the MHA Platform in accordance with the terms and conditions of the relevant data transfer agreement between it and MHA, to waive and forfeit all claims against the Hospital in respect of any harm, loss or damage arising out of the transfer.

I have read, had explained to me, and understand the effect of this request and waiver, and understand that two original copies of this document will be produced and will be kept by me and by ..... [the Hospital], respectively.

Signature of Patient: …….

Signature of Witness: .....

Name and address of Witness: .....

Date and Place: ……

Annex 5: Data Transfer Agreement between Hospital and MHA

BETWEEN

_____
Hereafter "the Hospital"

_____
(address and country of establishment)
AND

_____
("MHA")

_____
address and country of establishment)

Individually referred to as a "Party" or collectively referred to as the "Parties".

Preamble
The MHA Platform has been developed in the course of the MyHealthAvatar project (within the European Commission 7th Framework Program) to provide a secure, privacy-compliant infrastructure for the storage and presentation of individual health and lifestyle data under the control of the individual MHA Platform user, who may determine the uses made of their data, including who may access different parts of it and for which purposes. The key aim is to foster patient empowerment, by creating an environment for the user to make intelligent use of the data to inform lifestyle choices to reduce morbidity and/or allow the improved self-management of existing health conditions.

At the same time the MHA Platform is designed to be fully compliant with data protection requirements, also bearing in mind that the data processed generally falls within the 'special categories' of sensitive data under article 8 Data Protection Directive. Thus, users will be provided with specific and transparent information on the implications of using the data processing tools and services available via the MHA Platform (including ones from third party providers), and on how to exercise their full rights as data subjects under the law. In addition, the Platform will deploy state of the art data security and data encryption techniques to counter the risk of unauthorised data access or use. In this respect it aims to offer a level of data security at least as high as that found in an advanced hospital information system.

It is proposed that one source of the data to be stored in the MHA Platform will be health and clinical data of the relevant individual user collected by health professionals during the provision of treatment and care and retained in hospital information systems (HIS). This data has the potential to be of particular value in view of its generally high quality, richness

and accuracy, thus enabling processing operations that yield important and informative results for users. However, from the perspective of a hospital that is requested by a user (who is or was one of its patients) to transfer the data to the MHA Platform, there is a need to ensure the proper management of medical confidentiality and data protection risks stemming from the transfer.

Accordingly the present Data Transfer Agreement aims to formalise the legal position of the Hospital, providing the HIS data, and the MHA Platform, as recipient, by setting out the respective rights and duties of the Parties pertaining to the processing of the data. The intention is to ensure that the Parties process the data during and after the transfer in a manner consistent with ethical and legal principles of medical confidentiality, as well as in accordance with principles of European data protection law.

Clause 1: Scope and Precondition

1. This Agreement sets out the terms and conditions for the transfer by the Hospital of health data in its HIS for processing and storage in the MHA Platform in line with the purposes of the MHA Platform as formulated in the MyHealthAvatar Project;

2. The Hospital as data provider is responsible as data controller for the management of patient data within its organisation/ hospital database, while MHA is responsible for data that has been transferred to the MHA Platform for processing and storage;

3. The Agreement presupposes the receipt by the Hospital of a written request from a person (hereafter "the Patient") in respect of whom the Hospital holds personal health data in its HIS, asking the Hospital to transfer the data to the MHA Platform. The request shall be in the form provided for in Annex A;

4. Prior to the Hospital transferring and MHA receiving any data pursuant to the request, the Parties shall agree to be bound by the terms and conditions of this Agreement; equally, should either Party become unable to comply with the same, the data transfer shall cease immediately.

Clause 2: Obligations of the Hospital

The Hospital warrants and undertakes:

1. to transfer to the MHA Platform personal health data in its HIS relating to its current/former [delete as applicable] Patient ..... [full name], born on ..... [date] in ..... [town/city]; and further, where the Patient is a current patient of the Hospital, to effect transfers of such data on an ongoing basis to the MHA Platform within a reasonable time, which shall not exceed ..... [number] months of its entry into the HIS.

2. to transfer only such data as has been obtained and processed in accordance with the laws applicable to the Hospital and which are subject to a valid transfer request from the Patient; in this regard it shall take care to transfer only data than was the subject of the request;

3. to ensure that data is transferred to the MHA platform in securely encrypted form and using secure transit channels;

4. that it shall remain liable in case of any privacy breach resulting from its non-compliance with the terms of this Clause 2.

Clause 3: Obligations of MHA

MHA warrants and undertakes:

1. to process the data in compliance both with applicable confidentiality and data protection rules and with the terms of the Patient's specific informed consent;

2. to adhere to appropriate ethical and legal standards in its dealings with the Patient. This shall include provision of specific and transparent information to the Patient on the implications of using the data processing tools and services available via the MHA Platform (including ones offered by third party providers), as well as on the legal rights the Patient as data subject has against the MHA Platform and/or any third party processing the data.

3. to implement suitable means of a technical or other nature to allow the Patient to exercise her rights as a data subject, including (also in the case of data processed by third party providers) the ability to revoke her consent to the processing in question and secure the deletion of the data;

4. that it has implemented and follows appropriate technical and organisational security measures to protect the data against misuse and loss (including without limitation the measures stated in Annex B to this agreement), in accordance with the requirements of relevant provisions of European data protection law, and in particular article 17 of the Data Protection Directive 95/46/EC or any subsequent provision in an EU instrument that may re-enact or replace the same;

5. to ensure that any and each of its employees who has contact with the data is made aware of, and will be bound by, the terms of this Agreement;

6. that, except as otherwise expressly and specifically consented to by the Patient, or in case of an applicable court order, it shall not disclose or publish the data to any other party, which for the avoidance of doubt includes any of its subcontractors or party with which it has an equivalent arrangement;

7. that, in case of making the data available for research uses with the Patient's consent, it shall perform a de-identification process on the data, so as to ensure that no more personal identifiable elements remain in the data than are necessary for the agreed research purposes;

8. that, if for whatever reason, it is no longer able to comply with the terms of this Clause 3, it shall inform the Hospital of this circumstance immediately.

9. to deposit a copy of this Agreement with the relevant data protection supervisory authority if it so requests or if such deposit is required under the applicable law.

Clause 4: Liability and indemnity

1. Each Party shall be liable to the other Party for damage it causes by any breach of these clauses. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:
    - the Parties promptly notifying each other of a claim; and
    - each Party being entitled to cooperate in the defence and settlement of the claim.

Clause 5: Governing law and Jurisdiction, miscellaneous

1. This agreement shall be governed by German Law. The courts of Lower Saxony, Germany shall have exclusive jurisdiction. This shall also apply to disputes on the validity of this clause.

2. Changes and amendments to this agreement shall require written agreement signed by the parties and an explicit statement that they represent a change or amendment to these conditions. The same applies to the waiving of this formal requirement.

3. If any provision of this agreement shall be entirely or partly invalid or unenforceable, this shall not affect the validity and enforceability of any other provision. An invalid or unenforceable provision shall be regarded as replaced by such a valid and enforceable provision that as closely as possible reflects the privacy/security and/or economic purpose that the parties hereto had purposed with the invalid or unenforceable provision.

4. Each person signing below and each party on whose behalf such person executes this agreement warrants that he/she, as the case may be, has the authority and the legal capacity to enter into this contractual agreement and perform the obligation herein.

5. This agreement will enter into force on the effective date, ie the date of the last binding signature to this agreement.

Made in two signed copies, each party having received its own signed copy.

_____ _____

(Place, Date) (Signature [the Hospital])

_____ _____

(Place, Date) (Signature [MHA])

Annexes:

A: Patient data transfer request and waiver [included above as Annex 2 of the Deliverable]
B: Technical and organisational measures

Annex A ... [included above as Annex 4 of the present Deliverable]

Annex B

Technical and organisational measures
MHA will take appropriate technical and organisational measures to protect the data within the MHA Platform against misuse and loss, in accordance with European data protection rules, including all necessary and reasonable precautions:

- to prevent unauthorised persons from gaining access to data processing systems with which the data are processed or used (physical access control),
- to prevent data processing systems from being used without authorisation (denial of use control),
- to ensure that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that the data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage (data access control),
- to ensure, including through use of secure encryption, that the data cannot be read, copied, modified or removed without authorisation during electronic transmission, transport or storage and that it is possible to examine and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transmission control),
- to ensure that it is possible retrospectively to examine and establish whether and by whom the data have been inputted into data processing systems, modified or removed (input control),
- to ensure that the data being processed on commission are processed solely in accordance with the directions of the controller (contractual control),
- to ensure that the data are protected against accidental destruction or loss (availability control),

- to ensure that other data collected for different purposes is processed separately (separation rule).

Annex 6: Software licensing table

See next page.

	Component/Party	Tools used/Licenses	Method of use	License compatibility/Comments	Component license
1	Model repository ICCS	MySQL:GPLv2+[290] Django:3-Clause-BSD	Calls object code	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, GNU GPL will cover the whole combination*[291]. **For GPL compliance, component must go under GPL.** Section 9 GPL v2 applicable to My SQL allows a work to be licensed under GPLv2 or any later version. Code under GPLv2+ may be used in software licensed under GPLv3[292]. 3-Clause-BSD compatible with GPL[293].	**License options: GPLv2+/GPLv3+** **Recommended license: GPLv3+** **Commercial licensing not allowed; fees for transfer of copies and support may be charged (Section 4 GPL v3)** You can charge any fee you wish for distributing a copy of the program. If you distribute binaries by download, you must provide "equivalent access" to download the source—therefore, the fee to download source may not be greater than the fee to download the binary[294] **Release in object code must be supported by possibility to get the source (See Table 6).** **GPLv3 license requirements:** Section 6 GPL v3: distribution in object code allowed if accompanied by: (a) source code, (b) an offer to provide source code (valid for 3 years), (c) offer of access source code free of charge, (d) by peer-to-peer transmission – information where to get the source code Please See Table 6. Section 4 GPLv3: no license fees, fees for copies, warranty or support may be charged. **To license under GPLv3:** - please include GPLv3 license notice into each source file (See Table 1); -please include the text of GPL v3 license [295];

[290] See http://www.mysql.com/products/workbench.

[291] GNU, FAQ, Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? available at: https://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs.

[292] https://www.gnu.org/licenses/gpl-faq#AllCompatibility.

[293] GNU; Various Licenses and Comments about Them, available at: https://www.gnu.org/licenses/license-list.en.html.

[294] See https://www.gnu.org/licenses/gpl-faq#DoesTheGPLAllowDownloadFee.

[295] See https://www.gnu.org/licenses/gpl.html.

					-identify software dependencies and associated licenses (See Table 4). **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4).
2	Data Repository for Models ICCS	MySQL:GPLv2 Django: 3-Clause-BSD	Calls object code	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, GNU GPL will cover the whole combination*[296]. **For GPL compliance, component must go under GPL**. Section 9 GPL v2 applicable to My SQL allows a work to be licensed under GPLv2 or any later version. Code under GPLv2+ may be used in software licensed under GPLv3[297]. 3-Clause-BSD compatible with GPL[298].	**License options: GPLv2+/GPLv3+** **Recommended license: GPLv3+** See p.1.
3	Tool Execution Engine ICCS	MySQL: GPLv2 Django: 3-Clause-BSD Tastypie: BSD License, Celery: BSD License, RabbitMQ: Mozilla Public License v 1.1[299] MongoDB: GNU AGPL v3.0 (drivers: Apache license)	Calls object code	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, GNU GPL will cover the whole combination*[300]. **For GPL compliance, component must go under GPL.** 3-Clause-BSD compatible with GPL[301].	**License options: GPLv3+ with permission for MPL´d RabbitMQ** Please see p.1. Grant permission for linking component with MPL´d RabbitMQ under Section 7 GPLv3 (See Table 2); - identify software dependencies and associated

[296] GNU, FAQ, Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? available at: https://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs.

[297] See https://www.gnu.org/licenses/gpl-faq#AllCompatibility.

[298] GNU; Various Licenses and Comments about Them, available at: https://www.gnu.org/licenses/license-list.en.html

[299] See https://www.rabbitmq.com/mpl.html.

[300] GNU, FAQ, Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? available at: https://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs.

[301] GNU; Various Licenses and Comments about Them, available at: https://www.gnu.org/licenses/license-list.en.html.

				MPL v 1.1 is incompatible with GPLv2/AGPL[302] Apache v2 may be used in GPLv3[303]. Section 13 AGPLv3: AGPLv3 may be combined with GPLv3, combined work goes under AGPL, GPLv3 licensed code remains under GPLv3. Section 9 GPL v2 applicable to My SQL allows a work to be licensed under any later version.	licenses (See Table 4); - indicate that a tool under MPL is used, indicate its URL where to get the source (See Table 4). **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4).
4	Nephroblastoma Oncosimulator ICCS	N/A	N/A	No open source	**Licensing not restricted.** **Commercial and open source licensing allowed.** **Recommended license: Apache v2.** (a) flexible open source license; (b) compatible with many FOSS licenses; (c) popular for communication software and standards compliant (HTTP). Commercial licensing (in object code for fees) and as open source for research (source code for free) allowed. **Apache v2 license requirements:** Section 4 Apache v2: reproduction and distribution in any medium, with or without modifications, in Source or Object form, under additional or different license terms and conditions for use, reproduction, or distribution allowed. Copyright and license notices must be attached, changes identified. **To license under Apache v2**: - please attach Apache v2 license notice into each source file (Table 3)[i] - please include the text of Apache v2 license[304].
5	Nephroblastoma	N/A	N/A	No open source	**Licensing not restricted.**

[302] Ibid.

[303] ASF, Apache License v2.0 and GPL Compatibility, seehttps://www.apache.org/licenses/GPL-compatibility.html.

[304] See http://opensource.org/licenses/Apache-2.0.

	Application ICCS				**Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4
6	Personalized CHF Related Risk Profiles and "Real-Time Monitoring" (CHF) - mobile application FORTH	N/A	N/A	No open source	**Licensing not restricted.** **Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4.
7	Link with external Clinical Systems FORTH	N/A	N/A	Open source	**Licensing not restricted.** **Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4.
8	Osteoathritis mobile application FORTH	DCM4CHEE library: MPL v 1.1/GPL v2/LGPL v2.1[305]	Using the tool	No open source DCM4CHEE has triple license MPL v 1.1/GPL v2/LGPL v2.1. Either license may be used. Recommended license: LGPL v2.1. Section 6 LGPLv2.1: distribution under any terms possible as long as modification and reverse engineering are allowed.	**Licensing not restricted.** **Commercial and open source licensing allowed.** **License must permit:** modification for the customer's own use and reverse engineering for debugging such modifications (Section 6 LGPL v2.1). **Recommended license: Apache v2.** See p.4. **Additional requirements for DCM4CHEE Library under Section 6 LGPLv2.1:** (a) Use of DCM4CHEE Library under LGPL v.2.1 must be mentioned and LGPL v2.1 license text attached; (c) If the work during execution displays copyright notices, copyright notice for DCM4CHEE must be included as well as a reference to LGPL License v2.1[306]; (d) A user must be given a possibility to get the

[305] See http://www.dcm4che.org/.

[306] See http://www.gnu.org/licenses/old-licenses/lgpl-2.1.

					DCM4CHEE source code. Please see Table 5 **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4).
9	Virtuoso Triple Store FORTH/BED	virtuoso-opensource:GPLv2 with exemptions from GPLv2 for OpenSSL and Client Protocol Driver[307]	Using the tool	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, GNU GPL will cover the whole combination*[308]. **For GPL compliance, component must go under GPL.** Section 2 GPL v2: work based on the GPL´d Program must go under GPL v2. Section 9 GPL v2 allows a work to be licensed under any later version, i.e. GPL v3/GPL v3+.	**License options: GPL v2+/GPLv3+** **Commercial licensing not allowed; fees for physical distribution and support may be charged; release in object code must be supported by an option to get the source (See Table 6).** **Recommended license: GPL v3+** See p.1. **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4).
10	Exelixis FORTH	Ontop system: Apache v2 Teiid Data Virtualization Tool: LGPL v2.1	Use of algorithms Foreseen to be used	Linking to LGPL and release of the combined work under Apache 2.0 license is ok[309].	**Licensing not restricted.** **Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4. **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4). **LGPL:** If Teiid Data Virtualization Tool will be used, please follow one of the steps indicated in Table 5.
11	Cassandra Data	Cassandra: Apache v2 [310]	Using the tool	Section 4 Apache v2: distribution in object and	**Licensing not restricted.**

[307] See https://github.com/openlink/virtuoso-opensource.

[308] GNU, FAQ, Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? available at: https://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs.

[309] See http://stackoverflow.com/questions/7262068/apache-lgpl-closed-and-open-source.

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

	Repository FORTH/BED			source code with or without modifications allowed. Additional or different license terms and conditions for use, reproduction, or distribution of combined work allowed. Apache code stays under Apache, license and copyright notices in Apache code must be kept intact, changes identified.	**Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4 -identify that Cassandra under Apache v2 is used, indicate its URL; **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4).
12	Semantic Annotator FORTH	No external tools	N/A		**Licensing not restricted.** **Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4.
13	Semantic Search FORTH	No external tools	N/A		**Licensing not restricted.** **Commercial and open source licensing allowed.** **Recommended license: Apache v2** See p.4
14	MHA Web Application (Backend) BEDS	BSD 3-Clause License CDDLv1 Apache v2 LGPL v2.1 MIT License GPL v2 with CPE EPLv1 GPLv2+ GPL v3+	Calls object code	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, the terms and conditions of the GNU General Public License cover the whole combination*[311]. Component must go under GPL. BSD 3-Clause License, MIT License compatible with GPL[312]. Apache v2 is compatible with GPL v3[313]. Codes under GPLv2+, LGPL v2.1 may be used in software licensed under GPLv3[314].	**GPL v3+ with additional permission for use of tools under CDDLv2 and EPLv1 under Section 7GPL v3** **Commercial licensing not allowed; fees for physical transfer of copies, warranty and support may be charged (Section 4 GPL v3).** You can charge any fee you wish for distributing a copy of the program. If you distribute binaries by download, you must provide "equivalent access" to download the source—therefore, the fee to download source may not be greater than the fee to download the binary[316]

[311] See https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic.

[312] See https://www.gnu.org/licenses/license-list.en.html.

[313] See https://www.apache.org/licenses/GPL-compatibility.html.

[314] See https://www.apache.org/licenses/GPL-compatibility.html.

				CDDLv1 and EPL v1 are not compatible with GPL[315]. Use of these tools in GPL software requires additional permission under Section 7 GPLv3.	**Release in object code must be supported by possibility to get the source (See Table 6).** Section 6 GPL v3: distribution in object code allowed if accompanied by: (a) source code, (b) an offer to provide source code (valid for 3 years), (c) offer of access source code free of charge, (d) by peer-to-peer transmission – information where to get the source code. **To license under GPLv3:** - please include GPLv3 license notice into each source file (See Table 1); - please include text of GPL v3 license[317]; -grant permission to use tools under CDDLv1 and EPLv1 under Section 7 GPLv3 (See Table 2); -identify software dependencies and associated licenses (See Table 4) - identify that tools under CDDLv1 and EPL v1 are used, indicate the URL where to get the source codes; **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4). **LGPL:** - do one of the steps in Table 5.
15	MHA Web App Frontend BEDS	MIT License Standard "No Charge" GreenSock License[318] GPLv2+	Calls object code	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, the terms and conditions of the GNU*	**GPL v3+** **Commercial licensing not allowed; fees for physical transfer of copies, warranty and support may be charged (Section 4 GPL v3).**

[316] See https://www.gnu.org/licenses/gpl-faq#DoesTheGPLAllowDownloadFee.

[315] See https://www.gnu.org/licenses/license-list.en.html#GPLIncompatibleLicenses.

[317] See https://www.gnu.org/licenses/gpl.html.

[318] See https://greensock.com/standard-license.

		BSD 3 Clause License Creative Commons Attribution-Non-Commercial 3.0 License		*General Public License cover the whole combination*[319]. **For GPL compliance, component must go under GPL.** BSD 3-Clause License, MIT License, CC BY-NC 3.0 compatible with GPL[320]. GPL v2+ allows upgrade, tools under GPL v2+ may be used in software under GPL v3[321]. Green Sock License, II.b: You may use, duplicate, and distribute the compiled object code as embedded in Developed Works created by you, either for your own use or for distribution to a third party so long as end users of the Developed Work are not charged a fee for usage of or access to any portion of the Developed Work.	Commercial distribution would require "Business Green" Club GreenSock membership at: http://www.greensock.com/club/. **Release in object code must be supported by possibility to get the source (See Table 6)** **To license under GPLv3:** - please include GPLv3 license notice into each source file (See Table 1); - please include text of GPL v3 license[322]; -identify software dependencies and associated licenses (Table 4); **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4).
16	MHA Mobile App Frontend BEDS	MIT License Apache v2 GPL v3+	Calls object code	*Linking a GPL covered work statically or dynamically with other modules is making a combined work based on the GPL covered work. Thus, the terms and conditions of the GNU General Public License cover the whole combination*[323]. **For GPL compliance, component must go under GPL.** MIT License is compatible with GPL[324]. Apache v2 tools may be used in GPL v3 software[325].	**GPLv3+** **Commercial licensing not allowed; fees for physical transfer of copies, warranty and support may be charged (Section 4 GPLv3).** **Release in object code must be supported by possibility to get the source (See Table 6).** To release component under GPL v3, see p. 15.
17	MHA API and Data	CDDL v1	Calls object code	*Linking a GPL covered work statically or*	**GPL v3+ with permission to link component with**

[319] See https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic.
[320] See https://www.gnu.org/licenses/license-list.en.html.
[321] See https://www.apache.org/licenses/GPL-compatibility.html.
[322] See https://www.gnu.org/licenses/gpl.html.
[323] See https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic.
[324] See https://www.gnu.org/licenses/license-list.en.html.
[325] See https://www.apache.org/licenses/GPL-compatibility.html.

	Management BEDS	GPLv2+ with CPE Apache v2 CPL v1 GPL v3+ LGPL v2.1 MIT License		*dynamically with other modules is making a combined work based on the GPL covered work. Thus, the terms and conditions of the GNU General Public License cover the whole combination*[326]. **For GPL compliance, component must go under GPL.** MIT License is compatible with GPL[327]. Apache v2 programs may be used in GPL v3 software[328]. Programs under LGPL v2.1, GPL v2+ may be used in software under GPLv3[329]. CPL v1 and CDDL v1 are not compatible with GPL[330]. Use of these libraries in GPL software requires additional permission under Section 7 GPL v3[331].	**tools under CDDL v1 and CPL v1 under Section 7 GPL v3.** **Commercial licensing not allowed; fees for physical transfer of copies, warranty and support may be charged (Section 4 GPL v3).** **Release in object code must be supported by possibility to get the source (See Table 6).** **To license under GPLv3:** - please include GPLv3 license notice into each source file (See Table 1); - please include text of GPL v3 license[332]; -grant permission to use tools under CDDLv1 and CPLv1 under Section 7 GPLv3 (See Table 2); -identify software dependencies and associated licenses (See Table 4) - identify that tools under CDDLv1 and CPL v1 are used, indicate the URL where to get the source codes; **Notice preservation:** - keep copyright and license notices in sources of software tools intact (See Table 4). **LGPL:** - do one of the steps in Table 5.

1. GPL v3 license notice

Table 1: License notice for GNU GPL Version 3

[326] See https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic.
[327] See http://www.gnu.org/licenses/license-list.en.html.
[328] See https://www.apache.org/licenses/GPL-compatibility.html.
[329] See https://www.apache.org/licenses/GPL-compatibility.html.
[330] See http://www.gnu.org/licenses/license-list.en.html.
[331] See https://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs.
[332] See https://www.gnu.org/licenses/gpl.html.

How to apply	GPL v3 License notice
Attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found. Also add information on how to contact you by electronic and paper mail.	<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author> This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/>.
If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:	<program> Copyright (C) <year> <name of author> This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

2. Additional permissions under Section 7 GPL v3

Table 2: Additional Terms under Section 7 GNU GPL Version 3

How to apply	GPLv3 permission notice
If you want your program to link against a library not covered by the system library exception, you need to provide permission to do that under section 7. The following license notice will do that. You must replace all the text in brackets with text that is appropriate for your program. If not everybody can distribute source for the libraries you intend to link with, you should remove the text in braces; otherwise, just remove the braces themselves.	Copyright (C) *[years] [name of copyright holder]* This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, see <http://www.gnu.org/licenses>. Additional permission under GNU GPL version 3 section 7 If you modify this Program, or any covered work, by linking or combining it with *[name of library]* (or a modified version of that library), containing parts covered by the terms of *[name of library's license]*, the licensors of this Program grant you

	additional permission to convey the resulting work. {Corresponding Source for a non-source form of such a combination shall include the source code for the parts of *[name of library]* used as well as that of the covered work.}

3. Apache v2 license notice

Table 3: License notice for Apache License, Version 2.0

How to apply	**Apache v2 License notice**
To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.	Copyright [yyyy] [name of copyright owner] Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

4. Software dependencies and notice preservation

Table 4: Labeling of software dependencies

How to apply	**Notice preservation**
Label software dependencies using the following format:	name of software tool/library] licensed under [license applicable to software tool/library]available at [URL].
If you incorporate files from external projects without making changes to the code in the file itself, simply leave the file with all notices intact. If the external project uses the single COPYRIGHT file method, you should copy the names of all the copyright holders from that file and place them, along with any copyright, permission, and warranty disclaimer notices required by the license, at the top of the incorporated source file.	The top of the incorpoated file should look something like this: /* Copyright (c) YEARS_LIST, Permissive Project Contributor1 <contrib1@example.net> ** Copyright (c) YEARS_LIST, Permissive Project Contributor2 <contrib2@example.net> ** ... ** ** Permission to use, copy, modify, and/or distribute this software for ** any purpose with or without fee is hereby granted, provided that the

	** above copyright notice and this permission notice appear in all copies. ** ** THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL ** WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED ** WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR ** BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES ** OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, ** WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ** ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS ** SOFTWARE. */

5. Requirements for distribution of components which contain libraries or tools under LGPL v2.1

Table 5: Terms for distributing "work that uses the Library" under Section 6 LGPL v2.1

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must **do one of these things**:	a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the

	executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.
For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it.	

6. Distribution of GPL v3 software in object code

Table 6: Conveying Non-Source Forms under Section 6 GPL v3

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, **in one of these ways**:	a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange. b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge. c) Convey individual copies of the object code with a copy of the written offer to

	provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b. d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements. e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.