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

Project acronym: MyHealthAvatar

Deliverable No. 11.4

Legal framework for the exploitation of MyHealthAvatar

Grant agreement no: 600929

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

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	MyHealthAvatar
Project Full Name:	A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information
Deliverable No.:	D11.4
Document name:	Legal framework for the exploitation of MyHealthAvatar
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	PU
Version:	1
Actual Submission Date:	29/02/2016
Editor: Institution: E-Mail:	Prof. Dr. Nikolaus Forgó LUH forgo@iri.uni-hannover.de

[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)

ABSTRACT: This deliverable provides an overview of the legal and ethical issues that are likely to arise during the exploitation stage after the project's end. These issues mainly include e-consent systems, liability, medical devices and intellectual property rights.

KEYWORD LIST: General Data Protection Regulation, electronic consent, hospital information system (HIS), liability, medical devices, Intellectual Property Rights (IPR)

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

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

MODIFICATION CONTROL

Version	Date	Status	Author
0.1	15.09.2015	Draft	Nikolaus Forgó, Marc Stauch, Sarah Jensen, Stefanie Hänold, Alan Dahi, Iryna Lishchuk
0.2	12.10.2015	Draft	Nikolaus Forgó, Marc Stauch, Sarah Jensen, Stefanie Hänold, Alan Dahi, Iryna Lishchuk
0.3	12.11.2015	Draft	Nikolaus Forgó, Marc Stauch, Sarah Jensen, Stefanie Hänold, Alan Dahi, Iryna Lishchuk
0.4	11.01.2016	Draft	Nikolaus Forgó, Marc Stauch, Sarah Jensen, Stefanie Hänold, Alan Dahi, Iryna Lishchuk
0.5	10.02.2016	Pre-final draft	Nikolaus Forgó, Marc Stauch, Sarah Jensen, Stefanie Hänold, Alan Dahi, Iryna Lishchuk

0.6	12.02.2016	Review draft	Prof. Feng Dong (BED), Prof. Dr. Norbert Graf (USAAR), Dr. Emmanouil G. Spanakis (FORTH)
1.0	29.02.2016	Final	Nikolaus Forgó, Marc Stauch, Sarah Jensen, Stefanie Hänold, Alan Dahi, Iryna Lishchuk

List of contributors

- Alan Dahi (LUH)
- Nikolaus Forgó (LUH)
- Stefanie Hänold (LUH)
- Sarah Jensen (LUH)
- Iryna Lishchuk (LUH)
- Theresia Rasche (LUH)
- Marc Stauch (LUH)
- Emmanouil G. Spanakis (FORTH)
- Ziggy Kovacs (Larkbio)
- Norbert Graf (USAAR)

Contents

1. EXECUTIVE SUMMARY 7
2. INTRODUCTION 9
3. DATA PROTECTION 10
3.1. BACKGROUND 10
3.2. AN OVERVIEW OF THE EU DATA PROTECTION REGIME 10
3.3. IMPORTANCE OF CONSENT 13
3.3.1. The doctrine of informed consent during the project duration 13
3.3.2. Validity of e-consent systems in European Member States 14
3.3.3. The potential of e-consent forms to achieve an informed consent easier than with paper-based consent forms 16
3.3.4. How a voluntary consent can be achieved 18
3.3.5. Specific consent 19
3.3.6 Other relevant issues with regard to consent 20
3.4. FURTHER REQUIREMENTS 22
3.4.1. The need for fair data processing 22
3.4.2. Data security 23
3.4.3. Ensuring User Identity 24
3.4.4. Linking with Hospital information systems (HIS) 24
3.4.5. Data protection implications of Third Party apps including the risk of totalitarian-style monitoring 27
4. LIABILITY RISKS OF THE PLATFORM 31
4.1. LIABILITY OF APPS 31
4.2. POSSIBLE FORMS OF USER INJURY THROUGH PLATFORM USE AND THEIR COMPENSABILITY 32
4.2.1. Liability for physical bodily injury 33
4.2.2. Liability for mental distress 35
4.2.3. Conclusions on private law liability risks 37
4.3. PRODUCT LIABILITY ISSUES 37
4.3.1. The European Product Liability Regime 37
4.3.2. Software as a product? 38
4.3.3. Producer 42
4.3.4. Defective Product, damage covered and causality 43
4.3.5. Exclusion of liability 45
4.4. THE MEDICAL DEVICES REGIME 45
4.4.1. Background 45

4.4.2. Key aspects of the Medical Devices regulatory regime 46
4.4.3. Implications for the exploitation of the MHA platform 48
5. INTELLECTUAL PROPERTY RULES FOR THE EXPLOITATION 53
5.1. OPEN SOURCE AND LICENSE SOLUTIONS 53
5.2. LICENSING SOLUTIONS FOR MYHEALTHAVATAR COMPONENTS 53
5.2.1. Apache License Version 2.0 53
5.2.2. GNU GPL Version 3 55
5.3. LICENSING SOLUTION FOR THE MYHEALTHAVATAR PLATFORM AS A WHOLE 57
5.4. EXPLOITATION OPTIONS 58
5.4.1. GNU GPL Version 3 58
5.4.2. Release of source code for GPL components 59
5.4.3. Apache License Version 2.0 60
5.5. THIRD PARTY DEVELOPMENT LEGAL FRAMEWORK 61
5.5.1. MHA account 62
5.5.2. API license 62
5.5.3. Restrictions on use of MHA API 63
5.5.4. Use of MHA users' data 63
5.5.5. Use of user generated content 64
5.5.6. Warranty and liability 65
5.5.7. Duration and termination 65
5.5.8. Rules for processing IP protected content on MHA services 65
5.6. COLLABORATION WITH THE CHIC PROJECT 66
5.6.1. CHIC-MHA Memorandum of Understanding 68
5.6.2. CHIC-MHA Collaboration Agreement 68
6. CONCLUSION 72
7. REFERENCES 73
8. APPENDIX – ABBREVIATIONS AND ACRONYMS 75
9. ANNEXES 78
ANNEX 1: E-CONSENT FORM 78
ANNEX 2: GENERAL TERMS AND CONDITIONS FOR TESTING PHASE 79
ANNEX 3: PRIVACY POLICY FOR TESTING PHASE 87
ANNEX 4: EXTENDED TERMS AND CONDITIONS FOR EXPLOITATION STAGE AFTER THE PROJECT'S END 90
ANNEX 5: EXTENDED VERSION OF THE PRIVACY POLICY 99
ANNEX 6: MYHEALTHAVATAR API TERMS OF USE 103
ANNEX 7: CHIC-MHA MEMORANDUM OF UNDERSTANDING 110
ANNEX 8: CHIC-MHA COLLABORATION AGREEMENT 114
ANNEX 9: SOFTWARE COMPONENT LICENSE COMPATIBILITY TABLE 119

1. Executive Summary

This deliverable examines the legal and ethical challenges that are likely to arise during the exploitation stage after the project's end and gives recommendations on how to address them. The deliverable is divided into three main parts: the first addresses the data protection issues of the MyHealthAvatar platform; the second questions of liability and the final part intellectual property issues.

The data protection analysis focuses firstly on providing an overview of the EU data protection regime, highlighting the current reform process in which in 2018 the General Data Protection Regulation is set to replace the Data Protection Directive. Some aspects of the General Data Protection Regulation draft have already been pointed out in D11.2, but in view of the fact that there has been revision of the draft that was analysed in D11.2, it was crucial to consider the newest developments of the General Data Protection Regulation in this deliverable.

The focus then shifts to electronic consent. As an online health platform, MyHealthAvatar will prefer electronic consent to paper-based consent for two reasons: first, because signing e-consent forms is more convenient for users – the interested person does not have to print out the form and send an ink-signed version back to the operator. Secondly, the storage of large numbers of consent forms is much easier when they are electronic than when they are paper-based. Another big benefit of using electronic consent is that information can be presented in a user-friendly way, e.g. including tutorial videos, so the user can fully understand to what he signs up if he enters the MHA platform.

While e-consent systems were already addressed in D11.3 with respect to the context of digital avatars in general, this deliverable takes into consideration the final state of the platform and focuses on the questions of how a voluntary consent can be achieved in the exploitation phase after the project's end and how the risk of misuse by unauthorised third parties can be reduced to a minimum.

The Deliverable goes on to show how the clauses of the current and extended Terms and Conditions and Privacy Policy derive from data protection law. Additionally, different methods are analysed with a view to guaranteeing voluntariness of consent. The Deliverable also explains how the use of Hospital Information Systems (HIS) can help to meet the challenge that the data that are stored in the avatar are up to date and correct. These aspects are not only important for data protection requirements, but they are also crucial for the avatar to live up to its promise of facilitating patient-specific treatment. Therefore, section 3.4.4 shows how MHA can benefit from the epSOS approach and why a data transfer agreement between MHA and the respective hospital and a patient data transfer request (that can be used by the MHA user to mandate the data transfer from the hospital to MHA) are additionally needed. Concluding the section on data protection is an investigation into the data protection implications of Third Party Apps. One of the key features of MyHealthAvatar is its open Application Programming Interface (API), through which Third Parties will be able to connect their – independently developed – apps to the

MyHealthAvatar platform, thereby extending its functionality beyond the core services provided by the platform itself.

There are various risks of liability that need to be considered when exploiting the MHA platform. Apart from liability for breach of data protection laws or rules of privacy and confidentiality, liability for personal injury caused by the provision of faulty information or the wrongful omission of information is a key risk of exploiting the platform. Rules on liability which differ from member state to member state are complex and e-Health developments due to their speed and novelty pose special difficulties. Depending on the specific case the injured user might be able to make a claim for compensation in contract law or tort. He might also benefit from strict liability rules established by the EU Directive on Product Liability and the implementing national laws. One of the most prominent issues for all types of liability is that a multiplicity of parties contributes to the user/patient outcome, so that their roles in the chain of events that resulted in the harm must be assessed to apportion their share of liability to the injured user. The user's/patient's reaction might also reduce or disallow liability in total in the event of contributory negligence. The platform provider also must carefully consider that his liability might under certain circumstances also be extended to third party apps.

Next to the liability issue the deliverable will touch on the question of how far the platform and apps will also be subject to ex ante regulatory checks that are designed to offer protection to users in advance, as required by the European Medical Device Regime. Key aspects, including the qualification of the platform and third party apps as a medical device, their risk classification and required procedural steps are presented to the reader.

The third main part of this deliverable then deals with the rules for handling Intellectual Property Rights (IPR) that are important during the exploitation stage. This includes especially open source licensing and license solutions and a third party development framework.

2. Introduction

This deliverable is the outcome of task 11.4, which calls for a definition of the rules for the exploitation of the platform after the project's end in order to guarantee compliance with data protection and intellectual property regulation.

Included as Annexes are a sample e-consent form, privacy policy, and general terms and conditions for the exploitation phase, the privacy policy and the general terms and conditions used during the testing phase, as well as the MyHealthAvatar API License Agreement. Also presented is a Software component license compatibility table concerning the software components and licenses in MHA, as well as the CHIC-MHA Memorandum of Understanding and the CHIC-MHA Collaboration Agreement.

3. Data protection

3.1. Background

The MyHealthAvatar platform processes, by virtue of its nature and purpose, the health and lifestyle data of individuals who register with it. This data can be provided either by the users themselves, or by physicians and other medical professionals under the instruction of their patients/the users of the platform. Either way, citizens have become increasingly aware of the importance of data protection. A key factor in the successful exploitation of the MyHealthAvatar platform will consist not only in its compliance with EU data protection rules, but also in its ability to reassure users that their personal data is in good hands, i.e. that their personal data will be kept technically safe and that they will remain in control over what is done with their data.

This section will firstly present an overview of the EU data protection regime before discussing in more detail the importance of consent and the challenges and requirements of connecting Hospital Information Systems (HIS) and Third Party apps to the MyHealthAvatar platform. We are also aware of the potential risk to individual freedom of users and that the data collection and storage can lead to totalitarian supervision by non-democratic governments.

3.2. An overview of the EU data protection regime

The main piece of legislation in the EU on data protection is the Data Protection Directive 95/46/EC (DPD)[3] which is due to be replaced by the General Data Protection Regulation (GDPR), expected to enter force in 2018.[4] As already described in detail in Deliverable 11.1,[5] the DPD establishes a framework that regulates "the processing of personal data wholly or partly by automatic means", by placing various duties upon the 'data controller' who processes the data. As defined in Article 2d DPD, this is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.[6]

Because D11.1 already illustrated the legal regime put in place by the DPD, and because the DPD will be replaced by the GDPR, this Deliverable will focus in equal measure on the latter. In contrast to its predecessor, being a regulation and not a directive, the GDPR will not need to be implemented into Member State law. It will be directly applicable in Member States upon entering into force. In theory, this should harmonise the currently disparate Member

[3] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (DPD)*, 1995, OJ 281/31 (23.11.1995).

[4] See for the leaked version of the GDPR used as the basis for the analysis performed in this Deliverable: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.

[5] MyHealthAvatar, Deliverable No 11.1, The Ethical and Legal Framework of MyHealthAvatar, chapter 4, p. 14 ff.

[6] Article 3 (1) DPD.

State rules on data protection. Currently, while the fundamentals of data protection are the same in all Member States, the details, especially with regard to the processing of sensitive health data and the use of personal data for research purposes, differ greatly due to the DPD being implemented differently in the various Member States.

Admittedly, despite being a regulation, the GDPR will not necessarily do away with differing Member State approaches to the processing of personal data for research, as the draft as it stands permits Member States to derogate from certain rights.[7] Whether and how Member States will take advantage of these rights to derogate remains to be seen. Nevertheless, the GDPR still lays down basic principles that must be adhered to when personal data is processed. As is also the case in the DPD, data must be processed according to the globally acknowledged principles of:

1. lawfulness, fairness and transparency;
2. purpose limitation;
3. data minimisation;
4. accuracy;
5. storage limitation; and
6. integrity and confidentiality.[8]

In addition, the GDPR clarifies that the data controller is accountable for compliance with the principles.[9] As already examined in past deliverables, the provider of the MyHealthAvatar platform will be a data controller.

The data protection principles put forward in the GDPR can be seen as providing a guide for MyHealthAvatar in the exploitation stage, as they will need to be adhered to. First, the principle of lawfulness, fairness and transparency, will mandate that a legal ground, such as user consent (which will be discussed in more detail subsequently) is needed to justify any processing, as well as that, following from the ideas of fairness and transparency, any data collected must be continuously curated with a view to accuracy.

Second, the principle of purpose limitation means that personal data collected may only be collected for specified purposes and that it may not be processed for purposes incompatible with the original purpose. In the third place, it follows from the principle of data minimisation that only the bare amount of data necessary for the processing purpose may be collected – wholesale data collection is consequently prohibited. This idea also leads to the principle of storage limitation, i.e. that personal data shall not be stored longer than necessary for the intended purposes.

In addition to these basic principles, the GDPR sets forth further restrictions with regards to data concerning health[10] - exactly the type of data that will be processed in MyHealthAvatar. The default is that the processing of such data is prohibited.[11] Only where certain

[7] Article 83 (2) GDPR.

[8] Article 5 (1), GDPR.

[9] Article 5 (2) GDPR.

[10] Article 9 GDPR.

[11] Article 9 (1) GDPR.

requirements have been met, such as explicit consent by the data subject for specified purposes, does the prohibition not apply.[12] It must be noted, however, that again the GDPR permits Member States to derogate from the general rules in certain cases, to be discussed below.[13]

The general obligations of the data controller are stated in Article 22 (1) GDPR: "Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation."

Some of the obligations that the GDPR will impose upon the controller of the MyHealthAvatar platform compared to the DPD are to comply with the data subject's request to erase personal data concerning him,[14] and to give the user the data he provided to the controller in a commonly used machine-readable format.[15] The GDPR also introduces the concept of "data protection by design and by default"[16], i.e. technical and organisational measures through which the adherence to data protection principles, such as data minimization, becomes the default position, instead of an afterthought. We would like to point out that the embedding of data protection into the design of the MyHealthAvatar platform is something that was pursued from the beginning.

Another requirement that will be introduced by the GDPR is that of controllers and processors maintaining records of their processing activities, to include e.g. the purpose of the processing and the categories of personal data.[17] Similarly, the GDPR places great importance on organisational and technical aspects of data security,[18] and obliges, in case of a personal data breach that is likely to result in a risk for the rights and freedoms of the data subjects concerned, the controller to notify the competent supervisory authority,[19] and where there is a high risk for the rights and freedoms, also the data subject.[20] Furthermore, the controller will have to designate a data protection officer, as this is foreseen where special categories of data, such as health data, will be processed on a large scale.[21]

[12] Article 9 (2) (a) GDPR.
[13] Article 9 (2) (a), (5) GDPR.
[14] Article 17 GDPR.
[15] Article 18 GDPR.
[16] Article 19 GDPR.
[17] Article 28 GDPR.
[18] Article 30 GDPR.
[19] Article 31 GDPR.
[20] Article 32 GDPR.
[21] Article 35 GDPR.

3.3. Importance of consent

3.3.1. The doctrine of informed consent during the project duration

As previously discussed in deliverables D11.1 (p. 25 ff.) , D11.2 (p. 21 ff.) and D11.3 (p. 10 ff.), the doctrine of informed consent is crucial both in legal and ethical terms as arguably the primary basis for justifying data processing, while respecting to the dignity and autonomy of the data subject. Thus, insofar as it is possible to achieve informed consent for data processing, the data subject should normally be asked to consent. If this is impractical or undesirable in a particular case, and another legal basis for processing used instead, the onus will be upon the data controller to show why.[22] With respect to the legal aspects of the doctrine of informed consent, Article 2h DPD, Article 7 (a) and Article 8 DPD plays an important role. Consent is defined by Article 2h DPD as 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. This approach will be continued in draft Article 4 (8) of the new General Data Protection Regulation, which states that consent means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Pursuant to Article 8 (1) DPD the processing of sensitive health data is generally forbidden. According to Article 8 (2) DPD this is allowed only if one of the exemptions of the paragraphs 2-4 applies. With regard to health-related projects, in particular paragraph 2a (explicit consent), paragraph 3 (medical care) and paragraph 4 (public interest such as medical research) can be applicable. Similarly, under the new provisions of the General Data Protection Regulation draft Article 9 (1) stipulates that the processing of sensitive personal data shall be prohibited. Paragraph 2 includes the exemptions to paragraph 1: Pursuant to paragraph (2) (a) the processing of sensitive data is not forbidden, if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject. Paragraph 2 (g) and (hg) includes the exemption for the sensitive data processing for reasons of substantial public interest and public in the area of public health respectively. And according to paragraph (2) (h) the rule of Article 9 (1) does not apply if the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law or pursuant to contract with a health professional.

In terms of the development and testing stage of MyHealthAvatar, the consortium has always acknowledged the importance of the doctrine of informed consent and developed a legal framework that is based on the informed consent of data subjects. In this regard, LUH drafted different paper-based consent forms tailored to the differential needs of the addressed persons, as well as reflecting the different aims and implications of the

[22] See Nikolaus Forgó, Regine Kollek, Marian Arning, Tina Kruegel und Imme Petersen. 2010. 'Ethical and Legal Requirements for Transnational Genetic Research' p. 10.

processing in question (a shorter version for the consortium participants, and extended versions for volunteers who participated in the projects MyLifeHub[23] and Carre[24] and general volunteers without previous knowledge of the projects: see Appendixes 2, 3 and 4 of deliverable D11.1, p. 60 ff.).

For the later stage of the testing phase of the project, LUH drafted General Terms and Conditions, a Privacy Policy and an e-consent form (please see Annexes 2 and 3 of the present Deliverable, p. 78 ff.). These documents were used as a starting point for developing extended versions of the Terms and Conditions and the Privacy Policy (Annexes 4 and 5) for the exploitation stage after the project's end.

The purpose of the Terms and Conditions of MyHealthAvatar is not only to regulate the use of the platform in a detailed way and to resolve points of uncertainty. In addition, it seeks to regulate general risks, that are associated with the use of the platform, (please see section 4 'Liability risks of the platform, p. 31 ff.) and avoid the need for the operator of MyHealthAvatar to negotiate single clauses with each possible user. Another significant benefit of Terms and Conditions is that the operator can explain to the interested person and user respectively how the data processing will take place.

The purpose of the Privacy Policy of MyHealthAvatar is to describe the rights of the data subject regarding the processing of his personal data (Articles 12 ff. DPD), how his data is protected by security measures, how information can be shared with other users or third parties and how single personal data and the whole avatar can be deleted and under what circumstances (please see clause 1 'General information'). Individual clauses from both the Terms and Conditions and the Privacy Policy will be further presented and explained in the next sections whenever they are relevant for the specific aspects of consent then under discussion.

3.3.2. Validity of e-consent systems in European Member States

Many operators of web-based platforms, similar to MHA, which users access and interact with via the internet, wish to implement an e-consent form rather than a paper-based form because of the greater logistical convenience offered, including ease for users (who do not have to go to the trouble of printing-off, signing and mailing hardcopy documents), and for the operator in terms of managing the record storage for potentially large numbers of users. However, from the legal point of view, e-consent is not always possible in relation to the processing of sensitive data (please see also chapter '3.2.3.1 Achieving explicit consent electronically?' of D11.3, p. 13 ff.).

Here, the legal starting point is currently provided by Article 8 (2a) DPD, which states that consent has to be given explicitly, meaning the data subject must take some positive action to signify agreement: usually this is done by a hand-written signature.[25] According to the Article 29 Working Party's Opinion 15/2011 on the definition of consent[26], written consent

[23] See http://mylifehub.ccgv.org.uk/index.html.

[24] See www.carre-project.eu

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

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

can be replaced by using electronic or digital signatures,[27] albeit these are not widely used. Further, the Working Party is of the view that in principle explicit consent could also be given by clickable buttons, confirmatory mails etc.[28] At present, though, the latter is not true for every member state of the European Union because the Data Protection Directive sets only the minimum standards to be applied at national law.

This latitude accorded by the Data Protection Directive means that member states are allowed to apply stricter rules as long as these rules do not conflict with free movement and free market rules. In this regard, some national data protection laws contain the requirement that consent has to be in writing meaning that the data subject has to sign a piece of paper. For instance, Article 7 § 2 Greek Data Protection Act[29] requires a written consent form for the processing of sensitive health data pursuant to article 7 (2a) Greek Data Protection Act.[30] Similarly, section 4a German Federal Data Protection Act[31] requires an informed consent in writing, unless special circumstances warrant any other form. 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.[32]

Once the Data Protection Directive is replaced by the GDPR, there will be more harmonisation on the European level (cf. chapter 3.2 'An overview of the EU data protection regime, p. 10 ff. and D11.2 'Survey on strengths and weaknesses of related European data protection framework'), chapter 5.1 'Harmonisation of data protection in the EU', p. 15 ff.). According to Article 91 the GDPR shall apply two years after publication in the Official Journal of the European Communities. This will probably be in 2018. Harmonisation will be effected because the GDPR, as a regulation, will be directly applicable in Member States, superseding any national law. However, it must be noted that the GDPR does permit member state derogations in certain cases; indeed, respect to the processing of health data, Article 9(5) allows States to maintain or introduce further conditions including limitations. It remains to be seen what use individual member states will make of this power, but it carries the risk of jurisdictional differences across the Union, in opposition to a regulation's overall aim of harmonisation.

The current Data Protection Directive, on the other hand, needed to be implemented into member state law – with resultant member state variations of the principles laid down in the Data Protection Directive. For now, during the exploitation stage, MyHealthAvatar may

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

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

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

[30] Ibid.

[31] See http://www.gesetze-im-internet.de/englisch_bdsg/.

[32] In this case the information referred to in subsection 1 second sentence and the reasons the defined purpose of research would be seriously affected shall be recorded in writing. Article 4a German Federal Data Protection Act requires an informed consent in writing, unless special circumstances warrant any other form; Article 13 German Telemedia Act (applicable to electronic information and communication services) states that approval (consent) can be stated electronically under certain requirements; however it is not clear if data protection regulations from the Telemedia Act also apply to content data. Article 7 § 2 Greek Data Protection Act requires consent for processing of health data in writing.

be able to benefit from the fact that under the UK Data Protection Act[33] written consent is not required for the processing of sensitive data. Thus, simple e-consent is possible. This because according to Article 4 (1a) DPD the establishment of the data controller determines what national provisions of the member state is applicable for the processing of personal data.

During the testing phase, BED was the data controller. Therefore, e-consent was possible during the project's duration. Clause 17 'Applicable law' of the Terms and Conditions (and clause 13 of the current version respectively) informs the user that the applicable law is English law. For the exploitation stage after the project's end LUH recommends a data controller as the operator of the platform whose national law does not stipulate that explicit consent of sensitive health data must be given in written form.

3.3.3. The potential of e-consent forms to achieve an informed consent easier than with paper-based consent forms

Using electronic consent (e-consent) means for MyHealthAvatar that more interested people can be reached and that the process of granting consent can be simplified. At the beginning of the testing phase, when MyHealthAvatar used the paper-based consent forms, the volunteers had to wait for an invitation code after having signed the consent form. When MyHealthAvatar implemented the e-consent forms, interested persons could use the services of MyHealthAvatar right after having accepted the General Terms and Conditions and the Privacy Policy. This advantage should also be used for the exploitation stage of the project.

Another benefit of e-consent is that information can be presented in a user-friendly and active way, including videos that explain the functionality of MyHealthAvatar, and clickable links for receiving more information on a specific part. MyHealthAvatar has tried to benefit from these potential advantages already during the testing phase. Thus it has developed tutorial videos (including videos about the general purpose of MyHealthAvatar and the goals of the mobile application, but also videos about specific functionalities such as web settings, web diary, mobile journey, calendar, and the toolbox) that can be watched on the platform. The videos can also be seen on YouTube[34] and are embedded in the MyHealthAvatar Evaluation page[35]. Equally, during the exploitation stage potential users could gain a better understanding of the functionalities of MyHealthAvatar through these means.

To achieve an informed consent, the operator of MyHealthAvatar must inform the would-be user adequately about the points that are stipulated in Article 10 DPD:
- the identity of the controller, Article 10 (a),

- the purposes of the processing for which the data are intended, Article 10 (b) and

- further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of

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

[34] See https://www.youtube.com/results?search_query=myhealthavatar.

[35] See http://www.ehealthserver.com/mha/.

failure to reply, and the existence of the right of access to and the right to rectify the data concerning him, Article 10 (c).

These provisions, which will be re-enacted in the GDPR, namely in Article 14, are reflected in the Terms and Conditions drafted by LUH to cover the MHA exploitation stage. Thus Clause 1 'General Information' of the Terms and Conditions explains the identity of the controller according to Article 2d DPD to comply with Article 10 (a) DPD. The functionalities and the purpose of MyHealthAvatar are not only presented by the tutorial videos, but are also explained in clause 2 'Purpose of MyHealthAvatar' and clause 4 'Functionalities of MyHealthAvatar and Use of Content' of the Terms and Conditions. Clause 3 'Sharing your personal data via MyHealthAvatar Platform' of the Privacy Policy explains the user the functionality of sharing not-sensitive data such as data concerning food, drink and calories, events and activities.

By reading these clauses, the user will obtain a detailed understanding of the intention of the project and of the different ways in which the stored data may be processed. Thereby, the requirements of Article 10 (b) DPD can be met. Tutorial videos explaining how the different processing of data takes place can even increase the understanding and support to achieve an informed consent. This is not only true for the situation where an interested person wants to become a user of MyHealthAvatar, but also for the situation when a user can transfer the data to a third person or share it with selected friends.

Clause 5 'Your rights regarding the processing of your personal data' of the Privacy Policy explains the user his rights to information, access, rectification, erasure, blocking according to Article 12 DPD and object to the data processing pursuant to Article 14 DPD. Thereby, the operator of MyHealthAvatar meets the requirements of Article 10 (c) DPD.

The extended version of the Terms and Conditions also includes a clause referring to the various third parties that can receive the collected and stored data if the MyHealthAvatar user consents to the transfer of this data, and states that the user may exert his rights also against these persons (clause X 'Third Party Services'). According to clause 1 'General Information' of the extended Privacy Policy, the user will receive a copy of the Privacy Policy by email. Furthermore, the Privacy Policy can be downloaded from the platform. Clause 6 'Entitlement to Terms and Conditions of MyHealthAvatar' and clause 14 'Member Notices' of the extended Terms and Conditions (and clause 10 of the current Terms and Conditions) state that not only the Privacy Policy, but also the Terms and Conditions and the consent form will be sent to the user later. This will enable the user to re-read and comprehend the content of the Privacy Policy at their greater ease and leisure.

Admittedly, in some cases questions may occur to the user, which have not been fully anticipated in the text of the Terms and Conditions or Privacy Policy. In such a situation it is important that the user or an interested person can ask a qualified member of the platform administration team further and follow-up questions. Currently, interested persons and users can contact the project coordinator Professor Feng Dong by using the mail address mha@ccgv.org.uk. For the exploitation stage after the project's end, it would be desirable to constitute a contact point with qualified platform team members for these purposes (cf. clause 1 of the Terms and Conditions).

3.3.4. How a voluntary consent can be achieved

As explained in chapter 3.2 of D11.3, p. 10 ff., 'The challenges of granting consent digitally – electronic informed consent', the implementation of an electronic informed consent (e-consent) form has not only advantages, but poses also threats to the rights of the individual who wants to sign up to MyHealthAvatar. Especially when the data subject can give (electronic) consent from everywhere and there is no personal explanation by the operator of MyHealthAvatar or his staff before asking for consent, it is difficult to control if the data subject really has come voluntarily to the decision to allow processing of his sensitive health data. For example, third parties such as physicians, insurers, researchers, pharmaceutical companies and employers could have incentivized or exerted pressure to their patients, insured persons and employees respectively to create an account for MyHealthAvatar or to transfer already collected sensitive health data to them.

Freely given consent means that the consent has to be given without compulsion, force, duress and obligation.[36] The person concerned must have come to the decision to process his data (be it because he wants to become a user of MyHealthAvatar or be it because he wants to send his collected and stored data to a third party) without fearing disadvantages or expecting advantages, such as getting a higher position in a job or getting a better or more cost-efficient insurance. Here, the question arises of how it can be guaranteed that consent for the processing of (sensitive data) is given voluntarily during the exploitation stage after the project's end.

The possibility to withdraw the consent at any time without suffering any reprisal helps to minimise the risk of coercion. If the employer, insurer, or physician knows that the data subject can withdraw his consent easily (so that it remains necessarily contingent), they are less likely to expend effort in exerting undue pressure to obtain it in the first place. Here the mechanism of e-consent can help matters by enabling the grantor to withdraw his consent electronically easily and quickly without having to go back to the grantee, and without attracting the attention of others.

MyHealthAvatar is aware of the user's right to withdraw consent and guarantees the MyHealthAvatar user the right to withdraw his consent at any time without any disadvantages by clause 1 'General Information' of the Privacy Policy. If the user exercises this right and deletes his account by emailing the request to mha@ccgv.org.uk, all collected data will be permanently deleted as laid down in clause 6 'Deleting your account' of the Privacy Policy.

For the exploitation phase after the project's end, the extended General Terms and Conditions assume that there is a 'withdrawal button' that can be clicked by the MyHealthAvatar user. This is why cf. clause 4 of the extended version of the Terms and Conditions and clauses 1 and 6 of the Privacy Policy assume that MyHealthAvatar has such a button and that the user can choose between mailing the data controller and just using the 'withdrawal button'. Moreover, to ensure that the user does not feel forced to keep his avatar alive just because he is not aware of an alternative means for keeping the data

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

collected and stored in the avatar, clause 11 'Changes to Privacy Policy' of the extended Privacy Policy guarantees that the user can download his selected and stored data as a PDF file before his account is deleted. This means he will not lose all his data that he might have collected over a long time with some effort.

In addition, since it might be the case that a user does not want to withdraw his consent to the processing of all data, but just of specific health information, there is clause 7 'Deleting health information' of the Privacy Policy stating that the user can also delete a piece of health or lifestyle information and retain his overall account. If the user exercises this right, other users with whom the user has shared data will no longer be able to see the deleted data. However, permanent deletion of health and lifestyle information can technically only be guaranteed if the user deletes his overall account. This technical fact is pointed out to the user in clause 7.

In cases where a party that might be inclined to exert pressure on MHA users is itself a user of the platform, the risks of it doing so may also be contained through contractual provisions, e.g. in a contract between MyHealthAvatar and an insurer sponsoring a given third party app. Here the contractual licence, permitting use of the MyHealthAvatar API, should include a provision stating that exerting pressure, duress and coercion is prohibited and will lead to exclusion from the co-operation with MyHealthAvatar. The current license agreement includes such a clause. Moreover, the platform administrator should also consider establishing a central contact point where users can notify that other users or third parties have exerted pressure on them. By this means, the enforcement of the signed contract will be made easier for MyHealthAvatar.

3.3.5. Specific consent

Article 2h DPD requires that consent for the processing of sensitive health data must not only be given explicitly and freely, but also be specific in terms of the information provided to the user about the nature and purpose of the processing. Therefore, it is important to avoid an abstract consent. The more rights and freedoms of the MyHealthAvatar user are touched, the higher are the requirements concerning the degree of specification.[37] The user has to know what kind of personal data will be processed and to which specific activity his consent refers.[38] Accordingly, MyHealthAvatar aims to provide the user with the required specific information. Clauses 2 'Purpose of MyHealthAvatar' and clause 4 'Functionalities of MyHealthAvatar and Use of Content' of the Terms and Conditions explain the general purpose of MyHealthAvatar and how MyHealthAvatar can be used. The tutorial videos illustrate the different functionalities. If the purposes and/or functionalities of MyHealthAvatar or the Terms and Conditions and/or the Privacy Policy change, MyHealthAvatar will ask the user for fresh consent. This is also explained in clause 6 'Entitlement to Terms and Conditions of MyHealthAvatar', clause 16 'Modification to these Terms' of the extended Terms and Conditions (and clause 12 of the current version

[37] Ibid, p. 113.

[38] Ibid, p. 114.

respectively) and in clause 11 'Changes to Privacy Policy' of the extended Privacy Policy (and clause 9 of the current version respectively).

MyHealthAvatar also ensures that the user gives specific consent for the data transfer to other persons. During the project lifetime, MyHealthAvatar only allowed users to share non-sensitive data, such as data concerning food, drink and calories, events and activities with other users, so called 'friends'. This is explained in clause 3 'Sharing your personal data via MyHealthAvatar Platform' of the Privacy Policy. After the project's end it is envisaged that the user may be enabled to transfer sensitive health data to physicians, too. Therefore, clause 4 'Functionalities of MyHealthAvatar and Use of Content' of the extended version of the Terms and Conditions explains how the user can transfer a specific kind of data to his doctor. In order to increase the understanding of the user, a tutorial video should be produced to explain this functionality.

Furthermore, provision should also be made for the termination, or a material change in the nature or purpose, of the operations of the MHA platform. In such cases, they must be informed in detailed terms about the implications of such changes, including through their impact on the data processing, for them as individual data subjects.[39] Here, clause 21 'Data use for future research' of the extended Terms and Conditions (and clause 15 'End of Project' of the current version respectively) foresees that the MyHealthAvatar user will be contacted and asked for fresh consent in such a case.

For the exploitation stage after the project's end it is desirable to implement a button in the platform that can be clicked according to the user's wish to be contacted or not for related projects and/or future research. Other issues in respect of consent for data to be used for future research have previously been analysed in chapter 5.4 of D.11.1, p. 28 ff., 'Additional requirements in respect of secondary (research) data usage'.

3.3.6. Other relevant issues with regard to consent

3.3.6.1. Third Party Frameworks

During the MHA testing phase, third-party health information from Fitbit, Moves, Withings, and Twitter could be retrieved to MyHealthAvatar (cf. D11.3 'Understanding the Legal and IPR regime in MyHealthAvatar, section 3.4 'Collecting data by apps', p. 23 ff.). In this regard, clause 10 'Third party services' of the Terms and Conditions (and clause 9 of the current version respectively) alert the user to the fact that third parties are subject to their own third party privacy rules and that MyHealthAvatar may have limited or no control over the data processing practices of these third parties. This clause will also be crucial for the exploitation stage after the project's end, when the user may opt to transfer their data to further third party app developers, or to health care professionals and/or researchers.

[39] Ibid, p. 115.

3.3.6.2. Minors

To give a valid consent the MyHealthAvatar user must be mentally capable to take decisions.[40] Minors can give consent for the processing of their data if they are capable of insight and able to understand the implications of their decision. Currently, there is no general rule that assumes at what age this is the case. Instead, each specific case has to be examined. The ongoing debate (also at the level of European data protection policy[41]) whether minors can fully understand the implications of their consent has had impact on the GDPR. Article 8 (1) GDPR states that the processing of personal data of a child below the age of 16 years, or if provided for by member state law a lower age which shall not be below 13 years, shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child. This means an effort for children who want to collect all their health-related data in the 'personal bag'[42] that MHA offers, and also that they will not be in the position of being autonomous users (as their parents will be party to their membership of the platform). This may lead to higher risks of undue parental influence, including the possibility of parents pressurizing the child to share the data with them. For the exploitation stage, given the sensitivity of the data at issue, MyHealthAvatar has opted to take Article 8 (1) GDPR already in account. Therefore, clause 3 'Eligibility for Membership' of the Terms and Conditions requires that the user is at least 16 years old.

3.3.6.3. Relatives

Clause 7 'Restrictions on upload of data' of the Terms and Conditions determines that the MyHealthAvatar user must not upload or transfer data that have a strong and direct hereditary component to the avatar. The reason for this clause is that this kind of data could include information about a relative who does not want to share information about his disease. Relatives have the right to decide on their own if they want to reveal their diseases or not. Only if they have consented to the processing of these data, is the user allowed to upload them. The rights of the relatives are not only protected by the DPD (especially Article 8), but also by the rights to a private life according to Article 7 and the right to the protection of their personal data pursuant to Article 8 of the Charter of Fundamental Rights of the European Union[43]. In this regard, Clause 7 aims to enable MyHealthAvatar users to benefit from the platform as much as possible on the one hand, but also to respect the self-determination of other data subjects on the other. In the event of a breach, MyHealthAvatar will delete this data to protect the rights of the relatives.

[40] Pedroni, Pimple, 2001, 'A Brief Introduction to Informed Consent in Research with Human Subjects', p. 6 (available at https://ccts.osu.edu/sites/default/files/Subject%20Management%20and%20Site%20Activities_Informed%20Consent%20in%20Research%20%28Attachment%29.pdf).

[41] Jasmontaine, De Hert, 2015, 'The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet'.

[42] DoW, Part B, p. 4 of 55.

[43] See http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

3.4. Further requirements

3.4.1. The need for fair data processing

The operator of MyHealthAvatar must not only ensure a lawful data processing, but must meet the requirements for a fair data processing, too (please see D11.1 'The ethical and legal framework of MyHealthAvatar', section 4.3 'Need for fair processing, p. 18 ff.). The principles of fair data processing are stipulated in article 6 DPD and include the principles of data minimisation, purpose limitation and limited retention. These principles too have been given effect to by concrete stipulations contained in the MHA Terms and Conditions and Privacy Policy.

In the first place, during the testing phase of the platform, when features of overall usability are at the forefront of validation, users may evaluate through role-play, using profiles invented for this purpose, rather than their true profile (so avoiding the disclosure of sensitive information about themselves). Accordingly, clause 6 'Entitlement to Terms and Conditions of MyHealthAvatar' recommends that volunteers use fake data. Also clause 2 'Registration' of the Privacy Policy does so. In terms of the user's email address it is recommended using a real e-mail address because only then can the user be asked to grant fresh consent for the case that material aspects of the Terms and Conditions or Privacy Policy have changed. However, it remains the decision of the user if he wants to use his real email address or not. If the operator of MyHealthAvatar cannot contact the user for fresh consent, he must no longer process the data because there is no legal basis anymore.

Clause 6 of the Terms and Conditions and clause 2 of the Privacy Policy ensure that MyHealthAvatar meets the requirements of the principle of data minimization. According to this principle the data controller shall limit the processing of data that are adequate, relevant, and not excessive, Article 6 (1) (c) DPD. As noted, the purpose of the testing phase is to learn if users estimate the MyHealthAvatar platform as user-friendly and if they could imagine using such a platform. This can be also achieved by using fake data. For the exploitation stage after the project's end, the user should be allowed to use a pseudonym instead of his real name and surname (cf. clause 2 'Registration of the Privacy Policy).

Clause 15 'End of Project' of the current Terms and Conditions that is used during the project lifetime states that all uploaded data will be deleted by 31 May 2016. This is in compliance with the principle of limited retention of data pursuant to Article 6 (1) (e) DPD that requires that collected data must be erased as soon as it is no longer needed for the purposes for which it was collected. Moreover, clause 15 makes clear that MyHealthAvatar will not use the uploaded data for any other projects. In this way, MyHealthAvatar respects the principle of purpose limitation which is laid down in Article 6 (1) (b) DPD and means that once the data is collected for specified, explicit and legitimate purposes it must not be further processed in a way incompatible with the purposes at collection.

For the exploitation stage after the project's end it is difficult to draft a modification of this clause at this particular time. Therefore, clause 21 of the extended Terms and Conditions, which states that the user shall be approached in the future for fresh specific consent if and when distinct processing purposes should emerge in the course of exploitation, will be left as it is now.

3.4.2. Data security

As pointed out in Article 17 DPD the controller must implement appropriate technical and organisational measures 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. Similarly, the Council of Europe Recommendation on the Protection of Medical Data[44] of the Committee of Ministers to Member States, R(97)5, recommends the need for an appropriate level of security taking account of the technical state of the art and also of the sensitive nature of medical data and the evaluation of potential risks.[45] Furthermore, the opinion 03/2013 of the Article 29 Working Party states that the data controller has to adopt appropriate safeguards to ensure that the privacy interests of the data subject are protected so far as reasonably possible.[46]

These requirements are reflected in clause 4 'Security measures to protect your data' of the Privacy Policy, which acknowledges that users can upload highly sensitive data, and that state-of-the-art security measures are incorporated into the Platform to protect the user's data against risks of data misuse. In this regard MHA aims to utilize the latest architecture technology on cloud ensuring high information security.[47] At the same time, the manner in which this is achieved will differ (also reflecting the nature of the data to be protected) during the exploitation phase, when compared to the arrangements in place during the lifetime of the project.

As regards the project's lifetime, the user's data are stored in the public cloud server Linode, based in London and rented by ANS. This is also explained in clause 4 of the current Privacy Policy. For the exploitation stage after the project's end, if real sensitive health data will be uploaded by users, the level of security is higher as it was during the project's lifetime where only real lifestyle data have been uploaded. Presently, clause 4 of the Privacy Policy points out that only the institutions participating in the MyHealthAvatar project are able to access the uploaded data. After the project's end this section needs to be revised according to the identity of the platform operator.

During the exploitation stage after the project's end the MyHealthAvatar user will be able to upload and transfer sensitive health data. Then, a private cloud infrastructure will be indicated because only then can the controller fully control the data processing (cf. D11.1 'The ethical and legal framework of MyHealthAvatar, section 3.2 'Cloud Infrastructure', p. 10 f. and section 4.4.3 'Security of data processing, including in the cloud context', 22 ff.). At this stage the user will be able to manage his access rights, to decide who should have access to the data and to follow who has seen his data at what time for what reason.

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

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

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

[47] D3.1, p. 6.

3.4.3. Ensuring User Identity

Finally, there is the need for ensuring that the person who purports to be the user is indeed the user in reality. This is important for ensuring that an unauthorised person does not access the sensitive health data of a MyHealthAvatar user in order to see or transfer them, to adulterate data or to upload incorrect data. In order to avoid these scenarios, a secure user ID is crucial. However, some users might not want to include their real ID in their profile to sign up.

To verify the correct identity of the user, the Article 29 Working Party states that relying on authentication instead of full identification, should be sufficient in most scenarios.[48] An appropriate approach for the exploitation stage after the project's end would be to provide credentials checks to ensure that the user logging in is the person who created the account. This could include security questions and extra keywords that could be sent to the user's mobile phone. Another possibility is to check the IP and location from where the user is trying to log in.

3.4.4. Linking with Hospital information systems (HIS)

One of the objectives and challenges of MyHealthAvatar is to allow storage of medical data. In order to do that the platform must allow the users to enter such data into the system. In such a case there is the limitation of use of these data since they might be incorrect, not up to date or even incomplete and incomplete. Under such circumstances it is difficult to trust the data and make meaningful use of them for clinical analysis, prediction, prevention – offered services and purposes of MyHealthAvatar.[49] The risk of inaccurate data is especially high when a patient goes to his doctor or hospital and requests access to his data according to his rights under data protection law and/or other law and receives the data in a non-digital format. When entering such data into MyHealthAvatar the user could contaminate or corrupt the data inadvertently. Moreover, the risk to data security is increased when the user who has usually less technical expertise than technicians, stores the data on his own computer before entering them to MyHealthAvatar. And finally, going to the physician/hospital and asking for a copy of his data means also more effort for the user. This is especially true for the case when the user is receiving treatment for a current condition and the data is regularly updated. To overcome these challenges, MHA has looked at ways to achieve direct linkage with external health and health related data sources such as clinical information system, clinical trial management systems, activity tracking systems and links with social networks.[50]

This section will examine what has been done in the project's life time and how the exploitation stage can benefit from these findings. In WP3 research was conducted to find a means of linking MHA with hospital information systems (HIS) in order to bypass the above-mentioned challenges. In particular, FORTH has developed a direct link with an HIS to demonstrate a seamless, secure and consistent data sharing between MyHealthAvatar and

[48] Opinion 02/2013, p. 25.

[49] DOW, part B, p. 2 of 55.

[50] D3.2 v2.0 'Architecture design v2.0', chapter 5.1 'Link with hospital information Systems', p. 42 ff.

an HIS.[51] For the connection to function, proper mechanisms and a proper infrastructure were needed.[52]

Although during the project's lifetime only chimeric data have been linked, security is crucial in the field of HIS (and other external data warehouses) because MyHealthAvatar is a feasibility study[53] and needs to take into account that in the future time sensitive health data could be processed and the users need to be protected against the consequences a security breach can have. Moreover, unless the hospital from which the data are to be transferred is assured of the strength of the MHA security framework, it would almost certainly refuse to make the transfer (rather than risk breaching confidentiality duties and local data governance policies by doing so). FORTH was aware of this risk and analysed available standard interfaces before building the link between the HIS and MHA. The standard interfaces include the Clinical Document Architecture (CDA)[54] guidelines and set of specifications, the Operational Data Model (ODM) of the Clinical Data Interchange Standards Consortium (CDISC)[55], and the epSOS[56] Patient Summary interfaces.[57] Moreover, Digital Imaging and Communications in Medicine (DICOM)[58] and the "transactions" defined by the Integrating the Healthcare Enterprise (IHE)[59] initiative have been investigated for this work, too.[60]

FORTH decided to build the link between MHA and the HIS based on the epSOS guidelines and proposed architecture.[61] The EU-FP7 epSOS project[62] analysed how patient summaries (that include the most relevant clinical data to ensure safe and secure healthcare in an accident or emergency[63]) can be retrieved by the epSOS gateway from the National Contact Points (NCP).[64] The NCP acts as a technical, organisational and legal interface between the

[51] DOW, Workplan Tables, p. 9 of 40; cf. D3.2 v2.0 "Architecture design v2.0", chapter 5.1 "Link with hospital information Systems", p. 40; for further details see Haris Kondylakis, Emmanouil G. Spanakis, Stelios G. Sfakianakis, Vagenlis Sakkalis, Manolis N. Tsiknakis, Kostas Marias, Xia Zhao, Hong Qing Yu, Feng Dong. 2015. Digital Patient: Personalized and Translational Data Management through the MyHealthAvatar EU Project. International Conference of the IEEE Engineering in Medicine and Biology Society of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy.

[52] D3.2 v2.0, p. 40.

[53] DoW, part B, p. 5 of 55.

[54] See http://www.hl7.org/Special/committees/structure/index.cfm.

[55] See http://www.cdisc.org/.

[56] European Patients Smart Open Services (epSOS), see http://www.epsos.eu.

[57] D3.2 v2.0, p. 40.

[58] See http://dicom.nema.org/.

[59] See http://www.ihe.net/.

[60] D3.2 v2.0, p. 40.

[61] D3.2 v2.0, p. 41.

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

[63] See http://www.epsos.eu/epsos-services/patient-summary.html.

[64] D3.2 v2.0, p. 41.

existing different national functions and infrastructures.[65] Each participating nation of the project is represented by such a NCP.[66]

MHA benefits from these research results by transferring this idea to the MHA epSOS gateway. The MHA epSOS gateway operates both in the clinical field and the MHA platform and uses the epSOS Patient Summary documents to feed the central data repository of the platform and to filter and retain relevant patient data.[67] Due to this work there is great potential to use HIS in the exploitation stage after the project's end. This is especially so, given the size of the epSOS research project with many participating countries and industries that offer epSOS piloting services.

While the epSOS approach was a great opportunity to demonstrate a possible means for linking between HIS and MHA, for the exploitation stage it is intended that MHA should go beyond it by also fostering data collection by local hospitals that do not participate in the epSOS system. For this purpose, LUH has drafted a patient data transfer request to hospital[68] that a MHA user can use for mandating the data transfer to MHA and a data transfer agreement between hospital and MHA[69].

First, since hospitals might not be willing to share data with MHA because of patient confidentiality concerns and data governance policies, the patient data transfer request includes a waiver requiring that the patient agrees to release the hospital from potential liability for privacy-based harm. This will protect the hospital, provided it did not act negligently (e.g. by failing to check the adequacy of the MHA security framework).[70] For its part, the data transfer agreement sets out the rights and duties of the hospital and of MHA. The hospital must ensure the proper management of medical confidentiality and data protection risks stemming from the data transfer. MHA has to guarantee that it safeguards the shared data and meets the ethical and legal requirements for data processing.[71] Moreover, MHA must make sure that its employees who will have access to the data respect the data transfer agreement and that the user's data will be processed for future research purposes only if the user has consented to it. In addition, MHA acknowledges that the involvement of the relevant data protection supervisory authorities can be necessary.[72]

However, there remain two issues. First, the hospital must be able to check that the MHA user requesting transfer of HIS data to MHA really is the relevant hospital patient. Here, MHA would have to offer the same verification standards as required by hospitals when they release health records pursuant to direct patient access requests, in particular security

[65] See description at http://www.epsos.eu/legal-background/the-national-contact-point-and-framework-agreement.html.

[66] Ibid.

[67] D3.2 v2.0, p. 42.

[68] See Annex 4 of D11.3, p. 74.

[69] See Annex 5 of D11.3, p. 75 ff.

[70] Cf. D11.3, chapter 3.3.1.1 'Patient request and waiver', p. 20 f. for further information.

[71] Cf. D11.3, chapter 3.3.1.2.1 'Obligations on hospital' and 3.3.1.2.1 'Obligations on MHA', p. 21 f. for further information.

[72] D11.3, p. 22.

questions and extra keywords that are sent to the MHA user's mobile phone.[73] Second, there are interoperability issues with HIS.[74] This is especially true for imaging data. Here MHA would have to need to ensure that the data that are shared by the HIS must be structured in a format that can be used by MHA. These two issues will require to be resolved in due course in the light of experience gained with the day-to-day exploitation of the platform.

3.4.5. Data protection implications of Third Party apps including the risk of totalitarian-style monitoring

One of the most promising features for the future of the MHA platform is that Third Parties will be able to access it via an Application Processing Interface (API). This will permit Third Parties to extend the platform's functionalities via apps that can run on any type of device, be it mobile phones, personal computers, web servers, or medical devices, beyond those originally foreseen and introduced by the MyHealthAvatar consortium. However, the flip side of granting Third Parties access to the platform is that the platform will automatically relinquish, to a certain extent, control over the personal data entrusted to it by its users. Third Party apps will typically need access to data in order to provide their services and functionalities, and once Third Parties have access to the data, they can theoretically do with it as they please. [75]

As against this, and as previously noted, MyHealthAvatar will need to preserve respect and protect the trust its users have placed in it. The threat to user's privacy is real: the Article 29 Working Party has noted that there is a trend among app developers, both advertently and inadvertently, towards data maximization, and that technical security is frequently neglected during the development process.[76] Accordingly, this section will seek to examine the measures that MyHealthAvatar should adopt in the exploitation phase to safeguard its users against possible threats to their data by Third Party apps. Both technology (access control, technical security, etc.) and law (robust privacy agreements) can serve to protect a user's privacy and data.

The issue identified here is not a new one. Online Social Networks (OSNs) such as Facebook, Twitter or Google+ face and have addressed the same fundamental problems that MyHealthAvatar will need to tackle. An examination of the current privacy issues with OSNs can both guide practices that should be adopted by the MyHealthAvatar platform as well as illuminate areas for improvement. While OSNs generally implement access control, so that their users first have to authorise the access requests of Third Party apps, they frequently have an all-or-nothing strategy with the consequence that the user can either only grant a Third Party app access to all personal data stored on the OSN, even if not all data is relevant

[73] Ibid, p. 20.

[74] DOW, Workplan Tables, p. 9 of 40.

[75] Yuan Cheng, Jaehong Park, and Ravi Sandhu. 2013. Preserving user privacy from third-party applications in online social networks. In *Proceedings of the 22nd International Conference on World Wide Web* (WWW '13 Companion). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 723-728, 724.

[76] Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices, pp 5 et seq.

for the service offered by the Third Party app, or to no data at all.[77] One 2008 study showed that over 90% of the top 150 Facebook apps had access to more data than necessary, a clear violation of the data minimization principle.[78] Additionally, OSNs typically do not differentiate between the actions a Third Party app can perform on the data it is granted access to.[79] Moreover, even if the privacy settings/access levels of some Third Party apps can be adjusted on the OSN, this is only after having granted the app access and not already during the initial authentication stage.[80]

In terms of appropriate countermeasures, MyHealthAvatar must follow established best practices of OSNs and permit Third Party apps to access the platform only after user granted authentication (as detailed in Deliverable D3.3). In addition, MyHealthAvatar should allow the user to grant selective access to data already during the authentication process. This would already follow from the platform's "granular" approach to granting consent. The user should also be able to see clearly during authentication process what data the Third Party app is requesting access to, and what type of access is sought (read-only, write, execute, etc.). The user should be required to re-grant authentication in regular intervals, e.g. every six months. Doing so will remind the user that a Third Party app has access to her data and force her to evaluate whether the access should continue to be granted. Authentication should be re-sought whenever an app seeks new access rights.

Beyond such technical measures, however, there are also legal and organisational steps that can be adopted in order to minimize risks to the privacy of MyHealthAvatar users. Organizationally, the MyHealthAvatar platform should only grant access to its APIs after having reviewed the requesting Third Party app's technical and legal privacy approaches. This will allow the administrator of the platform to filter out any apps that do not measure up to the high MyHealthAvatar standards. Moreover, this review should not be a singular event, but should be conducted in regular intervals and particularly when the app requests new access rights. In this respect the platform's monitoring duties should mirror the user's duties of regularly assessing whether the access she granted in the past is still in her interests.

Legally, the Third Party and MyHealthAvatar should enter into an agreement regulating the use of the MyHealthAvatar API. An example of such an agreement is given in Annex 6 of this deliverable. In addition, the authentication process of Third Party apps should also include the review and acceptance of the Third Party's privacy policy. The privacy policy should adhere to minimum standards set forth in the MyHealthAvatar API agreement. It must be re-iterated that Third Parties can use data collected by their apps – as long as the use is both legally and ethically sound, which is the purpose of both the technical and legal organisational measures introduced above. However, we must also remain conscious of the

[77] Cheng, Park, Sandhu, p. 724.

[78] Cheng, Park, Sandhu, p. 725.

[79] Cheng, Park, Sandhu, p. 724.

[80] Na Wang, Heng Xu, Jens Grossklags. 2011. Third-party apps on Facebook: privacy and the illusion of control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology* (CHIMIT '11). ACM, New York, NY, USA, Article 4, 10 pages. DOI=http://dx.doi.org/10.1145/2076444.2076448

dangers that can arise from tools like the MyHealthAvatar platform and Third Party apps – even when used in full accordance with the law.

In this context, a worrying development is that the use of wearables is being encouraged by employers, insurance companies and other organisations in exchange for alleged benefits such as lower insurance premiums or other financial incentives.[81] A lifetime companion such as MyHealthAvatar will gather an immense amount of personal data of all categories. Beyond the obvious kinds, such as health and lifestyle data, it will also collect location data through GPS-enabled devices, the relationships between individuals, habits of individuals, and any other type of data that an app might request and that the user gives authorisation to. Knowledge is power, so the aphorism, and platforms such as MyHealthAvatar will be an immeasurable font of knowledge about an individual – but hence also a potential mechanism for totalitarian control.

Although, as noted, for now use of apps may be encouraged by incentives (such as discounted insurance premiums), there might in the future be a trend towards using punitive measures instead of positive rewards, such adding surcharges for non-compliant behaviour instead of offering rewards for compliant behaviour.[82] While the classification of an incentive as a punishment or a reward depends on how the incentive is framed within the overall situation, there does seem to be an instinctive aversion to being pressured instead of encouraged into behaviours. As Pam Dixon, executive of the World Privacy Forum has stated: "It's going to be very important that as we move towards the future we don't set up a system where people become pressured into wearing devices to monitor their health. That's a real problem. That's just not very free."[83]

Already, there is legislation in place to prevent discrimination and to address the problem of profiling individuals. The United States, for example, adopted the Genetic Information Nondiscrimination Act (GINA) of 2008.[84] This Federal law prohibits health insurers and employers from taking discriminatory decisions based on genetic information. As regards the position in Europe, Article 21 of the Charter of Fundamental Rights of the European Union[85] prohibits discrimination on grounds of, inter alia, genetic features. In terms of EU secondary legislation, the GDPR, when it replaces the DPD, will expressly restrict what it calls profiling. Article 4 (3aa) GDPR defines the term as

> *"any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"*.

---

[81] Forbes, Wearable Tech Is Plugging Into Health Insurance, June 19, 2014, http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/.

[82] Ibid.

[83] Ibid.

[84] Pub.L. 110–233, 122 Stat. 881, enacted May 21, 2008, GINA. Accessible at: https://www.gpo.gov/fdsys/pkg/STATUTE-122/pdf/STATUTE-122-Pg881.pdf.

[85] Charter of Fundamental Rights of the European Union, 2012/C 326/02.

Profiling is not to be equated with the mere tracking of an individual, for example on the internet or in stores. It requires an additional "predictive" or "decision-making" quality – there must be consequences arising out of the profiling. This understanding is supported by the Recitals and other Articles, which frequently refer to the "consequences" of the profiling.[86]

The restrictions the GDPR places upon profiling are embodied in a number of rights granted to data subjects, such as "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her",[87] subject to the exceptions of being necessary for a contract between the data controller and the data subject, being authorized by Union or Member State law and subject to safeguards, and being based on explicit consent.[88]

Of particular importance for MyHealthAvatar is that profiling based on health data and other special categories require either explicit consent for specified purposes or a substantial public interest on the basis of Union or Member State law, and always subject to safeguards for the data subject's rights and freedoms and interests.[89] In addition, as previously discussed in section 3 above, the API license agreement will obligate third party app developers to respect the general fair data processing principles, listed in the DPD and to be continued in the GDPR. This will preclude surreptitious, non-transparent data processing practices of the kind implicit in profiling. A further safeguard is that the GDPR will likely require regular data impact assessments as part of MHA platform exploitation, as special categories of data such as health data will be processed on a large scale, one of the automatic triggers of an assessment.[90] This will offer a mechanism for reviewing specific profiling risks as and when these arise.

[86] Eg Recitals 48, 51, 58, 71 GDPR, Articles 14, 14a, 15 GDPR.

[87] Article 20 (1) GDPR.

[88] Article 20 (1a) GDPR.

[89] Article 20 (III) GDPR.

[90] Article 33 (2) (b) GDPR.

4. Liability risks of the platform

In D11.3, p. 32 ff. '3.6 Liability for the correctness of the data' the issue of liability with respect to third party apps and MHA tools have been introduced. In this context, it has been pointed out that the Medical Devices Directive 93/42/EEC[91] and the product liability regime could have some impact on digital avatars. The following section will use this analysis as a starting point and will go into details whenever this is crucial for the exploitation stage after the project's end.

4.1. Liability of apps

There are various risks of liability that need to be considered when exploiting the MHA platform. Apart from liability for breach of data protection law and/or rules of privacy and confidentiality in respect of unlawful processing (as previously discussed), the key risk is that of ex post facto liability to users for personal injury caused to them as a result of using the platform. The main forms such injury could take are looked at below, and typically may lead to a claim by the user against the platform for redress (in terms of monetary compensation) under rules of contract and/or tort law, or possibly under statutory rules on product liability. In addition, there may be a risk of platform liability to regulatory bodies if there are failures to comply with ex ante rules designed to protect users: in particular such liability may arise if aspects of the platform (and/or some of the apps running via it) fall within rules that govern medical devices and the preconditions for placing these on the market.

At the outset it must be recognized that the above rules are complex to apply in the domain of e-Health, due to the speed and novelty of e-Health developments, and the diverse ways in which its applications work in practice. In this regard it will often be uncertain how legal rules developed to cover traditional health care interactions should be applied in the new context; this problem is added to by the relative lack so far of authoritative court decisions in point. In particular, two related features of the world of e-Health, and platforms such as MHA, may be mentioned that pose difficulties. The first is that of identifying the location of the harmful event. Traditionally, health care interactions took place between clearly defined actors in a specific geographical locus; it was then normally also clear which courts would be responsible for adjudicating liability disputes, and what law they would apply, where things went wrong, i.e. of the country where the interaction occurred.

This assumption does not hold for e-Health, where users seek advice and/or other health care from health care providers via a remotely located platform. Here several jurisdictions (where these differ in the given case) may come into question as the appropriate forum for hearing the dispute: that of the user, that of the provider, or that of the platform through which they interacted. A further challenge is that, even within the EU, the private law liability rules (determining the circumstances in which compensation will be awarded) differ between each member state, making the result of a claim very hard to predict.

The second point is that e-Health, with its electronically mediated interactions between remote actors, may involve a great multiplicity of different parties who all contribute in

[91] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31993L0042.

some way to the success or failure of the user/patient outcome. This means, even assuming every party was governed by the law of the same country, that complicated issues of attributing responsibility for a given harmful result must be navigated. The respective roles of each party in the chain of circumstances that resulted in the harm must be assessed, so to apportion their share of liability to the injured user in a fair and appropriate manner. In the e-Health world of software algorithms making decisions on the basis of inputted data, it will often be no easy task to untangle the various elements at play in a faulty output. Moreover, for platforms such as MHA, which are designed to support and/or interact with a multiplicity of third party apps, scenarios may arise where the platform's responsibilities are hard to demarcate from those of the app developers.

In the following analysis we shall first consider the key kinds of harm and injury that users may be at risk of suffering through platform use. At this point, the focus will be on the abstract nature of the harm and the legal elements that the user would need to establish in to succeed in a private law compensation claim against the platform. As noted, the private law rules that govern when compensation is payable for personal injury remain subject to member state law (rather than harmonized EU-level law), and differ sometimes significantly between each of the 28 member states. However, a common feature of most systems is the need for the user to prove faulty conduct on the part of the defendant operator; for the purpose of this deliverable, we will refer to relevant rules in illustrative jurisdictions, principally the UK (from where the MHA project is being co-ordinated), and Germany, whose codified approach has been influential in Europe and beyond.

Subsequently, we shall turn to consider the potential application to the platform of principles of Product Liability, which in contrast to the fragmented member state private law rules, derive from European-level legislation (namely, Directive 85/374/EC) and may allow awards of compensation based on objective defects in a given product, even without fault on the manufacturer's part. We then conclude the section by looking at further regulatory implications arising from the potential for the platform, and/or apps accessed via the platform, to fall within the ambit of EU-level rules applicable to the testing and marketing of medical devices. Unlike the compensatory regimes considered, these rules operate primarily 'ex ante' by imposing regulatory requirements – notably adherence to prescribed testing and certification procedures – before making devices available to users. Here platform non-compliance may give rise to administrative sanctions or even risk criminal liability.

4.2. Possible Forms of User Injury through Platform Use and their Compensability

As discussed in Deliverable D11.3, there are various risks of harm that e-Health systems such as the MHA platform create in the context of their use. This is so even when the platform and the apps running via it do not interact physically with the user – i.e. the impacts they have are instead virtual, with the mechanism for harm stemming from the faulty provision of information. The harm in question may take different forms and occur in a variety of ways, depending on factors such as how the information was faulty, how it was conveyed (directly to the citizen user or to another party such as a health professional?), and how it was acted upon. We look first at how a citizen user could suffer personal bodily injury as a

result of false information given by the platform, before considering other harm, in particular mental distress that may be caused in some cases by the faulty delivery of accurate information.

4.2.1. Liability for physical bodily injury

In the first place, the information fed back to a given user may wrongly identify a medical problem (which he in fact does not suffer from) and this leads him to undergo unnecessary medical intervention that causes injury. In this case, it is apparent that the information provided by the platform is the first step in a chain of further events, which will include the user's decision to seek further diagnosis or treatment, and the actual provision of such diagnosis / treatment (typically by a third party health professional). This would thus be one of the situations referred to above as often arising in e-Health scenarios, in which the actions of multiple parties together contribute to harm. However, a converse possibility is of harm by omission, where the platform fails to identify a given medical problem, which the user in fact has. This may lead the user to allege physical injury from the progress of the condition, which – so the claim - he would otherwise have avoided through timely diagnosis and treatment. A related category comprises cases where information was actually fed back by the platform, but was falsely reassuring, and which discouraged the user from obtaining a proper diagnosis and treatment. In this case (in contrast to the first scenario above) the series of events leading to injury may be attributed to platform failure alone.

In each case, the private law liability rules operating in European member states are in principle highly protective of citizens' physical interests (i.e. their interest in not suffering bodily injury). This will be so whether the user seeks redress in the law of contract (on the basis that the platform's performance was contrary to what was contractually promised by the operator) or under the law of tort/delict, which imposes general obligations (independent of any contract) on persons not to act in ways that may foreseeably injure others. Admittedly, insofar as no contract was found between the parties, there might be an issue – in the case of the platform failing to supply a relevant piece of diagnostic information - whether it should be subject in tort law to an affirmative duty to do so. However, against the background that the platform habitually provided other information to the user, it would almost certainly be found to have assumed such responsibility.

To actually succeed in their claim though, and obtain damages, the injured user would in nearly all jurisdictions need to prove two further key legal elements. The first is that the defendant platform operator behaved in a faulty way; and the second is that the physical injury to the user resulted from this faulty behaviour. The enquiry into fault involves satisfying the court that, in the circumstances, the defendant acted unreasonably by taking a risk of injuring another that an ordinary, careful person in a similar situation would not have taken. The second enquiry, which lawyers term 'causation', involves the claimant showing that this faulty conduct was a sine qua non cause of the injury (i.e. it would not

occurred if the defendant had acted with proper care) [92] and also the injury is not so unforeseeably 'remote' from the conduct to make it unfair to hold the defendant liable.[93]

Applied to the two main scenarios outlined above, in both cases a finding of fault may be made against the platform if it is shown that the operator – measured against a notional reasonable operator - should have been aware of the platform's propensity to give inaccurate information and/or, being so aware, failed to take adequate precautions to limit the impact of such information, such as by providing a clear warning to users not to rely on the uncorroborated information. However, as regards the causation element, the scenarios diverge and raise different problems. Thus, as regards the first scenario, as was noted above, the user's injury (from unnecessary medical intervention) would not have occurred unless – besides the provision of the faulty information – the user and an independent health professional had not also acted on it.

This opens up the possibility of attributing the injury to the faulty actions of other actors besides the platform (i.e. those of the user and health professional) if their subsequent conduct in relying on the information is found to be unreasonable. At the least this may lead to a reduction in the platform's share of liability (as discussed under point 4.2.3, it would generally only pay a portion of the damages rather than the whole amount); however, it is also possible that a court might find that the conduct of the user and/or health professional totally eclipsed the platform's role in the events leading to injury. If so, the platform would be relieved of liability, due to lack of adequate causation – i.e. the ultimate injury to the user would count as too remote.

Turning to cases where the user points to the failure of the platform to provide timely, accurate information alerting him to a medical problem that accordingly goes untreated, there may also be the possibility of arguing that some of the responsibility for the resulting harm should be borne by the user (via a finding of contributory negligence, leading to a corresponding reduction in platform liability). However, this argument may well be seen as unattractive (and be rejected by a court), particularly if the platform is held to have insufficiently advised users not to rely upon its diagnostic functions. Nevertheless, a real challenge for users in such a case may be of proving the sine qua non causation element: this would generally require the court to be satisfied that, had the correct information been provided to the user when it should have been, the latter would have sought further advice and treatment from a health professional, which in turn would have prevented the condition from progressing in the way that it did. As is evident, this argument contains several counterfactual assertions, and may be difficult to sustain to the level of proof required by the law. If so, the result would again be that the platform would be relieved from liability.

---

[92] Cork v. Kirby MacLan Ltd (1952) 2 All ER 402 (CA); Oetker, in: Säcker, Rixecker, Oetker, Limperg (eds.), Münchener Kommentar zum BGB, 7th edt. 2016. section 249 margin note 103.

[93] McKew v. Holland & Hannen & Cubitts (Scotland) Ltd (1969) 3 All ER 1621 (HL); In German case law it is asked whether the claimant/third party were challenged to a specific reaction by the breach of duty by the defendant which is assumed when the reaction of the claimant/third party was adequate and reasonable ('Herausforderungsfälle') (Oetker, margin note 141- 197).

4.2.2. Liability for mental distress

We next consider cases where the user suffers mental distress that results from the platform's communication of information. Here, as in the case of physical injury above, there are various scenarios that could arise. First, the information may, as in the first case looked at under 4.2.1, take the form of an inaccurate, positive diagnosis that the claimant user suffers from a given condition, and which leads to shock and distress (possibly including sequelae of a physical character, such as the user suffering heart failure or making a suicide attempt). Secondly, there is also the potential for information that is in itself accurate to produce especially distressing effects if it is communicated or presented to the user in an inappropriate way, e.g. without sufficient preparation or counselling options. As noted in deliverable D11.3, chapter 3.6 'Liability for the correctness of the data', pp. 32 ff., this may pose particular risks in the context of information imparted by or via the platform in a home environment (without immediate user access to professional advice or support).

At an ethical level the infliction by the platform of harm of the above kind on its users would breach the principle of non-maleficence, and likely lead to a swift loss of user trust and goodwill. Accordingly, the platform should be designed and configured so as to minimise this as much as possible. In terms of gaining legal redress, the user would, just as with a claim for physical injury, need to show the elements of faulty conduct (on the platform's part) plus causation. The way these matters, which here raise some distinctive challenges, are likely to be approached by domestic European courts, is considered below. However, first there is a more general added hurdle faced by claimants that should be mentioned. This is that the law in several countries has adopted a prima facie negative approach to mental distress / psychiatric harm as a type of claimable injury, reflecting a distrust of injury not discernible to the naked eye, and possibly susceptible to simulation. The default position in those jurisdictions is not to award compensation for such injury (unaccompanied by physical harm) unless special further legal conditions are met.

In the UK, for example, a claimant traditionally would have to show that their mental distress amounted to a recognized psychiatric illness, and was brought on by direct perception of a shocking event that would have caused similar injury to a person of 'reasonable phlegm and fortitude'. In Germany, too, the tendency has been to limit the scope of the claimant's protected legal interests (for which they may sue for damages) to severe cases of psychiatric illness, whose causation was understandable in the circumstances and that involve a particularly high degree of emotional suffering. Thus in cases arising from the death or injury of the claimant's loved ones in negligently caused accidents, their suffering must go beyond the usual level of grief in such situations, but still be understandable. On top of this the obligation to pay compensation is confined to close relatives.[94] By contrast, other jurisdictions, including France have taken a more liberal and claimant-friendly approach, which in principle allows compensation for mental distress to be claimed on the same footing as for physical bodily injury.

[94] Heß and Burman (eds.), Handbuch des Straßenverkehrsrechts, 2015, Section F. margin note 19; Oetker, as in note 70 above , margin note 149-156 with references to the settled case law.

Be that as it may, to date there are only a limited number of court decisions, across European member state jurisdictions, that specifically centre on the communication to the claimant of adverse health information. Instead, the bulk of reported cases have involved claims from claimants caught up in shocking accidents, which have caused them to fear physical injury to themselves, or witness actual physical injury to their loved ones. One relevant UK case, though, concerned an action brought by a group of claimants, who, as a result of industrial exposure to asbestos, had developed pleural plaques in their lungs.[95] The plaques, though visible on x-rays, did not produce any physical symptoms; however, their presence was associated with a heightened risk of developing lung cancer. The question was whether the claimants could recover damages for anxiety, brought on by the awareness of this risk. In denying this, the UK House of Lords held that anxiety alone was not compensable.

By contrast, the UK courts have awarded damages for the post-traumatic stress syndrome suffered by claimants wrongly informed by hospitals that their new-born babies were dead.[96] Similarly, in Germany a man was successful with a claim against his physician who wrongly informed him that he was suffering from cancer. The court accepted that the diagnosis of cancer had brought fears of death and loss on side of the claimant which had induced an infringement of the claimant's health.[97] Another German court awarded compensation to a claimant, who was falsely told that a malignant tumour needed to be removed from her leg and underwent painful surgery several times; in fact it was a benign tumour. In fixing the amount of compensation, the court noted the need to reflect, besides the claimant's bodily injury, the fact the defendants had let her remain with the belief of a cancer diagnosis for 20 years in an attempt to stave off litigation.[98]

Assuming that the claimant's mental distress injury is recognized as a suitable subject for compensation in principle, then as noted he must go on to prove his specific injury resulted from the platform behaving faultily in the given circumstances. As discussed above in the context of claims for physical injury, the court will look here at how the defendant behaved (in response to the risk of injury to others) compared to how it believes an ordinary, prudent person in the same position should have behaved. However, particularly in relation to the dissemination of true but distressing information, it may be difficult to find a uniform accepted standard of what amounts to reasonably careful communication. This point arose in another UK decision, in which a number of claimants sued for distress after they received a letter from a hospital, where they had recently been treated, informing them that they may have been exposed to the HIV virus during treatment.[99] One of the questions was whether it was faulty for the hospital to communicate this fact by letter, rather than to arrange for face-to-face counselling to occur; this was denied by the court.

[95] Grieves v F T Everard & Sons (the pleural plaques test case) [2007] UKHL 39.

[96] Allin v City & Hackney HA (1996) 7 Med LR 167.

[97] OLG Bamberg, 24.03.2003, 4 U 172/02.

[98] OLG Karlsruhe, 09.12.1987, 7 U 62/85.

[99] AB v Tameside and Glossop HA [1996] EWCA Civ 938.

4.2.3. Conclusions on private law liability risks

As appears from the above discussion, it will not be a straightforward matter for a claimant who brings an action for injury allegedly resulting from platform use, to successfully obtain compensation. Accordingly, the risk for the platform of having a finding of liability made against it may be regarded as relatively low. Nonetheless, aside from the need in ethical terms for the platform to be designed and operated so as to minimize risks of harm to users, there are other adverse effects for the platform in simply being a putative defendant to litigation, whatever the outcome. Most evidently, this may be expensive in terms of the resources (in costs and time) that will have to be deployed in defending the claim, particularly if this is in a complex multi-jurisdictional landscape (as mooted earlier). Moreover, the negative publicity generated by user claims, and indeed informal complaints, may have a serious impact upon overall user trust and goodwill. For these reasons, it will be important to have mitigation strategies in place to pre-empt 'harm' (in a broad sense) that users may experience through their platform use, including also where this is the upshot of unrealistic user expectations.

4.3. Product Liability Issues

4.3.1. The European Product Liability Regime

The European regime on product liability which has been implemented by the EU Directive on Liability for Defective Products in 1985[100] (Product Liability Directive) grants a special avenue of redress to consumers regarding damage arising out of the use of a defective product (as an alternative to the other private law liability regimes in contract and tort law). The aim of the Product Liability Directive is to balance the interests of the consumers and the producers (manufacturers) through establishing liability for producers of defective products regardless of fault / negligence on the part of the producer or the existence of a contract. The rationale behind the enactment is that it was regarded as unfair for the injured person to be without a legal remedy, even if the producers could not be blamed for the damage caused. This is because producers are able to get insurance against the damage that a defective product might cause and spread these additional costs by raising the market price of the product.[101]

The Directive establishes a system of strict liability. In order to claim compensation, the injured party must prove that the product is defective, that the type of damage is covered by the Directive and that a causal link exists between the defect and the damage suffered. It is therefore not necessary for the consumer to be in a contractual relationship with the producer, and nor for him to show that there was negligence on the part of the latter. The Directive does, however, not affect any rights an injured person may have according to the

[100] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products; see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31985L0374.

[101] Alheit, The applicability of the EU Product Liability Directive to software, The Comparative and International Law Journal 2001, vol. 34, no. 2, pp. 193-194.

rules of the law of contractual or non-contractual liability.[102] As a directive (and just as for the Data Protection Directive looked at earlier), it was then necessary for each EU member state to enact domestic law to bring the relevant rules into effect. In the United Kingdom this was done by the Consumer Protection Act 1987; in Germany the law on product liability (*Produkthaftungsgesetz*) was enacted in 1989 to implement the Directive.

4.3.2. Software as a product?

With regard to e-health services and products it must be determined first whether the product liability regime applies in principle. For tangible medical devices, such as monitoring devices, the applicability of the product liability regime is straightforward, but for intangible goods such as software it has been intensively debated in the scientific literature whether these fall within the scope of application of the Directive. Decisions by courts on this question are almost not existent (also because software producers do not want the establishment of case law in the matter).[103] And while the European Commission has declared that the Directive also applies to software,[104] there remains significant disagreement between EU authorities and member states, including the UK, on this point.[105] The academic literature for its part is heavily debating three issues relevant to the qualification of software as a product, which we look below at in turn. These are that:

- The Directive in its own definition for product does not seem to cover intangible products except for electricity;
- The Directive does not apply to services and it is unclear under which circumstances software qualifies as a product or service. This is especially relevant in the case of custom-fitted software and for software as a service applications available on the internet;
- Software is essentially information and the courts in analogous cases have refrained from applying strict liability against providers of false information.

(1) Intangible character of software

Software consists of information in the form of the particularly arrangement of source code and its transfer via the internet is steadily increasing. It possesses an intangible character. The Product Liability Directive in its definition of product states that:

> *"For the purpose of this Directive 'product' means all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable. 'Primary agricultural products' means the products of the soil, of stock-farming and of fisheries, excluding products which have undergone initial processing. 'Product' includes electricity"*.

[102] Art. 13 Product Liability Directive.

[103] Auer-Reinsdorff and Conrad (eds.), Beck'sches Mandatshandbuch IT-Recht, 2011, p. 192; Marly, Praxishandbuch Softwarerecht – Rechtsschutz und Vertragsgestaltung, 6th edt. 2014, p. 788.

[104] Rowland, Kohl, Charlesworth Information Technology Law, 4th edt. 2012, p. 479.

[105] Lloyd, Information Technology Law, 5th edt. 2008, p. 561.

As the Directive explicitly mentions electricity only in its definition of a product, it could be argued that other intangible things are excluded from the strict liability regime.[106] On the other hand, such a conclusion is not necessarily to be made as this reference could also be interpreted as just one example given by the European legislator for a broader interpretation of the term movable. As noted, the European Commission has also expressed the view that the Directive also applies to software.[107] Moreover, it is arguable that, in the light of its overriding objective of consumer protection, the provisions of the Directive should be interpreted broadly.[108] Here what should count are the item's character of being an exchangeable good, as well as the risk of harm it poses to users. In this regard, it should also make no difference whether the software is purchased on a data carrier or downloaded from the internet. In the end the user is using the same tool. A further argument presented is that a computer programme at its origin, and in case of a transfer to a new device, is always integrated in a material support. Once software is introduced into a hardware device, this gives rise to changes of a material and tangible nature.[109]

(2) Non-application of Directive to software qualifying as a service

Whether software is regarded as a product in the sense of the Directive or as a service has critical legal consequences as services do not fall under the strict liability regime established by the Product Liability Directive.[110] However, there is no general acknowledged rule how to distinguish a product from a service. Traditionally, courts in the UK developed within their national strict liability regime the "essence test" asking whether the essence of the contract is the work or the materials supplied. Similarly, the "English Rule" sought to distinguish between contracts with resalable tangible goods and contracts where no resalable tangible goods were produced. However, neither rule has been used by the courts since the beginning of the 20th century. In *G.H. Myers & Co v. Brent Cross Service Co*.[111] the court found that the contract was for services, but also imposed an implied warranty on the goods provided as part of the service.[112] For their part, some US courts evolved the professional/commercial test. If the defendant was a professional and the transaction arose out of that professional skill, then the transaction was characterized as a service; otherwise it was seen as a commercial transaction for which strict liability applies.[113] This rule was easy to use in case of doctors or attorneys, but it is not clear whether it would also apply to a software engineer who has a high degree of expertise.[114] Other US courts used the English

[106] Alheit, p. 200; Spindler, Verschuldensunabhängige Haftung im Internet, MMR 1998, pp. 120-121.

[107] Rowland, Kohl, Charlesworth, 4th edt. 2012, p. 479.

[108] Alheit, p. 194.

[109] Alheit, p. 200.

[110] Vihul, The liability of software manufacturers for defective products, The Tallin Papers 2014, vol. 1, no. 2, p. 9; A Proposal for a Council Directive on the Liability of Suppliers of Services, COM (90) 482 final, 20 December 1990 has been submitted by the European Commission.

[111] G.H. Myers & Co v. Brent Cross Service Co.

[112] Maule, Applying Strict Products Liability to Computer Software, Tulsa Law Review 1992, vol. 27, no. 4, p. 747.

[113] Ibid.

[114] Ibid, pp. 747-748.

essence test and others went for a case-by-case application of the policies supporting strict liability.[115]

In the more recent academic literature, software applications that are sold on a medium (e.g. a cd-rom) accessible to all interested users have generally been characterized as a product.[116] The same should arguably apply also to mass product software which can be downloaded on the device of the user.[117] By contrast, software designed for a particular customer is regarded by some authors as a service, as it embodies specific, tailored knowledge and work on the part of the software developer.[118] However, other commentators argue also in these cases that the essence of the contract is the delivered software which always remains a product[119] with the product-specific potential to cause future damage[120]. This seems also to accord with the reasoning in the above mentioned case of *G.H. Myers & Co v. Brent Cross Service Co*. Both software types at the end of the process offer the same material qualities and today's custom fitted software could be tomorrow's standardized mass product.[121]

On the other hand, one could interpret the Product Liability Directive in such a way that the product must be put by the producer into circulation (distribution chain) which requires a distribution network (producer, seller, consumer).[122] In the case of custom-fitted software this is usually not the case, and as the supplier has a limited market and usually does not have the chance to spread the costs for a software failure it would arguably be unfair to impose strict liability in such cases.[123] Not only does custom made software not have the advantage of safety tests aimed at assembly line production,[124] but the bespoke software customer will have a much greater opportunity to obtain corrections when necessary over a longer term, and a risk allocation by contract seems to be a fair solution.[125] Considering these arguments it makes sense to qualify software as a service where it is not an off-the-shelf product, but a custom made piece.[126]

---

[115] Ibid, p. 748.

[116] Kizza, Ethical and social issues in the information age, 4th edt. 2010, p. 178; German Commentators also support this view: e.g. Auer-Reinsdorff and Conrad, p. 192; Marly, p.790.

[117] Straub, Produktehaftung für Informationstechnologiefehler – EU-Produkthaftungsrichtlinie und schweizerisches Produktehaftungsgesetz, 2002, pp .12-13.

[118] Kizza, p. 178.

[119] Alheit, p. 199.

[120] Straub, p.15.

[121] Alheit, p. 199.

[122] Hoeren, IT-Recht, 2014, p. 153 with regard to the German implementation (Produkthaftungsgesetz) of the Directive.

[123] Rowland, Kohl, Charlesworth, p. 479; Maule, p. 753.

[124] Maule, p. 753.

[125] Rowland, Kohl, Charlesworth, p. 479.

[126] Maule, pp. 752-753; in Germany the same issue is discussed: Reese argues that custom-made software should also fall under the strict liability regime as the legislative text in the Directive does not require an industrially produced product (Produkthaftung und Produzentenhaftung für Hard- und Software, DSTR 1994, p. 1125; Hoeren takes an opposite view.

Further complications arise when considering the development towards offering the use of software via cloud solutions. Here the user is using software which is saved by the provider on a server that the customer can access via the internet, often together with storage or infrastructure capacities. Such cloud applications are often conceived of (by their providers and users) in terms of a service, as denoted by the term "software as a service" (SaaS).[127] However, the question remains whether, in legal terms, this form of using software should be treated as akin to buying mass product software. In particular (and in contrast to the case of bespoke software) a multitude of users may make use of it, and this is arguably a more pertinent liability policy consideration than whether the software is accessed via a cd-rom or downloaded directly to the device of the user. The product typical potential to cause damage remains essentially the same; and as with off-the-shelf software, a risk allocation via contract seems inappropriate, as the user will be in a take it or leave it position without having influence on the contractual arrangements or production/design process of the software application. Admittedly, unlike the case of software sold following incorporation in a tangible medium, the developer whose software is downloaded via the cloud, retains a greater ongoing influence over it, which includes the opportunity to address potential risks of user harm (e.g. by issuing updates to fix bugs). However, commentators currently remain divided over what implications, if any, should follow as regards the application or otherwise of the product liability regime.[128]

(3) Conflict with rules on liability for wrong information

Subjecting software to the product liability regime could mean strict liability would apply to the provision of false information, a result arguably contrary to established legal principle. In this regard there have been cases where courts have refused to apply strict liability to wrong information contained in books. For example, in Cardazo v. True,[129] a woman suffered poisoning from food made to the defendant's recipe, which included an exotic ingredient. The recipe was lacking the information that the concerned ingredient had to be cooked properly to become edible, but the court denied liability for breach of warranty. These cases may be relevant as software usually consists of and produces information. In a 1985 consultative document published by the UK Department of Trade and Industry, reference to faulty information in books was made and it was suggested that 'it would be absurd to hold the printers liable for faithfully reproducing errors in the material provided to them by giving bad instructions' and so causing indirectly injury.[130] Admittedly, in some cases software may be considered more than just information, namely where it interacts with the hardware components. When software is steering processes as opposed to simply supplying information, product specific functions exist, which may also justify stricter liability rules.[131] It remains to be seen what positions the courts will adopt. Ultimately it is

[127] Vihul, p. 9.

[128] Spindler, p. 122; Vihul, p. 9.

[129] Cardazo v. True.

[130] Department of Trade and Industry, Implementation of the EC directive on Product Liability, Department of Trade and Industry, 1985) para. 47.

[131] Straub, p. 12.

likely that questions relating to the scope of the Directive and the conformity of national implementations will have to be answered by the ECJ.[132]

As the above discussion shows, there is need for further clarification to obtain greater legal certainty on the issue of when software is covered by the product liability regime. Especially when there are online services where the customer/user is provided with the software, but does not download the software, the question arises whether this means that the user will be unable to make a claim under the product liability regime in case of damage suffered, and forced to pursue a (more difficult) claim under negligence. Moreover, the obscurity of the distinction, which arguably exists at present, between downloaded software and software used via cloud applications becomes clear in cases where – as for MHA itself- the same e-health service is provided via a web application and an app which is to be downloaded on the user's device.

4.3.3. Producer

A further issue, insofar as product liability is found to apply to software in principle, is to identify the party bearing liability. According to the Product Liability Directive, this will be the product's 'producer', defined in Article 3 as:

> *"the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer."*

In terms of the MHA platform web application, and also in terms of the MHA app, the producer would be the technical partners that have developed the app. The consortium is not a legal entity so these partners could not be seen as acting for it.

Besides the primary liability on the producer, a form of secondary liability is imposed by the Directive on any person responsible who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business. In relation to MHA, special consideration should be given here to the possibility of the platform featuring third-party-apps that can be downloaded from developers located outside of the EU. It needs to be investigated whether MHA when introducing such apps would act as an importer of these apps in the sense of the Directive. This would have the consequence that the platform's provider liability would be extended in respect of damages caused by those apps. The policy rationale for this extension of liability is to ensure that consumers can enforce their claims under the Directive which is not necessarily the case if the defendant is located outside the EU. Article 1 (2) of the Directive is straightforward in case of tangible goods. The product is brought into the community market where it then will be physically distributed by the importer.

This reasoning could also be applied to software on a data carrier, and potentially to cases where users access software placed (by the 'importer') on a platform located in the EU. In the latter case, it could indeed be argued that the user will have specific security expectations which he might not have if the platform is hosted by a corporation based in a

[132] Lloyd, p. 562.

third country. The likelihood of the platform being deemed the importer will be even higher if it active engages in promoting the app in question[133], e.g. by offering the download from a server controlled by the platform provider. By contrast, it is less certain if the provision of hyperlinks alone would be sufficient to qualify the platform provider as an importer.[134] A final requirement for importer liability is that the importer distributed the product in course of his business. This could also be in form of freebies or free samples as long there is a business purpose behind the distribution which could be making the platform more attractive for users and raising his profits.[135]

4.3.4. Defective Product, damage covered and causality

Notwithstanding the possibilities discussed that a platform such as MHA may be subject to the product liability regime, there remain various hurdles a user would need to overcome to obtain damages in a given case. In this regard (despite not having to show fault on the platform's part), the injured person is still required to prove their damage, the defective nature of the platform software (or relevant app), and the causal relationship between defect and damage. According to Article 6 Product Liability Directive, a product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including: the presentation of the product (e.g. user's manual and screen display); the use to which it could reasonably be expected that the product would be put and the time when the product was put into circulation. The Directive states that a product shall not be considered defective for the sole reason that a better product is subsequently put into circulation, Article 6 (2). However, there are software-applications which require stricter criteria, e.g. in cases of software for medical treatment where a malfunction may endanger the health or life of a human. In case of arrangements for regular updates the time factor will not diminish the producer's liability in the course of time.[136]

Typical kinds of defect that have led to litigation under the regime are manufacturing defects, design defects and instruction defects (failure to warn defect).[137] In this context, software is especially vulnerable to 'design' problems, in the form of 'bugs' that under certain conditions may cause it to behave unexpectedly. At the same time, it is often noted that software is never completely bug-free due to its complexity and the need to operate in many technical environments. However, there is still a reasonable expectation by users that the software will not infringe their negative interest in not suffering damage to other important goods, if they use the product for its intended purpose.[138] These expectations

[133] Spindler, p. 123.

[134] Spindler, p. 123.

[135] Wagner, in: Habersack (ed.), Münchener Kommentar zum BGB, 6th edt. 2013, Section 4 ProdukthaftG margin note 30.

[136] Alheit, p. 203.

[137] Alheit, p. 196.

[138] Marly, p. 791.

cover, for instance, protection against virus attacks. It is also important that the software protects from a system crash and data loss.[139]

The Product Liability Directive in fact only covers damage caused by death or by personal injuries and damage to, or destruction of, any item of property - other than the defective product itself - provided that the damage is higher than 500 €. It is also required that the damaged item is of a type ordinarily intended for private use or consumption, and was used by the injured person mainly for his own private use or consumption.[140] There is no compensation for purely pecuniary damage.[141] The Directive allows Member States to restrict a producer's total liability for damage resulting from death or personal injury and caused by identical items with the same defect to an amount which may not be less than 70 Mio €.[142] Germany, for instance, has set a total limit of 85 Mio €.[143]

As noted above, the claimant must also prove the causal link between the damage and the defective product. The rules here are in principle the same as for a private law claim brought either in tort or contract law. The claimant must satisfy, as a first step, the 'but for test' or 'conditio sine qua non' test, showing that the damage would not have occurred in the absence of the defendant's breach of duty.[144] As previously discussed, this test may be difficult to satisfy in cases of harmful omissions (e.g. where a defective app fails to spot a user's medical condition, which then goes untreated for longer: the medical evidence may be unable to say with any real certainty if earlier treatment would have saved the user.

Secondly, there may be cases where showing the aspect of 'adequate' causation (i.e. that the harmful result was not too 'remote' legally from the wrongful act) is difficult, as where a new actor intervenes. As noted above in discussing private law liability, e-health tools with an intellectual output usually cause damage only indirectly as, depending on the specific tool and case, either the doctor or the patient adjusts his behaviour according to the information or advice the tool provides, which then causes the particular damage. Special attention must be given in those cases to the particular circumstances of every single case. One criterion to assess causality used by the English courts is how reasonable it was to follow the advice of the tool which is similar to the approach of the German courts ('Herausforderungsfälle').[145]

Generally when assessing causality it must be considered that if such tools are produced to support the lay user in monitoring his medical conditions or exercising medical treatment, he usually depends on the decision of the system as he cannot verify the correctness of the information or advice provided. The trust of the patient in the correctness of the

[139] Marly, p. 791.

[140] Art. 9 Product Liability Directive.

[141] Wagner, margin note 3.

[142] Art. 16 Product Liability Directive.

[143] Section 10 ProdHaftG.

[144] Cork v. Kirby MacLan Ltd (1952) 2 All ER 402 (CA); H. Oetker, margin note 103.

[145] Oetker.

information and advice should therefore in principle be worthy of protection.[146] In case tools are used by doctors a more differentiated approach might be appropriate. Doctors will need to verify the result with a plausibility check in any case. Moreover, if the system's use is expressed to be aimed at testing, it does not invite trust, but requires users consciously to exercise carefully controlled usage.[147]

4.3.5. Exclusion of liability

The Directive provides several defences in Article 7 to the application of strict liability. One of the most important exemptions in the field of software is the state-of-the-art-defence or development-risk-defence, found in Article 7 (e). According to this, the liability of the producer is restricted if he can prove that the state of scientific and technical knowledge was at the time the product was marketed not such as to enable the existence of the defect to be discovered. Even so, adherence to voluntary standards - such as ISO - will not ipso facto exclude liability if it can be shown that more precautions should have been taken by the producer.[148]

In addition, according to the 'legal compliance' defence under Article 7 (d) the producer will not be liable if the defect is due to compliance with mandatory regulations, but if only minimum standards are prescribed the defence cannot apply.[149] A further means by which the producer may avoid liability consists in the 'later-defect-defence'. According to this, he will not be liable if, having regard to all the circumstances, it is probable that the defect that caused the damage did not exist at that time when the product was put into circulation. Finally, as in the case of private law liability, the liability of the producer may be reduced or disallowed in total (under Article 8 (2) of the Directive) in the event of the contributory negligence of the injured person (having regard to the circumstances).

4.4. The Medical Devices Regime

4.4.1. Background

As we have seen, the aim of the MyHealthAvatar platform is to offer an infrastructure in which 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. In addition, the platform software itself will perform operations upon the stored data in order to present it in a more attractive and intuitive way to users (e.g. through mapping it to the different bodily regions represented in the user's individual avatar, or by organizing it longitudinally, which allows the user to see trends based on changes in relevant data values across time).

Previously we have considered the consequences, in terms of potential ex post facto liability to users, if the information communicated by the platform or apps (or the manner of its

[146] Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, 1998, pp. 233-236.
[147] Ibid, pp. 236-243.
[148] Alheit, p. 204.
[149] Ibid.

presentation) is in some way faulty, and this causes harm to the user. However, another important issue to consider is how far the platform and apps will also be subject to ex ante regulatory checks that are designed to offer protection to users in advance. In this regard, the key rules requiring examination are those relating to the testing and marketing of medical devices, established at European level by the Medical Devices Directive 93/42/EC (hereafter 'MDD') and associated instruments, and transposed by domestic legislation into member state law. In subsection 4.4.2, we shall introduce the key regulatory principles that operate in respect of medical devices pursuant to this scheme, before considering its specific application and implications for MyHealthAvatar in subsection 4.4.3.

4.4.2. Key aspects of the Medical Devices regulatory regime

The MDD is the most general of three complementary EU Directives enacted in the 1990s that regulate the testing, certification and post-marketing surveillance requirements in Europe for various types of medical device for human use. The other Directives are the Active Implantable Medical Device (AIMD) Directive 90/385/EEC[150], and the In Vitro Diagnostic Device Directive (IVD) 98/79/EC[151], which contain the rules for powered devices implanted into the human body, and devices which analyse bodily specimens, respectively. By contrast, the regulation of medicinal products (pharmaceuticals) occurs under the separate regime established by the Clinical Trials Directive 2001/20/EC[152], whose provisions are due to be replaced by those of the Clinical Trials Regulation EU No 536/2014[153] at the end of May 2016. The rules for medical devices are themselves currently undergoing reform, with plans for the three 1990s Directives also to be replaced by an EU Regulation in the foreseeable future.[154]

Given the focus of the MHA project and platform, the ensuing discussion will centre upon the provisions of the MDD, including their application to medical devices that operate using computer software. First, as regards the meaning of 'medical device', this is defined in Article 1 (2) (a) as:

> *"any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:*
>
> *— diagnosis, prevention, monitoring, treatment or alleviation of disease,*
>
> *— diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,*
>
> *— investigation, replacement or modification of the anatomy or of a physiological process,*

[150] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1990L0385:20071011:en:PDF.

[151] See http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31998L0079&from=DE.

[152] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:121:0034:0044:en:PDF.

[153] See http://ec.europa.eu/health/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf.

[154] 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.

— control of conception,

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means;"

This is a wide definition that, as can be seen, includes express references to software; moreover Commission guidance, issued in 2012, makes it clear that software operating in its own right (independent of incorporation in a tangible device), is covered in principle as so-called 'stand-alone software'. In this context, in the UK the Medicines and Healthcare products Regulatory Agency (MHRA) - the competent national medical devices authority - has suggested decision support software, applying automated reasoning to data input from health records, or using algorithms to calculate dosage, track symptoms or give clinical guidance is likely to be covered.[155] As with any other form of device, the question will be whether its manufacturer (the person responsible for its design, manufacture, packaging and labelling) intended its use for one of the defined diagnostic or therapeutic purposes. Under Article 1 (2) (g), this will be judged objectively "*according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials*".

The MDD goes on to establish a set of pre-marketing testing and certification requirements. Only devices that go through the relevant testing procedures, and receive a CE mark attesting to this, may be lawfully placed on the European market. Such testing is designed to show that the device does not pose undue safety risks to users, and also that it performs in the way the manufacturer claims; the 'essential requirements' to be satisfied in the course of this evaluation are set out in Annex I of the MDD. At present there is no need to go further and show a positive clinical benefit (in terms of efficacy) from using the device; however, this is one of the things that may change as a result of the ongoing legislative reform process, aimed at the replacing the MDD by a future Regulation.

According to the MDD, Annex X, the evaluation that the device satisfies the essential requirements should be based upon 'clinical data'. For the present, and compared with the more homogenous testing rules for testing pharmaceutical products (where clinical benefit also has to be shown), there remain diverse testing approaches and procedures that may be deployed to obtain the relevant data. This also reflects the considerable diversity in the nature of products that may qualify as medical devices, which makes a single approach (e.g. use of randomized control trials) inappropriate and/or impractical. In many cases it will be sufficient to provide data on the past performance of a similar device to the new device, rather than undertaking fresh testing. Indeed a characteristic of the medical devices market is that of incremental development, where new devices typically incorporate step-by-step advances over previous devices rather than radical differences, and where new testing is correspondingly less indicated for identifying novel risks of harm.

At the same time, the MDD (in its Annex IX) undertakes a broad division of medical devices into four different risk-classes, based on their general characteristics. In Article 11, differential testing procedures are then specified for use in respect to each class, whose

[155] MHRA Guidance, *Medical device stand-alone software including apps* (8 August 2014), at https://www.gov.uk/government/publications/medical-devices-software-applications-apps.

rigour increases according to the potential for harm to users in case of malfunction. For Class I devices (low risk), the device manufacturer itself is generally permitted to evaluate the device in accordance with the Annex I essential requirements, and affix a CE mark;[156] but for the other categories (Class IIa: low-medium; Class IIb: medium-high; and Class III: high), this task must be performed by an independent entity, known as a 'notified body'. These are for-profit companies, licensed in each member state by the competent national medical devices authorities (set up by relevant domestic law transposing the MDD). In such cases the CE mark awarded will include the identification number of the notified body.

Subsequent to marketing, the device manufacturer remains under the duty to be vigilant and report cases of serious adverse incidents involving the device to its competent member state authority. According to Article 10 (1) (a) of the MDD, relevant incidents are ones "which might lead to or might have led to the death of a patient or user or to a serious deterioration in his state." In such cases, the competent authority is required in turn to submit the information to the central European Databank on Medical Devices (Eudamed), and in appropriate cases to take action leading to the device's withdrawal across Europe.

In the event of infractions of the rules under the MDD and relevant transposing legislation, such as marketing a device with no, or a faultily-affixed CE mark, or non-observance of post-market surveillance, the competent national authorities may in serious cases prosecute the device manufacturer in criminal law. For example, in the UK the MHRA has power to bring proceedings under the Consumer Protection Act 1987, resulting in a penalty of up to GBP 5,000 or six-months' imprisonment.

4.4.3. Implications for the exploitation of the MHA platform

In this section we shall consider more concretely the implications of the above scheme for the exploitation (involving placing on the market) of a platform like MyHealthAvatar. This will require in the first place answering the question as to whether the platform itself should be classified as a 'medical device' under Directive 93/42/EC, and if so into which risk-class it would fall (and what the attendant implications would then be in terms of the certification procedure mandated by the Directive). In the alternative, though, if the platform does not qualify as a 'device', it will still be pertinent to consider the implications for the platform, where third party apps that are offered to users and/or perform operations upon user data made available via the platform, do qualify as such devices.[157]

- *Status of the platform under the rules*

First, as regards the platform, as we have seen, this consists broadly of facilities for storing user health and lifestyle data within an integrated software infrastructure that provides a user interface offering various presentational and communication tools. The latter allow existing data to be presented to the user in novel ways, notably in the form of a 4-D avatar,

[156] For class I devices that provide a measurement function, the manufacturer will have to make as well an application to a notified body which will assess the aspects of manufacturing that concerns the conformity of the product with metrological requirements.

[157] The current apps of Twitter, Withings, Moves, do not qualify as medical devices. They are purely lifestyle apps.

but also offer input functionalities, so that the user may upload new data – including via a 'patient diary', and communicate with other users in a directed way, either 'horizontally' (i.e. with other 'citizen' users through support groups of users with a similar lifestyle goal and/or health condition), or 'vertically' with health care providers (offering advice), or third party developers (offering apps relevant to the user's goal/condition).

Here, as noted in part 4.4.2, the fact the platform is conceived entirely as a software infrastructure, as opposed to a 'device' in a traditional tangible sense, is no obstacle in principle to it falling under the rules in the Directive: instead it may qualify as 'stand-alone software' in accord with the relevant explanatory guidance issued by the EU Commission in 2012. Nonetheless, as noted, to do so it must satisfy the general condition that its manufacturer intended its use for diagnosis, prevention, monitoring, treatment or alleviation of disease, injury and/or disability, or for the control of conception. Admittedly, this definition is very broad; however, taken as an overall system, it is arguable the MHA platform would fall outside it as broader still. Thus the platform is not directed at any specific disease or diseases, or even 'ill health' as such, but offers a generalized resource (usable by the 'healthy' citizen as much as the already ill) for tracking all manner of data relating to his or her general lifestyle as much as to particular health conditions. A related point, is that the operations performed by the platform on user data are also of a general kind, presenting this in an enriched way (as a 4-D avatar), but not for the purpose of offering specific health advice to the user.

In this regard, the Commission in its 2012 Guidance stated that:

> *"if the software does not perform an action on data, or performs an action limited to storage, archival, communication, 'simple search' or lossless compression (i.e. using a compression procedure that allows the exact reconstruction of the original data) it is not a medical device.*
>
> *Altering the representation of data for embellishment purposes does not make the software a medical device. In other cases, including where the software alters the representation of data for a medical purpose, it could be a medical device."*

However, the Commission 2012 guidance also suggests that the platform should not be looked at as a non-divisible entity. Rather, as a complex software system, it will consist of many applications, each requiring discrete assessment. Those software modules that correlate to applications with a medical purpose will be covered by the medical device rules, and will need to carry a CE mark, whereas applications without such a purpose will not. As the guidance goes on to state, "*It is the obligation of the manufacturer to identify the boundaries and interfaces of the different modules*" based upon the intended use. This raises the question of who will count as the manufacturer for these purposes. According to Article 2(1)(f) of Directive 93/42/EC:

> *"'manufacturer' means the natural or legal person with responsibility for the design, manufacture, packaging and labelling of a device before it is placed on the market under his own name, regardless of whether these operations are carried out by that person himself or on his behalf by a third party.*

The obligations of this Directive to be met by manufacturers also apply to the natural or legal person who assembles, packages, processes, fully refurbishes and/or labels one or more ready-made products and/or assigns to them their intended purpose as a device with a view to their being placed on the market under his own name…"

In the case of MHA, this would be the consortium partner or partners who developed the relevant software module, insofar as they continue to attach their own name to the software at the point at which it reaches the market. Assuming they were to transfer ownership to a separate entity for exploitation purposes (involving the device's placing on the market), the latter would come under the same, manufacturer's obligations.

As discussed in section 4.4.2, the obligations in question relate both to the pre-marketing certification process, designed to ensure the safety and performance of the device, as well as to post-market vigilance and surveillance requirements. In terms of the former, the first matter is to determine the relevant risk classification (Class I, IIa, IIb, or III) of the device for the purpose of choosing the correct procedure for certification (allowing the affixing of the CE mark). Here, as the EU Commission guidance on stand-alone software notes, the key rules are 9-12 of Annex IX of Directive 93/42/EC, which apply to 'active' medical devices (i.e. ones that operate using an external power source).

The most relevant provision, in terms of potential applicability to software modules within the MHA platform, appears to be contained in Rule 10, which provides these will fall within the low-medium risk-class (IIa):

"… if they are intended to allow direct diagnosis or monitoring of vital physiological processes, unless they are specifically intended for monitoring of vital physiological parameters, where the nature of variations is such that it could result in immediate danger to the patient, for instance variations in cardiac performance, respiration, activity of CNS in which case they are in Class IIb."

Insofar as Class IIa applies, the manufacturer would need then to follow the routes to certification prescribed under Article 11(2) MDD, and which require the device's safety and performance to be checked by an independent notified body. In other cases, where the software module does not have a diagnostic or monitoring function (but is deemed still to have a purpose that qualifies it as a medical device) it will fall into the low-risk Class I, for which the manufacturer itself may perform the certification and affix the CE mark, unless it provides a measurement function; then the manufacturer will have to make as well an application to a Notified Body which will assess the aspects of manufacturing that concerns the conformity of the product with the metrological requirements.[158]

As regards post-market surveillance, the Directive in Article 10(1) requires member states to set up such systems; this includes establishing obligations in their domestic transposing laws for manufacturers to operate post-market audits and vigilance systems to identify problems that may call the device's certification into question. Where it becomes aware of relevant

[158] Section 5 Annex VII MDD.

concerns, a manufacturer should notify its relevant competent national authority, which will in turn forward the information to the European Eudamed database.[159]

- *Status of apps running via the platform under the rules*

Independently of the whether the MHA platform, and/or discrete software modules within it, are covered by the rules on medical devices under Directive 93/42/EC, it appears certain that (at least some of) the apps that are made available to users (and run on user data) via the platform, will be so caught. This will be true for example of apps that satisfy the definition of active devices intended for diagnosis under Annex IX, Rule 10 quoted above.

As noted, in such cases the apps in question, would fall within the risk-category, Class IIa or (in cases where they monitor vital parameters where a misreading may have serious immediate implications for the user's health) Class IIb, with the need for a notified body to assess the app's compliance with the essential requirement under Annex I, MDD. Other apps of more modest intent, such as those that allow users to calculate a given health value for themselves, e.g. 'heart age', based on publicly available data, may either be Class I or perhaps fall outside the scope of the medical devices regime altogether if they relate more to purposes of lifestyle than health.

Insofar as a given app is covered by the rules, the primary responsibility will be upon the app developer, as its manufacturer, to satisfy the pre- and post-marketing requirements under Directive, as previously described. However, from the platform's point of view there is also the possibility that in some cases it may be found to have similar obligations to the app developer, in accordance with Article 2(1) (f) of Directive 93/42/EC. As we saw earlier, this extends the obligations of the manufacturer to the *"natural or legal person who assembles, packages, processes, fully refurbishes and/or labels one or more ready-made products and/or assigns to them their intended purpose as a device with a view to their being placed on the market under his own name…"*

On the face of it, this would apply only if the app developer's own name is removed altogether, and the app in effect 'adopted' by the platform as a home-brand app. It is not clear, at this point, if this may be envisaged in the future as part of the MHA exploitation strategy. In the meantime though, and independent from legal compliance issues, it is evident that in order to maintain user trust and confidence the MHA platform should be active in seeking to ensure the apps it offers to its users have gone through proper medical device certification, where required (as noted, some apps – namely those whose purpose relates to issues of lifestyle rather than health – will not be caught). In this regard, the responsibilities of app developers to comply with MDD rules should be underscored in the API license agreement of the platform (as a condition for interacting with the platform).

Admittedly, as we saw earlier, the correct application of the rules to apps may pose challenges for developers – a problem also highlighted by respondents to the Commission's 2014 mHealth Green Paper, who noted difficulties in both how to draw the line between tools and apps that address 'health' as opposed to 'life-style', and in determining the correct risk class of a specific health app for certification purposes. It is suggested one approach

[159] See: https://medicaldeviceslegal.com/2011/04/28/eudamed-enters-into-full-force/.

may be to require app developers to seek relevant assistance in resolving such questions from their competent national authority. Alternatively, they could be asked to make use of emerging voluntary accreditation systems, such as that offered in the UK by the NHS health apps library, to vet and endorse the app.

5. Intellectual property rules for the exploitation

This section describes the rules for handling Intellectual Property Rights (IPR) for passing the MHA platform into the exploitation stage. In particular, open source licensing and license solutions, identified for the MHA software components, third party development legal framework, rules for providing the MHA platform to the end users and handling content, protected by IP rights, contractual framework for collaboration between MHA with the CHIC project are described in more detail below.

5.1. Open source and license solutions

This part considers the license solutions, which have been determined and are proposed for licensing of MyHealthAvatar platform and MyHealthAvatar software components. This includes a comparison of proprietary and open source licensing schemes, as well as an analysis of the exploitation options of how the MHA components can be commercialized. The exploitation interests of the individual project parties have been considered, and taken into account, where possible.

The license solutions for MHA software components have been determined on the basis of the legal analysis of software development and software licenses used in MyHealthAvatar. The selected licenses are suggested with the aim of avoiding potential license incompatibility issues – both in respect of downstream and upstream licensing. The legal issues, when a given developing party or parties have used incompatible programs in their components by default, have been examined and so far as possible resolved. The legal and technical arguments which determined the choice of those licenses are provided below. The legal guidelines on how to apply licenses to the codes and make the codes available to the public will follow.

The legal analysis was conducted on the basis of data provided by the software developing partners. It comprises components developed by: ICCS, FORTH and BED. Software dependencies and associated licenses, methods of software development, methods of communication and interplay between the components on the platform were analysed. The Software component license compatibility table for software licensing in MyHealthAvatar along with the software development tree are provided in Annex 9.

5.2. Licensing solutions for MyHealthAvatar components

This section gives a brief overview of the licensing solutions determined for MHA components. It describes what licenses have been defined for each component, and the license requirements for distribution and exploitation options, which these licenses provide. Detailed guidelines on how to apply licenses to the components and additional permissions, which some developing parties are recommended to add to the license text in order to avoid possible incompatibility issues identified for certain components, are stated in the Software component license compatibility table (please see Annex 9).

5.2.1. Apache License Version 2.0

There are a number of components, which project partners have developed from scratch and/or do not use any external software dependencies, which might affect licensing of the

component. According to the Software component license compatibility table, the Nephroblastoma Oncosimulator, the Nephroblastoma Application, developed by ICCS, the Personalized CHF Related Risk Profiles and "Real-Time Monitoring" (CHF) - mobile application and Link with external Clinical Systems, Semantic Annotator and Semantic Search, developed by FORTH, do not use any external software dependencies. In addition, there are components where, whilst external software is used, this does not affect the licensing of the component, e.g. installation and running a component on a particular operating system.

Consequently, licensing of the above components is not restricted by third party license terms. These components, if distributed as separate and independent programs on their own, can be released under any license at choice of the developing party. Dual licensing, such as release under an “open source” license for research and under proprietary license for commercial use may also be an option. As an open source license option, Apache License Version 2 is proposed. Such components, which are not subject to licensing implications by third part terms and are considered to go under Apache Version 2, shall have no implications on licensing of other components, integrated on the MyHealthAvatar platform, and shall not affect licensing of MyHealthAvatar platform itself.

Another category of MHA components have software dependencies or use external libraries, whose licenses do not affect licensing of the component, or use such libraries under the license terms and in a way that licensing of the component itself remains unaffected. The licensing of such components is in general not restrained by external license terms. These components may be distributed under license terms at the choice of the developing party under the sole requirement that license terms for distribution of software dependencies, if included in distribution, must be observed. Normally, such licenses ask to supply a license text for a program along with software distribution, attach the copyright notice and retain the license notices and disclaimer in the program files.

The Cassandra Data Repository, developed by FORTH/BED, relies on Cassandra, licensed under Apache v2. As applied to the original code, the Apache License allows a program to be used and distributed as part of another software distribution and allows that software to be licensed under other terms, provided the license terms for distribution of Apache program are complied with.

Software components Exelixis and Osteoathritis mobile application, developed by FORTH use external libraries, licensed under Apache v2 and/or LGPL v2.1 by linking.[160] LGPL v.2.1 in Section 6 allows the licensee to combine an application with a LGPL library and distribute the application under any license, provided that the terms permit modification for the customer's own use and reverse engineering for debugging such modifications.

Accordingly, the components developed from scratch or which use Apache or LGPL programs by linking may be distributed under the license at choice of the developing party (allowing modifications and decompiling such modifications for the customer´s own use). If included

[160] OSI, The GNU Lesser General Public License, version 2.1 (LGPL-2.1), http://opensource.org/licenses/LGPL-2.1.

in distribution, the Apache or LGPL program remain governed by Apache or LGPL and must be distributed in accordance with the distribution terms of the respective license.

As an open source license option for these components, the Apache License Version 2 (Apache v2)[161] is suggested. The latter is a classic open source license: it allows licensing software products both "open source" and on proprietary basis, does not require the source code to be disclosed, has rather lax license terms, is flexible and compatible with many forms of open source licenses.[162] Further, Apache v2 is standard compliant and is used in communications-oriented software, which adheres to HTTP protocol, e.g. Apache HTTP server.[163] Release of MHA components under Apache v2 would support the communication line via HTTP.

Apache v2 is therefore a good option for research projects which explore the technology and envisage commercialization upon successful implementation of research ideas.[164] Apache v2 allows Apache programs be used both under open source scheme and/or on proprietary basis, as long as the Apache license terms are complied with.[165] Another reason for use of Apache is because it is compatible with GPL v3.[166] By licensing under Apache v2, license compatibility among the components on the platform will be observed. Further details on application of the Apache license notice and what license requirements, as applicable to the distribution of Apache or LGPL programs the developing parties need to observe, are provided in the Software component license compatibility table for MHA.

5.2.2. GNU GPL Version 3

A number of MHA components have software dependencies licensed under GPL. For instance: ICCS Model repository and Data Repository for Models; FORTH/BED Virtuoso Triple Store; BED MHA Web Application (Backend); and MHA Web App Frontend rely on GPL software, either GPL v2 or GPL v3.

GPL is a copyleft license. It requires that *"a work based on the Program, or the modifications to produce it from the Program"* must be licensed under the same terms as a GPL program, i.e. under a GPL license as well[167].

Normally, the MHA components use such GPL software (most often libraries) by the method of dynamic linking (commonly named "calling the object code"). In view of the FSF, "*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*

[161] OSI, Apache License Version 2, http://opensource.org/licenses/Apache-2.0.

[162] Andrew M St. Laurent, Understanding Open Source and Free Software Licensing, 2004, p. 32.

[163] Ibid.

[164] Ibid.

[165] Section 4 Apache v2.

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

[167] Section 5 GPL v3, Section 2 GPL v2.

License cover the whole combination"[168]*.* Because of this copyleft requirement of GPL, components which use GPL software by linking, should be licensed under GPL in order to be compliant.

The components, which are thus affected by GPL copyleft may, though, be licensed either under the same GPL version under which the software dependency in question is licensed, or by a later version, where associated GPL so allows. Both Section 14 GPL v3 and Section 9 GPL v2 provide for a possibility to release a "work based on the Program" either under the version number of the license which applies to the Program or "any later version".

Because of a number of upgrades in its terms, GPL Version 3 or any later version (GPL v3+) is recommended here for components which have software dependencies under GPL, GPL v2+ or GPL v3+. The benefits of GPL v3 are inter alia as follows: it grants stronger protection against patent threats, is compatible with a number of other open source licenses, in particular, Apache v2, and allows making additional permissions to GPL license terms. This is a definite advantage of GPLv3, which allows to resolve potential license incompatibility issues between GPL licensed programs and GPL incompatible libraries. This permission is provided for by Section 7 GPL v3. The FSF advises software developers to add linking exception to the GPL license terms of their code, if a GPL code is supposed to link against a GPL incompatible library. The FSF recommends the following notice for this:

"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.}"[169]

Adding such a linking permission was also defined as a legal instrument to solve license incompatibility issues, which were revealed in some MHA components. Some MHA components come with incompatible libraries by default, for example, by using GPL and GPL-incompatible library in one component. For the sake of complying with GPL and for the purpose of solving license incompatibility, GPL v3+ with linking permission under Section 7 is advised as a license solution for such components.

Further details, what MHA components go licensed under GPLv3, what components go under GPLv3 with linking exception and what license notices such components need to attach to the codes are described in the Software component license compatibility table in Annex 9.

[168] FSF, FAQ, Does the GPL have different requirements for statically vs dynamically linked modules with a covered work? https://www.gnu.org/licenses/gpl-faq.html#GPLStaticVsDynamic.

[169] FSF, FAQ, What legal issues come up if I use GPL-incompatible libraries with GPL software? (#GPLIncompatibleLibs), http://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs.

5.3. Licensing solution for the MyHealthAvatar platform as a whole

Above we considered licensing solutions for individual software components. In this section we are concerned with defining the substance of MHA platform, composed of multiple software components integrated on it, and finding a licensing solution for the MHA platform as an integrative whole.

The MHA platform is composed of multiple software components. Some components are integrated on it, some components are designed to be located on mobile devices and communicate with MHA platform via API. While some components and their licenses, like Apache v2, do not have any licensing implications for the other components, the components covered by GPL v3 may affect licensing of other components and the entire MHA platform. In how far GPL copyleft may affect licensing of other components and MHA platform as a whole depends on the interplay and the mode of communication between the components, namely whether the MHA components constitute and communicate with each other as separate programs or run together combined into a larger program.

Section 5 GPL v3 provides: "*A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate*".[170]

The Free Software Foundation (FSF), the originator of the GNU/GPL licenses, permits combining and distributing compilation that qualifies as an aggregate, even when the licenses of the constituent programs are "non-free or GPL-incompatible". The only condition is the aggregate may not be released under a license that prohibits users from exercising rights that each program's individual license would grant them.[171]

What is essential in determining whether MHA platform may qualify as an aggregate in the meaning of GPL is whether MHA components are considered as separate programs in themselves or combined into a larger program.

The FSF considers that if the modules are included in the same executable file or are designed to run linked together in a shared address space, that would most likely mean combining them into one program. In contrast, pipes, sockets and command-line arguments are communication mechanisms, normally used between two separate programs. When such mechanisms are used for communication, the modules are regarded as separate programs.[172]

Components on the MyHealthAvatar platform interact and communicate with each other by exchange of files, command line arguments and/or by making HTTP calls. In view of the FSF,

[170] OSI, GNU General Public License, version 3 (GPL-3.0), http://opensource.org/licenses/GPL-3.0.

[171] FSF, FAQ, What is the difference between an "aggregate" and other kinds of "modified versions"? (#MereAggregation), http://www.gnu.org/licenses/gpl-faq#MereAggregation.

[172] Ibid.

such communication mechanisms are normally used between separate programs and when they are used for communication, the components are normally considered as separate programs. This communication background allows considering MHA platform as an aggregate. The recommended license solution for it would be such a license type which would not limit individual licenses of the components and would not restrain access or other legal rights of the users beyond what the individual components permit.[173]

Therefore, a licensing solution recommended for the MHA platform would be to distribute individual components under individual licenses identified for each of them.

5.4. *Exploitation options*

In order to maintain the sustainability of the project outcomes, the MHA project is considering licensing the MHA software components "open source" (insofar as the relevant copyright holders of the components agree). As open source license solutions for MHA components the GNU GPL Version 3 and the Apache License Version 2 are proposed. These two licenses are qualified as "open source" and free licenses and are widely used in modern software developments.

5.4.1. GNU GPL Version 3

The GPL license is a free software license and provides for the right to use, copy, modify and distribute the original licensed program and modified versions from it royalty free.[174] On these premises, the MHA components, which are covered by GPL, may not be licensed on proprietary basis for royalties. However, GPL v3 allows the licensee to distribute GPL programs and charge any price or no price for each copy and to offer the customer support or warranty protection for a fee[175].

One of the exploitation options for MHA components covered by GPL might thus be to charge fees for distribution of copies. For instance, when a GPL program is distributed from the site, fees for distributing copies can be charged. However, *"the fee to download source may not be greater than the fee to download the binary*".[176]

Provided the MHA components will be offered into use as "Software as a service", so that the users could interact with the platform via network, charging fees to subscribe to the platform or downloading MHA programs from the site should be permissible (to the extent as needed to cover the costs for maintaining the server). Apart from that, the MHA project also considers a possibility to upload the MHA components into public repository as "open source". This will open a possibility to access the MHA components and run them free of charge.

Offering warranty protection and additional liabilities would be another exploitation option. Section 15 GPL v3 allows that warranty protection can be offered in writing by the copyright

[173] Section 7 GPL v3.

[174] FSF, Free Software Definition, http://www.gnu.org/philosophy/free-sw.html.

[175] Section 4 GPL v3.

[176] FSF, Frequently Asked Questions about the GNU Licenses, available at: https://www.gnu.org/licenses/gpl-faq.html#DoesTheGPLAllowDownloadFee

holders and/or other parties. Hence, provision of warranties may be done by signing an agreement. A negative aspect is that a developer, who provides warranties and accepts additional liability, acts at his own risk and accepts that he will bear "*the cost of all necessary servicing, repair and correction*"[177] for the whole program, including modules provided by other developers. Warranty support may be problematic, because software is never "bug free" and the component may also include codes from third parties, which may have defects as well.

5.4.2. Release of source code for GPL components

One of the basic requirements of GPL is that the users shall have the possibility to "*receive source code."*[178] Both GPL v2[179] and GPL v3[180] contain such a requirement. Section 6 GPL v3 allows distributing GPL v3 software in object code, but requires the licensee to convey the source code in one or another way. Source code may be provided:

(a) on a physical medium (e.g., CD, USB, etc.) along with the executable, or

(b) by a written offer, valid for at least three years, to provide a source code or to grant access to the source from a network server at no charge (fees for download an executable may be charged), or

(c) by passing on such an offer from the previous licensor, or

(d) by offering access to the source code form a network server, if the binary executable is distributed from a network server as well, or

(e) using peer-to-peer transmission.

If the object code is provided for download from a network server, the source may be on a different server (operated by software developer or a third party) that supports equivalent copying facilities. In this case, there must be clear directions next to the object code, stating where the source code may be accessed.[181] If binaries are distributed via FTP, the source should be provided via FTP as well.[182]

On the other hand, if GPL v3 components are supposed to be provided into use from the network server so that the users are not able to download a copy, then the requirement to release the source code would not apply. The method of running a GPL program from the server does not fall under the method of "conveying" a GPL program, when the requirement to release the source code would apply.

[177] Section 15 GPL v3.

[178] Preamble GPL v3.

[179] Section 3 GPL v2.

[180] Section 6 GPL v3.

[181] Section 6 para d) GPL v3.

[182] FSF, FAQ, I want to distribute binaries via physical media without accompanying sources. Can I provide source code by FTP, https://www.gnu.org/licenses/gpl-faq.html#DistributeWithSourceOnInternet

In terms of GPL, "*mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.*"[183]

If MHA components are supposed to run from the server, the sole component, which will be subject to the requirement to provide the source code, will be the ICCS Tool Execution Engine, covered by the terms of AGPL. AGPL v3 is a modified GPL v3 with some additional terms. It is designed for programs intended to run on the web. AGPL enables the users *"who interact with the licensed software over a network to receive the source for that program."*[184] For this purpose, access to the corresponding source code shall be provided "*from a network server at no charge, through some standard or customary means of facilitating copying of software."*[185] The basic requirement is that the source code should be as easy to access as the object code.[186]

5.4.3. Apache License Version 2.0

The Apache License Version 2 is proposed as another open source solution for MHA components. The latter allows Apache software to be distributed 'open source' and/or on commercial basis. "*While there have been several proprietary commercializations of Apache (such as SSL-enabled Stronghold), the free version of Apache has retained its dominant market share."*[187]

The Apache license, as applied to the original code, allows the code to be used in proprietary software. It does not require that source code versions be distributed. The code created under Apache may go closed and developments can be made under proprietary license.[188] Hence, Apache components of MyHealthAvatar may be distributed in royalty based licensing schemes, as binary executables and/or in source form[189]. Dual licensing for Apache components - free "open source" for research and commercial for industry - is also possible. Thus, provided the MHA components will be provided into use "Software as a Service", so that the users could run the components from the network server, charging fees to subscribe for the platform or running or downloading Apache applications is acceptable.

Apart from that, according to Section 9, "*acceptance of support, warranty, indemnity, or other liability obligations*" in respect of Apache software may be offered for a fee. However, by accepting additional warranties and liability the licensor acts on his own behalf and own responsibility. Hereby he must accept the obligation "*to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability."*[190] It

[183] Preamble GPL v3.

[184] FSF, Why the Affero GPL, available at: https://www.gnu.org/licenses/why-affero-gpl.en.html

[185] Section 13 AGPL.

[186] FSF, Frequently Asked Questions about the GNU Licenses, available at: https://www.gnu.org/licenses/gpl-faq.html#SourceInCVS.

[187] St Laurent, p. 32.

[188] Ibid.

[189] Section 4 Apache v2.

[190] Section 9 Apache v2.

means that such a warranty obligation extends to the party making such warranty and not to any contributor. [191] This may be a negative aspect for software developers, as described above.

As regards advertisement, Apache v2 does not allow use of "*trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.*"[192] The release of components under individual licenses (either GPL v3 or Apache License v2), and the making of the source codes available, supports the "open source" commitment envisaged by MHA and observes license compatibility with GPL.

A detailed elaboration on the licensing solutions for MHA components, license requirements for distribution and guidelines on application of the license notices to the codes are provided in the Software component license compatibility table for MHA, Annex 9.

5.5. Third party development legal framework

In this section, we describe the main rules and terms under which the MHA project proposes to release its Application Programming Interfaces (API) and by that to allow third parties to develop apps designed to interact with the MHA platform.

API data exchange systems have made it possible to link platforms and apps and share the data. As already mentioned in D.11.3, MHA intends to increase the population of its own data via linking and sharing data from external platforms, inter alia Withings, Fitbit, Moves App. Also, for the purposes of expanding the functionality of MHA platform, MHA is considering the release of the platform API to the software development community. This will give external developers a possibility to develop apps, compatible with the MHA platform, which could interact and exchange data with it. In its turn, this will open a possibility for MHA users to connect and use the MHA platform from external devices, such as mobile phones.

The legal framework, envisaged for the exploitation stage, at the point when MHA will release its API to third party developers, is proposed to consist of:

(a) the API Terms of Use, which provide the legal terms and govern the use of MHA API by third party developers, and

(b) Guidelines for developers, which will provide the developers technical instructions what steps they need to follow in order to implement the MHA API into their applications. The guidelines will describe i.a. by what authentification mechanisms a developer may request permission to access a user's data, where to find a library for the developer´s programming language and framework to create an authorization flow, etc. These guidelines will be prepared by BED and should be available on the MHA website at https://myhealthavatar.org/mha/login.

[191] Laurent, p. 32.

[192] Section 6 Apache v2.

MyHealthAvatar API Terms of Use (or the API license agreement) govern the use of MHA API in third party applications and services, which are designed to interact with MHA platform and share the MHA user´s data. The API Terms of Use are attached to this Deliverable as Annex 6.

Acceptance of the MHA API Terms of Use is a prerequisite for getting access to and implementing the MHA API. By accepting the MHA terms of use, a developer enters into a license agreement with MHA and obtains the right to use the MHA API in its application.

5.5.1. MHA account

For implementing the MHA API into his application, a developer needs to register as an MHA user and register its application. The procedure of creating an MHA account and use of API client credentials is described in Section 5 MHA API Terms of Use.

The procedure for implementing MHA API includes the following steps:

(a) Creation of a MyHealthAvatar account;

(b) Registration as a MyHealthAvatar user;

(c) Registration of applications and/or services;

(d) Acceptance of the API terms of use.

Upon registering his application, a developer will get API client credentials, which a developer may use only on individual basis only and must handle with due care.

5.5.2. API license

The terms and the scope of license, which MHA grants to a developer on use the MHA API, are provided in Section 3 MHA API Terms of Use.

According to Section 3 API license agreement, MyHealthAvatar grants a developer a non-exclusive, personal, royalty free, non-transferable, non-assignable, non-sublicensable revocable license limited to the term and purpose of the API license agreement and to the country from which a developer connects to the API.

By entering into a license agreement, a developer obtains the following rights on use of the MHA API:

1. Use MHA API to develop applications and/or services intended to interact and exchange data with MyHealthAvatar.
2. Use MHA API in order to interact and exchange data with MyHealthAvatar platform, fetch and display MyHealthAvatar data in those applications and/or services. The scope of this right is limited to the extent as necessary to provide the applications and/or services to the MHA users (who will be able to interact with the MHA platform by means of such applications/services).
3. Modify MyHealthAvatar data to format it for display on the developer´s applications and/or services.

By that, MyHealthAvatar allows a developer to use the API for the purposes of data sharing, but does not grant any rights on use of the data itself. A developer is expressly required to get consent on processing the user´s data and user generated content, which may be included in the user´s data on MHA, from the user himself. How a developer may get such permissions is described in Sections 6 and Section API Terms of Use.

5.5.3. Restrictions on use of MHA API

Use of MHA API by a third party developer is subject to certain restrictions. For the purposes of keeping the MHA platform and MHA data secure, a developer may not:

- Compromise, circumvent, bypass any protection or authentication mechanisms implemented by MyHealthAvatar;
- Market, sell, transfer, disclose MyHealthAvatar Data to any third parties, unless as expressly permitted by the User or required by the law.
- Export MyHealthAvatar Data, including for account migration or service duplication, with any other purpose than enabling the Users to interact with MyHealthAvatar via your Applications and/or Services;
- Access and/or make yourself into any section of API or MyHealthAvatar Data that is not accessible to you via normal use of API;
- Other actions, which extend the scope of use of MHA API, as provided by the API license agreement, and may subject MHA to liability.

In addition, as discussed in section 5.4, consideration will be given to the inclusion of warranties from the developer as to the app's compliance with the rules on medical devices (if applicable in a given case). MyHealthAvatar may subsequently monitor use of API by a developer and may revoke or suspend access and rights to the API on temporary or permanent basis, if MHA has grounds to believe that a developer violates the terms of use of MHA API.

5.5.4. Use of MHA users' data

Use of the MHA users´ data is regulated in Section 6 API Terms of Use. It provides that any use of MHA user data requires prior informed consent of the user. A developer must respect the MHA users and their privacy, process their data in compliance with the European data protection law, due care and good processing practice.

In particular, a developer must do the following:

- Provide the privacy policy and terms of use to the user. The privacy policy must explain what data an application collects, for what purposes and what an application does with the data.
- Ask the user to read and accept the privacy policy and terms of use as a requirement for using an application.
- Not distribute, transfer, display or make user data available to any third party, unless the user expressly authorizes so.

- Respect and not allow an application to violate the user´s privacy settings.
- Use the user data as it is without any misrepresentations (except as needed to format the data for display on the application).
- Implement appropriate technical and organizational measures to protect the user data against accidental loss, unlawful or unauthorized access, use, destruction, alteration, disclosure, and other forms of processing which are not explicitly authorized by the user or MyHealthAvatar or by the law.
- Request and access only the data which an application needs.
- Use the user data in accordance with the developer´s privacy policy and terms of use.
- Comply with the developer´s own privacy policy and terms of use.
- If an application is tracking the user´s activity, it must allow the user to opt-out.
- Delete the user´s data if a user asks you so, unless retention of data is required by the law and for as long as the law permits.

By these provisions, a developer is instructed to the best knowledge of MHA to ensure the legitimate processing of data on its app. MHA explicitly advises that use of MHA users´ data in external applications is at risk of a developer and that the developer, and not MHA is responsible for processing of data in his applications.

The security aspects by transfer of the data from MHA and processing of such data on an external app are covered in Section 10, according to which a developer must ensure for secure storage and transfer of data on an external app and take reasonable steps to safeguard that his applications comply with Internet security rules.

5.5.5. Use of user generated content

The MHA platform allows its users to upload and post certain content, such as images, commentaries, data files, etc. Some of these content items, if produced by intellectual effort and expose certain degree of originality, may be protected by IP rights, most likely copyrights. Processing of content, protected by IP rights on digital media, including software applications, such as by copying, storage, display, transmission, making the content available to the public constitutes a copyright relevant action and requires authorization of the right holder.

The aspect, that the MHA platform may store some user generated content, which may be protected by IP rights, and the rules for third party developers how to deal with such content on their services are covered in Section 7 API Terms of Use.

As with the user´s data, MHA allows use of MHA API for sharing the user´s data on external apps, but does not grant the right on use of the user generated content to a third party developer. Therefore, a third party developer, who intends to share the MHA user´s data with MHA and display the MHA user´s data on its services, is required to get the publishing permission from the user on his own.

5.5.6. Warranty and liability

The provisions, addressed to cover liability issues associated with the use of MHA API on an external app, are set out in Section 10 API Terms of Use. The legal requirements surrounding the use of MHA data from data protection perspective are described in Section 3 above. The MHA API has been developed in a research project and has not undergone sufficient testing to prove workable and ready to use on external apps. Against this development background, MHA is not in a position to ensure proper functioning of MHA API on external apps. Therefore, for the early stage of MHA release, it is suggested to offer and expressly declare to the developers that MHA API is provided in its "Beta version". Express declaration that the MHA API is provided in its Beta version to the developers, who are familiar with the state of software being in "Beta version", is aimed to restrict the liability of MHA regardless of negligence or fault for defects, which the developers may reveal when using the MHA API, excluding those which may be present in the API at the moment of its hand-over[193]. This will be relevant to the liability risks described in Section 5. In order to improve and bring the MHA API to a proper functioning state, the developers are invited to notify MHA of the errors, which they reveal. Upon request, the MHA should be ready to fix the errors in reasonable time.

5.5.7. Duration and termination

The duration and termination of MHA license agreement are governed in Section 11 API Terms of Use.

The API license agreement comes into effect when a developer creates his MHA account and accepts the terms of use of MyHealthAvatar API and shall last until terminated by MHA of by a developer. A developer may terminate the agreement at any time by ceasing his use of MHA API or by deleting his account. MHA may suspend, if necessary, revoke the rights and terminate the use of API and API license agreement if MHA has grounds to believe that a developer violated the MHA API terms of use or engaged in fraudulent activity which may cause liability to MyHealthAvatar. MyHealthAvatar may also terminate the agreement upon 30 days' prior notice to a developer.

Upon termination of the agreement, a developer is requested to cease his use of and to delete to the extent technically possible MHA API, MHA data and any other materials and information related to the use of MHA API.

5.5.8. Rules for processing IP protected content on MHA services

As stated in Section 5.5.5. above, the MHA platform allows users to upload certain content on MHA services, which may be protected by IP rights, most likely copyrights. Processing of such IP content on digital services constitutes a copyright relevant action and requires authorization of the right holder.

This aspect is addressed in the extended MHA General Terms and Conditions, Annex 4, Section VIII. Accordingly, when a user submits certain IP protected content to MHA, he

[193] Thomas Hoeren, "IT Vertragsrecht", 2. Auflage, Verlag Otto Schmidt, Köln, 2012.

grants to MHA a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to process such content on its services in the scope as needed and for so long as needed for MyHealthAvatar to provide its Services.

A user, who uploads certain IP protected content on its services, is expected and is advised to have, and if necessary to obtain, the rights on use of the content which a user places in his account in MHA.

According to the EU law, Article 15 Directive on electronic commerce[194], a provider of service to transmit and host information, submitted by its users, who does not initiate and does not interfere with such information, should not have a general obligation to monitor such information nor actively seek facts or circumstances indicating illegal activity. Also, a service provider should not be liable for the information, processed on its services on behalf of the users, unless (a) a provider has actual knowledge of such illegal activity or information or circumstances indicating IP violations and (b) upon getting such knowledge, takes operative measures to remove or to disable access to such information. The MHA, acting as a service provider under the said directive, should also be covered by these rules.

In order to ensure that MHA may enjoy the position of an intermediary service provider, as provided by the directive, the "notice and take down" IP infringement policy is implemented in Section XI MHA General Terms and Conditions.

Accordingly, users, who have indicators of IP infringements on the MHA platform, are asked to notify MHA and provide supporting materials. Thus, a user, claiming copyright infringement, is asked to state an identity of the copyright owner, provide a copy of a copyright work alleged to be infringed and a copy of infringing materials, specify why use of a work is not authorized, indicate his contact details and prove his authority to represent the copyright owner.

Upon getting such notification and verifying materials proving the fact of illegal activity or information taking place on MHA services, MHA commits to take operative measures to remove or to disable access to such content.

5.6. Collaboration with the CHIC Project

This section describes the legal framework, which was set up to establish the collaboration between MHA with another FP7 research project CHIC, and defines the rules of this collaboration.

Connecting the avatar to external data/model warehouses, as provided by the DOW, WP3, T. 3.4, p. 11 of 40, is a key part of demonstrating the MHA platform's exploitation potential. This is being achieved by linking the MHA platform to another FP7 project CHIC and using the CHIC data repository for running oncosimulations in MyHealthAvatar. The IPR

[194] DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJEC, 17.7.2000, L 178/1; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML.

implications, which may arise and need to be handled in the scope of the said collaboration, were analysed and described in D.11.3, section 4.

The MyHealthAvatar project intends to demonstrate the utility of the MyHealthAvatar platform by allowing its users to perform oncosimulations of Nephroblastoma with the use of clinical data. The MHA decided to complete this endeavor with the use of the CHIC data repository.

The CHIC project, full title "Computational Horizons In Cancer (CHIC): Developing Meta- and Hyper-Multiscale Models and Repositories for In Silico Oncology" is engaged in the development of clinical trial driven tools, services and secure infrastructure that will support the creation of multiscale cancer hyper-models (integrative models). [195] As part of its work, the CHIC project has developed a clinical data repository that provides for a secure storage of clinical data, incl. imaging data, histological data, therapy, etc. The data types hosted by the repository include: imaging data (DICOM, etc), descriptive/structural data (age, sex, etc), other files (histological reports), links (to other data repositories), etc.

The workflow of this Nephroblastoma use case consists of the following steps:

(i) The MyHealthAvatar project will generate synthetic clinical data for running Nephroblastoma oncosimulations in MyHealthAvatar.

(ii) The CHIC project will create a section in the CHIC data repository specifically designated and restricted to MyHealthAvatar and will provide application programming interfaces (access API) to access the repository for upload and retrieval of data to MyHealthAvatar.

(iii) The CHIC project will generate an account for MyHealthAvatar in its clinical data repository and will provide account credentials to MyHealthAvatar. The MHA Parties will use these account credentials for logging in into the CHIC data repository in order to place and retrieve their data. In the process, the MHA Parties will not have access to any CHIC data located in the CHIC data repository, but only to their own synthetic data.

(iv) The MyHealthAvatar project will connect to the repository via the repository access API and will place its synthetic data into the repository section designated to MyHealthAvatar.

(v) An MHA Party, wishing to run Nephroblastoma oncosimulations in MyHealthAvatar, will log in into the CHIC data repository, select the data needed for the execution of the Nephroblastoma model and send a request to the Nephroblastoma oncosimulator to run.

(vi) Once the Nephroblastoma oncosimulator receives the request to run, the Nephroblastoma oncosimulator application will connect to the CHIC data repository via the repository access API and will fetch the data needed for the execution of the Nephroblastoma model.

(vii) The CHIC data repository will provide the data.

(viii) The Nephroblastoma oncosimulator will execute the model and send the output of execution to MyHealthAvatar using MyHealthAvatar platform API.

[195] CHIC; Project Summary, http://chic-vph.eu/project/.

(ix) Results generated by execution of the Nehproblastoma model will be saved back to the MyHealthAvatar platform.

The collaboration between the two projects, which enabled the linkage and use of the CHIC data repository in MyHealthAvatar, and the rules of collaboration were defined by contractual framework, specifically elaborated for this.

The contractual framework for the CHIC-MHA collaboration consists of the two agreements:

(a) the Memorandum of Understanding, the upper level agreement, by virtue of which the collaboration was established, and

(b) the Collaboration Agreement, the lower level agreement, signed on the premises of the said Memorandum, where the rules and access rights needed for collaboration were defined.

5.6.1. CHIC-MHA Memorandum of Understanding

The Memorandum of Understanding (in short "the Memorandum", abbreviated to "MoU") constitutes a legal document, on the basis of which the collaboration between the CHIC and MHA projects was established.

The coordinators of the collaborating projects: Prof. Georgios Stamatakos, ICCS-NTUA, Coordinator of CHIC, and Prof. Feng Dong, University of Bedfordshire, Coordinator of MHA, established the collaboration as of 12 January 2016. The Memorandum is included in this deliverable as Annex 7.

The Memorandum identified the scope of collaboration, the intended activities, the legal framework, within which the collaboration shall be conducted. The collaboration is done within the EU FP7 legal framework, consisting of application of the respective Grant Agreement no. 6000841 for CHIC and no. 600929 MyHealthAvatar and application of the respective Consortium Agreements of CHIC and MyHealthAvatar.

The areas of collaboration include, in particular, sharing of knowledge and data that advance the mutual interest of the projects, dissemination of results of collaboration, the shared use of infrastructure developed by each project in accordance with each project's policies and procedures. Through these intended activities MyHealthAvatar envisages to demonstrate the utility of its platform by allowing its users to perform oncosimulations with the use of medical data. CHIC proposes to grant access to its data repository to host the medical data of a synthetic patient for MyHealthAvatar.

The terms on which the collaboration should occur, including the access rights to be granted, is regulated in a separate CHIC-MHA collaboration agreement, signed between the projects. The basic rules, defined by the CHIC-MHA collaboration agreement and the terms on the grant of access rights are described below.

5.6.2. CHIC-MHA Collaboration Agreement

The CHIC –MHA Collaboration Agreement governs the terms on which the CHIC project grants to MHA project the rights on use of the CHIC data repository, associated infrastructure and components as needed for implementing the MyHealthAvatar project.

On the part of CHIC, the Agreement is signed by the parties, whose components or infrastructure will be used in MyHealthAvatar. These signatory parties are:

- UBERN, owner of rights in the CHIC data repository,
- ICCS, project coordinator and owner of rights in supporting services,
- FORTH, which provides infrastructure for hosting the CHIC data repository.

On part of MHA, the signatory parties are those MHA parties who need to have access to the CHIC data repository for implementation of the MyHealthAvatar project. The MHA parties include: ICCS, USAAR, BED, FORTH, TEI-C.

The Collaboration Agreement was agreed by the parties in its version 5 of 18 January 2016 and has been passed into the signing cycle. It is attached to this Deliverable in its word format as Annex 8.

The terms of the CHIC-MHA Collaboration Agreement are laid down under the legal framework, in compliance and on the premises of the EU FP7 contractual rules, i.e. the Grant Agreement and Consortium Agreement, applicable to the projects. In particular, the Agreement defines which CHIC components need to be used in MyHealthAvatar, which CHIC parties own the rights and on what terms they grant the access rights in those components to MyHealthAvatar. It also sets out the scope of use and defines the security rules, which both CHIC and MHA parties need to observe for secure transfer of data.

On the terms of the Collaboration Agreement, the CHIC parties grant to MHA parties Access Rights to the CHIC data repository, associated infrastructure and components as needed for implementation of MyHealthAvatar. In particular, such Access Rights include the rights to:

(a) access and use the CHIC data repository, in the section dedicated to MyHealthAvatar, and the repository access API for upload, storage and retrieval of data in MyHealthAvatar;

(b) access the CHIC IT infrastructure in order to access and use the CHIC data repository;

(c) permit officers and employees of the MHA parties to access and use the CHIC data repository, associated infrastructure and components for realization of rights, granted to the MHA parties above.

These rights are granted on a non-exclusive, worldwide, royalty free, non-assignable and non-transferable basis without the right to sublicense. The scope of use is limited to implementation of MHA project.

The rights are granted for the term of CHIC-MHA Collaboration, which upon the suggestion and agreement of the parties has been linked to the term of the CHIC project. This term of collaboration may be needed to demonstrate linkage between the projects, not only on part of MyHealthAvatar, but also on part of CHIC and to support the sustainability and initial exploitation of the MHA platform.

As regards the data needed for running oncosimulations in MyHealthAvatar and hosted in the CHIC data repository, this data will be artificially generated by the MyHealthAvatar project itself. This data will have the quality of synthetic data and thus not implicate the data protection rules (applicable in respect of real personal data). Access Rights and use of

this data in MyHealthAvatar is governed by the rules on Access Rights under Section 4 of MyHealthAvatar Collaboration Agreement.

The access of MHA parties to the CHIC infrastructure will be handled via a local account on the data repository, which will be opened for MHA by CHIC. By this means, the MHA parties, in order to access their data, would not need to pass through the overall security level of CHIC. CHIC will provide the secure interface and account credentials to MHA, by means of which the MHA parties will be able to log in into the CHIC data repository and use the MHA data.

As regards the access rights to the CHIC data repository, as noted in the description of collaboration and the workflow, the access of MHA to the CHIC data repository will be limited to one section only, which will be specifically organized for MHA. According to Section 5 of the Collaboration Agreement, UBERN grants the MHA parties Access Rights to the CHIC data repository and application programming interfaces (access API) to access the repository, upload, download, store and retrieve data for MyHealthAvatar. Also, UBERN agrees to assist the MHA parties in setting up and/or implementing the data upload/download.

The CHIC data repository is deployed in the private cloud infrastructure provided by FORTH. FORTH, in Section 6 of the Collaboration Agreement, agrees to support the needs of the MyHealthAvatar project in using the clinical data repository from CHIC, and agrees to provide additional resources as may be needed for hosting MyHealthAvatar data in the CHIC data repository to the extent reasonably achievable with its available resources.

The oncosimulator, which will be used in MHA, is the "Wilms Tumour Oncosimulator Hypomodel", defined as "*an integrated software system simulating the growth of nephroblastoma tumours and their in vivo response to chemotherapeutic modalities within the clinical trials environment*"[196]. Originally developed by ICCS (Georgiadi et al., 2012; Stamatakos et al., 2011), the Nephroblastoma oncosimulator was brought by ICCS, being a party to both collaborating projects, as its background to both CHIC and MyHealthAvatar. Access Rights and use of the Nephroblastoma oncosimulator and its application in MyHealthAvatar are governed by the rules on Access Rights set out by Section 7 MyHealthAvatar Collaboration Agreement.

Although, as noted, the data does not have the quality of personal data, data security remains an important aspect in the collaboration (and will function as a testbed for the technical and organizational safeguards required in the exploitation phase). This aspect is addressed in the Collaboration Agreement, Section 9, which states that data transfer from CHIC to MHA should occur via a secure interface, provided by UBERN. The MHA Parties shall keep the credentials and identification information for the MyHealthAvatar account in CHIC data repository secure and confidential and take measures to protect the credentials from unauthorized access and use by third parties. UBERN may disconnect access of the MHA parties to the CHIC data repository if there are reasonable grounds to suspect that the MyHealthAvatar account is being used in a fraudulent or negligent manner which may cause liability for CHIC.

[196] CHIC Deliverable D6.2 – CHIC cancer component models: initial tested versions, W2, p.143.

Both the CHIC and the MHA parties agree to implement adequate Internet security measures, including state of the art data encryption, to ensure secure transfer of data in compliance with Internet governance and applicable laws.

6. Conclusion

The exploitation phase is the culmination of the project. Even though MyHealthAvatar was foreseen as a feasibility study, the project has developed an impressive platform that can serve as the basis for a successful exploitation. In particular the API is a vehicle to increase the user base of the platform. Users will typically already be on Facebook, Twitter or other social networks, and wearables such as Fitbit and Withings are increasingly popular. By allowing the platform to connect to Third Party services greatly increase its attractiveness. Lifestyle data such as steps walked and calories burned can be quickly imported into the platform, serving as a foundation on which to build one's avatar.

Technical features are, however, not a guarantee for success. As the Betamax/VHS battle showed, adoption by users is influenced by a wide variety of factors beyond the mere technical. Especially in today's world, where privacy breaches are becoming ever more common and devastating – the Ashley Madison hack is a prime example – user privacy – data protection – is a "feature" that cannot be underestimated. User confidence in a product or service will depend to a great extent on both the legal and technical. In the deliverable, we highlight both legal and technical measures that should be adopted in order to secure user confidence in the platform.

Assessing liability risks is difficult due to the novelty of the developments in e-health, the multitude of parties as well as transborder processes involved. As it is envisaged that MHA, will support and/or interact with a multiplicity of third party apps, scenarios may arise where the platform's responsibilities are hard to demarcate from those of the app developers.

Finally, we also provided solid guidance on the intellectual property questions that would arise during the exploitation of the platform. We provided a robust API License Agreement that not only addresses intellectual property issues, but also guarantees the privacy of its users. Adherence to these should help minimize the risks of legal impediments to the commercial exploitation of the platform.

7. References

Alheit K (2001): The applicability of the EU Product Liability Directive to software, The Comparative and International Law Journal, vol. 34, no. 2, 188-209

Cheng Y, Park J, Sandhu R (2013): Preserving user privacy from third-party applications in online social networks, In Proceedings of the 22nd International Conference on World Wide Web (WWW '13 Companion), 723-728

Conrad I, Schultze-Melling J (2011): Beck'sches Mandats Handbuch IT-Recht, München: C.H. Beck Verlag

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

Hoeren T (2014): IT-Recht

Jasmontaite T, De Hert P, (2015): The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet

Kardasiadou Z (1998): Die Produkthaftung für fehlerhafte medizinische Expertensysteme, Baden-Baden: Nomos.

Kizza J (2010): Ethical and social issues in the information age, London: Springer

Kondylakis H, Spanakis E G, Sfakianakis S G, Sakkalis V, Tsiknakis M N, Marias K, Zhao X, Yu H Q, Dong F (2015): Digital Patient: Personalized and Translational Data Management through the MyHealthAvatar EU Project. International Conference of the IEEE Engineering in Medicine and Biology Society of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy.

Lloyd I (2008): Information Technology Law, Oxford: Oxford University Press

Marly J (2014): Praxishandbuch Softwarerecht – Rechtsschutz und Vertragsgestaltung, München: C.H. Beck

Maule M (1992): Applying Strict Products Liability to Computer Software, Tulsa Law Review, vol. 27, no. 4, 735-756

Oetker H (2016): in: F. Säcker, R. Rixecker, H. Oetker, B. Limperg (eds.), Münchener Kommentar zum BGB, München: C.H. Beck

Pedroni J, Pimple K (2001): A Brief Introduction to Informed Consent in Research with Human Subjects

Rowland D. Kohl U, Charlesworth, A (2012): Information Technology Law, Oxon: Routledge

Vihul L (2014): The liability of software manufacturers for defective products, The Tallin Papers 2014, vol. 1, 1-14

Spindler, G (1998): Verschuldensunabhängige Haftung im Internet, MMR, 119-124

Straub W (2002): Produktehaftung für Informationstechnologiefehler – EU-Produkthaftungsrichtlinie und schweizerisches Produktehaftungsgesetz, Studien zum Verbraucherrecht Band 7, Zürich: Schulthess

Wagner G (2013): in: M. Habersack (ed.), Münchener Kommentar zum BGB, Section 4 ProdukthaftG, München: C.H.Beck

Wang N, Xu H, Grossklags J (2011): Third-party apps on Facebook: privacy and the illusion of control. In Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT '11). ACM, New York, NY, USA

8. Appendix – Abbreviations and Acronyms

Acronym	Title
AGPL	GNU Affero General Public License Version 3.0
(A)(L)GPL v3+	GPL version 3 or any later version
ANS	AnSmart
Apache v2	Apache License Version 2.0
API	Application Programming Interface
ASF	Apache Software Foundation
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
BED	University of Bedfordshire
BSD 3-Clause-License	Berkeley Software Distribution License
CDDL	Common Development and Distribution License
CHF	Congestive Heart Failure
CHIC	Computational Horizons in Cancer
CPL	Common Public License
DPD	Data Protection Directive
DRM	Digital Rights Management
EC	European Community
EPL	Eclipse Public License Version 1.0
epSOS	European Patients Smart Open Services
EU	European Union

FAQ	Frequently Asked Questions
FORTH	Foundation for Research and Technology Hellas
FSF	Free Software Foundation
GDPR	General Data Protection Regulation
GNU	GNU's Not Unix
GPL	General Public License
GPL´d	GPL licensed
HIS	Hospital Information System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over Secure Socket Layer
ICCS	Institute of Communications and Computer Systems
IP	Intellectual Property
IPR	Intellectual Property Right(s)
LGPL	GNU Lesser General Public License
LUH	Leibniz Universität Hannover
MHA	MyHealthAvatar
MIT	MIT License
MPL	Mozilla Public License
PSF	Python Software Foundation License
OSI	Open Source Initiative
UK	United Kingdom
V1/2/3	Version 1/2/3

v3+	Version 3 or any later version
V3(+)	Version 3 (or any later version)
W3C	W3C SOFTWARE NOTICE AND LICENSE

9. Annexes

Annex 1: E-consent form

NOTICE:

At present the platform remains subject to ongoing testing and evaluation; and your, the user's, experience in making use of it and telling us what features you find more, and which less, useful, is an essential part!

At this time, it does not matter if the data you provide about yourself is accurate or not - it is fine for you to 'role play' by entering made-up data and considering in what respects, if you were the person to whom the data applied, you would find the platform's features and functions helpful. Please note, though, that we can only send you the Terms and Conditions, Privacy Policy and the consent form below if you submit a real email address.

CONSENT:

I declare my agreement to the processing of the (personal) data I provide (including health and life-style data, whether real or not) by the MyHealthAvatar private demo platform for evaluation purposes.

I have read, I understand and I agree to the <Terms and Conditions> and <Privacy Policy> which form a part of this declaration. I understand that the Terms and Conditions, Privacy Policy and this consent form will be sent to my email address (if I do not submit a fake email address).

Please click the following checkbox to confirm that you have read, understood and agree to the <Terms and Conditions> and <Privacy Policy> and that you give consent to the processing of your health and lifestyle data you provide for the evaluation of the MyHealthAvatar Platform.

Annex 2: General Terms and Conditions for testing phase

Thank you for testing the MyHealthAvatar platform!
To access and use the MyHealthAvatar Platform ("the Platform"), you will need to register with the Platform and become a member. When doing so, you will be asked to tick a box by which you confirm that you have read and understood both the following *General Terms and Conditions* and the <Privacy Policy>. The documents also include a number of warranties that relate to your own legally compliant use of the platform.
You may address any questions about the Platform or your registration to mha@ccgv.org.uk.

General Terms and Conditions

I. General Information

These Terms constitute an agreement between yourself as a registered user of MyHealthAvatar [www.myhealthavatar.eu] and the MyHealthAvatar project, composed of parties to the MyHealthAvatar Consortium, namely:

- University of Bedfordshire, the Coordinator (short name: BED)
- Foundation for Research and Technology – Hellas (short name: FORTH)
- Universität des Saarlandes (short name: USAAR)
- Institute of Communication and Computer Systems (short name: ICCS)
- Gottfried Wilhelm Leibniz Universität Hannover (short name: LUH)
- Larkbio
- AnSmart, Ltd (short name: ANS)
- Technological Educational Institute of Crete (short name: TEI-C)
- University of Lincoln (short name: LIN)

The Consortium is represented by the project's lead partner, the University of Bedforshire, England. Questions and comments may be addressed to the MyHealthAvatar coordinator Professor Feng Dong (mha@ccgv.org.uk).
By registering for an account and/or using MyHealthAvatar services you signify that you agree to these Terms and Conditions. MyHealthAvatar services consist of online and mobile services, including, but not limited to: MyHealthAvatar internet platform, software, an app developed by the Project to collect and access data that are stored at the platform and Third Party apps (Fitbit, Withings, Moves, Twitter) that you can link with your MyHealthAvatar account ("Services").

II. Purpose of MyHealthAvatar

MyHealthAvatar is a non-profit research project to study how technologies are able to help patients and citizens look after their own health and wellbeing. It aims to provide a proof-of-concept solution for the collection, access, 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 MyHealthAvatar will be valuable for clinical decisions concerning your care, in helping you to best manage your own health and lifestyle.

MyHealthAvatar will collect and store your data provided by you either through the sensors linked to MyHelathAvatar, or through the user interface of the system. The intelligent data analysis software in MyHealthAvtar will then:

- organise and display your data in a professionally designed layout with graphical illustrations to facilitate your understanding.
- work out your locations and movements on a daily basis to help you inform yourself about your past events and experience.
- calculate your risks to long term diseases using the established medical models.
- allow you to share your information with friends through social media (currently through Twitter).

The data will be stored in the public cloud server Linode, based in London and rented by ANS.

III. Eligibility for Membership

In order to register to use the Platform, you must be aged 16 years or above. By signing up to the Platform you confirm that you are aged 16 or above.
Organizations, companies, and businesses may not register with the Platform.

IV. Functionalities of MyHealthAvatar and Use of Content

The following are the main intended functions of the Platform:
- A sign in page to sign in or to sign up for your personal account in MyHealthAvatar.
- A dashboard with the following functionalities:

- a general overview of your automatically calculated health risks (including hypertension risk, diabetes risk, cardiovascular disease risk, stroke risk; please note that this functionality is for informational and research purpose only and does not replace any medical advice) and a health score
- You can also allow your browser using your computer's location to display location-related information like weather and town.

Moreover, you can see

- your walking distance and step counts in summary,
- your overall duration of activities and calories consumption,
- your transport duration and distance in summary,
- your location on Google map (if you choose to share your location),
- your activities and life patterns described via a timeline (Activity Stack", "24hour Activities", "Activity Cloud", "Activity Bubbles", "Movement - Place") and
- your activity durations.

You can also allow your browser using your computer's location to display location-related information like weather and town.

- A diary/journal that allows you to collect, store and show data such as data concerning walking, transport, running, cycling, calories, diet, mood and blood pressure. You can also show data concerning the history of your locations and activities acquired from location methods such as GPS, AGPS and wifi locations. The locations and activities include home, work, shopping, restaurant, transport, healthcare, sports, entertainment, hotel, public service, friend's home, children's school using a map together with a clockview for

visualising time information of the activities. The diary includes an event planner in which you can enter data via the "Event Table". Moreover, the diary gives you an overview of your Fitbit, Withings and Moves statuses.

- A LifeTracker that involves most of the functionalities of the diary/journal. The LifeTracker allows you to explore your daily activities and life patterns. You can choose between 13 categories of data (home, work, shopping, restaurant, transport, healthcare, sports, entertainment, hotel, public service, friend's home, children's school, unknown) to map all the locations and activities.

The LifeTracker includes

- a **multi layer timeline** that includes the layers year, month and day and represents the time at different scales.
- a **life pattern** that shows you your individual life patterns on an hourly basis at different levels of timescales. It can filter, highlight, and show specific daily activities. You can switch between the month mode that shows all days of a selected month, the year mode that shows the month summary of a selected year, and the long mode that shows the year summary in a selected year.
- a **chart view** that shows you the change of data such as duration of walking, running, cycling, transportation, and also calories consumption during the selected period of time
- during the selected period of time by using histograms and curves.
- a **key event list** that displays all the key events in a form of list with the ability of sorting by date, time, name, and category.
- a **key calendar** that shows you day summary information in colour, together with any key events that occurred on the day.
- a **statistics list** that shows you your statistics concerning the collected data.
- a **life map** that shows you daily activities and locations of the key events geographically via colour coded path lines, heatmap, glyphs, and interaction. These data are acquired from location methods such as GPS, AGPS and wifi locations.

- A toolbox that includes the following services for informational, educational and research purposes:

- Risk calculator for cardiovascular disease (10-year risk), hypertension (1, 2, 4-year risk), diabetes (8-year risk) and a stroke (10-year risk);
- Upload and view functionality for medical images;
- Functionality to order and present uploaded clinical data according to different categories (all clinical data, vital signs, drugs, medical images) and dates (today, this month, last month, this year, last year; chosen start and end date).
- Functionality to import your profile from IndivoX.
- Semantic search functionality to allow you to search for certified medical information related to the disease of interest for your health literacy.
- Simulation of a nephroblastoma (Wilms Tumour) Oncosimulator. With the Nephroblastoma Educational Tool you can specify a treatment scheme and see the

Tumor Volume Evolution over Time. This service is for informational, educational and research purposes only and does not replace any medical advice.

None of the functionalities of the toolbox are intended for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease. For more information, please see Section XIV (Medical advice disclaimer).

- A help button that you can click on to see different tutorial videos and help documents.

- A data sharing interface that will allow you to share different data with your friends and/or created groups, e.g. the diabetes and other program progress), food, drink and calories, event plans and activities.

- The MyHealthAvatar mobile app that helps you to access your data that is stored in the Platform from your mobile phone. Please note that you need an android based smartphone to install the MyHealthAvatar app. Before installing the app, the app will ask you to authorise the following functionalities:

- to read and access accounts, contacts and contact details,
- to determine the location of your mobile phone by using GPS, AGPS and wifi locations*
- to read, change, and delete memory contents of USB,
- to retrieve information from the internet,
- to access all networks,
- to use the camera of your mobile phone to take photos and record videos*

*You can disable this functionality later in the mobile setting. The app will only make use of its authorisation while using this functionality.

Please do only download and install the MyHealthAvatar app, if you agree with his.

- Application connections with Third Party apps allowing the sharing of your data as supported by these services.
In order to use the functions of MyHealthAvatar to its full extent, you will need to upload personal data. For the testing phase, you may prefer to submit fake data (i.e. information you make up about yourself), rather than real data. At this stage, this will already allow you to test the broad functioning of the Platform and provide the project with valuable insights and feedback. Insofar as you do provide your real data, the use of this is outlined in the Platform's Privacy Policy.

Your data may be stored in the following profiles, which represent categories of data: You may choose which of the possible elements you would like to submit to the Platform:

- General Profile
  Email, gender, birthday, state/county, country, ethnicity, qualification, weight, height, glucose, total cholesterol, HDL cholesterol, triglyceride, diastolic blood pressure, systolic blood pressure, pulse

- Health Profile
  Smoking, Alcohol, Diabetes, Parental Diabetes, Parental Hypertension, Prior Cardiovascular, Physical Activity, Mood, Social Engagement, Entertainment
- Medical Profile
  Care Provider (name, address, phone number), Immunisations (name, description, date given), Allergies (name, description), Problem and History
- Profile Overview
  Patient Profile, Medical History, Medical History Snapshot, Medications Summary and Schedule

- As a motivation for yourself, you may enter freely definable daily goals such as targeted number of steps, distance, active minutes, calories burned, body weight, BMI, systolic blood pressures, diastolic blood pressures.

- There is also a 3D Avatar representing an overall interactive anatomy model. The human anatomy model set can be explored by selecting different buttons from the toolbar. Depending on the adjustment of the toolbox, the anatomy model will be presented in different aspects. For instance, the anatomy model can be represented semi-transparent meaning that internal organs can be presented non-transparent whereas the rest of the model is transparent. Another example is that you can click on specific parts of the model and zoom it.

- Moreover, you may answer a questionnaire on your Quality-of-Life (QOL), and also a patient questionnaire to help your doctors keep track of how you are feeling.

- For the testing/evaluation phase, you will also be asked to answer questionnaires about the different aspects of the Platform and the MyHealthAvatar mobile app, including the toolbox, the signing up and setting, the diary, and the data collection and visualisation.

V. Your rights to use MyHealthAvatar Services

MyHealthAvatar grants you a personal, worldwide, royalty free, non-assignable, non-exclusive license to use MyHealthAvatar Services for the purpose, to the extent and for so long as the Services are provided to you under these Terms.
All rights, title, copyrights, and interest in MyHealthAvatar Services (excluding user generated content) are reserved and owned by MyHealthAvatar parties. The Services are protected by copyright and other applicable laws.

VI. Entitlement to Terms and Conditions of MyHealthAvatar

As noted, while the Platform is still subject to testing and evaluation, we would suggest that you submit fake data. However, we recommend that you use your real email address so that we can inform you in case of the need for a re-consent due to a change to the General Terms and Conditions and/or the Privacy Policy.

VII. Restrictions on upload of data

You warrant not to upload to the Platform any personally identifiable information about a Third Party unless you have their written and explicit consent to do so. In case of diseases with a strong and direct hereditary component, you warrant that you have obtained the explicit permission of your family members before uploading information that are related to such diseases. In case you are unsure about the hereditary nature of a given condition, please ask your physician.

You further warrant that you have the right to use, copy, display, perform, transmit and distribute any uploaded data.

MyHealthAvatar reserves the right to delete uploaded data that does not fulfil the above-mentioned requirements.

VIII. User generated content

You also agree that you have and/or have obtained all necessary intellectual property rights (IPR) required to allow posting, communicating, transmitting, using, copying, displaying, performing, distributing any IPR Content submitted to the Services by you.
All user generated content made available on MyHealthAvatar Services is the responsibility of the user who originated such content. MyHealthAvatar does not monitor the content made available on its Services by the users and does not accept any responsibility for such content, unless MyHealthAvatar has obtained knowledge or awareness of illegal activity or content on its Services. If you use and/or rely upon any user generated content transmitted via the Services, you do so at your own risk.

IX. Third Party services

MyHealthAvatar allows connections to Third Party services, and may provide links or references to websites, services and/or apps operated by third parties, in particular: Fitbit, Withings, Moves and Twitter. MyHealthAvatar neither monitors nor investigates such websites and is not responsible for the content, functionality, or practices of Third Party services. If you decide to access such Third Party services, you do so at your own risk. By agreeing to share your MyHealthAvatar data, information or content with Third Party services, you understand and agree that use of such data, information or content by Third Party services is governed by those Third Parties´ terms of use and privacy policies. MyHealthAvatar recommends that you read the terms of use and privacy policies (if any) on those Third Party services. You agree that MyHealthAvatar has no liability for any damage or loss of any kind that results from your use of a third party service.

X. Member Notices

By signing up to use the MyHealthAvatar Services, you agree that MyHealthAvatar may send you any necessary communication about the Platform by using your email address.

XI. Termination of Membership

MyHealthAvatar has the right to terminate your membership immediately for what it in its reasonable discretion considers to be a significant violation of any of these terms.

XII. Modifications to these Terms
MyHealthAvatar may modify these Terms in part, at any time and without prejudice to the validity of the other provisions. In such a case you will be notified by email, and asked to re-consent to your continuing membership.

XIII. Applicable law
These Terms are governed by English law.

XIV. Medical advice disclaimer
For the evaluation of the Platform, we would suggest that you submit made-up health data and focus on the usability and potential benefits offered by the Platform features and services to different categories of patients and citizens.

However, insofar as you submit real data this fact, plus your use and access of the Platform, will not in any event create a physician-patient relationship between you and the operator of the Platform.

The Platform and the MyHealthAvatar App do not offer medical advice and are not medical devices.

All material, information, content and Services (particularly the toolbox to calculate your risk of suffering from diseases, the Clinical Data functionality, the Medical Images Upload and View, the Nephroblastoma Educational and Semantic Search) are provided for informational, educational and research purposes only. They are not intended as a substitute for professional medical advice, diagnosis, prevention, monitoring, treatment or alleviation of disease. No medical decision should be based on anything coming from the Platform or App.

Please consult your physician or other qualified health care providers if you have any questions about your health, a medical condition, taking drugs, or possible courses of treatment.

Do not ignore professional medical advice or delay in seeking it because of information you obtained through the Platform.

MyHealthAvatar neither endorses nor assumes responsibility (whether tortious or contractual) for any advice given or information referred to on the Platform, including certain physicians, procedures, drugs or other information that may be mentioned.

XV. End of Project
The MyHealthAvatar project will end on 28.02.2016. All the data you have uploaded will be deleted by May 31, 2016.

In the event that we wish to use your data after the end of the project for the possible continuance of MyHealthAvatar or for another related project, we will inform you by email of the details and ask you for fresh consent to the continued use of your data before May 31, 2016. If we cannot reach you or if you decline to provide new consent, your data will be deleted by May 31, 2016.

Annex 3: Privacy Policy for testing phase

Privacy Policy

This Privacy Policy constitutes an agreement between yourself as a registered user of the MyHealthAvatar Platform ("the Platform") and the MyHealthAvatar project [www.myhealthavatar.eu], represented by the project lead partner, the University of Bedfordshire, England. Questions and comments may be directed to the project coordinator, Professor Feng Dong (mha@ccgv.org.uk)

I. General Information

This Privacy Policy describes

- your rights regarding the processing of your personal data
- how your personal data is protected by security measures,
- information about the circumstances in which your personal data may be shared with other users or third parties, and
- how to delete your personal data from MyHealthAvatar.

This Privacy Policy is necessary because the use of the MyHealthAvatar platform entails the submission of personal data. **Any data submitted will be processed by the Platform.**
Consequently, the registration process entails giving your consent to the processing of your data by the operator of MyHealthAvatar, as specified in the General Terms and Conditions.
Other information that will be collected to help operate and improve the service refers to how you interact with our services, including the browser that you're using, your IP address, location, cookies or other unique IDs, the pages that you visit and features that you use. We combine this with other users' information to get an overall view of how the service is used.
Your data will not be processed for any other purposes than mentioned in the Policy and to which you consent to.
You may withdraw your consent at any time without any disadvantages. In this case, any and all data that you uploaded to the platform will be permanently deleted as laid out in Sections VI and VII.

II. Registration

The registration process requires your name or a pseudonym and your email address. All such data may be fake for the present purposes of Platform evaluation. However, we recommend using a real email address, so we can ask for re-consent in case of any updates of the General Terms and Conditions and/or Privacy Policy.

III. Sharing your personal data via MyHealthAvatar Platform

You will be able to share your lifestyle data with other users of the Platform.
These are the main types of data you can share with your invited friends: diabetes and other program progress, food, drink and calories, events and activities. You are free to choose what types of data you would like to share and with whom. Other users of the Platform will only be able to access your data after you connect with them as "friends". You can create groups with your "friends" and share the selected data you would like to share within the created group, but also share the selected data with a single "friend". You can dissolve "friends" as well as delete groups created by you at any time.

IV. Security measures to protect your data

We are aware that the data you choose to upload can be highly sensitive. State-of-the-art security measures are incorporated into the Platform to protect your data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse.

At the moment (during the ongoing evaluation and demonstration of the Platform by the MyHealthAvatar project), unless you opt to share your data with other users of the Platform, the institutions participating in the MyHealthAvatar project are the only entities that have access to your uploaded data. Other users of the Platform will only be able to access your data after you connect with them as "friends" and only after you have selected the data you would like to share.

All data that you collect and store in the Platform may be currently used by the following institutions participating in the MyHealthAvatar project: BED, FORTH, ICCS, ANS, TEI-C and LIN. The addresses and further details of these each institutions may be found on the project website [www.myhealthavatar.eu]. As noted in the Terms and Conditions, the data will be stored in the public cloud server Linode, based in London and rented by ANS.

V. Your rights regarding the processing of your personal data

You retain at all times your full rights as a data subject under the EU Data Protection Directive (as implemented into UK law by the Data Protection Act 1998), as follows. You may contact the coordinator of the MyHealthAvatar project, Prof. Feng Dong, in order to exercise any of your rights: mha@ccgv.org.uk

1. Right to information

You have the right to inform yourself about the identity of the data controller and of the controller's representatives, if any.

The data controller is the University of Bedfordshire, represented by Prof. Feng Dong, the coordinator of the MyHealthAvatar project.

You have the right to inform yourself about the purposes of the processing and about the recipients of the data.

2. Right of access, rectification, erasure or blocking

At any time, you may check your 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 according to the conditions set out in Sections VI and VII of this Privacy Policy.

3. 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 Platform and/or other MyHealthAvatar Services according to the conditions laid down in Sections VI and VII of this Privacy Policy.

An exception may occasionally have to be made when the data is collected in order to comply with a legal obligation to which the data controller is subject, or when it is necessary for the performance of the user agreement between you and MyHealthAvatar.

VI. Deleting your account

You can delete your account by emailing the request to mha@ccgv.org.uk and supplying your username. Other users that you have granted viewing access to your profile will no longer be able to see the data. After deleting your account, your information will not be erased until a period of 30 days has passed in order to help avoid accidental or malicious removal of your health information. Afterwards, your avatar and the stored information will be permanently deleted.

VII. Deleting health information

When you delete a piece of health or lifestyle information, but retain your overall account, this information is archived. Other users with whom the archived health information has been shared with will no longer be able to see the deleted items. However, permanent deletion of health and lifestyle information can only happen by deleting your overall account.

VIII. Demo App Developers and Third parties

Where you opt to use one of the apps offered through the platform, you will be asked to read and agree to the separate terms and privacy policy of the app developer. Application connections with products from providers external to the project, including Fitbit, Withings, Moves, and Twitter are subject to their own privacy rules that MyHealthAvatar has no control over. However, these Third Parties will not have any access to your data in the Platform.

IX. Changes to Privacy Policy

If this Privacy Policy is to be changed, we will inform you and ask you to give fresh consent.
In case you do not consent to the changed Privacy Policy, your account will be deleted according to the rules laid down in paragraph VI.

X. Disclaimer

MyHealthAvatar is aware of the high sensitivity of the stored data. The platform features state-of-the-art security measures to protect your data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse.
Absolute security, however, is technically not possible. There is always a small risk that an unauthorised third party, might be able to gain access to your data. **In such cases, the liability of the data controller is limited to breaches of security that could have been reasonably foreseen and/or were contributed by the controller's failure to take due care.**
You are aware that you have the responsibility of keeping your login credentials safe and secure. MyHealthAvatar is not liable for any data breaches caused by the access and misuse of unsafely held credentials by third parties.

XI. Applicable national law

English law applies with regard to the processing by the MyHealthAvatar consortium of the user's personal data within the Platform.

Annex 4: Extended Terms and Conditions for exploitation stage after the project's end

General Terms and Conditions

To access and use the MyHealthAvatar Platform ("the Platform"), you will need to register with the Platform and become a member. When doing so, you will be asked to tick a box by which you confirm that you have read and understood both the following *General Terms and Conditions* and the <Privacy Policy>. The documents also include a number of warranties that relate to your own legally compliant use of the platform.

You may address any questions about the Platform or your registration to mha@ccgv.org.uk.

General Terms and Conditions

I. General Information

These Terms constitute an agreement between yourself as a registered user of MyHealthAvatar [www.myhealthavatar.eu] and MyHealthAvatar. The operator of MyHealthAvatar is [*operator of MyHealthAvatar whose national law permits electronic consent*]. [*sentences about his identity]*

He is the data controller according to [*relevant domestic provision implementing Article 2d DPD*]. Questions and comments may be addressed to the MyHealthAvatar operator or his qualified staff members ([*e-mail address*]).

By registering for an account and/or using MyHealthAvatar services you signify that you agree to these Terms and Conditions. MyHealthAvatar services consist of online and mobile services, including, but not limited to: MyHealthAvatar internet platform, software, an app developed by the Project to collect and access data that are stored at the platform and Third Party apps (Fitbit, Withings, Moves, Twitter) that you can link with your MyHealthAvatar account ("Services").

II. Purpose of MyHealthAvatar

MyHealthAvatar aims to provide a proof-of-concept solution for the collection, access, 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 MyHealthAvatar will be valuable for clinical decisions concerning your care, in helping you to best manage your own health and lifestyle. MyHealthAvatar will collect and store your data provided by you either through the sensors linked to MyHelathAvatar, or through the user interface of the system. The intelligent data analysis software in MyHealthAvtar will then:

- organise and display your data in a professionally designed layout with graphical illustrations to facilitate your understanding.
- work out your locations and movements on a daily basis to help you inform yourself about your past events and experience.
- calculate your risks to long term diseases using the established medical models.

- allow you to share your information with friends through social media (currently through Twitter).
- allow you to transfer data to your physician.

The data will be stored in the **private cloud** server [*name of private cloud server*], based in [*location*] and rented by [*organization*].

III. Eligibility for Membership

In order to register to use the Platform, you must be aged 16 years or above. By signing up to the Platform you confirm that you are aged 16 or above.

Organizations, companies, and businesses may not register with the Platform. Physicians may co-operate with MyHealthAvatar after having signed a contract with MyHealthAvatar that forbids the physician to exert pressure, duress and coercion to the MyHealthAvatar user. If the physician does not meet this contract, he will be excluded from the co-operation with MyHealthAvatar.

IV. Functionalities of MyHealthAvatar and Use of Content

The following are the main intended functions of the Platform:

- A sign in page to sign in or to sign up for your personal account in MyHealthAvatar.
- A dashboard with the following functionalities:
  - a general overview of your automatically calculated health risks (including hypertension risk, diabetes risk, cardiovascular disease risk, stroke risk; please note that this functionality is for informational and research purpose only and does not replace any medical advice) and a health score
  - You can also allow your browser using your computer's location to display location-related information like weather and town.

Moreover, you can see

- your walking distance and step counts in summary,
- your overall duration of activities and calories consumption,
- your transport duration and distance in summary,
- your location on Google map (if you choose to share your location),
- your activities and life patterns described via a timeline (Activity Stack", "24hour Activities", "Activity Cloud", "Activity Bubbles", "Movement - Place") and
- your activity durations.

You can also allow your browser using your computer's location to display location-related information like weather and town.

- A diary/journal that allows you to collect, store and show data such as data concerning walking, transport, running, cycling, calories, diet, mood and blood pressure. You can also show data concerning the history of your locations and activities acquired from location methods such as GPS, AGPS and wifi locations. The locations and activities include home, work, shopping, restaurant, transport, healthcare, sports, entertainment, hotel, public service, friend's home, children's school using a map together with a clockview for visualising time information of the activities. The diary includes an event planner in which

you can enter data via the “Event Table”. Moreover, the diary gives you an overview of your Fitbit, Withings and Moves statuses.

- A LifeTracker that involves most of the functionalities of the diary/journal. The LifeTracker allows you to explore your daily activities and life patterns. You can choose between 13 categories of data (home, work, shopping, restaurant, transport, healthcare, sports, entertainment, hotel, public service, friend’s home, children’s school, unknown) to map all the locations and activities.

The LifeTracker includes

- a **multi layer timeline** that includes the layers year, month and day and represents the time at different scales.
- a **life pattern** that shows you your individual life patterns on an hourly basis at different levels of timescales. It can filter, highlight, and show specific daily activities. You can switch between the month mode that shows all days of a selected month, the year mode that shows the month summary of a selected year, and the long mode that shows the year summary in a selected year.
- a **chart view** that shows you the change of data such as duration of walking, running, cycling, transportation, and also calories consumption during the selected period of time
- during the selected period of time by using histograms and curves.
- a **key event list** that displays all the key events in a form of list with the ability of sorting by date, time, name, and category.
- a **key calendar** that shows you day summary information in colour, together with any key events that occurred on the day.
- a **statistics list** that shows you your statistics concerning the collected data.
- a **life map** that shows you daily activities and locations of the key events geographically via colour coded path lines, heatmap, glyphs, and interaction. These data are acquired from location methods such as GPS, AGPS and wifi locations.

- A toolbox that includes the following services for informational, educational and research purposes:

- Risk calculator for cardiovascular disease (10-year risk), hypertension (1, 2, 4-year risk), diabetes (8-year risk) and a stroke (10-year risk);
- Upload and view functionality for medical images;
- Functionality to order and present uploaded clinical data according to different categories (all clinical data, vital signs, drugs, medical images) and dates (today, this month, last month, this year, last year; chosen start and end date).
- Functionality to import your profile from IndivoX.
- Semantic search functionality to allow you to search for certified medical information related to the disease of interest for your health literacy.
- Simulation of a nephroblastoma (Wilms Tumour) Oncosimulator. With the Nephroblastoma Educational Tool you can specify a treatment scheme and see the Tumor Volume Evolution over Time. This service is for informational, educational and research purposes only and does not replace any medical advice.

All functionalities of the toolbox are not indented for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease. For more information, please see Section XIV (Medical advice disclaimer).

- A help button that you can click on to see different tutorial videos and help documents.

- A data sharing interface that will allow you to share different data with your friends and/or created groups, e.g. the diabetes and other program progress), food, drink and calories, event plans and activities.

You can also transfer your stored data to a physician that co-operates with MyHealthAvatar. Please be aware that this is only voluntary and that you do not have to use this functionality. Please use the data transferring functionality only, if it was your decision to do so.
If you want to transfer data to your physician, we will send you a security question or an extra keyword (as specified by you) to your mobile phone.

- A 'withdrawal button' that you can click if you decide to withdraw your consent. If you tick this button, all your stored data will be deleted according to clause 6 of the Privacy Policy.

- The MyHealthAvatar mobile app that helps you to access your data that is stored in the Platform from your mobile phone. Please note that you need an android based smartphone to install the MyHealthAvatar app. Before installing the app, the app will ask you to authorise the following functionalities:

- to read and access accounts, contacts and contact details,
- to determine the location of your mobile phone by using GPS, AGPS and wifi locations*
- to read, change, and delete memory contents of USB,
- to retrieve information from the internet,
- to access all networks,
- to use the camera of your mobile phone to take photos and record videos*

*You can disable this functionality later in the mobile setting. The app will only make use of its authorisation while using this functionality.

Please do only download and install the MyHealthAvatar app if you agree with his.

- Application connections with Third Party apps allowing the sharing of your data as supported by these services.
In order to use the functions of MyHealthAvatar to its full extent, you will need to upload personal data. For the testing phase, you may prefer to submit fake data (i.e. information you make up about yourself), rather than real data. At this stage, this will already allow you to test the broad functioning of the Platform and provide the project with valuable insights and feedback. Insofar as you do provide your real data, the use of this is outlined in the Platform's Privacy Policy.
Your data may be stored in the following profiles, which represent categories of data: You may choose which of the possible elements you would like to submit to the Platform:

- General Profile
  Email, gender, birthday, state/county, country, ethnicity, qualification, weight, height, glucose, total cholesterol, HDL cholesterol, triglyceride, diastolic blood pressure, systolic blood pressure, pulse
- Health Profile
  Smoking, Alcohol, Diabetes, Parental Diabetes, Parental Hypertension, Prior Cardiovascular, Physical Activity, Mood, Social Engagement, Entertainment
- Medical Profile
  Care Provider (name, address, phone number), Immunisations (name, description, date given), Allergies (name, description), Problem and History
- Profile Overview
  Patient Profile, Medical History, Medical History Snapshot, Medications Summary and Schedule

- As a motivation for yourself, you may enter freely definable daily goals such as targeted number of steps, distance, active minutes, calories burned, body weight, BMI, systolic blood pressures, diastolic blood pressures.
- There is also a 3D Avatar representing an overall interactive anatomy model. The human anatomy model set can be explored by selecting different buttons from the toolbar. Depending on the adjustment of the toolbox, the anatomy model will be presented in different aspects. For instance, the anatomy model can be represented semi-transparent meaning that internal organs can be presented non-transparent whereas the rest of the model is transparent. Another example is that you can click on specific parts of the model and zoom it.
- Moreover, you may answer a questionnaire on your Quality-of-Life (QOL), and also a patient questionnaire to help your doctors keep track of how you are feeling.

V. Your rights to use MyHealthAvatar Services

MyHealthAvatar grants you a personal, worldwide, royalty free, non-assignable, non-exclusive license to use MyHealthAvatar Services for the purpose, to the extent and for so long as the Services are provided to you under these Terms.
All rights, title, copyrights, and interest in MyHealthAvatar Services (excluding user generated content) are reserved and owned by MyHealthAvatar parties. The Services are protected by copyright and other applicable laws.

VI. Entitlement to Terms and Conditions of MyHealthAvatar

You are allowed to submit fake data. However, we recommend that you use your real email address so that we can send you a copy of the General Terms and Conditions, the Privacy Policy and the consent form, and inform you in case of the need for a re-consent due to a change to the General Terms and Conditions and/or the Privacy Policy.

You agree to not upload to the Platform any, obscene or indecent, threatening, offensive, malicious, or libelous information, or information which infringes any copyrights, trademarks, patents or other proprietary rights.
It is also prohibited to upload media of any kind that may give rise to civil or criminal liability under applicable law or regulations or that otherwise may be in conflict with these Terms and the MyHealthAvatar Privacy Policy.

Furthermore, expressions of hate, abuse, obscenity or pornography are prohibited. You may not harass, threaten or stalk other members.
Any information gained from the use of the Platform is for your personal use only and may not be used for any commercial ventures, such as advertising services, products, events or initiatives. In particular, you may not use contact information provided by users, or collect information about the users in order to transmit unsolicited bulk communications.

VII. Restrictions on upload of data

You warrant not to upload to the Platform or to transfer any personally identifiable information about a Third Party unless you have their written and explicit consent to do so. In case of diseases with a strong and direct hereditary component, you warrant that you have obtained the explicit permission of your family members before uploading information that are related to such diseases. In case you are unsure about the hereditary nature of a given condition, please ask your physician.
You further warrant that you have the right to use, copy, display, perform, transmit and distribute any uploaded data.

MyHealthAvatar reserves the right to delete uploaded data that does not fulfil the above-mentioned requirements.

VIII. User generated content

You understand and agree that some of the content which appears on the MyHealthAvatar Services, such as: text, photographs, audio-visual works, comments, illustrations, sketches and other information, may be protected by intellectual property rights or other proprietary rights (“IP Content”). When you submit, upload post, display or otherwise provide to the Platform any IP Content, you grant MyHealthAvatar a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, reproduce, distribute, communicate, make available, transmit, process, display, digitally perform, modify, adapt and otherwise use such IP Content in any and all media, in any format or distribution methods, now existing or later developed, including, but not limited to websites, in audio format, and in any print media as needed and for so long as needed for MyHealthAvatar to provide its Services (“IP License”).

This license ends when you delete your content or account, unless you have shared such content with other users of the Platform and they have not deleted it. Please note that the deleted information is removed from a particular memory space on the Platform, but may subsist for the time being for backup purposes and/or as required by the law (while being unavailable to the others).

You also agree that you have and/or have obtained all necessary rights required to allow posting, communicating, transmitting, using, copying, displaying, performing, distributing any IP Content submitted to the Services by you.

You are responsible for complying with all laws applicable to your IP Content.

All user generated content made available on MyHealthAvatar Services is the responsibility of the user who originated such content. MyHealthAvatar does not monitor the content made available on its Services by the users and does not accept any responsibility for such content, unless MyHealthAvatar has obtained knowledge or awareness of illegal activity or

content on its Services. If you use and/or rely upon any user generated content transmitted via the Services, you do so at your own risk.

IX. IP Policy

If you have justifiable grounds to believe that any IP Content posted on the MyHealthAvatar platform infringes copyrights or other intellectual property rights, please notify us (mha@ccgv.org.uk). Please support your notification with the following: identity of the copyright owner; copy of a copyright work alleged to be infringed; copy of infringing materials; grounds why you believe that use of a work is not authorized by the copyright owner; your contact details, incl. name, address, email address; statement and supporting documentation that you have the authority to act on behalf of the copyright owner.
Upon obtaining notification on alleged violations, MyHealthAvatar will verify your claims and supporting materials and where such claims are considered justified, will take operative measures to remove or to disable access to such content.

X. Third Party services

MyHealthAvatar allows connections to Third Party services, and may provide links or references to websites, services and/or apps operated by third parties, in particular: Fitbit, Withings, Moves and Twitter.

These are the third parties that can receive your collected and stored data if you consent to the transfer of your data:

- [add third party]
- [add third party]
- …

Please note that you can exercise your rights to information, right of access, rectification, erasure or blocking and right to object (please see section 5 of the Privacy Policy) also to these third parties.

MyHealthAvatar neither monitors nor investigates such third parties and is not responsible for the content, functionality, or practices of Third Party services. If you decide to access such Third Party services or to transfer data to them, you do so at your own risk. By agreeing to share your MyHealthAvatar data, information or content with Third Party services, you understand and agree that use of such data, information or content by Third Party services is governed by those Third Parties´ terms of use and privacy policies. MyHealthAvatar recommends that you read the terms of use and privacy policies (if any) on those Third Party services. You agree that MyHealthAvatar has no liability for any damage or loss of any kind that results from your use of a third party service.

XI. No Interference with Operation

Interference with the operation of the Platform is prohibited. This includes the use of any automated device, process or means to access the Platform, such as robots, spiders and scrapers. You may not post content that contains any viruses or other computer codes, files

or programs designed to alter, interrupt, damage, destroy or limit the functionality of this Platform, such as Trojan horses, worms, and time bombs.

XII. User Password and Login Identity

You are responsible for the security of your passwords and for any use of your account including all activities that occur under your password or account with or without your knowledge. In case of any unauthorized use of your password or account or other breach of security, please notify us immediately. We are not liable for any harm that may result from unauthorised access to your credentials.
If you want to transfer data to your physician, we will send you a security question or an extra keyword (as specified by you) to your mobile phone.

XIII. Cost of Membership

Membership with MyHealthAvatar is free of charge. You will be notified should this change, and you will be asked to provide new consent.

XIV. Member Notices

By signing up to use the MyHealthAvatar Services, you agree that MyHealthAvatar may send you a copy of the Privacy Policy, these Terms and the form by which you indicated your consent, as well as any necessary communication about the Platform by using your email address.

XV. Termination of Membership

MyHealthAvatar has the right to terminate your membership immediately for what it in its reasonable discretion considers to be a significant violation of any of these terms.

XVI. Modifications to these Terms

MyHealthAvatar may modify these Terms in part, at any time and without prejudice to the validity of the other provisions. In such a case you will be notified by email, and asked to re-consent to your continuing membership. If you do not want to give re-consent in such a case, you will have the opportunity to download all your selected and stored data as a PDF file.

XVII. Applicable law

These Terms are governed by English law.

XVIII. Medical advice disclaimer

The use and access of the Platform and the app do not create a physician-patient relationship between you and the operator of the Platform.
The Platform and the MyHealthAvatar App do not offer medical advice and are not medical devices.
All material, information, content and Services (particularly the toolbox to calculate your risk of suffering from diseases, the Clinical Data functionality, the Medical Images Upload and View, the Nephroblastoma Educational and Semantic Search) are provided for informational, educational and research purposes only. They are not intended as a

substitute for professional medical advice, diagnosis, prevention, monitoring, treatment or alleviation of disease. No medical decision should be based on anything coming from the Platform or App.
Please consult your physician or other qualified health care providers if you have any questions about your health, a medical condition, taking drugs, or possible courses of treatment.
Do not ignore professional medical advice or delay in seeking it because of information you obtained through the Platform.
MyHealthAvatar neither endorses nor assumes responsibility (whether tortious or contractual) for any advice given or information referred to on the Platform, including certain physicians, procedures, drugs or other information that may be mentioned.

XIX. The Services "as is"

When you use MyHealthAvatar Services you do so at your own risk. The Services are provided on an "as is" basis. To the extent permitted by the applicable law MyHealthAvatar does not provide any warranties of merchantability or fitness for a particular purpose.
MyHealthAvatar declares that at the moment of conclusion of this agreement it is not aware of any legal defects in the rights on use of the Services which are provided under this agreement, in particular, third party claims, third party rights, prior rights which might be infringed by conclusion of this agreement and/or provision of the Services into use. MyHealthAvatar declares that to the best of its knowledge it is entitled to grant the rights which are provided into use under this agreement.

XX. Use of MyHealthAvatar Services

MyHealthAvatar specifically advises that Services of MyHealthAvatar have not been developed to meet individual requirements of a particular user. Therefore, it is the user´s own responsibility to ensure that the Services and their functions meet the user´s requirements.
MyHealthAvatar does not represent and does not guarantee the accuracy, reliability, truthfulness, completeness of any content or information transmitted or made available on the Services. MyHealthAvatar does not control and cannot assume any kind of responsibility or liability for the use which a user may make of MyHealthAvatar Services and/or for the consequences which a user may draw from such use. In this regard, MyHealthAvatar specifically advises that all physical activities which a user undertakes may be subject to certain risks corresponding to the health status of an individual user. Therefore, users of MyHealthAvatar may use the Services for informational purposes, but any change in the user´s behaviour as might be resulting from the use of MyHealthAvatar Services is at sole responsibility of the user. It may be necessary to consult a physician before any change in a user´s physical activity.

XXI. Data use for future research

In the case that we wish to use your data for a health-related project, please be assured that we will inform you by email of the details and ask you for fresh consent.

Annex 5: Extended version of the Privacy Policy

Privacy Policy

This Privacy Policy constitutes an agreement between yourself as a registered user of the MyHealthAvatar Platform ("the Platform") and MyHealthAvatar [www.myhealthavatar.eu], represented by the operator *[name]*.Questions and comments may be directed to the project operator, [name] or his qualified staff members ([e-mail]).

I. General information

This Privacy Policy describes

- your rights regarding the processing of your personal data
- how your personal data is protected by security measures,
- information about the circumstances in which your personal data may be shared with other users or third parties, and
- how to delete your personal data from MyHealthAvatar.

This Privacy Policy is necessary because the use of the MyHealthAvatar platform entails the submission of personal data. **Any data submitted will be processed by the Platform.**
Consequently, the registration process entails giving your consent to the processing of your data by the operator of MyHealthAvatar, as specified in the General Terms and Conditions.
Other information that will be collected to help operate and improve the service refers to how you interact with our services, including the browser that you're using, your IP address, location, cookies or other unique IDs, the pages that you visit and features that you use. We combine this with other users' information to get an overall view of how the service is used.
Your data will not be processed for any other purposes than mentioned in the Policy and to which you consent to.
You may withdraw your consent at any time without any disadvantages. In this case, any and all data that you uploaded to the platform will be permanently deleted as laid out in Sections VI and VII. To withdraw consent, you can contact the operator of MyHealthAvatar by using the e-mail address *[e-mail address of the operator*] or use the 'withdrawal'-button**.**

For your records, a copy of this Privacy Policy will be sent to your e-mail address and made available as a download.

II. Registration

The registration process requires your name or a pseudonym and your email address. We recommend using a real email address, so we can send you a copy of the General Terms and Conditions, this Privacy Policy and the consent form and can ask for re-consent in case of any updates of the General Terms and Conditions and/or Privacy Policy.

III. Sharing your personal data via MyHealthAvatar Platform

1. With other users

You will be able to share your lifestyle data with other users of the Platform.
These are the main types of data you can share with your invited friends: food, drink and calories, events and activities. You are free to choose what types of lifestyle data you would like to share and with whom. Other users of the Platform will only be able to access your data after you connect with them as "friends". You can create groups with your "friends" and share the selected data you would like to share within the created group, but also share

the selected data with a single “friend”. You can dissolve “friends” as well as delete groups created by you at any time.

2. With your physician

You can transfer data to your physician. Please be aware that this functionality is absolutely voluntary. In case of any duress, please notify our contact point (mha@ccgv.org.uk).

3. Possibility to Support Medical Research

In the longer term it is envisaged that MyHealthAvatar users will have the possibility to support medical research by providing their personal data to researchers. The information generated may offer a promising resource of population data to support clinical research, leading to future improvements in medical treatment and care. However, there will be no obligation to share data in this way: rather, users will retain full control, by giving or declining their consent, over whether their data is so used. We will ask you for fresh consent for this.

IV. Security measures to protect your data

We are aware that the data you choose to upload can be highly sensitive. State-of-the-art security measures are incorporated into the Platform to protect your data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse.

Unless you opt to share your data with other users of the Platform, the operator of MyHealthAvatar and his staff members are the only entities that have access to your uploaded data. Other users of the Platform will only be able to access your data after you connect with them as “friends” and only after you have selected the data you would like to share.

As noted in the Terms and Conditions, the data will be stored in the private cloud server [name], based in [location] and rented by [name].

V. Your rights regarding to the processing of your personal data

You retain at all times your full rights as a data subject under the Data Protection Directive, as follows. You may contact the operator of the MyHealthAvatar project, [name] or his qualified staff in order to exercise any of your rights: mha@ccgv.org.uk.

1. Right to information

You have the right to inform yourself about the identity of the data controller and of the controller’s representatives, if any.

The data controller is *[name],* represented by *[name],* the operator of the Platform.

You have the right to inform yourself about the purposes of the processing and about the recipients of the data, as well as any other relevant facts.

2. Right of access, rectification, erasure or blocking

At any time, you may check your 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 according to the conditions set out in Sections VI and VII of this Privacy Policy.

3. 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 Platform and/or other MyHealthAvatar Services according to the conditions laid down in Sections VI and VII of this Privacy Policy.

An exception may occasionally have to be made when the data is collected in order to comply with a legal obligation to which the data controller is subject, or when it is necessary for the performance of the user agreement between you and MyHealthAvatar.

VI. Deleting your account

You can delete your account by emailing the request to mha@ccgv.org.uk and supplying your username or by using the 'withdrawal' button. Other users that you have granted viewing access to your profile will no longer be able to see the data. We will give you the opportunity to download your selected and stored data as a PDF file. After deleting your account, your information will not be erased until a period of 30 days has passed in order to help avoid accidental or malicious removal of your health information. Afterwards, your avatar and the stored information will be permanently deleted.

VII. Deleting health information

When you delete a piece of health or lifestyle information, but retain your overall account, this information is archived. Other users with whom the archived health information has been shared with will no longer be able to see the deleted items. However, permanent deletion of health and lifestyle information can only happen by deleting your overall account.

VIII. Demo App Developers and Third parties

Where you opt to use one of the apps offered through the platform, you will be asked to read and agree to the separate terms and privacy policy of the app developer. Application connections with products from providers external to the project, including Fitbit, Withings, Moves, and Twitter are subject to their own privacy rules that MyHealthAvatar has no control over. However, these Third Parties will not have any access to your data in the Platform.

IX. Role as controller

The data controller according to part 1, section 1 UK Data Protection Act 1988 is [name]. He complies with the duties he has according to part 2, section 7 UK Data Protection Act.

X. Termination of service

If MyHealthAvatar closes down, we will inform you via your e-mail address or postal address (as specified by you) and will offer you the possibility to download your stored data as a PDF document. After this time all your data will be deleted.

XI. Changes to Privacy Policy

If this Privacy Policy is to be changed, we will inform you and ask you to give fresh consent.

In case you do not consent to the changed Privacy Policy, your account will be deleted according to the rules laid down in section VI. In such a case, we will first give you the opportunity to download your selected and stored data as a PDF file.

XII. Disclaimer

MyHealthAvatar is aware of the high sensitivity of the stored data. The platform features state-of-the-art security measures to protect your data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access or any other misuse.

Absolute security, however, is technically not possible. There is always a small risk that an unauthorised third party, might be able to gain access to your data. **In such cases, the liability of the data controller is limited to breaches of security that could have been reasonably foreseen and/or were contributed by the controller's failure to take due care.**

You are aware that you have the responsibility of keeping your login credentials safe and secure. MyHealthAvatar is not liable for any data breaches caused by the access and misuse of unsafely held credentials by third parties.

XIII. Applicable national law

English law applies with regard to the processing and storage of the user's personal data within the Platform.

Annex 6: MyHealthAvatar API Terms of Use

Version 0.9, February 2016

1. Scope of application

The MyHealthAvatar API terms of use govern your use of the MyHealthAvatar API in your applications and services designed to interact with MyHealthAvatar. The terms of use of MyHealthAvatar API consist of the terms of the API license agreement laid down below and in guidelines for developers located at: https://myhealthavatar.org/mha/login.

By registering for an account and/or using the MyHealthAvatar API you signify that you have read and agree to the API terms of use. By agreeing to these terms you conclude an agreement between yourself as an app developer, who is also a registered user of MyHealthAvatar [www.myhealthavatar.eu], and the MyHealthAvatar project, composed of the parties to the MyHealthAvatar Consortium, namely:

- University of Bedfordshire, the Coordinator (short name: BED)
- Foundation for Research and Technology – Hellas (short name: FORTH)
- Universität des Saarlandes (short name: USAAR)
- Institute of Communication and Computer Systems (short name: ICCS)
- Gottfried Wilhelm Leibniz Universität Hannover (short name: LUH)
- AnSmart, Ltd (short name: ANS)
- Technological Educational Institute of Crete (short name: TEI-C)
- University of Lincoln (short name: LIN)

The Consortium is represented by the project's lead partner, the University of Bedforshire, England. Questions and comments may be addressed to the MyHealthAvatar coordinator, Professor Feng Dong (mha@ccgv.org.uk).

2. Definitions

Applications – Applications developed by you designed to interact with MyHealthAvatar.

MyHealthAvatar API, API – The MyHealthAvatar Application Programming Interface ("API") and associated documentation, data, code and other materials which MyHealthAvatar makes available to you together with the API.

MyHealthAvatar Data, Data – Any information and data collected by MyHealthAvatar and accessible via API, including MyHealthAvatar User Data and User generated content.

MyHealthAvatar platform – The MyHealthAvatar platform, located at: https://myhealthavatar.org/mha/login.

MyHealthAvatar Services – Online and mobile services, including, but not limited to: the MyHealthAvatar internet platform, software, API, apps developed by the project to collect and access data that are stored at the platform easier and Third Party apps (such as Fitbit, Withings, Moves, Twitter) accessible via the platform.

Services – Your websites, applications and other software offerings designed to interact with MyHealthAvatar.

User - A registered user of MyHealthAvatar platform.

User Data - MyHealthAvatar User profile information, User generated content, any other information relating to a User who may be identified or identifiable, directly or indirectly, in

particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental , economic, cultural or social identity.
User generated content - any content including but not limited to user comments, photographs, images, files, text, other data and information which a User submits to MyHealthAvatar Services in digital form in any media or format.

3. API license

On the terms of this agreement MyHealthAvatar grants you a non-exclusive, personal, royalty free, non-transferable, non-assignable, non-sublicensable revocable license limited to the term and purpose of this agreement and to the country from which you connect to the API to:

1. Use the API to develop Applications and/or Services intended to interact and exchange data with MyHealthAvatar.
2. Use the API in order to interact and exchange data with MyHealthAvatar platform, fetch and display MyHealthAvatar Data in your Applications and/or Services to the extent as necessary to provide your Applications and/or Services to the Users.
3. Modify MyHealthAvatar Data to format it for display on your Applications and/or Services.

MyHealthAvatar allows you to use the API for data exchange purposes, but MyHealthAvatar does not grant you any rights in User Data and/or User generated content itself. Any use of the User Data and/or User generated content in, via and on your Applications and/or Services requires prior authorization of the User, as described in Sections 6 and 7 below.
When you use MyHealthAvatar Data in your Applications and/or Services, your use of such Data is at your own risk. You, and not MyHealthAvatar, are responsible and liable for the data processed in your Applications and/or Services and your usage of such data.

4. Restrictions

Use of MyHealthAvatar API is subject to certain restrictions and limitations, such as rate limits, access limits, method calls, etc., set out below and in MyHealthAvatar guidelines for developers. Please see MyHealthAvatar guidelines for developers [https://myhealthavatar.org/mha/login] for more details.
In particular, when using MyHealthAvatar API you may not:

- Interfere with, modify, disrupt, compromise, disable features and/or functionality of MyHealthAvatar API and/or Services;
- Compromise, circumvent, bypass any protection or authentication mechanisms implemented by MyHealthAvatar;
- Assign, transfer, sublicense or otherwise grant access to API to any third parties;
- Export MyHealthAvatar Data, including for account migration or service duplication, with any other purpose than enabling the Users to interact with MyHealthAvatar via your Applications and/or Services;
- Undertake any action and/or method enabling direct or indirect retrieval, extraction, migration and/or duplication of a substantial part of MyHealthAvatar Data or Services available via API;

- Access and/or make yourself into any section of API or MyHealthAvatar Data that is not accessible to you via normal use of API;
- Introduce harmful, malicious, destructive or otherwise inappropriate software, content or data into MyHealthAvatar;
- Use MyHealthAvatar API to develop anything other than your Applications and/or Services and with any other purpose than to exchange data with MyHealthAvatar and provide your Applications and/or Services to the Users;
- Make any modifications or misrepresent MyHealthAvatar Data, except formatting the Data for display on your Applications and/or Services;
- Market, sell, transfer, disclose MyHealthAvatar Data to any Third Parties not directly involved in the provision of the health or lifestyle services, unless as required by law.

MyHealthAvatar may monitor your use of the API in order to ensure your compliance with the API terms of use. If MyHealthAvatar has grounds to believe that you do not respect the API terms of use, MyHealthAvatar may revoke or suspend your access and rights to the API on a temporary or permanent basis.

5. Your MyHealthAvatar account

In order to use the API you are required to go through the following steps:

(i) create a MyHealthAvatar account;
(ii) register yourself as a MyHealthAvatar User;
(iii) register your Applications and/or Services;
(iv) read and accept the API terms of use;
(v) receive approval by the administrator of the MyHealthAvatar platform.

Upon registering your Applications and/or Services you will receive API client credentials. You may use this account and the credentials as a single individual or as a single legal entity.
You must protect your MyHealthAvatar account information and API client credentials from unauthorized use or access. You must notify MyHealthAvatar immediately if you become aware or suspect that a third party has unauthorized access to your account and/or MyHealthAvatar API through your account. In this case you must disconnect such access immediately. MyHealthAvatar may at its discretion and upon your request grant you a new access to enable you to continue lawful use of MyHealthAvatar API. MyHealthAvatar may disconnect or disable your use of API, if MyHealthAvatar suspects that your account or API credentials are used in a fraudulent way.
You are solely liable for the use of your account, API and API credentials provided by MyHealthAvatar to you.
By registering your account or an Application and/or Service you must provide true and accurate data. MyHealthAvatar may verify the accuracy and correctness of your information. Provision of knowingly false information, if MyHealthAvatar perceives so, will have a consequence that your rights under this agreement will terminate. MyHealthAvatar is not liable for any false information provided by you.
When you create a MyHealthAvatar account or use the API, MyHealthAvatar collects and stores personal data concerning you. Any collection and processing of personal data is carried out with your prior informed consent and governed by MyHealthAvatar Privacy Policy available at: [www.myhealthavatar.eu].

6. Use of MyHealthAvatar User Data

Any use of MyHealthAvatar User Data requires prior informed consent of the User whose data it is. You must respect other MyHealthAvatar Users and their privacy, process their data in compliance with European data protection law, due care and good processing practice.

In particular, your access to the API is subject to complying with the following requirements:

a) The app's primary goal is the provision of health or lifestyle services.

b) The app will respect and adhere to the principles of privacy by design and data minimization.

c) You may not use personal data collected as a result of connecting to the MyHealthAvatar platform through the API beyond the provision of such health or lifestyle services. In particular, you may not use the personal data collected for marketing, advertising or similar services.

d) You may not pass on in any way personal data to Third Parties not directly involved in the provision of the health or lifestyle services except as required by law.

e) Data may only be used for medical research after obtaining explicit consent from the user.

– You must have a robust privacy policy that complies with the above and with European data protection legislation.
  - When you ask the User to authorize your Applications and/or Services, you must provide your privacy policy and terms of use to the User. Your privacy policy must explain what data you collect, for what purposes and what you are doing with the data and other information you collect from the User.
  - You must ask the User to read and accept your privacy policy and terms of use as a requirement for using your Applications and/or Services.
  - Ensure that your privacy policy and terms of use are available to the User via the user interface when the User installs and uses your Applications and/or Services.
  - Use the User Data as it is. Do not misrepresent the User Data in your Applications and/or Services.
  - Request and access only the Data which your Applications and/or Services need.
  - If you are tracking a User´s activity, allow the User to opt-out.
  - Delete the User´s Data if a User asks you so, unless you are required to keep the data by the law and for as long as the law permits.
– Implement appropriate technical and organizational measures to protect the User Data against accidental loss, unlawful or unauthorized access, use, destruction, alteration, disclosure, and other forms of processing which are not explicitly authorized by the User or MyHealthAvatar or by the law.
– Your app complies, if applicable, with the relevant EU medical devices regulatory framework.
– You do not exert pressure to the MHA user to register with MHA and/or use your app.

7. User generated content

MyHealthAvatar stores certain User generated content. Some of this content may be protected by IP rights ("IP protected content"). Use of IP protected content, such as by copying, storage, display, transmission, and making the content available to the public on the electronic services requires authorization of the right holder. MyHealthAvatar does not give you any rights to the use of such content on your Applications and/or Services. In order to display such User generated content on your Applications and/or Services, you need to get the User´s permission to do so. MyHealthAvatar does not monitor and is not liable for the User generated content transmitted on MyHealthAvatar Services and is not liable for your use of such content on your Applications and/or Services. Your use of User generated content from MyHealthAvatar is at your own liability and risk.

8. Intellectual Property Rights

The MyHealthAvatar API is developed by and is property of MyHealthAvatar. API is protected by copyright, know-how and other intellectual property rights. All rights in MyHealthAvatar API and information associated with API are reserved by MyHealthAvatar. The rights granted to you under this agreement are licensed, not assigned. MyHealthAvatar does not grant you any intellectual property rights in relation to the API except those expressly specified in Section 3 above.

9. Website links

You may create a link to MyHealthAvatar platform in order to connect your Applications and/or Services to MyHealthAvatar and enable the Users to go from your Applications and/or Services to MyHealthAvatar. You may not use MyHealthAvatar link for endorsement, sponsoring or advertising purposes, nor in a defamatory, misleading or damaging manner.

10. Warranty and liability

MyHealthAvatar declares that at the moment of conclusion of this agreement it is not aware of any legal defects in the rights on use of the API which are provided to you under this agreement, in particular third party claims, third party rights, prior rights which might be infringed by conclusion of this agreement and/or provision of the API into use. MyHealthAvatar declares that to the best of its knowledge it is entitled to grant the rights provided to you under this agreement.

The MyHealthAvatar API is provided in its Beta version "as is". By this, MyHealthAvatar notifies and makes clear to you that your use of the API may be subject to certain risks which are common for software in this development status. The liability of MyHealthAvatar regardless of negligence or fault for defects which are present in the API at the moment when the API is provided to you is excluded. MyHealthAvatar does not guarantee that the API is error free and will take reasonable steps to correct the errors which you reveal in the course of using the API upon your request in reasonable time. Should you reveal some errors or defects in functioning of API, please notify MyHealthAvatar.

MyHealthAvatar specifically advises that MyHealthAvatar Services have not been developed to meet any individual requirements of a particular User. Therefore, it is the User´s own responsibility to ensure that the Services and their functions meet the User´s requirements.

MyHealthAvatar does not represent and does not guarantee the accuracy, reliability, truthfulness, completeness of any content or information transmitted or made available on MyHealthAvatar Services. MyHealthAvatar does not control and cannot assume any kind of responsibility or liability for the use which a User may make of MyHealthAvatar Services and/or for the consequences which a User may draw from such use. In this regard, MyHealthAvatar specifically advises that all physical activities which a User undertakes may be subject to certain risks corresponding to the health status of an individual User. Therefore, Users of MyHealthAvatar are allowed to use MyHealthAvatar Services for informational purposes, but any change in the User´s behavior as might result from such use is the sole responsibility of the User. It may be necessary and Users are explicitly advised to consult a physician before any change in a User´s physical activity. When you use the MyHealthAvatar API, you must ensure for secure storage and transfer of Data and take reasonable steps to safeguard that your Applications and/or Services comply with internet security standards.
You are allowed to use the API and offer your Applications and/or Services to the Users if you have the rights, including copyrights, trademarks and other IP rights as needed to provide your Applications and/or Services to the Users. Provision of your Applications and/or Services to the Users without having such rights will automatically terminate the rights granted to you under this agreement.
When you provide your Applications and/or Services to the Users you, and not MyHealthAvatar, are responsible for providing technical support and maintenance to the Users.

11. Duration and termination

The terms of use of the MyHealthAvatar API remain effective until terminated by MyHealthAvatar or by you. You may terminate this agreement at any time by deleting your account. MyHealthAvatar may suspend your access to API, and if necessary, revoke the rights and terminate this agreement if MyHealthAvatar believes that you have violated the terms of use of MyHealthAvatar API or otherwise engaged in fraudulent activity which may cause liability to MyHealthAvatar. MyHealthAvatar may also terminate this agreement for any reason upon 30 days prior notice to you. All costs and damages which may occur to you in the result of termination of this agreement go at your expense.
Upon termination of this agreement you agree to cease your use of and delete to the extent, technically possible, MyHealthAvatar API, MyHealthAvatar Data, MyHealthAvatar link, and any other materials and information related to your use of API as provided by MyHealthAvatar to you.

12. Applicable law and dispute resolution

Any dispute arising out of or in connection with this agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the LCIA Rules, which are deemed to be incorporated by reference into this clause.
The number of arbitrators shall be one.
The seat, or legal place, of arbitration shall be London, UK.
The language to be used in the arbitral proceedings shall be English.

The governing law of the agreement shall be the substantive law of UK.

13. Variation

MyHealthAvatar may revise the terms of use for the API from time to time. MyHealthAvatar shall notify you of any revisions with prior notice in reasonable time.
If you do not agree to the revised terms, you are not required to continue your use of API under those terms. In case of your disagreement to the revised terms, you must cease your use of API and related materials before such revised terms become effective.

14. Communications

Any communication between you and MyHealthAvatar in relation to this agreement and the use of API may be done via electronic means of communication, such as email. MyHealthAvatar may also send you relevant notifications through your MyHealthAvatar account.

15. Miscellaneous

The API terms of use are a subset of general terms of use of MyHealthAvatar. The API terms of use govern specifically use of MyHealthAvatar API by third party developers. In all matters relating to the use of API the API terms of use prevail.
The API terms of use comprise the terms laid down in this agreement above and the MyHealthAvatar guidelines for developers which are included into this agreement by reference and are a constituent part. In case of conflict between the guidelines for developers and terms of this agreement, the latter shall prevail. Nothing in the guidelines for developers expands the scope of rights granted to you under this agreement.

This agreement constitutes an entire agreement. Each of the provisions operates separately. If any provision becomes invalid, illegal or unenforceable, that provision shall be enforced to the full extent possible and the remaining provisions shall remain in full effect.

Annex 7: CHIC-MHA Memorandum of Understanding

Memorandum of Understanding

between

"Computational Horizons In Cancer (CHIC): Developing Meta- and Hyper-Multiscale Models and Repositories for In Silico Oncology"

(Grant Agreement: 600841; Short Title "CHIC")

and

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

(Grant Agreement: 600929; Short Title "MyHealthAvatar")

Made on: January 12th, 2016 (the "Effective Date")

WHEREAS

The **CHIC** project proposes the development of clinical trial driven tools, services and secure infrastructure that will support the creation of multiscale cancer hyper-models (integrative models). The project started on 1 April 2013 and will last for 4 years.

The **MyHealthAvatar** project is a proof of concept for the digital representation of patient health status. It is designed as a lifetime companion for individual citizens that facilitates the collection of, and access to, long-term health-status information. The project started on 1 March 2013 and will last for 3 years.

The **CHIC** and **MyHealthAvatar** are both concerned with developing ICT health care solutions in which Electronic Health Records (EHR) and other health data is used in an efficient intelligent way to improve the treatment and care of patients and citizens. The said projects share a number of common partner institutions. The parties of CHIC and MyHealthAvatar projects are interested in taking advantage of the potential synergies that could be achieved through a successful cooperation between the two projects.

The purpose of this **Memorandum of Understanding** (**MOU**) is to define the scope of the intended future collaboration between the projects in accordance with the policies and procedures of each project under their EU FP7 Grant Agreements and Consortium Agreements.

I. Subject Matter and Scope

The future areas of collaboration could include but are not limited to the following:

1. To develop and maintain effective communication between **CHIC** and **MyHealthAvatar** to identify areas of mutual research interest;
2. To share knowledge and data that advance the mutual interest of the projects in accordance with each project's policies and procedures;
3. To publish and disseminate the results of collaboration in accordance with the policies of each project;
4. To the shared use of infrastructure developed by each project.

The collaboration shall be within the EU FP7 legal framework that is:

- application of the respective Grant Agreement no. 6000841 for **CHIC** and no. 600929 for **MyHealthAvatar**.
- application of the respective Consortium Agreements of **CHIC** and **MyHealthAvatar.**

II. Intended Activities

The projects intend to collaborate insofar that CHIC grants access to its data repository to host the medical data of a synthetic patient. The medical data of the synthetic patient will allow MyHealthAvatar to demonstrate the utility of its platform by allowing its users to perform oncosimulations using the medical data. The terms on which this will occur, including the access rights to be granted, will be regulated between the relevant partners from the two projects in a separate CHIC-MHA collaboration agreement.

Both projects agree to respect the terms and conditions under their Grant Agreement and Consortium Agreement, in particular the confidentiality clauses, the intellectual property and access rights as well as the dissemination clauses.

III. Nature of MOU

This MOU describes in general terms the basis upon which the projects intend to collaborate. It does not create binding, enforceable obligations against any project. All

activities undertaken pursuant to the MOU are subject to the approval of the projects themselves.

This MOU does not affect the ability of the projects to enter into other agreements or arrangements.

This MOU enters into force from the Effective Date identified at the beginning of this MoU.

IV. Intellectual Property and Dissemination

The ownership of and access rights to any intellectual property (IP) jointly generated as a result of the collaboration of the projects shall comply with the IP provisions and access rights stipulated under the Consortium Agreement of each project.

V. Communications and Liaisons

For CHIC:

Research Prof. Georgios Stamatakos

Phone: +30 210 772 2287

Email: gestam@central.ntua.gr

For MyHealthAvatar:

Prof. Feng Dong

Phone: +44 (0)1582 743940

Email: feng.dong@beds.ac.uk

SIGNATURES OF PARTIES

We, the undersigned, coordinators of the two Consortiums, confirm our intention to proceed in the cooperative and mutually supportive spirit of this MOU.

For **CHIC:**

Research Prof. Georgios Stamatakos, ICCS-NTUA, Coordinator

_____ Date _____

For **MyHealthAvatar:**

Prof. Feng Dong, University of Bedfordshire, Coordinator

_____ Date _____

Annex 8: CHIC-MHA Collaboration Agreement

Collaboration Agreement
With Reference to the FP7 Research Projects:
"A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information"
(Grant Agreement: 600929; short title "MyHealthAvatar", abbreviated to "MHA")
and
"Computational Horizons In Cancer (CHIC): Developing Meta- and Hyper-Multiscale Models and Repositories for In Silico Oncology"
(Grant Agreement: 600841; short title "CHIC")
Version №: 5 dated January 18th, 2016

MADE Between:
The following Parties to the CHIC project:
Universitaet Bern (short name: UBERN)
Institute of Communication and Computer Systems (short name: ICCS)
Foundation for Research and Technology – Hellas (short name: FORTH)
(Collectively referred to as "the CHIC Parties" and each individually - as a "CHIC Party");
AND
The following Parties to the MyHealthAvatar project:
Institute of Communication and Computer Systems (short name: ICCS)
Universitaet des Saarlandes (short name: USAAR)
University of Bedfordshire, the Coordinator (short name: BED)
Foundation for Research and Technology – Hellas (short name: FORTH)
Technological Educational Institute of Crete (short name: TEI-C)
(Collectively referred to as "the MHA Parties" and each individually - as a "MHA Party").
Whereas:

(1) The CHIC and MyHealthAvatar projects are both concerned with developing ICT health care solutions in which EHR and other health data is used in an efficient intelligent way to improve the treatment and care of patients and citizens. The said projects share a number of common partner institutions. The respective coordinators of the two projects have recognized the potential synergies and scope for mutually beneficial and efficient cooperation in a Memorandum of Understanding dated 12.01.2016.

(2) As an aspect of its work, the CHIC project has developed a clinical data repository that provides for a secure storage of clinical data, incl. imaging data, histological data, therapy, etc. The data types hosted by the repository include: imaging data (DICOM, etc), descriptive/structural data (age, sex, etc), other files (histological reports), links (to other data repositories), etc. In accordance with Article 8.1 CHIC Consortium Agreement made on 18.01.2013, UBERN as the partner, who carried out the work generating the repository, owns rights in it as an individual owner and has a right to authorize its use to third parties (subject to Access Rights in CHIC under the CHIC Consortium Agreement).

(3) As an aspect of its work, the MyHealthAvatar project intends to demonstrate the utility of the MyHealthAvatar platform by allowing its users to perform oncosimulations of Wilms' tumor, also referred to as Nephroblastoma, with the use of clinical data and wishes to complete this endeavor with the use of the CHIC data repository. The workflow of this Nephroblastoma use case consists of the following steps:

(i) The MyHealthAvatar project will generate synthetic clinical data for running Nephroblastoma oncosimulations in MyHealthAvatar.

(ii) The CHIC project will create a section in the CHIC data repository specifically designated and restricted to MyHealthAvatar and will provide application programming interfaces (access API) to access the repository for upload and retrieval of data to MyHealthAvatar.

(iii) The CHIC project will generate an account for MyHealthAvatar in its clinical data repository and will provide account credentials to MyHealthAvatar. The MHA Parties will use these account credentials for logging in into the CHIC data repository in order to place and retrieve their data. In the process, the MHA Parties will not have access to any CHIC data located in the CHIC data repository, but only to their own synthetic data.

(iv) The MyHealthAvatar project will connect to the repository via the repository access API and will place its synthetic data into the repository section designated to MyHealthAvatar.

(v) An MHA Party, wishing to run Nephroblastoma oncosimulations in MyHealthAvatar, will log in into the CHIC data repository, select the data needed for the execution of the Nephroblastoma model and send a request to the Nephroblastoma oncosimulator to run.

The oncosimulator, to be used in MyHealthAvatar, is the “Wilms Tumour Oncosimulator Hypomodel” (hereafter “Nephroblastoma oncosimulator”). It is defined in CHIC Deliverable D6.2 – CHIC cancer component models: initial tested versions, W2, p.143, as “*an integrated software system simulating the growth of nephroblastoma tumours and their in vivo response to chemotherapeutic modalities within the clinical trials environment*”. Originally developed by ICCS (Georgiadi et al., 2012; Stamatakos et al., 2011), the Nephroblastoma oncosimulator was brought by ICCS, being a Party to both collaborating projects, as its background to both CHIC and MyHealthAvatar. As improved and adapted to the requirements of MyHealthAvatar, the Nephroblastoma oncosimulator qualifies as ICCS foreground in MyHealthAvatar (Section II.1.7 MHA Grant Agreement).

(vi) Once the Nephroblastoma oncosimulator receives the request to run, the Nephroblastoma oncosimulator application will connect to the CHIC data repository via the repository access API and will fetch the data needed for the execution of the Nephroblastoma model.

(vii) The CHIC data repository will provide the data.

(viii) The Nephroblastoma oncosimulator will execute the model and send the output of execution to MyHealthAvatar using MyHealthAvatar platform API.

(ix) Results generated by execution of the Nehproblastoma model will be saved back to the MyHealthAvatar platform.

The CHIC Parties and the MHA Parties (collectively referred to as “the Parties”) HEREBY AGREE to enter into this Collaboration Agreement (hereafter the “Agreement”) as follows:

1. Definitions

Words beginning with a capital letter shall have the meaning defined either herein or in the MyHealthAvatar Consortium Agreement or in the CHIC Consortium Agreement without the need to replicate said terms herein.

2. Scope of application

This Agreement governs terms of use by the MHA Parties of the CHIC data repository, associated infrastructure and components for the purposes of implementing the MyHealthAvatar project.

3. Grant of Access Rights

On the terms of this Agreement, the CHIC Parties grant to the MHA Parties Access Rights to the CHIC data repository, associated infrastructure and components as Needed for implementation of MyHealthAvatar.

In particular, such Access Rights include the rights to:

(a) access and use the CHIC data repository, in the section dedicated to MyHealthAvatar, and the repository access API for upload, storage and retrieval of data in MyHealthAvatar;

(b) access the CHIC IT infrastructure in order to access and use the CHIC data repository;

(c) permit officers and employees of the MHA Parties to access and use the CHIC data repository, associated infrastructure and components for realization of rights, granted to the MHA Parties above.

Each and all of these rights may be exercised by the MHA Parties together and/or by each MHA Party individually.

These rights are granted for the term of this Agreement on non-exclusive, worldwide, royalty free, non-assignable and non-transferable basis without the right to sublicense (except as permitted under clause 3 (c) above).

4. Access Rights in MyHealthAvatar synthetic data

MyHealthAvatar will generate the synthetic clinical data for running Nephroblastoma oncosimulations by itself. Access Rights and use of this data in MyHealthAvatar is governed by the rules on Access Rights under Section 9 of MyHealthAvatar Consortium Agreement.

5. Access Rights to the CHIC data repository and access API

UBERN grants the MHA Parties Access Rights to the CHIC data repository and application programming interfaces (access API) to access the repository, upload, download, store and retrieve data for MyHealthAvatar. These rights are restricted to the section designated for MyHealthAvatar. The MHA Parties do not have a right and should not have the technical possibility to access, use, extract, re-utilize and/or otherwise maintain themselves and exploit any other parts, contents and/or data from the CHIC data repository.

6. Access Rights to the CHIC IT infrastructure

All components of the CHIC data repository are deployed to the private cloud infrastructure provided by FORTH. Access Rights and use of the CHIC data repository in MyHealthAvatar

through the FORTH infrastructure are covered by the Access Rights to the CHIC data repository, as provided by UBERN. FORTH is aware that MHA Parties will access the CHIC data repository through its private cloud infrastructure, agrees to support the needs of MyHealthAvatar project in using the clinical data repository from CHIC and agrees to provide additional resources as may be needed for hosting MyHealthAvatar data in the CHIC data repository to the extent as doable by FORTH and as such resources are available to FORTH.

7. Access Rights to the Nephroblastoma oncosimulator and its application

Access Rights and use of the Nephroblastoma oncosimulator and Nephroblastoma oncosimulator application in MyHealthAvatar are governed by the rules on Access Rights set out by Section 9 MyHealthAvatar Consortium Agreement.

8. MyHealthAvatar account in CHIC data repository

UBERN agrees to create an account for MyHealthAvatar within the CHIC data repository, give account credentials to MHA Parties and provide a secure interface through which the MHA Parties may access the repository, upload and download their own data. UBERN agrees to assist the MHA Parties in setting up and/or implementing the data upload/download.

9. Security

The MHA Parties shall keep the credentials and identification information for the MyHealthAvatar account in CHIC data repository secure and confidential and take measures to protect the credentials from unauthorized access and use by third parties. For the avoidance of doubt, a third party includes any other party in the MyHealthAvatar project who is not an MHA Party that has signed this Agreement. The MHA Parties shall verify that credentials are stored and handled with due security, to disconnect the session with the CHIC data repository once the execution of the Nephroblastoma model is complete and the results are stored back in MyHealthAvatar.

Access to the account and/or any other means to get connected to the CHIC data repository is at risk and the responsibility of the MHA Parties. The MHA Parties or an MHA party must notify UBERN immediately if they or it become(s) aware of, or suspect(s), any forbidden connection to the CHIC data repository through the MyHealthAvatar account by a third party. In such circumstances, UBERN may at its own discretion grant MyHealthAvatar a new access allowing the MHA Parties to continue using the CHIC data repository. UBERN may alternatively, at any time, for a limited period or not, stop allowing the MHA Parties or an individual MHA Party to use the CHIC data repository if there are reasonable grounds to suspect that the MyHealthAvatar account is being used in a fraudulent or negligent manner which may cause liability for CHIC.

The CHIC Parties and the MHA Parties shall implement adequate Internet security measures, including state of the art data encryption, to ensure secure transfer of data in compliance with Internet governance and applicable laws.

10. Duration

This Agreement enters into force on the date when it is signed by all the CHIC and the MHA Parties, indicated above, and shall continue in full force and effect for the duration of the CHIC project, as defined in Article 3.2 CHIC Consortium Agreement.

11. Other rights

Nothing in this Agreement transfers or grants to the MHA Parties any right, title or interest in or to the CHIC data repository, associated infrastructure and components or any part of them, except as expressly set out in clauses 3, 5 and 6 above.

12. Miscellaneous

Should any provision of this Agreement become invalid, illegal or unenforceable, it shall not affect the validity of the remaining provisions. In such a case, the Parties concerned shall be entitled to request that a valid and practicable provision be negotiated which fulfills the purpose of the original provision.

This Agreement is concluded on the premises of and shall be interpreted in the spirit and according to the rules and principles of collaboration set out in the Memorandum of Understanding, signed between the two projects.

In case the terms of this Agreement are in conflict with the terms of CHIC and/or MyHealthAvatar Consortium Agreement and/or the CHIC and/or MyHealthAvatar Grant Agreement, the terms of the latter shall prevail.

Annex 9: Software component license compatibility table

	Component/Party	Software dependencies/Licenses	Method of use	License compatibility/Comments	Component license
1	Model repository ICCS	MySQL:GPLv2+[1] 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*[2]. **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[3]. 3-Clause-BSD compatible with GPL[4].	**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[5] **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

[1] http://www.mysql.com/products/workbench

[2] 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

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

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

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

					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 [6]; -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*[7]. **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[8]. 3-Clause-BSD compatible with GPL[9].	**License options: GPLv2+/GPLv3+** **Recommended license: GPLv3+** See p.1.
3	Tool Execution Engine ICCS	MySQL: GPLv2 Django: 3-Clause-BSD Tastypie: BSD 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*	**License options: AGPLv3+ with permission for MPL´d RabbitMQ** Please see p.1.

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

[7] 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

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

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

		Celery: BSD License, RabbitMQ: Mozilla Public License v 1.1[10] MongoDB: GNU AGPL v3.0 (drivers: Apache license)		*work. Thus, GNU GPL will cover the whole combination*[11]. **For GPL compliance, component must go under GPL.** 3-Clause-BSD compatible with GPL[12]. MPL v 1.1 is incompatible with GPLv2/AGPL[13] Apache v2 may be used in GPLv3[14]. 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.	Grant permission for linking component with MPL´d RabbitMQ under Section 7 GPLv3 (See Table 2); - identify software dependencies and associated 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:**

[10] https://www.rabbitmq.com/mpl.html

[11] 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

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

[13] Ibid.

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

					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) - please include the text of Apache v2 license[15].
5	Nephroblastoma Application ICCS	N/A	N/A	No open source	**Licensing not restricted.** **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	DCM4CHEE library: MPL v 1.1/GPL v2/LGPL v2.1[16]	Using the tool	No open source DCM4CHEE has triple license MPL v	**Licensing not restricted.** **Commercial and open source licensing**

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

[16] http://www.dcm4che.org/

	FORTH			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.	**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[17]; (d) A user must be given a possibility to get the 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[18]	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*[19]. **For GPL compliance, component must go under GPL.** Section 2 GPL v2: work based on the GPL´d	**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+**

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

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

[19] 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

				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+.	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[20].	**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 Repository FORTH/BED	Cassandra: Apache v2 [21]	Using the tool	Section 4 Apache v2: distribution in object and 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.	**Licensing not restricted.** **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.**

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

[21] http://cassandra.apache.org/

					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*[22]. Component must go under GPL. BSD 3-Clause License, MIT License compatible with GPL[23]. Apache v2 is compatible with GPL v3[24]. Codes under GPLv2+, LGPL v2.1 may be used in software licensed under GPLv3[25]. CDDLv1 and EPL v1 are not compatible with GPL[26]. Use of these tools in GPL software requires additional permission under Section 7 GPLv3.	**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[27] **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

[22] https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic
[23] https://www.gnu.org/licenses/license-list.en.html
[24] https://www.apache.org/licenses/GPL-compatibility.html
[25] https://www.apache.org/licenses/GPL-compatibility.html
[26] https://www.gnu.org/licenses/license-list.en.html#GPLIncompatibleLicenses
[27] https://www.gnu.org/licenses/gpl-faq#DoesTheGPLAllowDownloadFee

					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[28]; -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[29] GPLv2+ BSD 3 Clause License Creative Commons Attribution-Non-Commercial 3.0 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, the terms and conditions of the GNU General Public License cover the whole combination*[30]. **For GPL compliance, component must go under GPL.** BSD 3-Clause License, MIT License, CC BY-NC 3.0 compatible with GPL[31]. GPL v2+ allows upgrade, tools under GPL	**GPL v3+** **Commercial licensing not allowed; fees for physical transfer of copies, warranty and support may be charged (Section 4 GPL v3).** 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**

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

[29] https://greensock.com/standard-license

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

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

				v2+ may be used in software under GPL v3[32]. 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.	**6)** **To license under GPLv3:** - please include GPLv3 license notice into each source file (See Table 1); - please include text of GPL v3 license[33]; -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*[34]. **For GPL compliance, component must go under GPL.** MIT License is compatible with GPL[35]. Apache v2 tools may be used in GPL v3 software[36].	**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 Management BEDS	CDDL v1 GPLv2+ with CPE Apache v2 CPL v1 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*[37].	**GPL v3+ with permission to link component with 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**

[32] https://www.apache.org/licenses/GPL-compatibility.html
[33] https://www.gnu.org/licenses/gpl.html
[34] https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic
[35] https://www.gnu.org/licenses/license-list.en.html
[36] https://www.apache.org/licenses/GPL-compatibility.html
[37] https://www.gnu.org/licenses/gpl-faq#GPLStaticVsDynamic

		LGPL v2.1 MIT License		**For GPL compliance, component must go under GPL.** MIT License is compatible with GPL[38]. Apache v2 programs may be used in GPL v3 software[39]. Programs under LGPL v2.1, GPL v2+ may be used in software under GPLv3[40]. CPL v1 and CDDL v1 are not compatible with GPL[41]. Use of these libraries in GPL software requires additional permission under Section 7 GPL v3[42].	**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[43]; -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

How to apply	GPL v3 License notice
Attach the following notices to the program. It is safest to attach them to the start of	`<one line to give the program's name and a brief idea of`

[38] http://www.gnu.org/licenses/license-list.en.html
[39] https://www.apache.org/licenses/GPL-compatibility.html
[40] https://www.apache.org/licenses/GPL-compatibility.html
[41] http://www.gnu.org/licenses/license-list.en.html
[42] https://www.gnu.org/licenses/gpl-faq#GPLIncompatibleLibs
[43] https://www.gnu.org/licenses/gpl.html

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.	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.