Deliverable No. 4.3.1

Development of the data protection

and copyright framework for CHIC

first iteration

Grant Agreement No.:	600841
Deliverable No.:	D4.3.1
Deliverable Name:	Development of the data protection and copyright framework for CHIC first iteration
Contractual Submission Date:	31/05/2014
Actual Submission Date:	31/05/2014

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:	**CHIC**
Project Full Name:	Computational Horizons In Cancer (CHIC): Developing Meta- and Hyper-Multiscale Models and Repositories for In Silico Oncology
Deliverable No.:	D4.3.1
Document name:	Development of the data protection and copyright framework for CHIC first iteration
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	RE
Version:	9.0
Actual Submission Date:	31/05/2014
Editor: Institution: E-Mail:	Nikolaus Forgó LUH forgo@iri.uni-hannover.de

ABSTRACT:

This deliverable is the first of a two part iteration deliverable that describes the data protection, data security and intellectual property rights framework developed for the CHIC project. It builds on the previous deliverables – D4.1 and D4.2, and shows the concrete legal, organisational and technical measures put in place to safeguard the medical data used for the project. Part of these measures include data protection agreements to be concluded between project partners and a dedicated central data protection authority (CDP), created to act in place of the consortium, which for lack of legal personality could not conclude such agreements.

Regarding IPR issues, this deliverables also shows the various forms of protection that could be extended to the both the background and foreground involved in the project, especially, the models and hypermodels. Frameworks considered in this regard include: protection as computer program, protection as trade secret and knowhow, as well as protection of the medical data involved in the project as copyright or database right under EU law. Similarly, an IPR memorandum of understanding is also presented, to address gaps in the IPR management envisaged in the project, and which were not fully tackled by the Consortium Agreement.

KEYWORD LIST:

Data Protection, Data Security, Intellectual Property Rights

---

[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)

MODIFICATION CONTROL			
Version	Date	Status	Author
1.0	28/02/2014	Draft	Iheanyi Nwankwo, LUH
2.0	14/03/2014	Draft	Iryna Lishchuk, LUH,
3.0	15/04/2014	Draft	Marc Stauch, LUH, Iryna Lishchuk, LUH
4.0	06/05/2014	Draft	Iheanyi Nwankwo, LUH
5.0	09/05/2014	Draft	Marc Stauch, LUH,
6.0	14/05/2014	Draft	Iheanyi Nwankwo, LUH, Elias Neri, Custodix
7.0	19/05/2014	Draft	Nikolaus Forgò, LUH
8.0	27/05/2014	Internal Review	Jos Devlies, Custodix, Elias Neri, Custodix
9.0	30/05/2014	Final	Marc Stauch, LUH, Iheanyi Nwankwo, LUH

List of contributors

- − Elias Neri, Custodix
- − Iryna Lishchuk, LUH
- − Iheanyi Nwankwo, LUH
- − Marc Stauch, LUH
- − Nikolaus Forgò, LUH

Contents

1 Executive Summary

The CHIC project aims at developing cutting edge ICT tools, services and secure infrastructure to foster the development of elaborate and reusable integrative models (hypermodels) in the field of cancer diagnosis and treatment, as well as larger repositories so as to demonstrate benefits of having both the multiscale data and the corresponding models readily available in the VPH domain. In the course of developing these tools, both retrospective and prospective patient data will be used to test these models as well as validate them. In Deliverable D4.1 (submitted at PM6 in September 2013), the legal and ethical requirements for the processing of this sensitive health data were analysed; the present deliverable builds upon that outcome by outlining a concrete data privacy framework, including an updated security framework and set of agreements for the CHIC partners to sign, so as to permit the safe, ethical and legally compatible sharing and processing of data by the partners during the initial lifetime of the project (up until PM42), within a secure, closed and trusted network.

In the second place, this deliverable provides a follow-up analysis, to that of Deliverable D4.2 (submitted at PM9 in December 2013), of intellectual property right (IPR) issues arising out of the development of the CHIC models and tools. Here, the analysis considers in further concrete detail both the nature of rights likely to be generated, and the question who owns the relevant rights. Given the importance of safeguarding against the possible loss of economical and scientific interest of the research as a consequence of sharing creativity, this will also address how far the default rules set out in the FP7 GA (Annex II) and provisions of the CA are sufficient to deal with potential matters (both as regards the project background and foreground), and whether further augmentation or clarification of the rules may be desirable in a specific addendum or memorandum of understanding.

As regards both of the above areas of analysis, this Deliverable presents the first iteration of the data protection and copyright framework, expected to cover the majority of the project development phase (up until PM42). Subsequently, to take account both of progress in the project itself – including a putative targeted service phase towards the end of the project - and likely changes in the external legislative position, not least the probable passing and entry into force of the new EU General Data Protection Regulation (to replace the current Directive 95/46/EC), a second iteration of the framework will be submitted as Deliverable D4.3.2 in PM42.

2 Introduction

2.1 *Purpose of this document*

This document describes the data protection, data security and IPR framework developed for the CHIC project. It is the first of a two part iteration deliverable that shows the concrete data protection and IPR framework, and builds on the previous deliverables – D4.1 (Initial analysis of the ethical and legal requirements for the sharing of data) and D4.2 (Initial analysis of the copyright-related legal requirements for the sharing of data). Here, the concrete legal, organisational and technical measures put in place to safeguard the medical data used for the project is emphasized. Part of these measures include data protection agreements to be concluded between project partners and a dedicated central data protection authority (CDP), created to act in place of the consortium, which for lack of legal personality could not conclude such agreements. These are annexed as appendices 2-4 of the current deliverable. For the technical security measures, the analysis in this deliverable has been simplified due to the fact that the D5.1.1 (The CHIC technical architecture –initial version) already contains in-depth analysis of the security framework. In order not to repeat such details, a simplified approach has been adopted here, and it is advised that both documents be consulted together for a fuller technical overview of the security layer of the project.

Regarding IPR issues, this deliverable also shows the various forms of protection that could be extended to the both the background and foreground involved in the project, especially, the models and hypermodels. Frameworks considered in this regard include: protection as computer program, protection as trade secret and knowhow, as well as protection of the medical data involved in the project by copyright or database right under EU law. Similarly, a model IPR memorandum of understanding has also been formulated to take care of the gaps in the IPR management envisaged in the project, and which were not fully tackled by the Consortium Agreement. The IPR memorandum is included as appendix 5 of the deliverable.

3 Structure

3.1 Structure of the Deliverable

The deliverable describes the first iteration of the data protection and copyright framework of the CHIC project. It is divided into two broad parts. The first part consists of chapter 4, and presents the data protection and data security framework. Here the legal and organisational measures, as constituted and set out in three contractual agreements, the data Provider Agreement, the End User Agreement, and the Trusted Third Party Agreement, are presented in part 4.2, and their key provisions described. As explained in part 4.3, the relevant measures are designed to create and sustain a 'network of trust' between the project partners providing and utilising clinical data within the Project, allowing the use of the data to achieve the Project purposes in a safe, well-considered, and respectful manner. The technical security measures that are equally essential for the proper and effective functioning of the framework are then elaborated in parts 4.4-4.6.

The second main part of the deliverable, chapter 5, describes the intellectual property framework of the project. This expands upon the initial IPR analysis presented in Deliverable D4.2, by presenting (in parts 5.2-5.4) a detailed examination of the legal issues associated with the protection of model, hypermodels, and medical data, and the potential implications for the CHIC project. Subsequently, in parts 5.5-5.6, attention is given to IPR ownership, and licensing compatibility issues that may arise from deploying open source components.

At the end of the document, in Appendices 2-4, the draft data protection agreements developed for the above purposes are presented, as well as (in Appendix 5) the model IPR memorandum. Appendix 6 contains the ethics approval obtained by partner KU Leuven for the provision to CHIC of further glioblastoma image data, and Appendices 7-8 then present explanatory material, further detailing the operation of the project's technical data security framework.

4.   CHIC Data Protection Framework

4.1   Introduction

The project CHIC (Computational Horizons In Cancer) aims at creating and developing models and hypermodels for use in the diagnosis and treatment of cancer. For these purposes, the technical partners in the project, modellers in particular, will require real clinical data to work with that has been provided to the project by the clinical partners. As set out in Deliverable D4.1, the CHIC project will initially proceed by using data on Wilms tumour (to be provided by partner USAAR), glioblastoma multiforme (provided by partners KU Leuven and UBERN), prostate cancer (provided by partner UNITO), and non small cell lung cancer (provided by USAAR), but it is projected to involve further cancer types in the future. The data from these concrete clinical scenarios will undergo processing within the CHIC environment, and validation will be based on the clinical and oncological data produced by the same scenarios. In these scenarios, various data to be dealt with include: clinical data, imaging data, metadata, annotations, added semantic information to data and model / hypermodel configuration parameters.[3] The final purpose of such scientific research is to improve cure and management of future cancer patients.

Accordingly data repositories will be set up within the CHIC infrastructure to enable the project's partners to share clinical data. At the same time, as discussed in Deliverable D4.1, it remains of critical importance to protect such data, not only as a legal obligation, but also as an ethical requirement due to their sensitive nature. Here the CHIC project will make use of a tried and trusted approach, which has been successfully deployed in a number of past and on-going EU projects, where it was also important to work with real clinical data after setting up the platform, namely ACGT, P-Medicine, and EURECA. The basic assumption of the relevant data protection framework is that the best way to safeguard patients' rights would be achieved, if only anonymous data were processed in the project. This led to the difficulty, that – even after the removal of the more obvious patient identifiers – the absolute anonymity of clinical micro-data (as opposed to purely statistical data compiled from multiple patients) cannot be guaranteed due to the fact that rare (and potentially individuating) values may need to be retained in the datasets to meet the needs of the project. Secondly, given the possibility of project findings with significant potential benefit to a patient, a feedback procedure would be required in order to let patients participate in such an outcome. In order to deal with these matters, a data protection and ethics framework has been developed, which incorporates secure technical, organisational and legal measures to so far as possible eradicate risks to the privacy and/or autonomy interests of relevant patient subjects. In the result the projects have been able to work with de facto anonymous data, backed up by additional features acting as a 'safety net'.

As applied to CHIC this framework can be seen to consist in three core aspects or 'pillars'. In the first place a set of contracts are in the process of being concluded between the project partners and a legal entity representing the consortium, providing amongst others data protection policies, clauses on liability, in case data is unlawfully matched or disclosed, as well as provisions to ensure the safe disposal of data once it is no longer required for the purposes of the Project. Since the consortium had no legal personality, the Center for Data Protection 'CDP', a Belgian non-profit organisation, originally founded during the ACGT project, will act on behalf of the consortium.[4] The CDP will conclude these contracts, whose legal effect is to create a closed-world 'network of trust' for secure, lawful and ethical data sharing, with all partners providing and/or having access to clinical data. Drafts of the relevant contracts (Data Provider Agreement; End User Agreement; Trusted Third Party Agreement) are annexed in Appendices 2-4 at the end of this deliverable, and the scope and

---

[3] See the Description of Work (DOW) Part B, pp. 5-8.

[4] Ibid, pp. 99-100.

effect of their individual provisions will be further analysed in parts 4.2 and 4.3 of this deliverable below.

In the second place, as detailed below in part 4.4, a security infrastructure is being set up, including dedicated de-identification software (CAT) and user-identification and authentication services. The 'context of anonymity' thereby established will provide an environment in which the re-identification of participating patients from inside or outside the project is not possible with means likely reasonably to be used with respect to time, expense and labour. From a legal point of view therefore, in accordance with the criteria set out in Directive 95/46/EC, only anonymous data, which is no longer subject to the data protection regime, will be processed. Thirdly, prior to providing their data to the CHIC infrastructure, the relevant clinical partners – as well as undertaking initial on-site de-identification of the data – are either to obtain the specific informed consent of the relevant patients to the processing of the data within CHIC, or (where gaining such consent is not reasonably practical, as may be the case with previously collected, retrospective data) relevant ethical body approval. As examined in Deliverable D4.1, this safeguard is crucial, not only for ethical reasons of respecting patient autonomy, but also under data protection law in order to provide a valid legal basis for further processing the data (by de-identifying it and transferring it to the CHIC infrastructure) at a time when *ex hypothesi* it is not yet within the ambit of the CHIC data protection framework of de facto anonymity, so still qualifies as personal data.

As discussed further in part 4.2, in order to ensure the project proceeds in a fully ethically unimpeachable manner, using validly obtained data, and also to provide a fall-back basis for the project to lawfully process the data, the relevant consent/ethics approval obligations are placed on data providers as part of the CHIC contractual framework. As presented in Deliverable D4.1 (Appendix 4), such approvals already exist for the retrospective data to be provided to the Project by partners USAAR, KU Leuven, and UNITO. Subsequently, KU Leuven has obtained ethics committee approval for the use within CHIC of additional gliobastoma image data: that approval is appended to the present deliverable, as Appendix 6. As also discussed under 4.2, later in the project, as regards prospective data sent by data providers to the project, it will be crucial for patient subjects when consenting to this, to provide for what should happen in the event that analysis of their data reveals clinically relevant information for their future treatment. The first iteration framework presented in the current deliverable is, though, principally directed at ensuring the ethical, lawful, and secure processing of the retrospective patient data required by CHIC.

4.2   Legal and Organisational measures

As explained above, the legal and organisation component of the CHIC data protection framework is constituted by a series of three contractual agreements: the CHIC Data Provider Agreement, to be signed by the (clinical) partners providing patient data to the CHIC infrastructure; the CHIC End User Agreement, to be signed by any partner (primarily the technical partners) that will access and process the clinical data within CHIC; and the CHIC Trusted Third Party (TTP) Agreement, to be signed by the entity (here the project's data security partner, Custodix) performing the special function of trusted third party (as detailed in subsection (3) below). In each case the other party to the contract will be the Center for Data Protection (CDP), which as explained in 4.1 assumes a co-ordinating role, not only in CHIC but other similar EU projects, such as ACGT, in ensuring the maintenance of a stringent and coherent data protection and security framework.

4.2.1 CHIC Center for Data Protection

As mentioned, the CHIC CDP serves as the central data controller for the project with the primary aim of ensuring compliance with the data protection and security framework established for the project. The utilization of the CDP as a central data controller has solved

the need for a legal body in lieu of the consortium, with the capability of concluding binding data protection contracts among the multiple parties involved in the project. The CDP also serves as a hub where data subjects or supervisory authorities can obtain information about the project, as well as clarify any issues that they may have.

After the data transfer to the CHIC infrastructure, the CDP will be responsible for the security of data processing within the CHIC project. The technical security aspects of the framework, have been delegated by the CDP to the security expert partner (Custodix), and there is a long-standing contractual relationship under which Custodix has successfully fulfilled the same function in respect of other projects (ACGT, P-medicine, EURECA). Custodix in this respect has the direct control and responsibility for the deployment of state of the art security measures to protect the CHIC infrastructure. Further, the CDP monitors and controls the compliance with these contractual agreements. It thus serves as a central data protection authority for the CHIC framework, and a contractual party to the above mentioned data protection agreements. In the subsections below, the governing provisions of each of these agreements are considered in turn.

4.2.2 CHIC Data Provider Agreement

The CHIC Data Provider Agreement sets out the terms and conditions under which patient data will be transferred to the CHIC infrastructure by the CHIC data providers (participating hospitals/investigators). The agreement consists of a preamble followed by nine clauses, and makes it a prerequisite for the data provider to transfer data based on the patients´ informed consent to use their data for research within CHIC and/or the approval of the relevant data provider's responsible ethical board or committee. Under the agreement, the patient data remain under the control of the respective hospital/investigator (data provider) where the data are collected until the data have been transferred to the CHIC infrastructure. Thus the data provider is obligated to ensure the confidentiality and protection of the data within its domain.

The parties to the Data Provider Agreement are the individual clinical partners and CDP, and their obligations are defined in two of the clauses of the agreement. Clause 3 outlines the obligations of the CDP to implement appropriate technical and organisational measures to secure data within the CHIC domain, including a secure double encryption of the transferred data. Clause 4 on the other hand outlines the obligations of the data provider. Importantly, these include obtaining valid informed consent of each patient and/or ethics body approval and/or required notification to data protection authorities before transferring the data to the CHIC infrastructure as earlier indicated. Furthermore, the data providers shall first perform a de-identification process on the patient data before the transfer.

4.2.3 CHIC End User Agreement

End user contracts are concluded between the partners using data within CHIC and the CDP that guarantee the protection and security of the CHIC data that the users need to access and process to carry out their work in the project. These provisions also ensure that patient data are not transferred to any party outside the project and no matching of data sets takes place that could identify the patients concerned. Similarly to the data provider agreement, the end user agreement also consists of a preamble followed by nine clauses. Obligations of the parties are set out in clauses 3 and 4. The CDP is obligated to implement appropriate technical and organisational measures to secure data within the CHIC domain under clause 3. The end users on the other hand, as stipulated in clause 4, have to ensure that appropriate technical and organisational measures are implemented within their processing environment to secure the data they obtained for research. In addition, they shall not attempt to identify any patient from the CHIC data either by external matching of the data or by any

other means; and will refrain from disclosing or publishing the CHIC data to any third party, including their subcontractors. To ensure strict compliance, the liabilities under data protection laws for negligent violation of these obligations are adverted to, and an indemnity from a party in breach required to the benefit of other project partners. In addition, a penalty clause is proposed in the agreement that foresees a set amount of liquidated damages that the party may be required to pay to the consortium in such circumstances.

4.2.4 CHIC TTP Agreement

The TTP agreement consists of a preamble, plus eight further substantive clauses, and will be concluded between a Trusted Service Provider (TSP) on the one part and the CDP on the other. It is needed to state the conditions and obligations under which the TSP, who will be the data security specialist partner Custodix, will act as a trusted third party (TTP). All data transferred to the CHIC infrastructure will be initially pseudonymised on-site by the data provider concerned; it will then be pseudonymised a second time by the CHIC TSP using dedicated state of the art pseudonymisation software, in which the initial data provider's pseudonym is replaced by a second pseudonym. The pseudonymisation key needed to link the double-pseudonymised data set to the initial pseudonymised set will be kept by the CHIC TSP acting as a Trusted Third Party. The CHIC TSP's independence from both data providers and end users will be guaranteed, as set out in the contractual obligations with the TSP in the TTP agreement. In essence, the TTP is obligated to retain the key in a secure manner, protected by state of the art access security, and shall not disclose the key to any third party including project researchers or its subcontractors as stipulated in clause 4 of the agreement. That means that the end user using the data will be unable to re-establish a link to the patient to whom the data relates. In interaction with strong technical and organisational security measures, patient data in CHIC is to be seen as de-facto anonymous.

At the same time, the key held by the TTP preserves the possibility in exceptional circumstances of re-identifying a given patient, in particular in the event that a new treatment for him/her is developed. This can occur only with the help of the TTP and with permission of the CDP, and where the patient concerned has indicated to his/her physician that he/she wishes to be informed. For the avoidance of doubt, insofar as project-goals, such as the need to test or validate the performance of hypermodels later in the project, make it necessary to re-link data in the CHIC infrastructure to real patients, such re-linkage shall not be permitted without the further specific consent of the patients concerned and/or the obtaining of appropriate ethics body approval. Due to the involvement of at least three different and independent parties (treating physician, TTP, CDP) the risk of misuse of this re-identification possibility is sufficiently remote so as not to jeopardize the de-facto anonymisation.

4.3 Framework rationale

4.3.1 Justificatory basis during Project development phase

There are several reasons for having a framework of the form described, which sets out the interactions and reciprocal responsibilities of the key participants in CHIC, especially as regards to handling the sensitive health data processed using the platform. First, from the data providers' point of view, it allows the rights, responsibilities and potential liabilities that they may have in relation to the data (including to their patients as sources of the data) to be catered for in the Data Provider Agreement. Admittedly, as noted above and further detailed in Part 4.4 below, the intention is that all CHIC data processed by End Users will already have undergone a rigorous de-identification procedure. Thus the data are already well protected at a technical level. However, also of great importance – apart from such technical safeguards – is to respect the patient's autonomy interest in the use made of their data. In

this regard, the Data Transfer Agreement ensures, in conjunction with the reciprocal obligations on technical partners in the End User Agreement, that data are not processed incompatibly with the purposes for which patients originally consented to its collection.

More generally, data anonymity itself cannot be maintained sufficiently by technical means only, but requires a combination of technical, organisational and legal controls that together ensure that a link cannot be reasonably re-established between the data and the human subject from which it derived. In this regard, the CHIC data protection framework, including the set of ancillary agreements, forms a necessary complement to the use of technical privacy enhancing measures at the point that identifiable health data are converted into doubly-de-identified CHIC data. Above all, there is a need to ensure that the technical partners who process the data for Project purposes maintain strict control of the data to prevent it from escaping into unforeseen interpretational contexts, including the general public domain where they could be freely accessed (and, notwithstanding the previous rigorous de-identification measures), possibly be re-linked by a sufficiently determined person through matching them against other external data.

In this regard, and by reference to the analysis in the last-mentioned Deliverable of other European projects that LUH has been party to where sensitive health data are processed for research, such as ACGT, p-medicine and EURECA, a key indicator favouring such a framework is that data originally stemming from individual patients are to be made centrally accessible via a central IT-infrastructure to a potentially unlimited number of users. Moreover, there are the examples of UK Biobank,[5] and the confidentiality framework of NHS England's Health and Social Care Information Centre (HSCIC),[6] which similarly utilise contractual undertakings from expert users accessing centralized repositories of (pseudonymous) patient data to maintain requisite data security and confidentiality. This approach is also recommended by the Article 29 Working Party, set up under Directive 95/46/EC, as an essential safeguard when reusing clinical data for research purposes.[7]

If the above framework operates properly, and each of the parties abide by their respective obligations, as outlined above, then this should guarantee full, legally and ethically required protection of both patient autonomy and data confidentiality and privacy. However, in order to take account of the possibility that one or other party might act in breach of their primary obligations, it is also necessary for the set of Agreements to contain a number of *secondary* obligations (i.e. obligations that are triggered by a party defaulting on a primary obligation). Such secondary obligations deal with matters such as assigning and clarifying liability, for example if a given breach of data privacy occurs, etc, thereby offering reassurance to innocent parties, i.e. those not responsible for the breach in question. In this regard, the Data Provider and End User Agreements each contains an 'liability and indemnity clause' (clause 6), in which each respective party agrees to indemnify and hold harmless the other parties in the event that a claim is made against them in respect of a matter for which it is responsible.

It is also advised that a further secondary obligation in the form of a fine or penalty of a liquidated sum to the Project Consortium should be utilized, as seen in both the Data Provider and End User Agreements (clause 7). A key justification for such a clause is to establish internal obligations between partners within a closed data user community or "network of trust". The formation of this implies that partners accept reciprocal accountability towards each other and the Center for Data Protection (as overseer of the community). This includes enforceable commitments to look after the data appropriately, not disclose it beyond the community, and not to try and re-identify it. The clause would act as a deterrent against a

---

[5] See UK Biobank's Ethics and Governance Framework (v.3), at: https://www.ukbiobank.ac.uk/wp-content/uploads/2011/05/EGF20082.pdf?phpMyAdmin=trmKQIYdjjnQIgJ%2CfAzikMhEnx6.

[6] The HSCIC guidance, from 2013, is avilable at: http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf.

[7] See Art 29 WP, Opinion 03/13 on Purpose Limitation (00569/13/ENWP203), available at p 32; at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

wilful or negligent breach of the primary obligations leading to unauthorised re-identification of data subjects. In particular, it is critical to guard against breaches that might compromise the security or privacy of the CHIC data with adverse implications for the fundamental interests of the patients from whom the data stemmed. This reinforces the awareness of compliance issues, and by thereby minimizing the circumstances in which re-identification would likely occur (in line with the terms of recital 26) is significant in terms of ensuring the data remain anonymous for the purposes of the EU Data Protection Directive.

A final important matter the framework of Agreements regulates is the circumstances in which the participation of one or more parties within the CHIC platform shall terminate, as well as what should happen in such cases to the data in the platform. This is covered under the 'termination clause' found in each Agreement (as clause 8). The effect here broadly is that each party may by writing bring the relevant Agreement to an end in the event of a breach of obligation by the other party to it, or by otherwise showing good cause. At the same time the obligation on the parties to take all necessary steps to maintain the privacy and security of the data (up until such time as it is erased) remains.

4.3.2 Additional considerations arising during putative targeted service phase

The above agreements have been designed to take care of the development phase of the project, and will operate within a closed community of researchers. Afterwards, there is the potential, during the service phase of the project, i.e. during the latter stage of platform validation, when the services are running, that a new model of service level agreement will be in place. This is envisaged to happen at the end of the project, when the infrastructure will be open to external researcher and clinicians, who would want to get some treatment predictions based on the developed models and hypermodels. Users then will be required to enter into a service level agreement that will incorporate data protection obligations of the parties. In this regard, the external user who will upload data into the CHIC infrastructure will be regarded as the data controller, and be responsible for obtaining the consent of the data subjects or any other approval that may be required in that case. The CHIC infrastructure will maintain all the technical, organisational and security features that have been embedded into the design of the system to protect data. The CHIC service provider in this scenario will be regarded as a data processor. The second iteration of this deliverable presented in D4.3.2 will incorporate a detailed analysis of this phase of the service including the service level agreement which will be developed once the specifics of the CHIC services have been clearly mapped out.

4.4 Technical Measures

Apart from the legal and organisational measures described above, the data protection framework of the CHIC project also comprises a number of technical measures aimed at secure processing of the CHIC data. As indicated in D4.1, security will be imbedded in the whole data protection framework. As organisational measures alone may not be adequate to implement the required safeguard, a combination of technical controls that together ensure that a link cannot be reasonably re-established between the data and the human subject from which it derived is a necessary complement. Below, we will describe the technical tools to maintain the de facto anonymous nature of data in the CHIC framework.

4.4.1   Security Tools and Services

Two important documents, Deliverable "D5.1.1: The CHIC technical architecture – initial version", which describes in detail the CHIC Security Tools and Services, and deliverable "D5.2: Security guidelines and initial version of security tools", which will be due in M18 as an

update of the former, contain the security aspect of the CHIC infrastructure. As a result of the fine grained technical analysis in those documents, this section will not go into much technical detail but instead gives a short summary of the security framework relevant for the purposes of this current framework.

The CHIC Security Tools and Services are based on a security framework developed in past and ongoing European projects such as ACGT, P-Medicine and EURECA. It provides components dealing with authentication, authorisation and auditing. These components are based on widely used industry standards such as SAML, WS-*, XACML.

The security tools and services encompass the following components:

1. Authentication and Identity Management Components
   a. The **Identity and Access Management Site** (IAM) is responsible for user enrolment and management. IAM allows (virtual) organisations, attributes and roles to be assigned to users. These are then used through access rules defined in the authorisation policies to give the user access to restricted resources.
   b. The **Identity Provider** (IdP) is responsible for the authentication of users who access CHIC services through a browser. It provides identity assertions, which identify the user, to all CHIC Web Sites.
   c. The **Secure Token Service** (STS) is responsible for the authentication of users who access CHIC Web Services (through a non-browser client). It provides identity assertions to all CHIC Web Services.
2. Authorisation components
   a. The **Policy Decision Point** (PDP) is the entity which takes authorisation decisions. A PDP accepts authorisation requests.
   b. The **Policy Administration Point** (PAP) is the endpoint responsible for managing policies. The PAP provides the PDP with all policies required to produce an authorisation decision. The PAP has management services through which authorisation policies can be defined.
   c. The **Policy Information Point** (PIP) provides the PDP with the needed information (attributes) to take an authorisation decision. Most resource and subject attributes are already provided through an authorisation request. If the PDP needs an attribute that was not provided, this can be obtained through the PIP.
   d. A **Policy Enforcement Point** (PEP) is a component which integrates the authorisation services with application code. The PEP is responsible for creating the authorisation request and sends it to the PDP.
3. Audit Service
4. Security gateway/proxy
5. Integration modules and extensions
   a. Various integration modules are available within CHIC to integrate JAVA, PHP and .NET applications into the security framework.
   b. Extensions (e.g. for Liferay)

4.4.2 Data Transfer Protocol

Health data of a patient is collected by the treating physicians and analysed and stored within the treating hospitals. This data is imported into the CHIC research project by uploading it to the CHIC data repository. CHIC users and researchers can then work with this data through the CHIC tools accessible from the CHIC portal.

As previously explained in Deliverable D4.1 there is a clear distinction between the treatment domain, where the treating physician collects information on the patient for medical treatment, and the research domain where data is used for scientific research. The collection, storage and processing of treatment data at the hospital is typically covered within the treatment contract with the patient. When exporting data from the hospital for research purposes though, anonymisation is the best way to protect a patient's privacy. CHIC envisages the re-identification of a patient when the research results reveal that a certain therapy would be highly effective for that given patient. Therefore data cannot be fully anonymised.

The CHIC data protection framework is based on "de facto anonymous data".[8] Sources will upload their data in a pseudonymous form to the CDP Pseudonymisation Services. The CDP pseudonymisation services will then encrypt all pseudonyms, with a key held by the TTP. This implies that it is not possible to go back from the encrypted to the original pseudonym without the involvement of the CDP resulting in de facto anonymous data as explained in the CHIC Framework of Terms in the annexed data protection agreements.
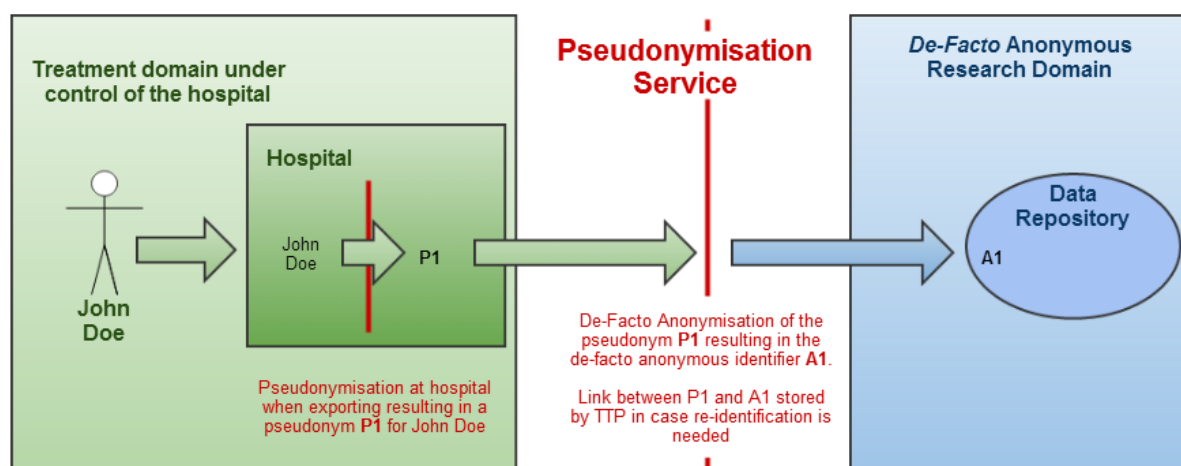
Figure 1 Data transfer flow

If a patient agrees to participate in CHIC, it is the physician who triggers the transmission of the respective medical data to the CHIC data store. The data is first pseudonymised at the source, in this case the hospital. This pseudonymised data is then uploaded through the CHIC Pseudonymisation Service into the CHIC data store. The Pseudonymisation Services de facto anonymises the data with a second pseudonymisation round. The TTP holds this second round's pseudonymisation key and thus also serves as vault for the link back to the patient.

CHIC Pseudonymisation Tools

4.4.2.1.1   CATS (Custodix Anonymisation Tool Services)

CATS (the Custodix Anonymisation Tool Services) is a set of tools and services responsible for the de-identification of data files. It consists of the CATS Engine, CATS Privacy Profile Store, CATS Data Upload Interfaces, CATS Upload Client and CATS Server.

The CATS Engine de-identifies a data file based on a set of pre-configured transformation rules (privacy profiles). The privacy profiles that need to be executed on a data file are matched based on the data file's mime type and schema. The CATS Engine can currently

---

[8] See the general framework of terms in the annex for explanation of the term.

process XML, CSV, DICOM, CEL, plain text, PDF and WORD documents. Other data formats can be added as needed through engine extensions.

Key privacy transformation rules are:

- Scan for and replace patient identifying data by pseudonyms.
- Clear patient identifying data.
- Encrypt (parts of) the pseudonymised result file.
- Generalise sensitive indirect identifying data (e.g. replace age by age groups such as 40-50).
- Make visit dates relative to the patient data of birth and randomise that date.
- Remove identifying information from embedded free text.

The CATS Engine downloads the privacy profiles it needs from the CATS Privacy Profile Store. CATS provides a browser interface through which privacy profiles can be uploaded. Privacy profiles are XML files and can be edited through the standalone tool CAT (Custodix Anonymisation Tool).
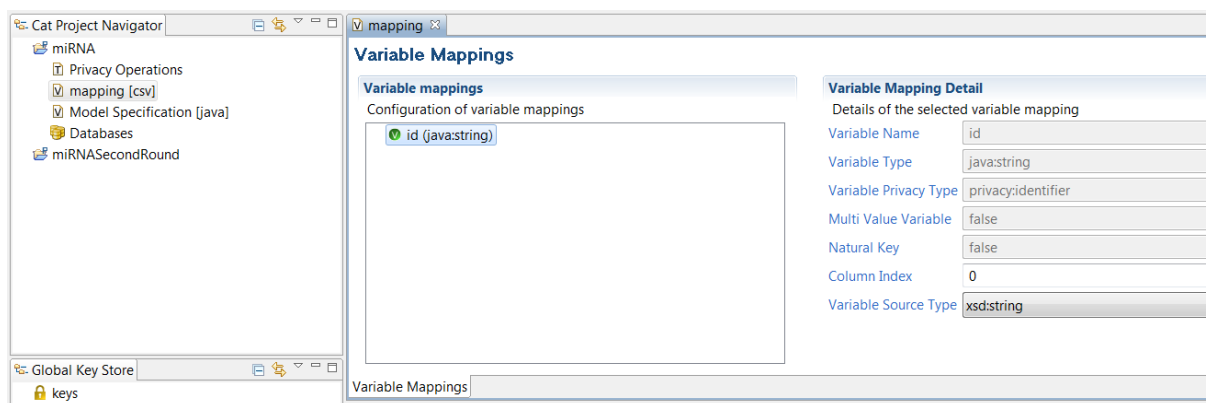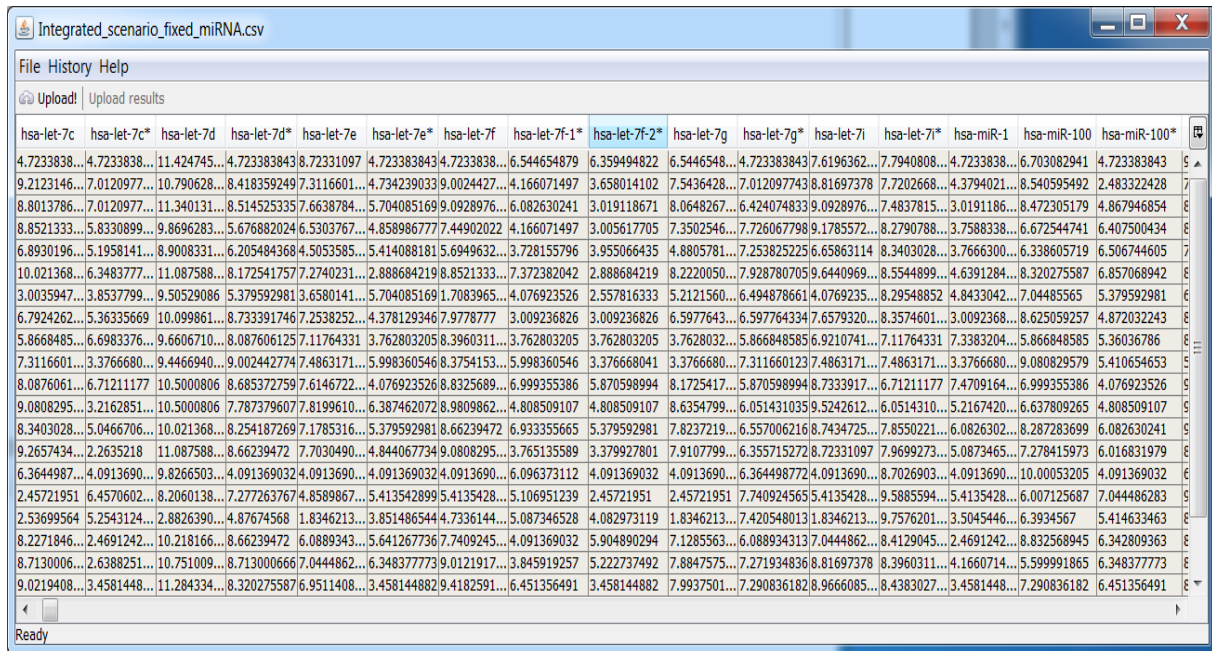
Figure 2 CAT workbench through which privacy profiles are created

The CATS Server is a web frontend and REST/SOAP web service endpoint which glues together the CATS engine, privacy profile store and upload interfaces. Data files uploaded to the CATS server are processed through the embedded engine by downloading profiles from the embedded privacy profile stores. Processed files are then uploaded by CATS to a backend data repository.

The CATS Upload Client is a client application with embedded CATS engine, responsible for the client side pseudonymisation and upload of data files to the CATS Server. The CATS Upload Client is not the standard CHIC upload tool, but it can be used if data formats need to be processed and uploaded which are not supported by the CHIC Upload Tool. The CATS Upload Client supports any of the data formats supported by the CATS Engine.

4.4.2.1.2 CHIC Data Upload Tool

The CHIC Data Upload Tool with embedded CATS engine can be used by a source/hospital to pseudonymise a data file (first round) and upload it through CATS (responsible for the second round) into the CHIC data repository.

Figure 3 CHIC Upload Tool

Currently CSV and DICOM are supported. Other file formats can be added as needed. The big advantage of the Data Upload Tool compared to the CATS Upload Client is the graphical user interface through which data files can be reviewed before uploading them. This allows the data source to verify whether a file is pseudonymised correctly.

4.4.2.1.3   The CHIC Pseudonymisation Service

The CHIC Pseudonymisation Service is implemented by the CATS Server. Data files which are already pseudonymised at the client can be uploaded to the CATS Server. The CATS Server performs a second pseudonymisation round and upload the resulting de facto anonymous files to the CHIC Data Repository.

4.4.2.1.4   Patient Identity Management System (PIMS)

PIMS indexes patients through common characteristics such as names, former names (e.g. maiden name), date and place of birth and other identifying information. From a data protection perspective it has to be pointed out that this approach requires the transfer of personal data of the patient to a third party holding the common PIMS database. Such a transfer of personal data requires a legal basis, which will have to be the patients´ prior informed consent, since the data protection law does not allow for the creation of a comprehensive patient identity management database for various hospitals.

A client (e.g. CATS) using PIMS should ideally encrypt all identifying information. However, due to the nature of cryptographic algorithms, very similar attributes (e.g. typos) will be transformed to different encrypted values. For this PIMS allows matching of encrypted data through Q-grams and bloom filters. It is important to keep in mind that there is still a risk of re-identification when using encrypted attributes. Through statistical or frequency analysis techniques, re-identification of (parts of) encrypted attributes can still be achieved.

Data Upload Scenarios

4.4.2.1.5   Upload Scenario using CHIC Tools

A source hospital wishes to import clinical data into the CHIC data repository.

4.4.2.1.5.1 Step 1: Create Privacy Profiles
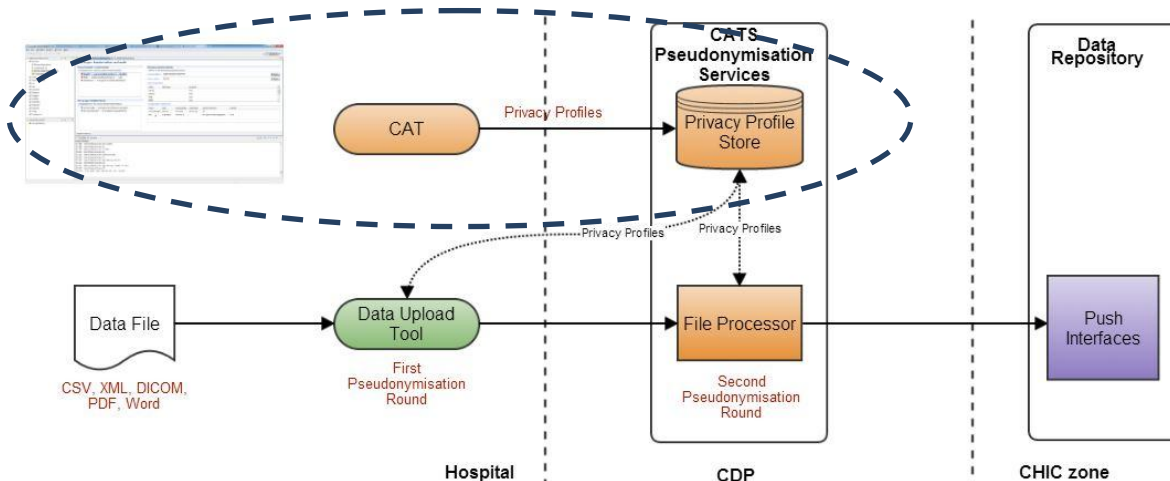
As a first Step the data uploader in collaboration with a CDP operative create 2 sets of privacy profiles on the data file. One which defines the client site de-identification processing and one which defines the second pseudonymisation round executed on the CATS server.

CHIC provides a tool, CAT, which can be used to easily created privacy profiles. These profiles then need to be uploaded to the CATS privacy store together with a media type and schema mapping.

4.4.2.1.5.2 Step2: Process and Upload Data
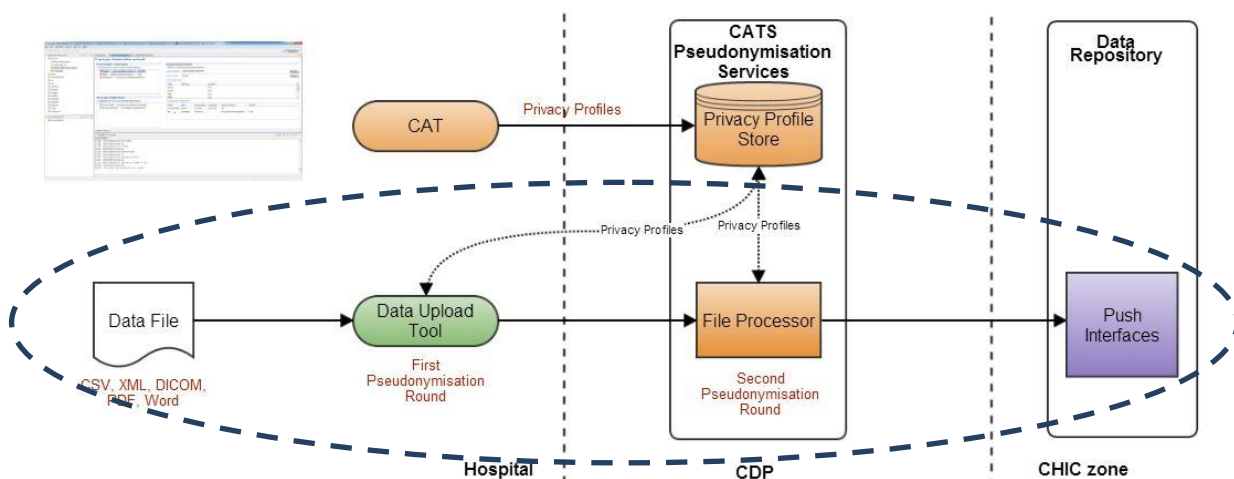
Now that all privacy profiles have been created the actual data file can be imported into CHIC.

The source data uploader exports the data to be imported from the hospital database or information system to his local drive. Through the data upload tool the file is selected. The Data Upload Tool downloads and executes the relevant privacy profiles. The resulting pseudonymised file is next rendered on screen for verification (whether the data has been correctly de-identified).

Once the data uploader confirms that the data has indeed been correctly de-identified the data is uploaded to CATS. CATS will select the matching second round pseudonymisation profile which defines all the pseudonymisation to be processed during the second round. Those pseudonyms are encrypted with the AES encryption algorithm by using the 256 bit TTP key. CATS will not automatically upload the resulting de facto anonymous file to the CHIC data repository. Instead, a CDP operative needs to validate the resulting file and

approve that it is indeed de facto anonymous. Once approved the file is uploaded to the CHIC Data Repository.

4.4.2.1.6 Upload Scenario by using external client side pseudonymisation tool.

Data sources are allowed to use any state of the art pseudonymisation tool for the first round. In this scenario the source wishes to upload a data file using its own pseudonymisation tool. This implies that no first round CATS privacy profiles need to be defined. Nevertheless it is still needed to create a privacy profile which defines the second pseudonymisation round.

4.4.2.1.6.1 Step 1: Create Second Round Privacy Profile

As first round processing is not done using the CATS engine, no privacy profiles needs to be created. As the second de facto anonymisation round is still required, a privacy profile for the CDP service must still be created. This privacy profile defines the location of the pseudonyms that need to be encrypted during that second round.
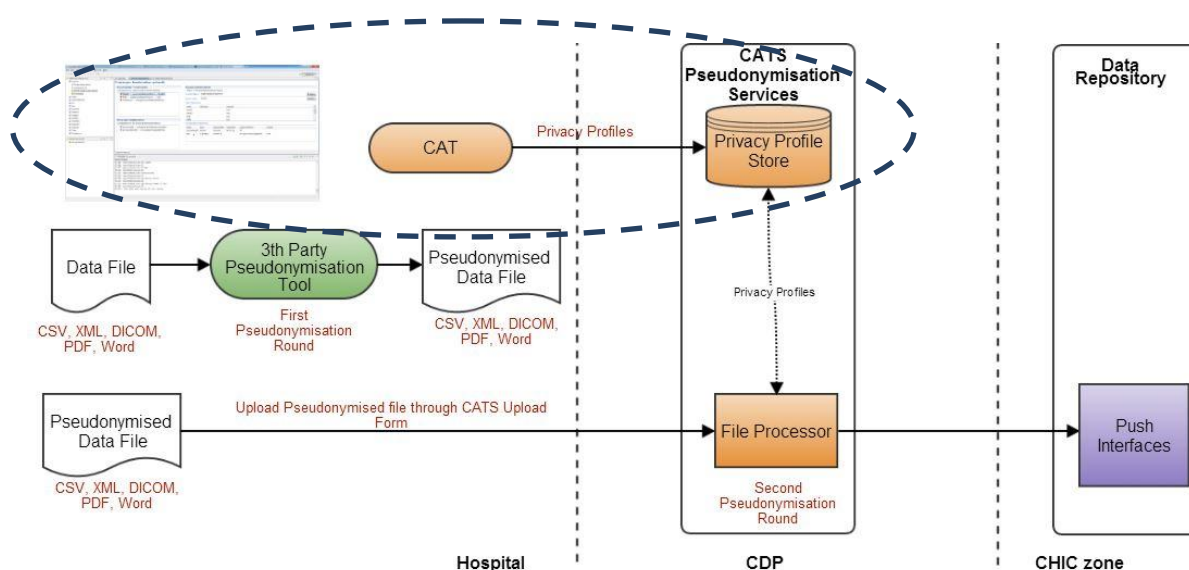
The CHIC Cat tool can be used to define the second round privacy profiles. This profile should be uploaded to the CATS privacy store together with a media type and schema mapping.

4.4.2.1.6.2 Step 2: First Round Pseudonymisation
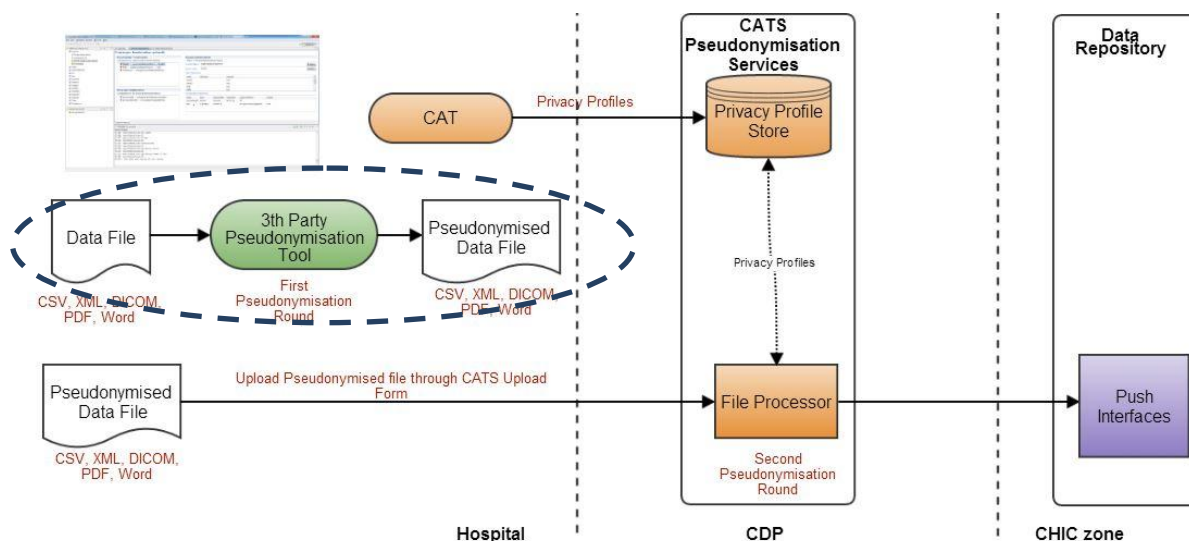
In this scenario, before data can be uploaded to the CHIC Pseudonymisation Service it needs to be pseudonymised on the client by using a 3th Party Pseudonymisation Tool. This tool probably also requires some configuration to be made for the given data file. Thereafter the file can be processed resulting in a pseudonymous data file which should then be verified by the data source.

4.4.2.1.6.3 Step3: Upload Data

Once pseudonymised and confirmed, the data can be uploaded. CATS provides an HTTP upload form through which a data uploader can upload pseudonymous files (Note that the 3th Party Pseudonymisation Tool can also integrate the CATS web service upload interfaces allowing upload to CHIC directly from the Tool).
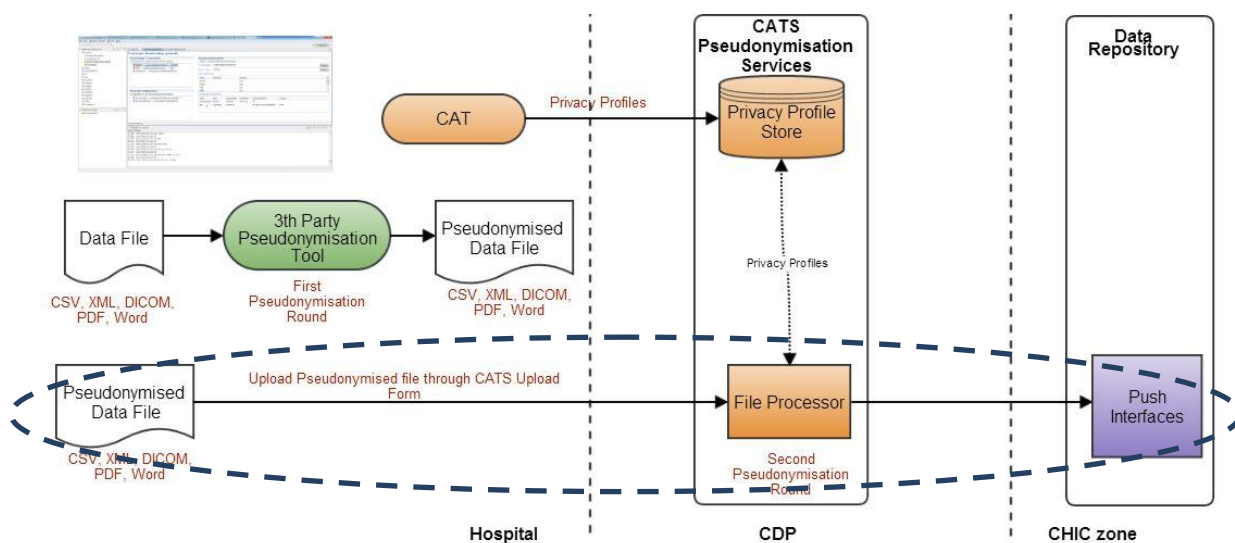
CATS will select the matching second round pseudonymisation profile which defines all the pseudonymisation to be processed during the second round. Those pseudonyms are encrypted with the AES encryption algorithm by using the 256 bit TTP key. CATS will not automatically upload the resulting de facto anonymous file to the CHIC data repository. Instead, a CDP operative needs to validate the resulting file and approve that it is indeed de facto anonymous. Once approved the file is uploaded to the CHIC Data Repository.

4.4.2.1.7 Data Import through clinical trial software such as ObTiMA

When data is collected in a clinical trial web application, such as ObTiMA, it can be imported into CHIC through one of the previously described scenarios by exporting the data from the web application to the data uploader's local drive.

For ObTiMA as an example, this would imply that a physician or data nurse exports the trial's content to his local drive in CDISC ODM XML format. In collaboration with the CDP, as explained in above, he then would need to create the privacy profiles. Through the CHIC Data Upload tool the data is next uploaded into CHIC.

When data is uploaded from multiple sources such ObTiMA and a DICOM image store common patient characteristics are required to be able to issue the same pseudonyms. To support this ObTiMA should allow the export of some identifying patient characteristics so that they can be taken up in the pseudonymisation algorithm (e.g by using PIMS as explained in part 4.4.2.1.4 above).

As the use of ObTiMA within CHIC is currently in investigation, the actual full technical solution will be presented in "D5.2: Security guidelines and initial version of security tools".

4.4.3 Access Control within the CHIC Network

All CHIC services and front-ends are required to be protected by the CHIC Security Framework as defined in D5.1.1. and D5.2. This ensures that only authorised persons are able to access the CHIC services and sensitive data. In case of system administrators they typically do not access the servers they manage through the web page and web service frontends, but instead they access the server through a remote connection. As system administrators have full access on the system they administer, remote connections should always go over a secured connection:

- Unix & Linux based servers must only allow remote connections by using at least a 2048 bit authentication key. Username/Password based authentication is not allowed for SSH access.

- For Windows servers SSH, as defined for Unix & Linux servers, is also strongly advised. If Windows Remote Desktop is considered, it must only be allowed over a secure VPN connection. A secure VNP connection, makes use of 2048 bit keys and preferably key-based client authentication. Username/password authentication is allowed if secure random passwords (4.4.4) are used.

- Other administration endpoints which are not protected by the CHIC Security Framework should only be accessible from a secure VPN connection as defined above.

4.4.4 CHIC Password Policy

The CHIC password policy adds some additional criteria to the NHS password policy v1.8[9].

All CHIC user and admin passwords MUST adhere to the following criteria:

- A password MUST contain at least 10 characters;

- A password MUST contain at least one lowercase alphabetic character;
  a b c d e f g h i j k l m n o p q r s t u v w x y z

- A password MUST contain at least one uppercase alphabetic character;
  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- A password MUST contain at least one numerical character;
  0 1 2 3 4 5 6 7 8 9

- A password MUST contain at least one special character;
  < > ? , . / : @ ~ ; ' # [ ] } { = + - _) (* ! " £ $ % ^ &

- A password MUST NOT contain 4 or more consecutive characters as are laid out on a keyboard, such as „azer" or „wqer";

- A password MUST NOT contain 3 or more consecutively repeating characters such as „aaa";

- A user's username is not allowed to occur in his password, neither are some commonly used security terms such as „admin", „user", „test".

A user will be prompted to change his password every 180 days.

---

[9]

http://www.institute.nhs.uk/images//documents/Freedom_of_information/Class_5/Password%20Policy.pdf.

As regards additional organisational safeguards, the providing of a user's password to any other person is forbidden, and users are instructed, in case anyone requests their password, to contact the CDP. Any suspected password compromise must similarly be reported to the CDP.

4.5 Data Protection Guidelines

As defined in D4.1 digital data can reside in three states. It can be in use (active data), at rest (stored data) or in transit (data which is traversing a network). This section will contain guidelines on how to handle and protect the data for each of states.

4.5.1   Data in Transit

Sensitive data in transit **must** always be encrypted to ensure confidentiality. All communication within CHIC must always be secured by using either transport or message level security. As different communication protocols can be used (e.g. HTTP, SMIME, FTP) it is up to the architecture to define for each allowed communication protocol how it should be secured.

For all HTTP communications for example (typically used by web services and web content accessed through a browsers), the initial architecture deliverable D5.1.1 defines that the HTTP SSL/TLS protocol must be used. D.5.1.1 in Chapter 9.1 further defines the allowed protocol versions, encryption algorithms and minimal key sizes.

Although transport level security ensures the confidentiality of data transferred directly between two hosts (possibly over multiple intermediate hosts that cannot decrypt the data), it is not sufficient if there are intermediate hosts that need to parse parts of the data before executing a specific task (e.g. routing such as email, SOAP and REST messages). In these situations message level security should be used where each message is encrypted for the final recipient to ensure that only the final recipient can see the content. Possible technologies are S/MIME for email, WS-Security for SOAP. D5.1.1 Chapter 9.2 further defines the technical details on how to encrypt web service messages through e.g. WS-Security.

4.5.2   Data at Rest

Data at rest, whether it is on hard disk or flash drives (both mobile and fixed in a server or laptop), floppy drives, DVD's or tapes (such as backup tapes), must always be encrypted. This ensures that when someone steals the medium he still cannot access the data without access to the decryption key.

Guidelines for data at rest on end user devices

To encrypt data on end user devices user can choose their own tool as long as it fits the cryptographic requirements as defined in D4.1:

- An asymmetric block cipher either AES or Twofish must be used in CBC mode. A 256 bit encryption key must be used.

- Stream ciphers should not be used, instead one of the two above block ciphers should be used in CBC mode.

- An asymmetric cipher RSA should be used with a key of at least 2048 bit.

A good example encryption tool that can be used is TrueCrypt[10]. See Appendix 7 on how to create and use an encrypted TrueCrypt volume.

---

[10] http://www.truecrypt.org/.

Guidelines for data at rest on servers and backup devices

The hard drives of servers and backup devices such as tapes or external drives should also be encrypted. The same limitations on encryption algorithms and key sizes apply as with end user devices. Actual implementations strongly depend though on the operating system and backup tool used. This will therefore be described in more detail in later deliverables such as Deliverable 5.2.

4.5.3   Data in Use

D4.1 proposed initially that data in use should also be encrypted. Data in use typically implies data stored in memory and CPU registers and cache. Although there are solutions for encrypting data in use, e.g. by doing full memory encryption, further assessment has shown that this is not practical and enforceable in a project such as CHIC. CHIC instead aims to ensure that services where sensitive data is processed cannot be accessed by unauthorised persons. Therefore we can assume that data in use is not easily observable and thus encryption of data in use is not required.

Data in memory can be stored in caches on a system's disk drive. During system power off, it is also possible that all data from the memory is temporarily stored on the disk drive for quicker startup. This implies that when someone steals such a drive he will be able to access sensitive data which has been involuntary stored on the disk drive. There is further on no guarantee that data stored once on a hard disk drive, can ever be removed. Data stored on a disk drive, is data at rest and thus the guidelines as defined in part 4.5.2 apply.

4.6 Secured Data Upload Interfaces – Implementation

This section will describe the CHIC Data Upload Interfaces.

4.6.1   Upload file / Create processing Request

Method	POST
URL	/services/rest/processingRequest/?name={name}
Request	POST https://ttp-dev-chic.custodix.com/services/rest/processingRequest/?name=<FileName> HTTP/1.1 Accept-Encoding: gzip,deflate Content-Type: application/octet-stream Authorization: SAML auth=<Encoded SAML Token> Content-Length: <Content Length> Host: ttp-dev-chic.custodix.com Connection: Keep-Alive User-Agent: Apache-HttpClient/4.1.1 (java 1.5) <Data File Content>

Response	HTTP/1.1 200 OK Server: nginx/1.2.2 Date: <Date> Content-Type: application/octet-stream Content-Length: <Content Length> Connection: keep-alive <File ID>
Remarks	Only upload pseudonymised files to CATS. CATS should have knowledge of the schema of the uploaded file, otherwise processing will fail.

Get request status

Method	GET
URL	/services/rest/processingRequest/status/{id}
Request	GET https://ttp-dev-chic.custodix.com/services/rest/processingRequest/status/<FileID> HTTP/1.1 Accept-Encoding: gzip,deflate Authorization: SAML auth=<Encoded SAML Token> Host: ttp-dev-chic.custodix.com Connection: Keep-Alive User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
Response	HTTP/1.1 200 OK Server: nginx/1.2.2 Date: <Date> Content-Type: application/octet-stream Content-Length: <Content Length> Connection: keep-alive <?xml version="1.0" encoding="UTF-8" standalone="yes"?> <UploadStatus

	state="DELIVERED" name="<FileName>" id="<FileID>"/>
Remarks	

Get request status by name

Method	GET
URL	/services/rest/processingRequest/status?name={name}
Request	GET https://ttp-dev-chic.custodix.com/services/rest/processingRequest/status?name=<FileName> HTTP/1.1 Accept-Encoding: gzip,deflate Authorization: SAML auth=<Encoded SAML Token> Host: ttp-dev-chic.custodix.com Connection: Keep-Alive User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
Response	HTTP/1.1 200 OK Server: nginx/1.2.2 Date: <Date> Content-Type: text/xml Content-Length: <Content Length> Connection: keep-alive <?xml version="1.0" encoding="UTF-8"?><UploadStatuss><UploadStatus state="DELIVERED" name="<FileName>" id="<FileID1>"/><UploadStatus state="DELIVERED" name="<FileName>" id="<FileID2>"/><UploadStatus state="DELIVERED" name="<FileName>" id="<FileID3>"/></UploadStatuss>
Remarks	File names are not unique. Multiple response can thus be returned.

Get all requests

Method	GET

URL	/services/rest/processingRequest/status
Request	GET https://ttp-dev-chic.custodix.com/services/rest/processingRequest/status HTTP/1.1 Accept-Encoding: gzip,deflate Authorization: SAML auth=<Encoded SAML Token> Host: ttp-dev-chic.custodix.com Connection: Keep-Alive User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

Response	HTTP/1.1 200 OK
	
	Server: nginx/1.2.2
	
	Date: <Date>
	
	Content-Type: text/xml
	
	Content-Length: 463
	
	Connection: keep-alive
	-- 	
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<UploadStatuss>`
	`<UploadStatus state="DELIVERED" name="<FileName>" id="<FileID1>"/>`
	`<UploadStatus state="DELIVERED" name="="<FileName>" id="<FileID2>"/>`
	`<UploadStatus state="DELIVERED" name="="<FileName>" id="<FileID3>"/>`
	`<UploadStatus state="CONFIRMED_ERROR" id="<FileID4>"/>`
	`<UploadStatus state="CONFIRMED_ERROR" id="<FileID5>"/>`
	`<UploadStatus state="CONFIRMED_ERROR" id="<FileID6>"/>`
	`<UploadStatus state="CONFIRMED_ERROR" id="<FileID7>"/>`
	`</UploadStatuss>`

Remarks	File names are not unique. Multiple response can thus be returned.

5 Intellectual Property Aspects

This part covers analysis of IPR issues which are crucial for the project implementation. The analysis proceeds in four main parts: (i) legal protection of models and hyper models; (ii) IPR ownership issues; (iii) contractual arrangements inside the Consortium and the software licensing issues (focus on open source); and (iv) mechanisms for the commercial protection of data. The analysis is performed on the basis of information provided in the DoW, data supplied by the Parties within the IPR questionnaires and by the follow up procedures (e.g. email correspondence, telephone conferences, etc.). Subsequently, with progression of the project the analysis will be subject to a second iteration that is to be presented in Deliverable D4.3.2 (M42).

As indicated by the reviewers at the CHIC interim review in November 2013 (Period 1: Consolidated Report, p. 3), it would be desirable for outstanding IPR issues to be identified and resolved in an IPR memorandum to be signed by the partners. Accordingly, in the light of the analysis in this part, and identification of where there are gaps in the existing contractual framework (as outlined in the GA, Annex II and Consortium Agreement, or otherwise potential for misunderstandings, LUH has developed a model memorandum of understanding to this end. This is annexed as Appendix 5 to this Deliverable.

5.1 Legal protection of models

5.1.1 Application of copyright to models

The CHIC Project aims at the development of mathematical and computational models and hyper-models along with the tools, services and infrastructure to facilitate their accessibility and reusability[11]. Consequently, computer models and hyper-models as well as software and the legal protection of such constitute the main subject of this legal analysis. Protection of other materials, which may be used and/or produced in the course of the Project implementation, such as biological prototype models, biological and mathematical constructs used in modelling, etc., will be covered as associated with and adhering to the software and computer models. For the purposes of this Deliverable computer models and models are used as synonyms.

Protection of models in CHIC depends on their nature and the mode of implementation. From the DoW it can be derived, that models (also referred to as component models) can be combined from hypo-models and can also constitute integrative parts of hyper-models. Accordingly, there are two main types of models to be distinguished: (*a) component models, each describing a biological process at a characteristic space-time scale, and (b) relation models, which define the relevant relations across scales*[12]. The CHIC models shall integrate the prototype models, e.g. models of elementary biological processes (e.g. cell cycling, the angiogenesis process, etc[13]) and computer codes of these.

At the current stage of the Project development several definitions of a term "model" have been suggested. Some definitions are as follows:

"computer model" - a <u>computer program</u> that implements a scientific model, so that when executed according to a given set of control instructions (control inputs) computes certain quantities (data outputs) on the basis of a set of initial quantities (data inputs), and asset of execution logs (control outputs)[14];

---

[11] CHIC Description of Work, p.3.

[12] Ibid, p.27.

[13] Ibid, p.23.

[14] CHIC Deliverable D7.101, see Hyper-models: definitions.

"model" - *a mathematical or computational construct that is able to virtually generate an entity or phenomenon*[15];

"*hypo-model*" – *a model that is simpler than a reference model or a reference hyper-model and can simulate a simpler entity or phenomenon compared to a model or a hyper-model*[16].

From these definitions it can be inferred that a model (computer model) shall simulate or virtualize a specific entity or phenomenon in digital environment; be expressed in terms of mathematical or computer science and be executable by a computer. For this, the data of a biological model, including the structure of their compilation and representation shall be converted into software code, which will instruct and command the simulation by the computer (IT Infrastructure).

Such simulation (execution) of a prototype model by a computer model is achieved by converting a biological model (data) into a form executable by a computer (so that a prototype model is simulated). A computer model is made executable by a computer on the basis of its code, which sets out a series of commands which a computer shall follow (e.g. compilation of biological data in a certain order of procedure from separate files, repositories, etc.) so that in the result a prototype model (its compiled form) is simulated (made executable) by a computer. Following this logic, what makes a model executable is its code. The code of a model in CHIC is analogous to the CPU of a computer. Although the CPU is not the computer as an end product, it is its engine and without it the computer will not work.

The legal nature of a model as such is questionable (i.e. whether it should be regarded as a construct, idea, invention, knowhow, etc.). However, what is definitely identifiable in legal terms and qualifies for protection is its code. Thus, as apparent from the explanatory definitions above, the code for a given model will be written as *a <u>computer program</u> that implements a scientific model, so that when executed according to a given set of control instructions (control inputs) computes certain quantities (data outputs) on the basis of a set of initial quantities (data inputs), and asset of execution logs (control outputs)*[17].

Hence, a model code should be considered as a computer program within the meaning of Article 1 Software Directive and be subject to copyright protection as such. In particular, the EU Software Directive defines the relevant object of protection in Recital 7 in the following terms: "*the term 'computer program' shall include programs in any form, including those which are incorporated into hardware. This term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.*" In the following sections, relevant criteria for a computer program to enjoy legal protection will be considered.

5.1.1.1 Object of protection

Copyright protection, as granted to computer programs under the Software Directive, applies *to the expression in any form of a computer program… including the preparatory design material*[18]. *Computer programs, whether in source or object code,* are defined as object of copyright protection under Article 10 TRIPS which is in line with the WCT.

The definition of computer program as protectable subject matter is admittedly not given, either in the Software Directive, or in the TRIPS, or in the WCT. However, the WIPO Model Provisions on the Protection of Computer Programs (WIPO Model Provisions) define a computer program as a "*set of instructions capable, when incorporated in a machine-readable medium, of causing a machine having information-processing capabilities to*

---

[15] CHIC Hyper-modelling glossary, as suggested by G.Stamatakos on 18 March 2014.
[16] Ibid.
[17] Deliverable No. D7.101, Hyper-models: definitions.
[18] Article 1 Software Directive.

indicate, perform or achieve a particular function, task or result"[19]. The European Court of Justice (ECJ) has also established that copyright protection applies to the expression in any form of a computer program which permits reproduction in different computer languages, such as the source code and the object code[20] and includes the preparatory design work capable of leading, respectively, to the reproduction or the subsequent creation of such a program[21].

In the context of CHIC, the term "software" is generally used instead of "computer program", as defined in Article 1.2 CA. Software stands *for sequences of instructions to carry out a process in, or convertible into, a form executable by a computer and fixed in any tangible medium of expression.*[22]. Although a computer program might not always constitute software, software always includes computer programs. Thus a computer program is just a set of instructions to be executed by a computer, whereas software is a broader, technological term, which includes programs, APIs, procedures, processes, other components which are necessary for a program to be executable in the IT environment. It may thus cover a collection of programs, procedures, algorithms invoked by operation of a system having data processing capabilities.[23] In the context of this Deliverable and in legal practice, in general, both terms are used as synonyms if not indicated otherwise.

5.1.1.2 Form of expression

For a model code to qualify for copyright protection as a computer program, it would need to be expressed in a form which can be *reproduced in different computer languages.* Such expression can be made either in source or object code. Whereas source code covers a human readable form of a program, normally written in a programming language, like Java, C, C++, etc., the object code constitutes its *machine-readable form, i.e. compiled and/or executable* by a computer.

Within the CHIC Project, Source Code is defined as *software in human readable form normally used to make modifications to it including, but not limited to, comments and procedural code such as job control language and scripts to control compilation and installation*[24]. For its part Object Code shall mean *software in machine-readable, compiled and/or executable form including, but not limited to, byte code form and in form of machine-readable libraries used* for linking procedures and functions to other software.[25]

Therefore, once a model code is produced, the form in which it is uploaded into CHIC, be it in original version (source code) or compiled (object code), will make no difference in terms of it qualifying for copyright protection as a program. Upload of the models into CHIC (model/tool repository) with various versions of the source code available for interoperability purposes, is foreseen (DoW, WP 8, p.30).

5.1.1.3 Intellectual creation

Another important criterion for copyright to subsist is intellectual creation. According to Article 1 paragraph 3 Software Directive, *a computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.* At the same time the product to be protected must be

---

[19] Section 1 (i), Model provisions on the protection of computer software - 1978 - WIPO PUBLICATION, NO 814(E) - GENEVA: WIPO - 27p.

[20] ECJ, Judgment of 22 December 2010, Case C-393/09 *Bezpečnostní softwarová asociace v Ministerstvo kultury,* paragraph 35.

[21] Ibid, para 37.

[22] Article 1.2. CHIC Consortium Agreement.

[23] Enriquiez L.A., "Dynamic Linked Libraries": Paradigms of the GPL license in contemporary software, p. 13.

[24] Article 9.8.1. CHIC Consortium Agreement.

[25] Ibid.

more definite in nature than something at the level of logic, an idea or principle, which enjoy no protection as described in D4.2.[26]

The same applies to functionality, programming language and the format of data files used in a program, which the ECJ found as such do not constitute a form of expression of a program and are therefore beyond the scope of copyright protection of a particular program. As the Court held in SAS Institute Inc. v World Programming Ltd*., "neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression of that program and, as such, are not protected by copyright in computer programs for the purposes of that directive"[27].*

However, while the programming language used in a program thus does not qualify categorically for protection, still, provided a particular programming language satisfies the criterion of "expression of intellectual creation" on its own, it can be protected by copyright on that basis. This is relevant for high-level object oriented programming languages, like, Java, which do enjoy copyright protection in their own right and are licensed under their own licenses. For instance, *PHP is a "widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML"[28]. PHP is owned by the Zend[29] Company, and is licensed under the PHP license[30], a non copyleft license*[31]. Therefore, writing programs in a particular language might be subject to license from the right holder. In such cases, to avoid potential license compatibility issues, care will need to be taken in choosing an appropriate (compatible) license for software written in that language. Issues of license compatibility are addressed in detail in part 5.5 below.

The exclusion of ideas, principles, logic and algorithms which underlie a computer program from the scope of copyright protection is particularly relevant for the modelling work in CHIC. Taking into account, that the modelling work will be done on the basis of and comprise certain modelling methods, topologies, parameters, mathematical formulae, etc. which shall have been identified and set out at previous stages (DoW, WP 6, p.24), some of these parts, namely those that are rather principles per se, would remain beyond the scope of program protection. In its *Infopaq* ruling from 2009, the ECJ commented in this regard that, "*The keywords, syntax, commands and combinations of commands, options, defaults and iterations consist of words, figures or mathematical concepts which, considered in isolation, are not, as such, an intellectual creation of the author of the computer program….. It is only through the choice, sequence and combination of those words, figures or mathematical concepts that the author may express his creativity in an original manner and achieve a result… which is an intellectual creation*"[32].

Therefore, in order that a model code be considered and protected under copyright as an integrated whole, the selection, combination, and integration of those parameters, mathematical concepts, equations into a code must be performed in an original and creative manner so that an intellectual creation arises. The same applies to the preparatory design work, which is included in the scope of protection granted to a program. The term "preparatory design work", as defined in Recital 7 Software Directive, shall mean: "*work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage*".

---

[26] CHIC Deliverable D4.2, pp. 18-25.

[27] ECJ, Judgment of 02.05.2012, Case C- C 406/10 *SAS Institute Inc. v World Programming Ltd*.

[28] http://php.net/.

[29] http://www.zend.com/en/.

[30] http://www.php.net/license/3_01.txt.

[31] Enriquez L.A., supra, p.68.

[32] ECJ, Judgment of 16.07.2009, *Infopaq International A/S v Danske Dagblades Forening*, para 45.

5.1.1.4 Extension of program protection to preparatory design work

As just noted, such work may qualify in principle for copyright protection within the scope of a computer program. However, to determine whether in the context of CHIC, the preparatory design for a model would do so, the whole process of how the model code is developed in a given case will need to be analysed. From the DoW it is apparent that before the models and hyper-models are developed, a lot of pre-modelling will be done, in particular: cancer hypo-modelling and hyper-modelling strategies will be developed, algorithms and sets of parameters that could describe and make useable elementary bioprocess models will be identified, network topologies, multi-scale functional interactions will be inferred, etc[33]. Hence, it follows that to a certain extent, at least at the initial stage, modelling will consist in extraction and development of modelling methods, mathematical constructs, basic modelling algorithms, parameters and principles which will be implemented at the stage when the models will be developed and tested.

To become part of the protectable subject matter along with the model code as preparatory design work, the modelling materials must first satisfy the basic criteria of copyright protection. For this, the contributed materials should constitute a creative expression under the copyright law. The contribution may claim no copyright, if it is non-expressive, because the data are too straightforward, or well known or limited in creative substance or because the contribution is too abstract and is rather an idea, than expression[34]. Here the principle laid down in Recital 11 of the Software Directive, that ideas and principles which underlie any element of a program, including those which underlie its interfaces, as well as logic and algorithms which comprise those ideas and principles are not protected by copyright, applies to the preparatory design work as well.

Therefore, in order to claim copyright protection along with the model code, first of all, the modelling materials should constitute creative expression, and be beyond the level of abstract idea or well-known principles or logic. Even if non-copyrightable subject matter, like mathematic, technical or graphic symbols, etc. might be integrated, it is through the choice, selection and arrangement of those elements in which author´s creativity may be expressed. Moreover, its nature should be such *that a computer program can result from it at a later stage[35]*. As interpreted by the ECJ, the preparatory design work of a program should be *"capable of leading… to the reproduction or the subsequent creation of such a program".[36]* The preparatory design work may include "*development documentation or any other pre-products of development which are laid down in writing, inter alia data flow plans, designs of commands and information cycles, exhibits of scientific or technical art, expressed in any form, including mathematic, technical or graphic symbols*"[37]

Another plausible approach to argue for copyright in the modelling work, however, would be to consider such work as preparatory design materials and program description. The relevant criteria that would tend to support such an approach are detailed in the next section.

5.1.1.5 Program description

As laid down in a narrow sense in the WIPO Model Provisions, a program description means *a complete procedural presentation in verbal, schematic or other form, in sufficient detail to determine a set of instructions constituting a corresponding computer program[38]*. A program description, as interpreted by the WIPO expert group on legal protection of computer software[39], is an indispensable part of the software development process and shall indicate

---

[33] CHIC DoW, p. 24-25.

[34] Nimmer, supra, p.43.

[35] Recital 11 Software Directive.

[36] ECJ, Case C-393/09, para 37.

[37] BGH, Urteil vom 09.05.1985 - I ZR 52/83, BGHZ 94, 276 – 292.

[38] Section 1 (iii) WIPO Model Provisions.

[39] WIPO expert group on legal protection of computer software, LPCS/I/2, 30.09.1979.

the steps to be taken in execution of a computer program. A computer program is just a set of instructions which controls operation of the computer ("machine having information processing capabilities") and is an end product of a complex process.

The software development process usually consists of several stages: analysis of the problem to be solved by a computer; design and adoption of the method of solving the program and stages of running the program; break down of the stages into detail so that instructions can be developed which will enable a computer to perform all the operations necessary for the execution of the program. Hence, software development involves preparation of problem description, description of method, description of the main stages of the program execution and steps to be taken in execution of the stages[40].

As the WIPO expert group further stated, "All in all *a program description shall set out all the instructions to be followed by the computer so that the only thing that remains to be done is to convert them into form executable by a computer*"[41]. Program description, shall be complete, i.e. set out steps to be taken in the execution of a program; it shall be specific to be able to determine "corresponding computer program".

This interpretation of program description by the WIPO expert group goes in parallel with the interpretation of the preparatory design work by ECJ as work *capable of leading… to the reproduction or the subsequent creation of such a program[42]*.

As released during the follow-up procedures, it is apparent that the modelling work covers and, in general, is composed out of the same stages as the software development process, i.e. analysis of the problem to be solved by a computer (simulation of biological models in CHIC Infrastructure); design and adoption of the method of solving the program (development of modelling strategies, etc.) and stages of running the program (construction of biological models, then mathematical models, then computer models); break down of the stages into detail so that instructions can be developed which will enable a computer to perform all the operations necessary for the execution of the program (expressed in schemes, flow charts, mathematical constructs, etc.).

On the basis of these observations it can be concluded, that insofar as the modelling design work reflects the above stages of software development and ultimately completion, i.e. such work sets out steps to be taken in the execution of a model code; is specific to determine "corresponding model code", which is expressed in some plausible form (schemes, designs, charts, mathematical or visual constructs, etc.); provides for intellectual creation and goes beyond the level of abstract idea, then the odds are rather high, that the whole modelling work underlying code development can be covered as a preparatory design work and included into the scope of program protection as applicable to the model code. The program description should, however, be distinguished from explanatory materials, such as manuals, handbooks, etc. Such explanatory materials are not covered by program protection, but may, however, be protected as literary works[43].

Another aspect, worth mentioning, is that, as a rule, a number of different but similar sets of instructions can in most cases be developed from the same program description[44] That is to say, that the same process or task can be executed and the same result will be achieved when the machine follows the same stages and executes the same processes, irrespective of the programming language in which the code is written or whether the script is written in one file or is collected from distributed files, or method how the functions are called. Applied to CHIC, this means that the same model may be converted in different codes or the same model code may be written in different source code versions. This option, namely, that the

---

[40] WIPO expert group, supra, p. 5.

[41] Ibid.

[42] ECJ, Case C-393/09, para 37.

[43] ECJ, Judgment of 02.05.2012, Case C-406/10, *SAS Institute Inc. v World Programming Ltd*, paragraph 64.

[44] WIPO expert group; supra, p.5.

models shall be loaded into the CHIC model/tool repository in different versions of the source code, is foreseen in the DoW, WP 8, p. 30. Hereby, the result and the model appearance would still be the same, irrespective of from what source code the model originates and is executed.

5.1.2 Secondary forms of protection: trade secret and knowhow

A further, or alternative means (besides copyright) by which software and the modelling work may be protected is by qualifying as knowhow or a trade secret. In this regard the source code of software is usually considered to be a trade secret[45].Other parts of software can also be protected as knowhow. A practical example, how part of a program can be protected as a trade secret would be *a mathematical formula saved in the EPROM of the slot machine that only apparently steers the machine by chance but which is in reality controlled by a certain algorithm* ; and which falls under the scope of secret-keeping by the developer[46].

The criteria for something to qualify as knowhow vary under national legislations. The general criteria for protection are as follows: secrecy, i.e. the data should not be generally known and not easily available in specialized sources and circles dealing with such information, the data shall be disclosed within an authorised circle and subject to special confidentiality measure, and must have economic value[47]. In this regard, it will be necessary for the relevant data to be subject to special measures to keep them secret. Contractual arrangements can be sufficient[48]. The data should not be made public, as publication in any mode or form will remove its status of being "secret". Economic value of the information will be present when the information provides a competitive advantage to a company which could be lost through publication[49]. Secrecy and economic value of information are the minimum criteria for protection, as laid down in Article 39 TRIPS.

As regards to the work carried out in CHIC, protection under knowhow might face a difficult hurdle when protection of the modelling materials is sought. Materials, which are generated in course of modelling and which contain data obtained by experience and which are not readily available in some even specialized sources, might be protected as knowhow, provided these data, by being secret, provide a competitive advantage to the party holding the information (e.g. reputational, industrial, scientific concerns, etc.). For instance, certain scientific data written in scripts or comments in the source code or associated documentation might be protectable as knowhow. A CHIC partner might have certain concerns against disclosure of these data, even by the Project implementation, and be interested in treating such data as confidential and protecting as knowhow. For this it should be sufficient to define the information, which must be kept secret, , i.e. mark as "confidential" and, as provided for in Section 10 CA, subject disclosure and use of such information to the contractual obligation to keep secret , e.g. under contractual arrangements or internal policy or other confidentiality measures. For safeguarding such data from disclosure in the context of CHIC, the modelling party may make use of Article 9.2.6. CA and make *granting of Access Rights subject to* acceptance (by the other party) of *certain conditions, aimed at ensuring that these rights will be used only for the intended purpose and that appropriate confidentiality obligations are in place*[50].

To the extent that these data are contained in a source code (e.g. written in scripts like comments or separate data files, etc.), then upload of a model in an object code and API

---

[45] Lodigkeit Klaus, Intellectual Property Rights in Computer Programs in the USA and Germany, 2006, p.99, OLG Köln, Judgment of 30.07.1997, CR 1998, 199.

[46] Ibid, p.100; LG Stuttgart, Order of 02.07.1990, NJW 1991,441,442.

[47] TRIPS, Article 39.

[48] BGH, Judgment of 09.05.1985, GRUR 1985, p.1045.

[49] Lodigkeit, supra, p. 101.

[50] Article 9.2.6. CHIC Consortium Agreement.

only might be considered. This applies, provided the interoperability measures are in place (API), so that access to the source code is not required. As to the latter, according to Article 9.8.3 CA, access to software shall indeed, as a rule, be provided to the object code and API only. Disclosure of the source code, though, comes in question, *if a Party can show that the execution of its tasks under the Project or the Use of its own Foreground is technically or legally impossible without Access to the Source Code. Background shall only be provided in* Object Code unless otherwise agreed between the Parties

Qualification as knowhow or confidential information may also offer itself as the primary mechanism for protecting the core value in the substance (as opposed to mode of presentation) of the medical data used to populate the models and hyper-models within the Project. This issue is discussed further below in part 5.3.

5.2 Legal protection of hyper-models

The legal analysis here extends the analysis made on models and applies to generation of hyper-models. . Here, given by their complex definition, composite nature (as integrations of the component models), an important question relates to the potential for multiple ownership of IPR to subsist.

As noted earlier, the analysis conducted here, is made on the basis of information and data available as of the current stage of Project progression and reflects the stage as it is. At present there are several approaches in interpreting the notion of a "hyper-model" and several definitions available. For instance, the following definitions can be considered:

- A hyper-model means a model that emerges from the merging or connection of simpler models each one of which is capable of simulating a specific entity or phenomenon. The hyper-model can simulate an entity of phenomenon that may be more complex than the ones simulated by each separate simpler model[51].

- A hyper-model (or integrative model) means a choreography of component models, each describing a biological process at a characteristic space-time scale, and of relation models, which define the relevant relations across scales[52].

- Integrative models can become component models for other integrative models[53].

- Hyper-models of tumour response to standard therapies will be modelled on the basis of stand-alone models simulating their effects as functions of time[54].

- Hyper-models of specific tumour types shall represent modular recreation of existing models referring to the specific cancer type by fitting together standardized elementary tumour bioprocess models[55].

As envisaged in the DoW, hyper-models are understood as an aggregation of models and shall be protected as such. For this, a hyper-model shall be considered as a composite whole. General legal issues relating to composite works and variations under the national laws[56] were covered in Deliverable D4.2., part 6, p.38, et seq.

---

[51] CHIC Hyper-modelling glossary, supra.

[52] CHIC DoW, WP 7, p.27.

[53] Ibid.

[54] DoW, WP 6, p.25.

[55] Ibid.

[56] Kooperationsstelle EU der Wissenschaftsorganisationen, IPR Helpdesk, Joint Ownership in Intellectual Property Rights, http://www.kowi.de/Portaldata/2/Resources/FP6/ipr_joint_ownership.pdf, date: 28.03.2014.

5.2.1 Protection of a hyper-model by copyright

The legal analysis on copyright issues in hyper-models is based on the initial understanding and presumption of how the models will be integrated in practice, Hereby, when the hyper-modelling is performed in practice, additional technical factors, such as linkage methods, interaction and inter-dependency of the components, location of the created whole (the data on which may be lacking as of now) may be crucial when the substance of a hyper-model is qualified in terms of copyright and licensing issues involved. Therefore, the part below provides general approaches in broad terms only, the copyright issues may vary and each modelling scenario, implemented in practice, shall be qualified on case by case basis. A more definitive analysis will be provided in line with new information available in the second iteration copyright framework of Deliverable D4.3.2. A major goal of this first iteration of the framework is to make partners aware of the legal consequences technical decisions on the hyper-models might bring.

For creating the hyper-models, the tumour models will be broken down in the models and computer codes of elementary biological processes, which will be provided in the model repository. The standardized elementary bioprocess models will have to be linked to elementary bioprocess models of complementary mechanics[57]. For linking the models with the other models/ tools, each model shall be available from the repository, where each model will be provided along with the input/output parameters and different versions of the source code[58]. The hyper-models will be re-created from the existing models referring to the specific cancer type[59]. It follows, that in constructing the hyper-models codes of the elementary models will be involved.

In terms of copyright, any alteration, modification, translation, aggregation, integration of a pre-existing work into a larger work, and the performance of other alterations of the work is a prerogative of the right holder (in the pre-existing work) and subject to his/her authorisation. This includes the performance of such acts in relation to software components, in order to achieve interoperability. Here such acts of modification would, in normal practice, require access to and modification of the source code and the resulting work, considered within the licensing issues, is most likely to be classed as a derivative work. Linking the model codes which are licensed under GPL license either statically or dynamically, with other programs is considered, following the GPL logic, to make a combined work based on the GPL covered work. *Thus, the terms and conditions of the GNU General Public License cover the whole combination*[60].

The above issue becomes even more important in the context of hyper-modelling, where the codes of several pre-existing models are supposed to be linked or merged with each code written in its language and source code version, licensed under its own license, residing in ownership of different modelling parties. Moreover, additional technical factors, such as linking methods and interoperability also come into play. The practical scenarios, licensing issues and technical factors involved might vary from case to case. Therefore, when the hyper-modelling and hyper-models are analysed in terms of copyright all such parameters will need to be considered in detail on a case by case basis. In general, such figures as derivative works, joint works and composite/collective works may come into consideration and copyright issues for each will be outlined below.

Given its aggregate structure, a hyper-model is most likely to qualify as a collective work, once the level of intellectual creation *by reason of the selection or arrangement of the contents* in it is achieved. According to Article 2 Paragraph 5 Berne Convention c*ollections of literary or artistic works …which, by reason of the selection and arrangement of their*

---

[57] CHIC DoW, WP 6, p. 23.
[58] CHIC DoW, WP 8, p. 57.
[59] CHIC DoW, WP 6, p. 23.
[60] https://www.gnu.org/licenses/gpl-faq.html#GPLStaticVsDynamic.

contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections.

In light of the above definition, a hyper-model can qualify for copyright, when it constitutes such a collective work with an expression of intellectual creation by *reason of the selection or arrangement* of the models in such. Intellectual creation of the author *might be expressed through the choice, sequence and combination of* certain elements, even unprotected, like words … *that the author may express his creativity in an original manner and achieve a result which is an intellectual creation[61].*

5.2.1.1 Hyper-model: structure and copyright

As indicated by the modelling parties, complex technical parameters as well as biological, genetic, mathematical, side effect factors, etc., which might be crucial, shall be considered in the design of how a hyper-model is to be developed. The hyper-modelling is performed in a semi-automated way facilitated by the IT infrastructure (hyper-modelling editor, personalized decision making support systems, software tools, etc.)[62], managed by a person skilled in the art. When a hyper-model is compiled, then again it is the code which makes the hyper-model executable and defines its structure: component models, sequence, relations, principles of compilation, etc.

First, the code of a hyper-model as such qualifies for copyright as a computer program within the meaning of Article 1 Software Directive. In this regard, a code which designs the *choice, sequence and combination* of models *in a hyper-model* produces intellectual creation and will produce copyright in the hyper-model structure. At the same time, it is not the models as such, but the codes of models which are collected in a hyper-model, as extracted from the model/tool repository. By "amalgamation" of models, linkage or integration of the codes of respective models in a hyper-model is implied. Hence, depending on the technical mode by which the models are linked to or combined in a hyper-model, the substance of a hyper-model in terms of copyright might vary.

5.2.1.2 Composite works

The main legal issues which are of practical relevance when a hyper-model code is considered as a composite or a collective work are the ownership and the rights in the code. The copyright in a collective whole *is independent of, and does not affect or enlarge the scope, duration, ownership, or subsistence of any copyright protection in the pre-existing material[63].* Copyright in a hyper-model code passes to the compiler and is without prejudice to the copyright in the preexisting works.

Therefore, copyright in the hyper-model code will be independent of the copyright in the model codes. At the same time, linking or integration of the model codes into a hyper-model code will require authorisation of the pre-existing right holders. According to the DoW, WP 8, p 30, information about model access permissions will be loaded into the model/tool repository along with the model as its related information. Therefore, access terms to the model will be provided along with it. Should the access terms thus granted be insufficient to use the model for implementing the tasks in the Project, including the use of the model for hyper-modelling, then Access Rights to use the model shall be requested, as regulated in Section 9 CA.

The copyright ownership of the hyper-model code for its part depends on the way in which that code is designed, i.e. individually or through collaboration of the parties, intent of the parties, etc. One scenario would be that a single Party A develops the hyper-model by compiling the relevant hyper-model code, whereby the hyper-model incorporates one or more component models contributed by a different Party B. In that case the hyper-model

---

[61] ECJ, Case C-5/08, para 37,39, 45.

[62] Innovation questionnaire (As completed by G. Stomatakos 2014).

[63] Nimmer R.T., Legal issues in open source and free software distribution, adapted from Chapter 11 in Raymond T. Nimmer, The Law of Computer Technology (1997, 2005 Supp.), p. 44.

would most likely qualify as a derivative work or as a collective work with individual ownership of the developer, Party A, in it. *In a collective work and in a derivative work, no intent exists to jointly develop; the creator of the derivative works alone on an existing product.*[64] However, integration of models into a hyper-model and making collective works from these is a prerogative of the right holder in the original component, i.e. Party B.[65]

In the words of Article 4 Software Directive, the right holder "shall have the right to authorize "*the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program*".

5.2.1.3 Derivative works

When hyper-models are considered against the technical background, each hyper-model can be viewed as an interplay of the models combined in it. Interoperability and connectivity between the models are supposed to be achieved through interfaces[66], which usually come in form of software libraries. By combination of models different linkage methods can be involved (e.g. dynamic/static linking). Considering that the models will be linked together to produce the integrative whole, then, speaking in terms of software licenses, interplay of the models in it can produce a derivative work. Some licenses exclude combined or linked works from the scope of derivatives (e.g. Apache license v.2), some licenses consider linked works as derivatives (GPL, LGPL v.2, Preamble) and subdue the derivatives under the scope of license. Qualification as a derivative is especially relevant in view of licensing considerations, as will be analysed in part 5.6 below.

5.2.2 Copyright Ownership issues within the CHIC framework

Legal issues relating to copyright ownership were previously considered in Deliverable D4.2. As noted there, software and models, which will be developed under the Project, shall be considered in the legal framework governing Foreground. Hence, ownership in software and models are subject to the rules on Ownership of Foreground, as laid down in EC-GA Article II.26 – Article II.29, as specified in Articles 8.1. – Article 8.2. CA. Foreground is defined as r*esults, including information, whether or not they can be protected, which are generated under the project, including rights related to copyright; design rights; patent rights; plant variety rights; or similar forms of protection*[67].

In the context of rules governing ownership two ownership regimes are distinguished and regulated: individual ownership (Article 8.1.CA) and joint ownership (Article 8.2 CA).

5.2.2.1 Individual ownership

As noted above, individual ownership is regulated in Article 8.1. CA. The Party which carried out the work generating the Foreground shall be the Individual Owner of the Foreground.

As regards copyright, the Party which is designated as owner of Foreground will inherit the legal status of right holder and possess the economic rights in the software and dispose of the rights at its own discretion. Thus, the Party being the individual owner shall have the right to use software as it sees fit by itself, to license it to third parties upon license terms, as it wishes (proprietary, OS, dual license) but is under an obligation to grant Access Rights to the other parties in the Consortium upon conditions, as laid down in Article 9.8.4 CA.

In the CHIC Project, individual ownership shall apply, when one Party works on its contribution into the Project (development of separate tools, models, etc.) individually, without the other Parties involved. In this way individual ownership is comprehensively and clearly dealt with in the CA, and raises no overt copyright challenges for the project.

---

[64] Ibid, p. 42.
[65] Article 2 bis of the Berne Convention.
[66] CHIC DoW, WP 5, p. 20.
[67] European Commission –Grant Agreement Article II.1.

On the other hand, when a contribution is developed on top of or with use of the preexisting works, such as software components, models, etc., use of the former components would require a license.

5.2.2.2 Joint Ownership

Joint Ownership is regulated in Article 8.2 CA and applies to the Foreground when more than one Party ("Joint Owners") carried out the work generating it together and *if the contributions to or features of such Foreground form an indivisible part thereof, such that under applicable law it is not possible to separate them for the purpose of applying for, obtaining and/or maintaining and/or owning a patent or any other IPR protecting or available to protect such Foreground, Joint Owners agree that, all patents and other registered IPRs issued thereon, and any other IPRs protecting such Foreground, shall be jointly owned by the Joint Owners.*

As regards software, it follows that this is a joint work where several authors merge their contributions as inseparable and/or inter-dependent parts with the intent of using the software as a whole[68]. In the context of software development where several programming parties work together at one piece of software and produce individual contributions into it, joint ownership is rather a typical case. At the same time, the contributions or programs of each contributor into the whole software should not be separable or distinct from the whole and shall not make exploitable units or modules on their own. Otherwise, such program parts might qualify as individual programs with copyright on their own within the composite whole with the result of composite ownership over the whole.

Another example, where joint ownership might apply, and which, however, is not covered in the CA, is where the respective contributions are interdependent. Here, *although . . . separately identifiable, each may be said to be written pursuant to an implied . . . agreement that the product of the several contributions will be jointly regarded as an indivisible work*[69].

Copyright ownership in software produced jointly shall vest with the relevant contributors jointly with equal rights of the co-owners in the whole[70]. The rule as to how the rights in Foreground generated jointly in CHIC shall be exercised is laid down in Article 8.2 CA. In such cases, *each of the Joint Owners shall be entitled to use their jointly owned Foreground as it sees fit, and to grant non-exclusive licences, without obtaining any consent from, paying compensation to, or otherwise accounting to any other Joint Owner, unless otherwise agreed between the Joint Owners*[71].

By sharing the rights in the whole work, neither of the co-owners holds fully exclusive rights in the whole and may not decide on exploitation, inclusive licensing, of the whole on his own. In the software produced jointly with the right of each co-owner to license the whole as it sees fit, a situation might arise when one co-owner licenses the whole on the proprietary basis, i.e. with the source code undisclosed, while the other licenses the software open source.

Another issue, upon which the co-owners should reach agreement, is in relation to the licensing of the whole work. Here the co-owners will need to ensure that the final license is compatible with the licenses of software components used inside the software and that software licenses inside the software are compatible. For instance, integration of software code licensed under GPL v2 inside the whole may have effect that the entire whole shall also be licensed under the GPL v2 or its versions. In this regard, Article 2 Paragraph 2 GPL v2 stipulates *…when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part*

---

[68] Nimmer, supra, p.42.

[69] Ibid., p. 45.

[70] Chris Reed, John Angel, Computer Law, Sixth Edition, 2007, p.353.

[71] Article 8.2. paragraph 2 CHIC Consortium Agreement.

regardless of who wrote it. In addition, pursuant to Article 2 Paragraph 4 GPL v2 *mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.*

The issue of the scope and potential viral effect of the GPL license is a complex legal issue, which is subject to more detailed legal analysis in part 5.5. However, the risk of license incompatibility will need to be considered and prevented by the software developing Parties. In particular, license incompatibility inside the software or non-observance of the license terms when distributing and licensing the entire whole may result in loss of copyright in it[72]. Thus Article 4 GPL v2 makes clear that: any attempt [except as expressly permitted by the terms of the license] to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. It shall, however, be without prejudice to the rights of subsequent licensees so long as such parties remain in full compliance. The issues of ensuring license compatibility are not addressed in the CA. Accordingly, rules that attempt to ensure license compatibility by the Parties are provided for in the IPR memorandum annexed to this deliverable.

5.2.2.3 Composite Ownership

If a hyper-model is developed by the Parties who created the models, from which a hyper-model is compiled, and who own the copyright in these models, then following the principle of divided or composite ownership in copyright (as outlined in D 4.2, p.38) that hyper-model is most likely to be considered as a composite work with composite/divided ownership in it.

A potential scenario may be as follows: Party A created and holds ownership in model A, including its code. Party B generated and holds ownership in model B, including its code. Parties A and B combine their models A and B to make a hyper-model AB and write a code for a Hyper-model AB to make it executable. In a scenario such as this, Parties A and B generate the hyper-model and its code together, and at the same time the Parties A and B contribute their models as separate works and hold separate copyrights in these. Furthermore, the models A and B, even as integrated into a hyper-model, remain separate models and each can be used on its own (as a component for another hyper-model, like AC, or BD, etc.) and are distinguishable and separable from the hyper-model.

Similarly, a software package made up of a number of programs or modules each separately owned (like models with separate copyrights in a hyper-model) shall reside in the composite or divided ownership of the contributors. Examples would be when several Parties collaborate on one piece of software with each Party contributing separable, but inter-dependent components or modules in such, or when the Parties generate a hyper-model and the same Parties hold copyright in the component models integrated in it. As stated above, generation of contribution with use of or on top of other works may also have other copyright implications, depending on such technical parameters, as the linkage methods and interdependency, modification, interaction of the component works. In such cases, various types of works as derivative or combined works may come into play again.

Composite ownership is not explicitly regulated either in the Grant Agreement, Article II.26. - Article II.29, or in the Consortium Agreement, Article 8.1 – Article 8.2. However, infringement of copyright will occur if any of the owners seeks to exploit the package as a whole without the consent of all the others and, unless agreed otherwise, exploitation of the whole would require consent of all the owners[73]. Hence the contributing parties will need to reach consensus on the exploitation of the whole (e.g. licensing strategy). Alternatively, if one contributor refuses to cooperate, a solution might be to exclude or replace the part of the uncooperative party. This, however, would not be an option where the respective part, e.g. a particular model, cannot be rewritten or substituted.

---

[72] Rowland, supra, p. 425.

[73] Ibid., p.354.

A reasonable step to reduce the risk of misunderstandings about ownership and exercise of any rights in software and works produced under divided authorship/ownership, would be to reach an agreement in advance. Concerning regulation of composite ownership and exercise of rights of the co-owners in composite works produced in the Project, the most effective solution would be to subject the composite ownership under the Joint Ownership format, as set out in Article 8.2 CA. A suggestion for regulation is provided in the IPR memorandum in appendix 5.

5.3 IPR Protection of medical data used in models

Apart from data to be supplied by clinical partners in the project, some partners engaged in the modelling to utilize the data on site as gathered by themselves from private or publicly available databases:

- UNITO uses for prostate cancer modelling data, available in the database held by UNITO and maintained by the Institute for Cancer Research and Treatment (IRCC), Turin, Italy;

- UPENN uses for modelling of biomechanical models, sub-cellular cancer models, nephroblastoma models data from the publicly available databases: EBI[74], PDB[75], NCBI[76], TCGA[77].

- UOXF uses for colon cancer modelling data from literature and experimental collaborators;

- UBERN uses for visualization and image processing purposes brain tumour MRI scans from BRATS;

The data used in some models may come from literature or clinical trials: glioblastoma data from the clinical trials HGG-IMMUNO-2003, HGG-2006, HGG2010 (DoW, WP 6, p.25).

From the above factual data follows that the medical data utilized in CHIC may originate from different sources (e.g. Parties, private databases, publicly available databases) and may come in different forms (raw or processed) and be integrated in different formats (e.g. repository, models). Therefore, depending which form the data are represented in CHIC (raw or processed), where the data are located (data repository or as integrated into a model), source and quality of data (data from publicly available databases or confidential data of clinical partners) several forms of protection may be considered as plausible.

5.3.1 Protection of medical data under copyright or under EU data base right

Protection of medical data under the copyright law can be considered, either in raw or processed form, as outlined above. The raw data may qualify for copyright protection, if choice, sequence and combination of words provide for expression of author´s creativity[78]. The processed medical data converted into digital format to be used as model input and/or as integrated into the models or tools, may in theory be protected under copyright along with the respective model or tool, in which it is integrated. However, since the core value of the medical data lies in the biological and/or medical substance, and not in the form in which the data are expressed, the protection of medical data by copyright, which protects against copying the expression, can hardly be considered as an adequate form of protection.

A more promising avenue of protection, which might be applicable to the data, would be under the *sui generis* database right. As was analysed in Deliverable, D4.2, such protection

---

[74] http://www.ebi.ac.uk/about/terms-of-use.

[75] http://rcsb.org/pdb/static.do?p=general_information/about_pdb/policies.

[76] http://www.ncbi.nlm.nih.gov/About/disclaimer.html.

[77] https://dbgap.ncbi.nlm.nih.gov/aa/wga.cgi?page=DUC&view_pdf&stacc=phs0.

[78] ECJ, Judgment of 16.07.2009, C 5/08, Infopaq Int., ref.45.

is granted on the EU level only as provided for by Directive 96/9/EC on the legal protection of databases (the Database Directive). The object and scope of protection under the *sui generis* right, term of protection and rights of the right holder are regulated in Article 7 et seq of that Directive. This form of protection might apply to the data, stored in the CHIC data repository, provided the data repository qualifies for protection under the sui generis right itself. If so, access, use, copy, transfer of the data and distribution of data from the data repository to the public would require authorisation of the right holder and the like access and use of the data may be placed into contractual regime and be limited in scope, purpose and terms of use.

As noted, the data for the CHIC data repository will be provided by different data providers (KU Leuven (GBM) and USAAR (Wilm´s Tumour Data (in ObTiMA), NSCLC data (from ContraCancrum)). Given that the data providers specialize in clinical research, the data will come from the clinical trials[79], the conduct of which requires deployment of professional human resources, time and effort, the criterion of substantial investment in obtaining the data must be fulfilled. In this regard, the DoW, WP 8, states that use of the data repository will be facilitated by multiple ICT services to allow import and export, reusability and exploitability of data, which require considerable technical resources, the criterion of substantial investment in representation of data must also be satisfied. Based on the above analysis, it may be concluded that the data repository will qualify for protection under sui generis right in the meaning of Article 7 Database Directive.

Protection under the sui generis right shall provide for the right of the maker of the database to *prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database*[80]. Here, the database right is aimed to protect against unauthorised extraction and reutilization (acts of appropriation and distribution to the public by any means of transmission[81]) of data in substantial part and the same acts done in systematic and repeated manner, provided the like extraction and reutilization are in conflict with normal use or legitimate interests of the right holder82. Thus the *maker of a database can reserve exclusive access to the database to himself or reserve access to specific people*[83].

This approach, namely closing access to the CHIC data repository the authorised users only, is also expected in CHIC. As follows from the DoW, WP 10, the data in CHIC shall be made available to the VPH research community via secure storage solution, such as Grid or Cloud, in a specialized platform. Hereby, access to the data will have the authorised users only. According to Article 7 (3) Database Directive, the right to use the database may be granted under contractual license. The use of data may be limited in scope, purpose and terms of use. It may be noted, that when the users have the right to access and use the database, or a part thereof, consultation of the database may not be prevented by the right holder. Following Recital 46 of the Database Directive the sui generis right does not *give rise to the creation of a new right in the works, data or materials themselves*[84] and shall be without prejudice to the existing rights over the contents[85]. *Copyright works and protectable subject matter incorporated into the database remains subject to the respective rights and may not be extracted from the database without permission of the right holder*[86].

From the above analysis, the following conclusions can be drawn:

---

[79] CHIC DoW, Part B 2.2, p 51-53.

[80] Article 7 (1) Database Directive.

[81] ECJ, Judgment of 09.11.2004, Case C-203/02, para. 67.

[82] Article 7 (5) Database Directive.

[83] ECJ, Judgment of 09.11.2004, Case C-203/02, para 55.

[84] Database Directive, Recital 46.

[85] Ibid., Recital 18.

[86] Ibid, Recital 26.

i.   The resources spent on collection, verification and representation of data in the data repository shall render the data repository to qualify for protection under the sui generis right;

ii. Access and use of the data repository may be provided to the closed circle of authorised users (from the VPH research community only);

iii. Protection under the sui generis right would allow that access, use and extraction of the data from the data repository be made under authorisation of the right holder and be limited in scope, purpose and terms of use.

5.3.2 Protection as knowhow/undisclosed information

Another possibility is that the medical data might be protected as undisclosed information (also referred to as knowhow). In examining this, first the legal framework, object and scope of protection, rights of the right holder will briefly be outlined. In the subsequent legal analysis it will be considered whether the medical data, residing in CHIC, constitute a protectable subject matter. Should the result be positive, measures which shall be taken to safeguard that medical data are protected as undisclosed information and that the rights in such are enforceable will be considered further. Results, made in the legal analysis, and legal guidelines will be drawn up in the end.

5.3.2.1 Legal framework

Protection of information as knowhow has a principally commercial genesis, with its roots in the Paris Convention[87] as a protection from anti-competitive practices and shall protect such information unauthorised access, use and disclosure by third parties *"contrary to honest practices in industrial or commercial matters"[88].* There are no harmonized legal rules on protection of undisclosed information (also referred to as knowhow or trade secrets) on the EU level, albeit a draft Directive on the issue has recently been proposed by the Commission.[89] In none of the EU Member States is knowhow the subject of autonomous legal protection. Rather, the legal provisions which consider the acts of unauthorised access, use and disclosure of knowhow as prohibitive and provide for sanctions are implemented via a variety of legal figures under different national laws, such as competition laws (e.g. Disclosure of trade and industrial secrets, Paragraph 17 Unfair Competition Act of Germany[90], Paragraph 11 Unfair Competition Act of Austria[91]), the law of confidence (UK and Ireland[92]) as well as criminal, labour, tort, contract laws. The uniform definition of knowhow on the EU level is provided for in the Commission Regulation (EC) No 772/2004 of 27 April 2004 on the application of Article 81(3) of the Treaty to categories of technology transfer agreements, Article 1 (i), which is applicable to regulation of competition on the market. Therefore, legal provisions dealing with protection of knowhow shall be sought for in national laws depending on the practical area, where such protection is applied and remedies sought, e.g. unauthorised use of knowhow by competitors, employees, public officers, etc.

The main legal document, which provides for definition and scope of protection of knowhow on the international level is TRIPS, Section 7, Article 39 et seq. TRIPS adheres to protection of such information in the area of competition, as provided for in the Paris Convention, and defines the kind of information to be protected as undisclosed information. Protection of undisclosed information is provided for in Article 39, as follows: "*Natural and legal persons*

---

[87] Paris Convention for the Protection of Industrial Property of March 20, 1883, available at: http://www.wipo.int/treaties/en/text.jsp?file_id=288514#P220_36426.
[88] Article 10bis, Paris Convention.
[89] European Commission - IP/13/1176, issued on 28/11/2013.
[90] The Act Against Unfair Competition of Germany, available at: http://www.gesetze-im-internet.de/englisch_uwg/.
[91] Bundesgesetz gegen den unlauteren Wettbewerb 1984 - UWG, available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002665.
[92] Hogan Lovells LLP, Report on Trade Secrets for the European Commission, Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D, available at: http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.html.

shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices[93] so long as such information:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".

These criteria, as set out in TRIPS, provide a legal basis and general legal framework for protection of data as undisclosed information.

5.3.2.2 Implications for the data in CHIC

Following the DoW, WP 8, all the medical data produced or collected by the project shall be stored in the CHIC data repository. The data in CHIC will be de-identified and (de facto)-anonymized, the patient data will contain all related information, incl. clinical data, imaging data, histological data, therapy etc., and be stored under the data types: imaging data (DICOM etc), descriptive/structural data (age, sex etc), other files (histological reports). Here, considering, that the medical data to be provided to CHIC will mostly come from clinical trials, conducted by research and therapy institutions (KU Leuven, USAAR) and that the data will be submitted for the research purposes, the medical data in CHIC can be considered as R&D information relating to medical scientific research and may be considered as protectable subject matter, provided it meets the basic criteria of knowhow.

As set out above, the criteria in question are that the data are secret, have economic value and be subject to measures to keep it secret. To stand the criterion of secrecy the data, as a whole or as accumulated from its parts, shall not be *generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question[94].* This implies that such data shall not be exposed to knowledge of the public or *the circles that normally deal with the kind of information in question.* In contrast, making the data available to the public in any form, such as through publication, will remove the status of data as being secret[95]. The same rule applies if the data are made available within the circle of people dealing with the kind of data, such as cancer research or treatment community. In relation to CHIC, this means that should the results of clinical trials, which are supposed to be transferred to CHIC as de-identified/pseudo-anonymized, be exposed to the knowledge of public or specialized circles, like publication in any specialized magazine, the criterion of secrecy for such data will not be fulfilled. The result is that such data will come out from the scope of protectable subject matter.

The confidentiality of data implies that such data be only known to a closed circle of people. As a rule, confidentiality of data is achieved by a contractual duty to keep the data secret and not to pass these to outsiders. A contractual duty to keep the data secret is, in general considered, as a sufficient measure for maintaining the confidentiality[96]. As regards CHIC, it follows that the data, which are supposed to be protected as knowhow, should be subject to the measures on non-disclosure of information, as stipulated in Section 10 CA, unless such data have not been transferred in the status of being "confidential" already. For this the data when being transferred to CHIC shall be explicitly marked as "confidential", the scope and

---

[93] For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

[94] Article 39 TRIPS.

[95] Lodigkeit, supra, p. 100.

[96] Ibid.

purpose of use (in strict compliance with the informed consent of the data subject), as well as other requirements for maintaining the data secret shall be defined. Unless otherwise defined, treatment of such data as confidential will be subject to the confidentiality measures, as set out in Section 10 CA.

Another essential criterion for protecting CHIC data as knowhow consists, according to Article 39 (b) TRIPS, in the commercial or economic value of the data. It is general practice to assess this value by reference to the owner´s business, and in particular the competitive advantage that the owner derives from the data remaining secret. As established by the court practice in some Member States, it must be sufficient if the owner shows an economic interest in keeping the facts secret, which is present when the competitiveness of the company could be weakened through publication of the facts[97]. When transposed to the situation with medical data in CHIC, it must be noted that the CHIC Consortium would qualify as the secondary possessor of the data; the primary entities which are in possession of the medical data would be the data providers themselves. As of the data available be now, the pure clinical data will be provided by KU Leuven and USAAR. Consequently, the criterion of economic value of the medical data shall be analysed in relation to the data providers, which might attribute economic value to the data they have provided to CHIC.

According to the data provided in the Collaborative Project, Part B, [98]USAAR, and its departments of Paediatric Oncology and Haematology and the Department of Pathology, which provide clinical data on nephroblastoma and brain tumour, are part of the comprehensive Cancer Center of the University Hospital (which is responsible for treatment of patients in the Saarland area), both departments are engaged in research (clinical studies and trials and basic research) and have expertise in the treatment of cancer of respective tumour types. KU Leuven, which provides data on clinical trials of Wilm´s Tumour, Glioblastoma and non-small cell lung cancer, has extensive expertise in combining translational and clinical research with optimal patient care, plays major role in neuro-oncology community worldwide, is engaged in preclinical research and production of vaccines for GMP, draining patients for immunotherapy and conduct of clinical trials[99]. Considering, that both institutions are engaged both in clinical research and patient care, have expertise, reputation and competitive advantage in the cancer research community and will provide data to CHIC, as obtained through the expertise of running cancer research and clinical trials, the data, thus provided can be considered as research data (recognized as a type of knowhow) and, once confidentiality applies, can be deemed as such.

In summary, the medical data which will be provided and stored in CHIC, constitute highly sensitive patient data, which shall be dealt with the highest level of security. Based on the results of the above analysis, it may be concluded that the medical data to be provided to CHIC may satisfy the main criteria of being treated as undisclosed information in the meaning of Article 39 TRIPS and be protected as such, provided confidentiality measures (Section 10 CA) are in place.

5.4 Other IPR ownership issues of concern for the CHIC framework

In addition to the issues of (hyper-)model ownership discussed in 5.1 and 5.2, there are other more general copyright ownership issues pertinent to the software development under the Project. The analysis here builds on legal analysis conducted in previous Deliverables D4.2 and data provided by the modelling parties. Again, for present purposes it is important to identify gaps in the applicable regulatory framework (under the GA, Annex II and the CA), so as to be able to address these in the model IPR memorandum of understanding annexed to the present Deliverable.

---

[97] Ibid, p. 101.
[98] Collaborative Project, Part B, p.51.
[99] Ibid., p. 52.

5.4.1 Potential rights held by Partner employees

As previously discussed in Deliverable D4.2, according to the first ownership rule (under the Berne Convention and Article 2 Paragraph 1 Software Directive, the author of a program shall own the copyright in it, which would generally be the programmer. However, there is an important exception to this rule, in particular in cases where the programmer developed a program in the employment relation. Here, it will instead be the employer who holds the economic rights in the program on the exclusive basis as designated by the law. This is provided for by Article 2 Paragraph 3 Software Directive, which states: *where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.*

As noted, the employer is designated the right holder, *unless otherwise provided by contract[100].*The employer may rely on these rights as derived by the law, once he can prove that the program is created "*in the execution of* the employee´s *duties or following the instructions given by his employer*". For this, the development of a program must either have been explicitly ordered by the employer to the respective employee, or development of programs belongs to the ordinary tasks of the employee in the employment relation. Otherwise, the employer may derive his rights in the program thus developed from other provisions of the laws, for instance, when the employee by program developing used materials and knowledge which he has acquired exclusively through the employment[101].

To the extent that the employer acquires the rights in the software by contract, it is important that fair compensation from exploitation of the work should be attributed to the employee (author). Some national laws provide, that in cases where the agreed financial compensation of the author turns out to be inadequate to the benefits from exploitation of the work, then the author may claim the right on equitable participation in the proceeds from the work so derived[102].

It is in the main expected that model codes and software in the CHIC Project will be developed by the programmers employed by the Parties (the project partners). Hence, it is presumed the Parties shall derive the status of exclusive right holder in the software thus developed and hold all economic rights on exclusive basis by virtue of Article 2 Paragraph 3 Software Directive (as transposed into national laws). The employee´s rights are addressed in Article 8.5 CA, pursuant to which the Parties shall *ensure that it can grant Access Rights and fulfil the obligations …notwithstanding any rights of its employees or Subcontractors in the Foreground they create.*

The wording of this provision is such that it implies that the Parties shall procure the IPRs from the employees. The scope of rights as sufficient for the Parties to grant Access Rights and fulfil other obligations is left at sole understanding and discretion of the Parties. With regard to securing the rights in the works produced by their employees, a legal advice to the Parties would be to address potential employee rights directly, as provided for in the memorandum on disposal of Intellectual Property Rights (hereinafter referred to as the "IPR memorandum", Appendix 5)

5.4.2 Potential rights of third parties which develop software for Partners

Copyright and rights in the software developed upon commission follow the first ownership rules. Hence, copyright in the software shall vest in the software developer (freelance worker or software development house), unless assignment or license of the rights in software is not explicitly regulated in the agreement.

---

[100] Article 2 Para 3 Software Directive.

[101] LG München, Judgment of 16.01.97, 7 O 15354/91 - Software-Entwicklung.

[102] BGH, Judgment of *23. 10. 2001, Case X ZR 72/98 - Wetterführungspläne II, GRUR 2002, 149.*

The rights in the software which are not licensed or assigned explicitly by the contract, remain with the developer and are considered as not assigned or licensed at all. *Even if it had been understood from the start, and possibly even agreed orally, that the commissioner would in all respect "own" the product, this will not be sufficient to alter the operation of the first ownership rules*[103]. Accordingly, unless the rights are explicitly licensed, a legal issue in CHIC might arise where the Parties wish to bring commissioned software to the project: the first question is whether the rights are assigned or licensed at all, and if yes, what scope and terms of use apply.

In this context, it is an accepted practice in the software industry that pre-existing codes are used for software development for multiple customers, with the result that grounds for assignment of rights or grant of exclusive license to the commissioner are insufficient[104]. The fact that the commissioner paid for the work would normally be insufficient for assignment, but might however be sufficient to infer *an implied license to use the work for the purpose for which is was commissioned[105]*. A software license, as implied in the commission agreement, might be subject to recognition by the court[106]. Such a license might extend to the software use for the purpose, as commissioned, and would, as a rule, not entitle the commissioner to sublicense the software[107]. This scope of implied license would definitely be insufficient for grant of the Access Rights to the Parties for Implementation and for Use.

The legal issues dealing with the third parties rights are partially addressed in the CA, in particular, Articles 4.3., 8.5, 6.9.3.3 CA. These provisions imply that the Parties shall ensure that they and other Parties in the Project can perform their rights and obligations in an unaffected way. However, as indicated above, the Party commissioning work under the Project to third parties may rely on the commission agreement and ownership of the product in the result, without addressing the IPRs in particular. The legal consequences would be as indicated above. For legal certainty the acquisition of IPRs in works carried out and software developed under the Project by third parties should be addressed directly.

For this, each Party which commissions development of software or other works under the Project to the third parties should procure the IPRs in the works/software produced by the third parties into the Project, and software in particular. The scope of rights, should, first, cover the rights, as necessary for use of the work in the Project and performance of the tasks of the commissioning Party in the Project.

Second, the rights in software should be sufficient to grant Access Rights for Implementation and for Use to the other Parties, as provided for in Article 9.8.4 CA, with the adhering right to sub-license to the end-users (Articles 9.8.4.1.2, 9.8.4.2.2 CA), as well. Even if the Party may not need the rights itself, it cannot license what it does not have. Therefore, the rights, provided for in Article 9.8.4 CA should also be included into the license for the purposes of sublicensing to the other Parties. Such scope of license with the right to sub-license to the Consortium Parties and to the end-users should allow the Party concerned to comply with its obligations to grant Access Rights. The scope of rights may, however, vary on a case by case basis and will need to be verified by the commissioning Party itself, depending on the work concerned.

The procurement of IPRs can be made either by concluding an assignment agreement (which can hardly be achieved in practice) or license agreement with the right to sub-license or by including the license terms into the commission agreement itself. Important is that the grant of IPRs, in whatever contractual arrangement it is embedded, should be executed in writing, i.e. upon handwritten signature of the parties, i.e. authorised representatives thereof.

---

[103] Reed C., Angel J, Computer Law, Sixth Edition, Oxford University Press, 2007, para 7.3.1. p.352.
[104] Rowland, supra, p. 400.
[105] Reed, supra, p. 353.
[106] Rowland, supra, p.400.
[107] Ibid.

Contractual arrangements on copyright, assignments of copyright and agreements on future use of copyright to be enforceable under certain national laws[108] shall be done in writing[109]. Insofar as a software license is concerned, then a non-exclusive, royalty-free, irrevocable, unconditional, worldwide, perpetual copyright license with the right of sublicensing, to the Consortium Parties (Articles 9.8.4.1.1, 9.8.4.2.1 CA) and the end users(Articles 9.8.4.1.2 CA, 9.8.4.2.2 CA) shall, in general, be sufficient.

Software shall pursuant to Article 9.8.3 CA be provided in Object Code, and Application Programming Interface (API), as use of the Object Code thus requires. Source Code might be needed, if without it, the execution of tasks or use of the Foreground by the Parties in the Project is technically or legally impossible; to the extent thus necessary. For instance, source code might be needed for inter-interoperability purposes. Source code is rather seldom disclosed by the software developers, since, software developers tend to produce software based on their pre-existing codes and are unwilling to make the source code available[110]. A possible solution might be to negotiate disclosure of the source code through an escrow agreement.

Accordingly, Partners in the CHIC Project which involve any third parties in the software development under the Project, should procure the rights in the software (either by assignment or license executed in writing) in the scope needed for the Project Implementation and for Use pursuant to Article 9.8.4 CA with the right to sub-license. The software should be provided in object code and API, but source code might also be provided if technically or legally necessary for the Project Implementation or for Use. Should access to the source code be not provided under the license agreement, then its disclosure and conditions of release may be negotiated through an escrow agreement. In this regard, appropriate obligations upon the Parties will be included in the IPR memorandum.

5.5 Software licensing inside the Consortium

In this section, and building on the preliminary analysis presented in Deliverable D4.2, the IPR issues relating to software licensing in the Project will be considered. The further analysis will focus especially upon contractual arrangements and software licensing inside the Consortium as set out in the CA, rules on introduction and use of software under Controlled License Terms, as well as open source licensing and license incompatibility issues.

The terms of software license inside the Consortium are subject to general rules on grant of Access Rights, as provided for in Section 9 CA and specific provisions relating to Software, laid down in Article 9.8 CA. The provisions govern most important aspects of software use, in particular: how the Access Rights shall be granted, what is the scope of rights (in terms of time, territory, scope of use), remuneration, what modes of software use are allowed, and in what form access to the software shall occur. These terms can be deemed as sufficient in order to qualify for a license agreement. The basic structure of the license agreement can be divided into the following clauses: the parties, object of license, modes of software use, form of the code to be supplied, the right to sublicense and assign the license, duration, territorial scope, and financial terms[111].

5.5.1 Form of contract

There is no binding rule as to the form in which a software license agreement shall be concluded to be deemed effective. The written form is not prescribed as mandatory in the Software Directive. Hence, agreement of the parties on basic terms of software license in any form might be sufficient. However, to be enforceable in the national jurisdictions, like

---

[108] German copyright act, Urheberrechtsgesetz, U.K. Copyright Act, CDPA 1988.
[109] Chris Reed, supra, p.352.
[110] Rowland, supra, p.400.
[111] Ibid, p.401.

Germany and Austria[112], the agreement shall be executed in writing, i.e. signed with a handwritten signature or as certified by a notary act. Also, to be enforceable under certain national laws[113], contractual arrangements on copyright, assignments of copyright and agreements on future use of copyright shall be made in writing[114]. Therefore, in order that the software license agreement and the rights of the Parties in software be enforceable, written form might be required, at least under some jurisdictions.

General rules on the form in which the Access Rights shall be made are provided in Section 9 CA. Article 9.2.6 CA prescribes that requests for Access Rights shall be made in writing. As in the case of the software license above, the overall form in which the Access Rights shall be granted is not explicitly regulated. Thus the written form and procedural rules on grant of Access Rights based upon conclusion of the written agreement is prescribed for the grant of Access Rights to Background for Use (Article 9.4.2 CA) only. By contrast, there is no such requirement of concluding the written agreement for grant of Access Rights to Foreground or to Foreground and Background for Implementation.

The requirement of concluding a written agreement for grant of Access Rights for Implementation might delay the performance of tasks in the Project and the Access Rights for Implementation should thus, in general, be enforceable under the CA. When, however, grant of Access Rights to Software for Use, which is Foreground, is concerned, then in order to ensure that the license terms are agreed between the Parties and that the rights are enforceable, the optimal approach for ensuring legal certainty would be to subject the grant of Access Rights to Foreground for Use to conclusion of the written agreement as well, as for the Background. This proposed regulation is provided for in the IPR memorandum.

5.5.2 Software license terms

The software license terms are subject to the rules on grant of Access Rights in general (Section 9) and specific provisions relating to Software (Article 9.8 CA). The general rules are as follows. First, as conferred from the general provisions, the Access Rights to Software are granted on non-exclusive basis, non-transferable, without the right to sub-license, unless agreed otherwise, and worldwide (Article 9.2.6 CA).

In this regard Royalty-free Access Rights to Software, either Foreground or Background, are provided for Implementation (Article 9.3 CA) and to Foreground for Use (Article 9.4.1 CA), unless software is reported for patenting (which though is scarcely likely in practice). The Access Rights to Background for Use shall be granted upon Fair and Reasonable conditions (Article 9.4.2 CA). Requests by Parties for the Access Rights for the Project Implementation (Access Rights as needed to performance of the requesting Party´s tasks in the Project, Article 1.2 CA) can be made up to completion of the Project. For their part Requests for the Access Rights for Use (Access Rights needed for Use of the requesting Party´s Foreground, Article 1.2 CA) may occur up to twelve months after completion of the Project, in case of a Party´s withdrawal from the Project (Article 9.7.2.1.2 CA); and up to twelve months after termination of the Party´s participation in the Project (Article 9.4.3 CA)

In the second place, the form, in which software shall be provided, is regulated in Article 9.8.3 CA. In general, only Object Code and API, if required for use of the Object Code, shall be provided. Access to Source Code might be requested, if without the Source Code the execution of the Party´s tasks under the Project or the Use of its own Foreground is technically or legally impossible Access to the Background, shall cover the object code and API, only, unless agreed otherwise (Article 9.8.3 CA). Specific rights, which are granted, are explicitly regulated for Software which is Foreground for Use (Article 9.8.4 CA).

---

[112] Article 416 Code of Civil Code of Germany, as promulgated on 5 December 2005 (Bundesgesetzblatt (BGBl., Federal Law Gazette) I page 3202; 2006 I page 431; 2007 I page 1781), last amended by Article 1 of the Act dated 31 August 2013 (Federal Law Gazette I page 3533); available at: http://www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html.

[113] German copyright act, Urheberrechtsgesetz, U.K. Copyright Act, CDPA 1988.

[114] Chris Reed, supra, p.352.

These general rules provide for basic conditions of Software license (for Implementation and for Use), regulate essential terms and license scope (parties, object, financial terms, territory, sublicensing right, etc), the rights on software use may inferred either from scope and purpose of general formulations or specific provisions. Hence, these terms may be deemed to be sufficient to infer that the Parties reached agreement on Software license on these terms, unless specifically provided by contract otherwise.

5.5.2.1 Background and Foreground for Implementation

The rights as granted to the Parties to access and use each other's Software for Implementation are not explicitly regulated and shall cover the scope of rights for carrying out the Project and might be inferred from the definition of "Needed" for the Project Implementation. From the definition of "Needed" for Implementation, as regulated in Article 1.2 CA, only those rights shall be granted for Implementation *without which carrying out of the tasks of the Requesting Party would be impossible, significantly delayed, or require significant additional financial or human resources*. From this definition follows that the scope of Software use for Implementation is limited by the scope of tasks of the requesting Party in the Project and shall cover all possible modes of software use.

The scope of rights to software use for Implementation may be inferred from the purpose, for which the rights are granted, subject, however, to the following. First, the modes of software use, like reproduction, modification, distribution, making available to the public, belong to the exclusive rights of the right holder and are subject to the authorisation, i.e. license, as provided for by the Software Directive, Article 4.

Further, there are differential national approaches to contractual interpretation in this area. Thus while some national laws interpret agreements based on the purpose, which by software license shall cover all software uses necessary for achievement of the object of the agreement[115], in other national jurisdictions agreements might be interpreted restrictively. Thus, the rights which are not explicitly mentioned as licensed or assigned under the agreement might be considered as not granted at all. Accordingly, in order to promote legal certainty, the rights as granted for Implementation shall be specified, as proposed in the IPR memorandum.

5.5.2.2 Background and Foreground for Use

Access Rights to the Background for Use are subject to conclusion of the written agreement (Article 9.4.2 CA). Sublicensing rights, meaning the right to license the software to any other third parties, are excluded by Article 9.8.4.1.3 and 9.8.4.2.3 CA, may however be negotiated. Access Rights to Background for Use shall be granted on Fair and Reasonable conditions (Article 9.4.2 CA). On these premises, the Parties may follow the principle of freedom of contract and negotiate other terms, they deem necessary to include at their own discretion.

Access Rights to Software which is Foreground for Use are more or less regulated in Article 9.8.4 CA. The rights on use of Software use, access to Software, the scope of use, the right to sublicense, including to the end-users, are provided for and shall be sufficient to make a software license agreement. The main license terms apply the following conditions: non-exclusivity, non-transferability, worldwide application, royalty free license, without the right to sublicense, except end-user license (Article 9.8.4 CA) and unless otherwise agreed (Article 9.2.4 CA). The scope of rights is limited within the scope as needed for Use of the Foreground (Article 9.8.4 in conjunction with Article 1.2 CA). The rights can be requested up to twelve months after the end of the Project, with certain deviations for the leaving Parties (Article 9.4.3 CA).

---

[115] Article 31 Paragraph 5 Copyright Act of 9 September 1965 (Federal Law Gazette Part I, p. 1273), as last amended by Article 8 of the Act of 1 October 2013 (Federal Law Gazette Part I, p. 3714), available at: http://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html.

The conditions form the basic terms with some scope left to the Parties to agree the terms, which they deem necessary or reasonable to negotiate. Access to Software for Use shall, in general, be granted to the Object Code and API. Source Code can be made available upon proof that the Use of the Party´s Foreground is legally or technically impossible. The Source Code shall only be granted to the extent necessary (Article 9.8.3 CA). The rights of using the Object Code and API comprise the right of normal use as needed for Use of the Foreground and the basic rights adhering to exploitation of the Foreground (Article 9.8.4.1.1 CA). In general, these default rules may be regarded as sufficient for the purposes of CHIC, and hence do not need to be subject to additional coverage in the IPR memorandum.

For its part, use of the Source Code, as needed for Use of the Foreground, shall cover a worldwide *right to use, to make copies, to modify, to develop, to adapt Source Code for research, to create/market a product/process and to create/provide a service* (Article 9.8.4.2.1 CA). When the above scope of rights in the Source Code for Use is considered in the context of the purpose for which the Source Code is granted, namely because without the Source Code Use of the Party´s Foreground would be legally or technically impossible, it follows that the right *to develop, to adapt Source Code for research, to create/market a product/process and to create/provide a service* definitely extends the scope of normal Use of the Foreground, which must have been developed already. Normal use of the Foreground would suggest use of the Source Code for maintaining the Foreground, including error correction, upgrades, etc., achieving inter-operability inside the Foreground, etc.

Taking the collaborative approach, the Parties may deem such scope of rights as reasonable. Considered overall, it may be concluded that the terms of Access Rights to Software which is Foreground for Use provide for a fully-fledged software license agreement with the basic rights of software use included.

5.5.3 Sublicenses to the end-users

The Access Rights to Software for Use, as provided for by the CA, shall cover the right to sublicense to the end-users. Here, the right to sublicense Object Code and API to the end-users, is provided for in Article 9.8.4.1.2 CA. This covers the Software use to the extent necessary for the normal use of the relevant product or service, and applies to use of the Software *alone or as part of or in connection with or integrated into products and services of the Party having the Access Rights.* The scope of Software use is limited *as technically essential to maintain such products and services and crea*te interoperable software, as provided for in Software Directive.

The end-user license also foresees disclosure of the Source Code, which according to Article 9.8.4.2.2 CA can be used *solely for purpose of adaptation, error correction, maintenance and/or support of the Software* and when the Party has access to the Source Code, as acquired along with the Access Rights for Use. With respect to release of the Source Code the end-user license following considerations can be made.

5.5.3.1 Error correction

Certain acts of software use as *necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose* are exempted from authorisation of the right holder by virtue of Article 5 and Article 6 Software Directive. These rights include, in particular, the right of reproduction of a computer program in so far as necessary for loading, displaying, running, transmission or storage of the computer program, the right of modification, including for error correction, the right to observe and study the program, the right of making a backup copy and the right of de-compilation. *The acts of loading and running necessary for the use of a copy of a program which has been lawfully acquired, and the act of correction of its errors, may not be prohibited by contract*[116].

---

[116] Recital 13 Software Directive.

In contrast to the right of making a backup copy, which as the Directive says *may not be prevented by contract in so far as it is necessary for that use[117]*, the right of modification, also as necessary for the error correction, may be regulated by the parties by the contract. Error correction and maintenance of software may, for instance, be agreed under a separate maintenance agreement, or it may be the obligation of the software provider to upgrade and maintain the software, or maintenance of the software may be delegated to third parties.

When, however, maintenance service of software is not agreed by the parties, the lawful acquirer might derive his right for error correction as *necessary for the use of the computer program in accordance with its intended purpose* by virtue of Article 5 Paragraph 1 Software Directive. The scope of software use would thus come within normal use as part of in connection with the Party´s Foreground (Article 9.8.4.1.2 CA).

What may provide for legal controversy, is that the right of modification for maintenance is provided along with the Object Code (Article 9.8.4.1.2 CA), and the Source Code is also provided along with the right of adaptation, error correction, maintenance and or support of the Software (Article 9.8.4.2.2 CA).

Error correction and any modification of the Software would normally require access to the Source Code, rather than merely to the Object Code, however, grant of the Source Code to the end-users extends the scope of software licensing to the end-users and making the Source Code available to the end-users is not an obligation of the software providers, as dictated by the Software Directive.

The exercise of these rights can generally be performed by a lawful acquirer by virtue of exempted acts, as laid down in Article 5 Software Directive. Here the latter provides that: *Whatever the extent of the right conferred by the Directive, it is not the acquirer´s right to have errors corrected; he or she can merely correct them without being in breach of copyright. …. there is no obligation for the seller to supply the source code…* as needed for error correction… *the Directive would not seem to make the source code available to the greater extent to the acquirer…*[118]

Therefore, when the Parties make source code available to the end-users, even for the error correction (which is the natural way to understand the technical terms), it definitely extends the minimum scope of exempted acts of software use, as foreseen by the Software Directive, which does not explicitly mentions that for the error correction source code shall be provided. It follows that it is up to discretion of the Parties to decide whether they wish to provide the source code to the end-users or rather abstain from making the source code available. In any case, there is no such obligation of the software providers to grant source code to the end-users, even for error correction, as binding by the Software Directive. If the Source Code is not granted, but the right to error correction (how the end-user shall exercise this right is left at discretion of the end-user) is provided, it shall be enough for the end-user license to be compliant with the rules of the Software Directive on the exempted acts. In view of this ambiguity, a proposed improvement to the regulation is provided in the IPR memorandum.

5.5.3.2 De-compilation

The right of de-compilation, as foreseen in Article 9.8.4.1.2 CA, is also provided within the exempted acts *where reproduction of the code and translation of its form ….are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs…* upon certain conditions[119]. The underlying idea is to make it possible for the end-user *to connect all components of a computer system, including those of different manufacturers, so that they can work together…*without prejudice to the right holder´s rights, however *[120]*. This right of de-

---

[117] Article 5 Paragraph 2 Software Directive.
[118] Rowland, supra, p.405.
[119] Article 6 Software Directive.
[120] Recital 15 Software Directive.

compilation cannot be derogated from by the agreement and the conditions and scope, under which the de-compilation may be performed, are explicitly specified in the Directive.

What is peculiar is that de-compilation suggests translation of the object code into the source code with subsequent conversion of it into the language of another computer program to achieve inter-operability. Since Access to the Source Code might already be granted pursuant to Article 9.8.4.1.2 CA, it may be questioned how far such a right in respect of the Object Code is needed. The right to translate the source code to achieve interoperability would arguably be adequate. In any case, it may be assumed that source code would be granted to the end-user only when the Party itself requires it for the use of its own Foreground.

5.5.3.3 Back-up copy

Another act of software use, which falls under exempted acts for the end-users, which cannot be derogated from by the agreement and which is not explicitly provided for in the CA, is the right to make a back-up copy. This right is granted in Article 5 Software Directive to the lawful acquirer *in so far as it is necessary for the* normal use of the program according to the intended purpose and, as further specified in the Article, *may not be prevented by contract*.

A concept of a backup copy in modern technical environment (cloud computing, servers, data securing mechanisms) is rather controversial. The initial concept of a back-up copy, as implied by the traditional copyright law, is significantly extended. Where a backup copy as embodied in a tangible medium must have been implied by the law, tangible items are obsolete now and data and programs are stored for the back-up purposes on servers[121].

The Parties, which know the technical parameters of their Software, may provide for the scope and conditions within which a back-up copy would be adequate. In any case, the right of making a back-up copy may not be prevented by the contract and, even if not granted by the agreement, the end-user would still derive this right from the Software Directive. The right of making of a back-up copy by the end-user shall also be provided in the CA, as proposed in the IPR memorandum.

5.6 Open Source and Controlled License Terms

The Project envisages the use of the open source approach, and in the legal framework of CHIC regard to the open source software and Controlled License Terms is given in Article 9.8.6 CA. Access to Software is regulated in Article 9.8.3 CA. According to this, such access shall be granted to the Object Code and API, if required for use of the Object Code. Source Code, which is Background, may be made available upon agreement of the Parties, and Source Code which is Foreground, shall be provided upon request if legally or technically indispensable for performance of the tasks of the Party under the Project or use of its own Foreground.

On the other hand, according to Article 9.8.6 CA, the use of open source software is envisaged, where disclosure of the source code is implied. In some cases, the Parties may be willing to make the source code available. This may to some extent be incompatible with the Article 9.8.3 CA. In order to give these provisions practical efficacy in line with the concrete situations likely to arise within a given project, parties are enabled to compile a list of Software with the Source code disclosed via an attachment. Additional specific regulation of these aspects for the purposes of CHIC is provided in the IPR memorandum.

5.6.1 Controlled license terms

The criteria according to which an open source license will fall into the category of Controlled License Terms and the regulations on these are specified in Article 9.8.1 CA. According to this, Controlled License Terms shall mean license terms which require (not permit) that the

---

[121] Diedrich, Kary, Nutzungsrechte für Systemsicherungen nach §69dURhG, CR 2/2012.

use, copying, modification and/or distribution of Software/Work and/or any Derivative Works be subject, in whole or in part, to one or more of the following:

- Right for the Source Code to be made available whether royalty-free or not;

- Right to create modified versions or derivative works of the Work or Derivative Work;

- Grant of royalty-free licence relating to the Work or Derivative Work.

Given that only one of the above criteria will be sufficient to make a license subject to Controlled License Terms, it may be anticipated that a rather high number of open source licenses might be implicated.

5.6.1.1 Rules applying to Controlled License terms under the CHIC CA

Software and Works released into the Project under Controlled License terms are subject to special regulations, as provided for in Article 9.8.6 CA. Most concerned are the Software and Databases. Such regulations are laid down in Article 9.8.6 CA and provide that introduction and use of a Work or Software subject to Controlled License Terms, as defined in Article 9.8.1 CA, shall be reported and its introduction by a Party shall be subject to approval of the (other) Parties. The request for approval shall contain sufficient information to enable the Parties to assess whether their use of or Access Rights to such Software or Work may be impaired by the Controlled License Terms (Article 9.8.6 paragraph (iii)). The form of the request and details of the data, deemed sufficient for assessment, are further not specified.

A particular concern in this regard is the potential impact of such terms upon the right to sublicense the Software/Work, as provided for in Article 9.8.6 paragraph b) CA. This reflects the potential impairment of that right as a consequence of the viral effect of some open source licenses, which might require that any derivative work (modified or improved version made with use of the original work subject to definition of a particular license) be licensed under the same license terms, as the original.

Therefore, consent of the Parties that the Software or Work, once subject to the Access Rights, shall be sublicensed under the same Controlled License Terms is required. The implied right to sublicense under the same license terms naturally results from the licenses, to which the requirements on the Controlled License Terms apply. The agreement that the Software/Work in question shall be sublicensed under Controlled License Terms may be expressly made in writing by the Party granting the Access Rights or be necessarily implied in the approval of the Parties (Article 9.8.6 b CA).

The contents of the Request containing information which shall allow the Parties to assess the effect of the Controlled License Terms on their rights and obligations along with the agreement/approval on inclusion of the right to sublicense Controlled License Terms are provided in Attachment 4 to the IPR memorandum.

5.6.1.2 Present position within the Project

At the present stage of Project Implementation a number of Parties have not yet come to a concluded decision as to which licenses they will apply to release their Software/Works into the Project. However, from the data submitted by the Parties it appears that a significant number of licenses, either certified as open source or the like licenses, which provide for the source code being disclosed, may be involved. To assess whether a certain license fulfils the criteria of Controlled License Terms, as laid down in Article 9.8.1 CA, the terms of each particular license shall be analysed. The licenses and license terms and the wordings of license vary. The same license condition formulated in one license may be formulated in a quite different way and style in another license and in specific language, subject to the jurisdiction of origin.

Admittedly, without having an overview of the concrete licenses involved and license terms, in place, it remains a complex undertaking to assess definitively which licenses will fulfil the

criteria of the Controlled License Terms. On the other hand, the criteria for the Controlled License Terms are defined in plain text, and shall allow the Parties, who have the license terms they use at hand, to prove whether a particular license, under which they are going to release their Software or Work into the Project is concerned. The recommendation at this stage of Project development would be that each Party which uses external sources and codes for the performance of its tasks in the Project and which intends to release the Software or Work into the Project as open source shall:

- check whether the license under which the Software or Work will be released meets one or more requirements laid down for Controlled License Terms (Article 9.8.1 CA);

- where the answer is in the affirmative, assess the chances whether use of the Software/Work would be approved by the Parties;

- where those chances are assessed as negative, seek alternative solutions, i.e. Software/Works with alternative licenses, which are not subject to the Controlled License Terms.

When major ICT tools and components, which play a crucial role for the Project success and have hardly any analogues in place, are licensed under licenses which might contain Controlled License Terms, like RICORDO Infrastructure under Mozilla Public License v.2, the odds are rather high, that use of such Foreground under Controlled License Terms would be approved. However, a different situation may apply with respect to smaller components, which do not play such a crucial function and might be interchangeable. In this case, the introduction and use of such software in the Project would be subject to the discretion and approach of the Parties.

What can be said from the data, available as of now, is that a number of permissive FOSS licenses, like BSD, Apache, and the like, are used. These licenses do not contain Controlled Licensed Terms (or copyleft), but subject licensing of the program simply to attribution of the copyright notice, warranty disclaimer and allow distribution of the program in either source and/or object code. Still, terms under different license versions may vary and shall be analysed and complied with in each particular case. The issue of license compatibility – both as it may arise between some permissive licenses, and – more likely – in respect of licenses with strong copyleft terms (such as the GPLx licenses), so far as these figure in the Project, is considered under 5.6.2.

From the above legal analysis it may be concluded, that the terms of licensing software inside the Consortium are more or less regulated in the Consortium Agreement and cover most essential terms and conditions. However, proposals for addressing residual omissions in the legal framework, as could be identified at this stage of Project development, are made in the CHIC IPR memorandum.

As outlined above, a major concern in software licensing, which if not anticipated and addressed, may give rise to IPR problems in software development and exploitation, concerns potential incompatibilities resulting from the introduction and use of software and other works under open source licenses, including those that contain Controlled License Terms. This issue will be examined further in the next section.

5.6.2 License compatibility issues

The issue of license compatibility was outlined in the Deliverable D4.2. As noted there, the license incompatibility may arise at different stages of Project development:

- Downstream licensing: phase of software development. The licensing issues here might arise when software is developed by use of pre-existing programs or components each of which has its own license.

- Upstream licensing: phase of software integration. At this phase standalone software (tools, components, models etc.) of different Parties, each having its own license, are merged into separate exploitable units. The licensing issues by development of the IT Architecture will be considered in WP 5.

- License of the Integrated Platform: exploitation phase. Here license of the Platform shall be compatible with the licenses of the components inside.

At this stage of Project implementation, the key focus will be placed on downstream licensing and licensing issues which arise by the software development with use of the pre-existing programs or components. As regards the upstream licensing license compatibility issues these will be considered as they arise *in concreto* in the light of interaction and combination of components with each other: central questions will concern whether the components, each of which is used under its own license, are used as standalone or whether the source codes of several components are merged into an aggregated whole and whether license compatibility issues arise. The upstream licensing will be analysed when it is known under which licenses the software will be released in CHIC. Licensing issues by integration of the IT Architecture are expressly addressed in WP 5, and will also be looked at so far as required as part of the second iteration Copyright/IPR framework in Deliverable D4.3.2. Lastly, with respect to the license of the integrated platform, it will be pertinent to consider how far it allows for software components, each licensed under separate license, to be hosted on it so that compatibility concerns between the licenses do not arise.

5.6.2.1 Downstream licensing in CHIC

As a result of the follow-up questions addressed to the relevant CHIC partners (Parties) it was established that a majority intend to develop software under the Project by using programs or software components which are already available in the research community. In this regard, separate software components, each licensed under a particular license, like programs, libraries, repositories, etc. are merged. Licenses of the major part of components are open source licenses, like BSD, Apache, Mozilla License, GPL, etc. Some components are licensed under the licenses available in the research community, which also provide for the source code being disclosed.

In some cases, the Parties are at the preparatory stage of software development and in the process of devising the preparatory materials, such as modelling paradigms, methods, mathematical constructs, etc. These Parties have not yet come to the programming phase (writing programs to convert the data into a form executable by a computer) and could not provide data as to the licenses of the programs they are going to use. Similarly, in most cases the Parties have not yet decided under which license they are going to release their software into the Project.

Therefore, the data, as have been collected up to now, for the first iteration framework, should not be regarded as complete, and are likely to be subject to changes. As of now, the following data relating to licensing have been collected by LUH in one-to-one telephone conferences held with the relevant Parties up to and including April 2014:

Software	Party	Components and licenses used	Comments	End license
Software platform for the Assessment of Tumor Response of the Image Processing Toolkit	FORTH	Development on the basis of own experience. Use of MatLab (academical license) for calculations.	MatLab is not used for the source code. No licensing issues.	Open source tbc
Prostate cancer modeling paradigm	UNITO	Development on the basis of own experience. Use of MatLab (academical	MatLab is not used for the source code. No licensing issues.	Open source tbc

		license) for calculations.		
In-silico oncology hyper-models and hyper-modeling infrastructure	ICCS	Development on the basis of own experience with use of pre-existing models.		Object code tbc
IT Architecture, Hyper-modeling infrastructure,	USFD			
VPH-HF tool	USFD/ CINECA	Development on the basis of own experience. VPH-HF components: Physiome space, BSD Taverna, LGPL Tomcat, Apache 2 Apache web server, Apache 2.0 Libraries: MAF 3:BSD like QT LGPL CTK Apache2.0 fervour BSD-like MSVTK BSD-like OpenCV BSD PythonQt Apache2.0 QtSoap BSD QuaZip LGPL qxmlrpc LGPL VTK BSD OpenSSL Apache 2.0	BSD like: copyright license. Redistribution, either in object code or open source and commercial use allowed, redistributions must retain the copyright notice and disclaimer. CTK/ Python Qt/OpenSSL: Apache 2.0: copyright license. Redistribution open source and commercial use allowed, changes must be documented and redistributions must retain the copyright notice and disclaimer. Qt/QuaZip/Qxmlrpc/ LGPL: Copyleft license. Strong copyleft for derivative works, weak copyleft for executables. Executables can be licensed either open source or proprietary, Distribution of library along with the executable must be under LGPL, Section 6.	Open source tbc
Modeling, colon cancer modeling paradigm	UOXF	Development on the basis of own experience. Current software versions are licensed under LGPL and BSD.	Stage of preparatory design work (modeling paradigms).	Open source tbc
RICORDO	UCL	Development on the basis of own experience. RICORDO: Mozilla Public License v.2[122]	RICORDO/Mozilla Public License v.2: copyleft license: distribution in source and object code, aggregation into combined works and license of the combined works under another license, also GPLx, allowed, unless incompatible. Source code is governed under the Mozilla License and must be made available with each distribution royalty free. RICORDO is supposed to be used as a standalone component. The copyleft shall not come in force. Use and integration in CHIC will be under the Mozilla license v.2.	Mozilla Public License v.2.
Modeling, nephroblastoma model, models of other tumor types	UPENN	Development anew or via use of preexisting models. GROMACS: LGPL[123] VMD:UIUC (BSD like)[124] NAMD:UIUC (BSD like)	GROMACS/LGPL: Copyleft license. Strong copyleft for derivative works, weak copyleft for executables. Executables can be licensed either open source or proprietary, Distribution of library along with the executable must be under LGPL, Section 6.Pymol/ASL: license for academic institutions for internal use on site only.	Open source, tbc.

---

[122] http://opensource.org/licenses/MPL-2.0.

[123] http://www.ks.uiuc.edu/Research/vmd/plugins/pluginlicense.html.

[124] Ibid.

| | | Pymol: Academic Software License[125]

Svmlight: tbc.

Modeller: Modeller License[126].

Autodock: Apache 2.0[127] | Modification, distribution alone or integrated into other software requires another license.

If Pymol is used as a tool for writing software, no licensing issues appear.

If Pymol must be used and transferred in CHIC, such use requires academic or commercial license (commercial use/commercial entity).

Modeller/AL: license for internal non-commercial research without the right to transfer. Non-commercial means (a) is not undertaken for profit, or (b) is not intended to produce works, services, or data for commercial use, or (c) is neither conducted, nor funded, by a person or an entity engaged in the commercial use, application or exploitation of similar works. Redistribution and transfer of program and improvements requires written consent of the licensor.

If Modeller is used as a tool for writing software, no licensing issues appear.

If Modeller must be used or transferred to CHIC, its use is not covered by the license and would require written permission of the licensor.

The licensee is obliged to supply copy of improvements to the licensor under a royalty free worldwide, perpetual license, with the right to sublicense (at any tier).

Autodock/Apache v2.: copyright license. Modification, redistribution open source and commercial use allowed, changes must be documented and redistributions must retain the copyright notice and disclaimer.

VMD, NAMD/BSD: copyright license. Redistribution open source and commercial use allowed, redistributions must retain the copyright notice and disclaimer. | |

As noted, the license list provided above does not provide a complete overview of all the licenses that will be involved in CHIC, but is based upon information available at the current stage of the Project. Later, other components and programs and licenses might be added. However, as of now, only the implications which relate to the use of the above licenses are analyzed.

5.6.3 Licenses overview and license implications for CHIC

The precise effect of the above licenses in relation to the programs or components inside software to which they apply, will depend on the way the component is used. Two modes of use can be distinguished: end-use as a tool for writing the software for CHIC and use of the component as combined or integrated into the software. End-use of the component will have no licensing implications. On the other hand, integration of the component inside the software may give rise to licensing issues.

The acts of running a program and acts associated with the end-use (such as copying in the memory of computer) of a program under the intended purpose come within the end use and are subject to the end-use license. Use of a program under the intended purpose of use,

---

[125] https://rostlab.org/owiki/index.php/Academic_Software_License_Agreement

[126] http://salilab.org/modeller/registration.html

[127] http://vina.scripps.edu/LICENSE

such as a tool for modelling and/ or as a tool, when the source code is written, (e.g. use of MatLab for making calculations), shall come within the scope of end-use and end-use license. End use of such programs will have no license implications, unless the program created in the result is considered as a derivative. Consideration of a program as a derivative and license implications may come into question when, for instance, a program needs to interact with a tool in order to run, or contains parts of its source code incorporated into it, or when a tool and a program are incorporated into one product, etc.

In this regard, if the program is deployed inside of the software, or a component of it needs to interact with the software or software components in order for the software to run, then such use may pose licensing issues. The licensing issues would vary, depending, first, upon the technical way how the component is used (linking method), its functionality and interaction with the software, location and distribution, license, etc. The licenses, listed above, can be divided into three main groups: academic licenses, permissive copyright licenses and copyleft copyright licenses. The implications for CHIC in turn will vary:

5.6.3.1 Academic licenses

Into the group of academic licenses fall the Modeller License, applicable to the component Modeller, and Academic Research License, applicable to Pymol. Both components are used by UPENN. These licenses are end-use academic licenses, and apply to academic non-profit institutions for non-commercial end-user research on site only. Modification and distribution are allowed within the scope of end use for research only; any other modifications and distributions of copies and derivatives require license (academic or commercial ARL) or subject to written permission of the licensor (Modeller). The licenses are non-transferable and without the right to sublicense.

Use of these components as tools for writing software should have no license implications. When the components must be used in CHIC either by other Parties or as being integrated into the software, then the like use would require separate authorisation of the licensor: either academic or commercial license for Pymol or written permission of the licensor for the Modeller. It is presumed that the components licensed under these licenses are used as tools by modelling and will have no licensing implications for CHIC. These issues, how the components are used by software development, shall be clarified by UPENN.

5.6.3.2 Permissive copyright licenses

Another major group of license, used for components in CHIC, make the so called permissive or non-restrictive copyright licenses[128]. Into this group fall the BSD[129] and BSD like licenses, e.g. VTK license, MIT, Apache v2. These licenses permit redistribution and use in source and binary forms, with or without modification, either royalty free or commercial, either stand alone or combined, provided copyright notices and disclaimer are attached. Apart from that, some licenses (BSD-3-clause, Apache v.2) forbid use of the authors´ names for promotion purposes. Components under Apache v.2 license may be licensed open source and proprietary, provided the terms of the Apache License are complied with, changes must be documented, and copyright notices and copy of the license attached. Use of the components under Apache license v.2 along with GPL components may cause license incompatibility issues, in particular GPL v2 and GPL v3. "*Apache 2 software can … be included in GPLv3 projects. However, GPLv3 software cannot be included in Apache projects. …The FSF has never considered the Apache License to be compatible with GPL version 2*"[130]. The issue is relevant for software, which combines Apache with the GPL v2/ GPL v3 components, what has not been recorded by now. Release of such software under a particular license shall be analysed.

---

[128] Rowland, supra, p. 415.

[129129] http://opensource.org/licenses/BSD-2-Clause.

http://www.vtk.org/VTK/project/license.html.

[130] http://www.apache.org/licenses/GPL-compatibility.html.

For the CHIC Project in the development stage, this means that the components under these licenses can be combined or aggregated with other components, also proprietary, in any form or on any medium, or/and can also be used as standalone components and may be licensed on proprietary and non-commercial open source basis, either for research and commercial purposes. Although these licenses should not cause adverse compatibility implications, either in relation to downstream or upstream licensing, the license terms for the respective components must be observed.

As the data above show, most of components used by the Parties by software development are released under permissive copyright licenses. In this context, most Parties, which are willing to release their software open source, have indicated that they are going to use the BSD like licenses for contributing the software into CHIC. Provided both the components inside the software and the software as a whole are contributed under BSD like licenses, use of such components and software in CHIC will have no licensing issues by upstream licensing, either for other software or license of the Integrated Platform, either by Project development and exploitation, both on commercial and non-commercial basis. Terms of the respective licenses for the respective component must be observed.

5.6.3.3 Copyleft licenses

The group of copyleft licenses may cause major licensing considerations both by downstream and upstream licensing. According to the data collected by LUH up until now, two licenses fall under this category: the Mozilla Public License v.2, applicable for RICORDO infrastructure, developed by UCL, and the LGPL, applicable to several components used by software development by a number of Parties.

The first license concerned is the Mozilla Public License v.2. Under the Mozilla License v.2 the RICORDO Infrastructure has been released originally, as developed by UCL under another project. As UCL has indicated, it intends to introduce the RICORDO into CHIC under the Mozilla License v.2 as well.

i.   Mozilla Public License v.2

The Mozilla License v.2[131] allows the licensee to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit the software, either on an unmodified basis, with modifications, or combined as part of a larger work. Here, the source code of the covered software is governed and must be distributed under the terms of Mozilla license, meaning that it shall be licensed royalty-free, recipients shall be informed about the license terms, have access to the source code and have the same rights. For the CHIC Project in its development stage this means that the other Parties will have access to the source code of RICORDO, as might be necessary for interoperability purposes, and will have the rights and source code to be able to perform their tasks under the Project, without additional Access Rights required.

Further, the Mozilla License v.2 permits the covered software to be combined with any other software and the distribution of the combined work under any license. The covered software and its source code are still governed under the Mozilla License v.2. The Mozilla License v.2 permits combination of the covered software with software licensed under GPLx and, unless incompatibility by reason of Mozilla prior versions or other reasons arises, the combined software may be distributed under the GPLx license. The recipient shall have an option to distribute the covered software either under the Mozilla License or the respective GPLx license.

For CHIC, both at the development stage and at exploitation, it follows that the RICORDO Infrastructure may be combined with the other software and be integrated into the platform. Hereby, the RICORDO source code will still remain subject to the terms of the Mozilla License v.2, whereas the combined software or platform as a whole may be licensed under

---

[131] http://opensource.org/licenses/MPL-2.0.

another license, also GPLx, if possible and applicable. As partner UCL indicated, RICORDO is proposed to be used in CHIC as a standalone component. Hence, RICORDO as a standalone will be used and distributed in CHIC under the Mozilla License v.2 governing its source code. RICORDO may be released either compiled or in source code and the other Parties will have the rights and will have access to the source code to be able to perform their tasks. The other components interacting with RICORDO and the platform as such might be distributed under their own licenses.

ii. LGPL license

LGPL represents another category of copyleft licenses, the so called GPLx licenses, which, as a rule, provide for stringent copyleft rules and give regard to technological factors concerned, such as: dependency, interaction, distribution medium, volume of storage, etc. As the information collected by LUH on downstream licensing above shows, a number of components the partners plan to use in software development are licensed under LGPL license, in most cases version 2. The effects of using the LGPL v2 will be subject to further legal analysis in part 5.6.4.1 below.

5.6.4 Derivative works and linking

In considering license compatibility it is essential to determine whether software in the interplay of the components constitutes a derivative work. The notion of a derivative work was previously considered in part 5.2, and is controversial both in legal practice and within the software development community. In practice, the term is controversially discussed, and defined differently by different forms of license, thereby giving rise to legal uncertainty and litigation risks[132].

The GPL license came up with its own interpretation of derivative works, as understood in the context of software development with due regard given to the underlying technical parameters. According to the said license, *a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".)*[133].

Here, considering that software are almost always developed on top of other software, in determining whether a particular program makes a derivative work from the used former one, such parameters, as modification, dependency, interaction, distribution medium and location will be relevant, as assessed by the FSF.[134]. With regard to software that communicates with other software through interfaces (usually in form of libraries) further GPL licenses tailored to libraries have appeared, and also in versions LGPL v2 and LGPL v3[135].

GPLx licenses, in general, extend the copyleft effect not only to the derivative works as modified works in general understanding, but also to the combined and aggregate works based on the Program depending on such factors, as: interdependency, medium of distribution, volume of storage. Where, however, the GPLx licensee includes into the strong copyleft effect modified and combined works based on the Program, irrespective of the linking criteria, the LGPL license has strong copyleft for modified works and weak copyleft for the executables. The LGPL license, on the other hand, removes the executables from the strong copyleft effect. *The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library*[136].

---

[132] Dreier/Vogel, Software- und Computerrecht, 2008, S. 211.

[133] GPL v.2, para 0.

[134] https://www.gnu.org/licenses/gpl-faq.html.

[135] https://www.gnu.org/licenses/licenses.en.html.

[136] LGPL v2, Preamble.

For its part, the Apache License v.2, one of the most popular OS licenses and recorded to be used in the Project, also takes technological factors into account when dealing with derivative works, such as linking, interdependence, interfaces. Apache License v.2 defines a derivative work as *any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.*[137]

Against this backdrop, a general approach in deciding whether a given interplay between coded components produces a derivative work, will require the assessment of a number of discrete factors. These include the type of software at issue and method of its development, the manner in which the pre-existing component is used within the software development, the license attached to the component, and the ultimate recognisability of the component as a distinct feature in the generated software. Other factors that may also be of decisive relevance in determining when software constitutes a derivative include the distribution medium, volume of storage, and method of linking (either 'dynamic linking', where the software calls the object code from the library of the component in question, or 'static linking', where the source codes are merged).

5.6.4.1 Implication of LGPL license for CHIC

As noted above, a number of components the partners plan to use in software development are licensed under LGPL. The LGPL license *applies to some specially designated software packages--typically libraries*,[138] and may also be chosen to license other works, typically software, as well. The peculiarity of the LGPL license is that, it removes a category of executables linked with the LGPL program (referred to as Library) from the strong copyleft effect, allows linking proprietary software with a free library and provides more lax criteria for distribution of the executables. LGPL v.2 Section 6 provides: "*you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications*"[139].

Based on this permission, executables linked with the library may be distributed either open source and on proprietary basis at discretion of the developer. Where distribution of the executable based on the Library may be done under the license terms at choice of the developer, the distribution of the Library (modified version) itself is still subject to LGPL. These terms for distribution of executables, linked with the Library are set out in Section 6 of the license, including the requirement that each distribution of the work includes a notice that the Library is used in it, and that the Library and its use are covered by the LGPL. In such a case, a copy of the license must also be provided. [140]

However, in such a case it may make a difference whether the linking to the library is done by static or dynamic linking. Static linking occurs when a program is linked to the LGPL component (library) in such a way that a copy of object files that hold the functions and data referenced in the program are incorporated into the executable at link time. Due to the copying involved, the terms of distribution of executables laid down in Section 6 definitely apply to executables connected to the Library via static linking. In relation to the CHIC Project, this means that where the CHIC executable uses the LGPL library via static linking (files with the functions from the LGPL component library are copied into its source code at link time), then distribution of the executable may be done under the license at choice of the developer with additional terms for the Library, as set out in Section 6 LGPL.

---

[137] Apache License v.2, para 1. http://opensource.org/licenses/Apache-2.0
[138] LGPL v 2, Preamble.
[139] http://www.gnu.org/licenses/lgpl-2.1.html.
[140] Ibid.

By contrast, where dynamically linked executables are used, additional criteria and technical parameters arise, which are laid down in Section 5 LGPL. Dynamic linking differs from the static linking in a way that the files with the functions from the library are not literally copied into the source code of the executable, but are mapped by the machine via virtual address space. Such linking is performed via shared libraries which contain functions and data, referenced by an executable. The dynamic linking is carried out by the link editor which stores the name of the library and data about the symbols referenced by the executable (undefined symbols). At run time the dynamic linker maps the shared library into the virtual address space of the process image of the executable and resolves by name the symbols in the shared library used by the executable.[141]

Here the most significant potential implication, according to Section 5 is that w*hen a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.* The threshold for this to be true is not precisely defined by law. However, if such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. The same is true for any executables containing that work, whether or not they are linked directly with the Library itself[142].

When the LGPL licensed library is modified, its distribution is subject to the LGPL terms, as laid down in Section 2,[143] and follow the main principles *and* freedoms of the free software foundation. It should be noted, that only software libraries may constitute derivative works under LGPL[144]. Hereby, if the LGPL component inside a software is a modified library and if the components are interactive and interdependent with each other, then following the extended copyleft logic of the LGPL license (Section 2), the whole software, including other software components in it, distributed as an integrated product shall be subject to LGPL or GPL other versions. By contrast, the mere location of components near each other, without any interaction in place, would not produce a copyleft effect.

The above effect is limited to distributions where the new code and the original library code are distributed as one product. If, instead, a developer creates code that alters the performance of a GPL product, but distributes that code as "separate works", the separate distribution is not covered by GPL, even if, when blended together in a user's system, the GPL and new code form an integrated whole[145].

To conclude, it may be noted that the LGPL license has weak copyleft and allows linking proprietary programs and applications to LGPL libraries and distribution of the executables under the license at choice of the developer, provided the distribution terms for the library, specified in Section 6, are met. The exception criteria for dynamically linked executables are rather strict, therefore, a legal advice for distributing both dynamically and statically linked executables would be to comply with the distribution terms set out in Section 6 LGPL (i.e. subject distribution of the LGPL library to its own terms).

5.6.5 Other potential license incompatibility issues

Apart from compatibility of licenses inside the software and between the programs, libraries and software, license incompatibility issues might also arise, when by software development languages or databases released under own licenses are used. As the data provided by the

---

[141] http://l4u-00.jinr.ru/usoft/WWW/www_debian.org/Documentation/elf/node6.html.

[143] http://www.gnu.org/licenses/lgpl-2.1.html.
[144] Section 2 para a) LGPL; Andrew M.St.Laurent, Understanding open source and free software licensing, 2004, p. 53.
[145] Nimmer, supra, p. 58.

Parties engaged in the software development for CHIC show, some software are written in Python, a programming language distributed under its own license.

All Python releases are Open Source, and´most, but not all, have also been GPL-compatible. The table below summarizes the various releases:[146]

Release	Derived from	Year	Owner	GPL compatible?
0.9.0 thru 1.2	n/a	1991-1995	CWI	Yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	Yes
1.6	1.5.2	2000	CNRI	No
2.0	1.6	2000	BeOpen.com	No
1.6.1	1.6	2001	CNRI	No
2.1	2.0+1.6.1	2001	PSF	No
2.0.1	2.0+1.6.1	2001	PSF	Yes
2.1.1	2.1+2.0.1	2001	PSF	Yes
2.1.2	2.1.1	2002	PSF	Yes
2.1.3	2.1.2	2002	PSF	Yes
2.2 and above	2.1.1	2001-now	PSF	Yes

The same may apply when databases, repositories (or to be precise, the software which underlies their operation) or API (software libraries) to such are written using a special programming language, such as Java, Python, C++. Release of such software, databases, APIs, etc. should be managed in a way, that license incompatibility issues between a given software and a programming language, in which it was written, do not arise.

As of the current stage of Project development and information available as of now, the data in place are not sufficient to allow making of legal assertions concerning licensing issues and license compatibility, either in respect of downstream or upstream licensing. Therefore, at the stage of software development, the licensing issues and technical parameters in place will need to be addressed in more detail. As the above analysis shows, though, when dealing with the license compatibility issue legal and technical criteria are important and should be considered at an early stage. To ensure that licenses of the components and programs, used inside the CHIC components, are compatible with each other and the license of the CHIC component as such, factors or software development and use of the former components should be clarified.

In this regard, the most important factors will include the nature of the software and method of development (anew or with use of pre-existing components), the manner in which the pre-existing component is used, interaction of the components within software, method of linking (static or dynamic), the applicable license attached to the component, the function of the component in the potential software, etc.). In order to achieve clarity on these matters, a questionnaire dealing with licensing issues will be compiled and circulated among the

---

[146] https://docs.python.org/2/license.html.

Parties. On the basis of the collected data, a further legal analysis will then be undertaken in Deliverable D4.3.2 in good time to ensure an effective resolution of the highlighted issues.

6. Conclusion

As could be seen from the previous chapters, various factors have been considered in developing this data protection and IPR framework. Most importantly, the complex nature of the requirements for processing sensitive health data under the European legal regime has made it imperative to have a workable solution where researchers could have freedom to process the data for achieving the purposes of the CHIC project, without being under significant administrative burdens imposed by EU data protection law. As explained earlier, the uniqueness of the project indicates that complete technical anonymisation may not provide a solution at every point because, at least for ethical reasons, there should be the possibility to contact the data subjects in the event that research findings could influence their treatment. Accordingly, this framework aims at ensuring the highest level of data protection while maintaining this flexibility. In this approach, a safety net has been devised using strong technical, organisational and legal measures to ensure that data is processed within a context of anonymity during the infrastructure development phase. These measures are meant to ensure an appropriate level of security of the data processing, taking into account the state of the art and the costs of their implementation relative to the risks inherent in the processing and the nature of the data to be protected.

The contractual obligations in the annexed agreements to this deliverable highlight the commitments of the parties to look after the data appropriately, use it as strictly required for achieving the purposes of the project, not disclose it beyond the project, and not to try and re-identify it. Similarly, appropriate organisational measures augmented with technical security measures as described in part 4.4 above, shall be maintained against unauthorised or unlawful processing of the CHIC data by all the CHIC-participants processing data. However, in the project service phase, a new model of service level agreement will be put in place, which will be open to a larger user network. In this regard, the external user who will upload data into the CHIC infrastructure will be regarded as the data controller, and be responsible for obtaining the consent of the data subjects or any other approval that may be required in that case. The CHIC service provider in this scenario will be regarded as a processor.

As regards the IPR issues in the project, it is pertinent to note that the CA and EC Grant Agreement have provided a basis for resolution of some of the issues. In chapter five, a concrete analysis of the nature of rights likely to be generated in the foregrounds of the project and how to protect them has been presented. Furthermore, an IPR memorandum which seeks to bridge residual gaps in the substantive CA has been drafted for the partners' consideration. It is intended that a second iteration phase of this framework due in M42 will cater for any putative issues encountered during this development phase of the project.

7. References

[1] Art 29 WP, Opinion 03/13 on Purpose Limitation (00569/13/ENWP203), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[2] Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), 1994.

[3] BGH, Urteil vom 09.05.1985 - I ZR 52/83, BGHZ 94, 276 – 292.

[4] BGH, Judgment of *23. 10. 2001, Case X ZR 72/98 - Wetterführungspläne II, GRUR 2002, 149.*

[5] Bundesgesetz gegen den unlauteren Wettbewerb 1984 - UWG, available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002665.

[6] BGH, Judgment of 09.05.1985, GRUR 1985.

[7] Berne Convention for the Protection of Literary and Artistic Works, 1971 as amended.

[8] CHIC Deliverable D7.10.

[9] CHIC Hyper-modelling glossary.

[10] CHIC Description of Work.

[11] CHIC Consortium Agreement.

[12] CHIC Deliverable D4.2.

[13] Code of Civil Code of Germany, as promulgated on 5 December 2005 (Bundesgesetzblatt (BGBl. Federal Law Gazette) I page 3202; 2006 I page 431; 2007 I page 1781), last amended by Article 1 of the Act dated 31 August 2013 (Federal Law Gazette I page 3533); available at: http://www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html.

[14] Directive 2009/24/EC on the legal protection of computer programs (Software Directive).

[15] Directive 96/9/EC on the legal protection of databases (Database Directive).

[16] Dreier/Vogel, Software- und Computerrecht, 2008, S. 211.

[17] Diedrich, K., Nutzungsrechte für Systemsicherungen nach §69dURhG, CR 2/2012.

[18] ECJ, Judgment of 22 December 2010, Case C-393/09 *Bezpečnostní softwarová asociace v Ministerstvo kultury.*

[19] ECJ, Judgment of 02.05.2012, Case C- C 406/10 *SAS Institute Inc. v World Programming Ltd*.

[20] ECJ, Judgment of 16.07.2009, *Infopaq International A/S v Danske Dagblades Forening*.

[21] Enriquiez L.A., "Dynamic Linked Libraries": Paradigms of the GPL license in contemporary software.

[22] European Commission –Grant Agreement.

[23] European Commission press release IP/13/1176   28/11/2013 on the proposed rules to help protect against the theft of confidential business information.

[24] German Copyright Act of 9 September 1965 (Federal Law Gazette Part I, p. 1273), as last amended by Article 8 of the Act of 1 October 2013 (Federal Law Gazette Part I, p. 3714), http://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html.

[25] Lovells, H., Report on Trade Secrets for the European Commission, Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D, available at: http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.html.

[26] Laurent, A., *Understanding open source and free software licensing*, 2004.

[27] LG München, Judgment of 16.01.97, 7 O 15354/91 - Software-Entwicklung.

[28] LG Stuttgart, Order of 02.07.1990, NJW 1991,441,442.

[29] IPR Helpdesk, Joint Ownership in Intellectual Property Rights, available at: http://www.kowi.de/Portaldata/2/Resources/FP6/ipr_joint_ownership.pdf.

[30] Klaus, L., Intellectual Property Rights in Computer Programs in the USA and Germany, 2006.

[31] Model provisions on the protection of computer software - 1978 - WIPO Publication No 814(E) – Geneva.

[32] Nimmer, R.T., "Legal issues in open source and free software distribution", in Nimmer, R.T, *The Law of Computer Technology* (1997, 2005 Supp.).

[33] OLG Köln, Judgment of 30.07.1997, CR 1998, 199.

[34] Paris Convention for the Protection of Industrial Property, 1883.

[35] Reed, C. and Angel, J., *Computer Law*, Sixth Edition, Oxford University Press, 2007.

[36] The HSCIC guidance, from 2013, at: http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf.

[37] The Act Against Unfair Competition of Germany, available at: http://www.gesetze-im-internet.de/englisch_uwg/.

[38] U.K. Copyright Act, CDPA 1988.

[39] UK Biobank's Ethics and Governance Framework (v.3), at: https://www.ukbiobank.ac.uk/wp-content/uploads/2011/05/EGF20082.pdf?phpMyAdmin=trmKQIYdjjnQIgJ%2CfAzikMhEnx6.

[40] WIPO expert group on legal protection of computer software, LPCS/I/2, 30.09.1979.

Websites

[41] http://php.net/.
[42] http://www.zend.com/en/.
[43] http://www.php.net/license/3_01.txt
[44] http://www.ebi.ac.uk/about/terms-of-use
[45] http://rcsb.org/pdb/static.do?p=general_information/about_pdb/policies
[46] http://www.ncbi.nlm.nih.gov/About/disclaimer.html

[47]   https://dbgap.ncbi.nlm.nih.gov/aa/wga.cgi?page=DUC&view_pdf&stacc=phs0

[48]   http://opensource.org/licenses/LGPL-2.1

[49]   http://opensource.org/licenses/MPL-2.0

[50]   http://www.ks.uiuc.edu/Research/vmd/plugins/pluginlicense.html

[51]   https://rostlab.org/owiki/index.php/Academic_Software_License_Agreement

[52]   http://salilab.org/modeller/registration.html

[53]   http://vina.scripps.edu/LICENSE

[54]   http://opensource.org/licenses/BSD-2-Clause

[55]   http://www.vtk.org/VTK/project/license.html

[56]   http://www.apache.org/licenses/GPL-compatibility.html

[57]   http://opensource.org/licenses/MPL-2.0

[58]   GPL v.2, http://www.gnu.org/licenses/gpl-2.0.html

[59]   https://www.gnu.org/licenses/gpl-faq.html.

[60]   https://www.gnu.org/licenses/licenses.en.html

[61]   LGPL v2, https://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

[62]   Apache License v.2, http://opensource.org/licenses/Apache-2.0

[63]   http://www.gnu.org/licenses/lgpl-2.1.html

[64]   http://www.gnu.org/licenses/lgpl-2.1.html

[65]   http://l4u-00.jinr.ru/usoft/WWW/www_debian.org/Documentation/elf/node6.html

[66]   https://docs.python.org/2/license.html

[67]   http://www.truecrypt.org/

[68]   http://www.institute.nhs.uk/images//documents/Freedom_of_information/Class_5/Password%20 Policy.pdf

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

Appendix 1 – Abbreviations and acronyms

CA   Consortium Agreement

CHIC   Computational Horizon in Cancer

CATS   Custodix Anonymisation Tool Services

CDP   Center for Data Protection

DoW   Description of Work

EC   European Commission

ECJ   European Court of Justice

GPL   General Public License

GBM   Glioblastoma Multiforme

HSCIC   Health and Social Care Information Centre

IAM   Identity and Access Management

IdP   Identity Provider

IPR   Intellectual Property Rights

ICT   Information and Communication Technology

LGPL   Library General Public License

NSCLC   Non Small Cell Lung Cancer

PDP   Policy Decision Point

PAP   Policy Administration Point

PEP   Policy Enforcement Point

PIMS   Patient Identity Management System

PIP   Policy Information Point

SAML   Security Assertion Markup Language

STS   Secure Token Service

TTP   Trusted Third Party

TSP   Health and Social Care Information Centre

TRIPS   Agreement on Trade-Related Aspects of Intellectual Property Rights

VHP   Virtual Physiological Human

WIPO   World Intellectual Property Organisation

Appendix 2 – Data Provider Agreement

CHIC Data Provider Agreement

(Version 1.0, March 2014)

between

CHIC Center for Data Protection

Rempart de la Vierge, 5, Namur, Belgium 5000

hereinafter "CDP*"*

and

_____

("CHIC data provider")

_____

(address and country of establishment)

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

Preamble

The Computational Horizons In Cancer (CHIC) project is a EU-financed FP7 project that aims to create an infrastructure for the development of a number of integrative multiscale cancer models and hypermodel oncosimulators. These will be clinically adapted and partly validated, a process which will involve sharing of clinical and genomic data of patients within the project. At the same time, each of the partners recognises as a priority the imperative need to respect the fundamental interests and rights of patients, including the need to preserve the security and privacy of personal data involved in the project.

Therefore the infrastructure of CHIC is embedded in the CHIC Data Protection Framework, which guarantees compliance with current European data protection legislation, primarily by de facto anonymising the patient data. Due to the diverse participation of researchers in the project, it is of high importance to process patient data in compliance with all applicable laws and regulations, including without limitation, privacy and medical secrecy laws applicable to the activities of the parties.

To fulfil the objectives of the project, the data will be de-identified, using secure state of the art pseudonymisation/de-identification tool (eg, CATS), on-site by the respective data providers to the project, before it is subject to a second round of encryption by the Center for Data Protection (CDP) and transferred to secure, access-controlled data repositories within the CHIC infrastructure. The CDP will transfer the original (data provider) code to an independent trusted third party, and the latter alone

will retain the pseudonymisation key (cross table) needed to link the double-encrypted CHIC data set to the initial de-identified data sets provided by the data providers. This shall enable the project's partners to exchange patient data as end users, within a closed community, in which each of the partners is contractually bound to implement all necessary technical and organisational safeguards to protect the data. Pursuant to the CHIC description of work, the CDP operates as the central data controller for the CHIC infrastructure.

This agreement is needed to state the obligations and conditions under which a CHIC data provider will transfer data to the CHIC infrastructure.

Clause 1:   Definitions

For the purposes of this agreement, the terms used in these clauses shall have the same meaning as attributed to them in the General Framework Terms in Annex A to this agreement.

Clause 2:   Scope and responsibility

1.   This agreement sets out the terms and conditions for the transfer of patient data to the CHIC infrastructure by the CHIC clinical partners for the purposes of the project.

2.   The data provider is responsible as data controller for the management of patient data within its organisation/ hospital database, while the CDP is responsible for the data that has been transferred to the CHIC infrastructure.

Clause 3:   Obligations of the CDP

The **CDP** warrants and undertakes:

1.   to have in place appropriate technical and organisational measures to protect patient data within the CHIC infrastructure against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, including by entering the 'CHIC Trusted Third Party Agreement' with the CHIC TTP;

2.   to maintain the transferred data in a strictly de-identified state, protected by secure double encryption as further detailed in Annex A to this agreement, such that it is not reasonably possible either for the CDP or the CHIC end user to re-link the data to the original data subject;

3.   to conclude contracts with the CHIC end users (in the form of the CHIC end user agreement) in order to secure that any authorised CHIC end user which has access to the transferred data respects and maintains the confidentiality and security of the data;

4.   to comply with data protection laws applicable to its operations as well as the conditions set forth in this agreement;

5.   to support the data provider by providing all necessary information and documents that may be needed in case of any request by supervisory authorities.

Clause 4:   Obligations of the data provider

The **data provider** warrants and undertakes:

1.   to transfer to the CHIC infrastructure only data that have been collected and processed in accordance with the laws applicable to the data provider;

2.   that it shall obtain patients' data in accordance with applicable ethical and legal norms, and subject to the valid informed consent of each patient concerned and/or required ethics body approval and/or required notification to data protection authorities before transferring the data to the CHIC infrastructure;

3.   that it shall be fully liable in case of any breach that results from non-compliance with the applicable laws, including national data protection law applicable to the data transfer. Neither the CHIC Consortium nor the CDP will be liable in case of any issues arising from any deficiency in the consent of the patients, or non-notification of relevant national data protection   authorities or local ethics bodies prior to the transfer of the data to the CHIC infrastructure;

4.   to perform a de-identification process on the patient data, by using a state of the art de-identification tool in converting the personal data into de-identified data, so that under no circumstances are personal data transferred to the CDP and/or the CHIC infrastructure. The assessment whether data has been properly de-identified remains with the CDP.

5.   to support the CDP by if necessary performing further de-identification measures as reasonably directed by it, and by providing all necessary information and documents that may be needed in case of any request by supervisory authorities.

Clause 5:   Cooperation with supervisory authorities

1.   The CDP agrees to deposit a copy of this agreement with the supervisory authority if it so requests or if such deposit is required under the applicable regulation.

Clause 6:   Liability and indemnity

1.   Each party shall be liable to the other party for damage it causes by any breach of these clauses. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

the parties promptly notifying each other of a claim; and

each party is given the possibility to cooperate in the defence and settlement of the claim.

2.   The parties agree that each party shall be liable to the patient for damage caused by any wilful or negligent violation by it of data protection legislation or any analogous provisions of national or international law. The enforcement of this clause shall be subject to the finding of wilfulness or negligence by the court under Clause 9 below.

 Clause 7:   Penalty

1.   The parties agree that subject to the exception in clause 7.3 below, a party in wilful or negligent breach of clause 3 or 4 of this agreement shall pay a penalty of 10.000 (ten thousand) EUR. The enforcement of this clause shall be subject to the finding of wilfulness or negligence by the court under Clause 9 below.

2.   The penalty shall be paid to the CHIC Consortium and can be used for specific project purposes which will be determined by the Consortium. A user account approved by the whole CHIC Consortium will be supplied for this purpose.

3.   In the event that the breach or series of breaches does not lead to the identification of any data subject, then provided that the party in breach timeously corrects the breach in accordance with the terms of clause 8.2 below, it shall escape the penalty set out in this clause.

4.   The above provision shall be without prejudice to the parties' right to terminate the contract, to seek compensation for damages or to enforce any claims under this agreement.

Clause 8:   Termination and obligations of the parties after the termination

1.   This agreement will terminate, if not otherwise superseded or amended by new provisions extending it, at the latest by 31st March 2017.

2.   In case of breach of clauses 3 or 4 by one of the parties, the other party is entitled to give written notice requiring the party in breach to be repair the breach within 72 hours, after which time if the breach remains outstanding it may terminate this agreement.

3.   Without prejudice to the foregoing provisions, any party may terminate this agreement for good cause.

4.   Each party must inform the other party in written form in case of termination of the agreement.

Clause 9:   Governing law and Jurisdiction, miscellaneous

1.   This agreement shall be governed by Belgian Law. The courts of Brussels/Belgium shall have exclusive jurisdiction. This shall also apply to disputes on the validity of this clause.

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

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

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

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

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

_____   _____

(Place, Date)   (Signature of Nikolaus Forgó (president of the CDP)

_____   _____

(Place, Date)   (Signature [CHIC data provider])

Annex:

A.   General Framework Terms – (Version1.0 - March 2014)

Annex A

GENERAL FRAMEWORK TERMS

(Version 1.0, March 2014)

The project CHIC (Computational Horizons In Cancer) in this present document, aims at creating and developing models and hypermodels for use in the diagnosis and treatment of cancer. The CHIC project will initially proceed by using data on Wilms tumour, glioblastoma multiforme (GBM), prostate cancer, and non small cell lung cancer (NSCLC), but it is projected to involve further cancer types in the future. The final purpose of such scientific research is to improve cure and management of future cancer patients.

Therefore data repositories will be set up within the CHIC infrastructure to enable the project's partners to share patient data. These repositories will contain patient data transferred to the CHIC infrastructure by the CHIC data providers (participating hospitals/investigators), based on the patients´ informed consent to use their data for research within CHIC and/or the approval of the relevant data provider's responsible ethical board or committee.

The patient data remain under the control of the respective hospital/investigator (data provider) where the data are collected until the data have been transferred to the CHIC infrastructure. Prior to transfer, the data provider is thus obliged to ensure the confidentiality and protection of the data. These obligations are defined by the contractual agreements concluded with the CDP. After transfer the CDP will be responsible for the security of data processing within the CHIC project.

All data transferred to the CHIC infrastructure will be initially deidentified on-site by using a state of the art de-identification tool such as CATS by the data provider concerned; it will then be subject to a second round of encryption by the CDP using dedicated state of the art encryption software, in which the initial data provider's pseudonym is replaced by a second pseudonym. The pseudonymisation key (cross table) needed to relink the double-pseudonymised data set to the initial pseudonymised set will be transferred from the CDP to the CHIC Trusted Third Party (TTP). The CHIC TTP's independence from the CDP, the data providers and end users will be guaranteed. That means that neither the CDP nor the end user using the data will be unable to re-establish a link to the patient to whom the data relates. In addition contracts are concluded between the partners providing data to, and using data within CHIC and the CDP guaranteeing that patient data are not transferred to any party outside the project and no matching of data set takes place in order to identify the patients concerned. In interaction with strong technical and organisational security measures, patient data in CHIC is to be seen as de-facto anonymous. Further, the CDP controls the enforcement of these contractual agreements. It thus serves as a central data protection authority for the CHIC framework.

At the same time, the key held by the CHIC TTP preserves the possibility in exceptional circumstances of re-identifying a given patient, in particular in the event that a new treatment for him/her is developed. This can occur only with the help of the CHIC TTP and with permission of the CDP, and enables physicians at the data provider institution alone (where the patient concerned is treated) to link the data to the original patient where the patient has expressed their wish for this to occur in their own interests. For the avoidance of doubt, insofar as project-goals, such as the need to test or validate the performance of hypermodels later in the project, make it necessary to re-link data in the CHIC infrastructure to real patients, such re-linkage shall not be permitted without the further specific consent of the patients concerned and/or the obtaining of appropriate ethics body approval.

The CHIC data will be stored for a length no longer than the CHIC project. During the whole term of storage it will always be provided that the data remain de-facto anonymous for the CHIC end users. For a longer storage of patient data the explicit informed consent of the patient or ethics approval will be required. The users (researchers) are not allowed to publish the data or to transmit or disclose data received via CHIC to any third person outside of CHIC.

These General Framework Terms are applicable to the CDP (as a legal person), the CHIC TTP, the CHIC data providers and the CHIC end users.

Explanatory Glossary (forming part of the General Framework Terms):

Anonymous data / Rendering anonymous

Rendering data anonymous means to modify personal data in a way that the information concerning personal or material circumstances can no longer be identified, or it is only possible with a disproportionate amount of time, expense and labour to attribute the data to an identified individual. Data that have been anonymised are no longer "personal data" in the legal sense. It will be an aim to have as much anonymised data within CHIC as possible and reasonable. With the technical and organisation measures taken to secure the data, including the present contractual agreement as well as the CHIC End User Agreement, the data processed within the CHIC infrastructure shall be regarded as (de facto) anonymous data only.

Center for Data Protection (CDP)

The CDP shall mean the central data protection authority of the CHIC infrastructure, which agrees to receive from the healthcare organisations/hospitals (data providers) data intended for processing in accordance with the terms of the Data Provider Agreement. The CDP guarantees privacy within the CHIC infrastructure and repositories.

CHIC data

CHIC data means patient data provided in securely deidentified form by the CHIC data provider partners and, following a second round of encryption by the CDP, transferred to the CHIC infrastructure and repositories for access by the CHIC end users, subject to contractual duties of care, for use in accordance with the purposes of the project.

Confidentiality duty

Persons engaged in data processing within the CHIC project shall not, without authorisation, collect or process personal data, nor publish or disclose such data to any third party. On taking up their duties such persons shall be required to give an undertaking to maintain confidentiality, as set out in Annex C of the End User Agreement. This undertaking shall continue to be valid after termination of their activity. Any person acting under the authority of the CDP who has access to CHIC data must not process them except on instructions from the controller, unless he/she is required to do so by law.

Consent

Informed consent means any express indication of data subject´s wishes, expressing his/her agreement to data relating to him/her being processed, provided that he/she has sufficient information about the purposes of the processing, the data or categories of data concerned, the recipient of the data, and the name and address of the controller and of his/her legal representative if any. The consent must be freely given and specific, and may be withdrawn by the subject at any time. If the subject is incapable of a free decision or domestic laws do not permit the subject to act on his/her own behalf, consent is required of the person recognised as legally entitled to act in the interest of the data subject or of an authority or any person or body provided for by law (legal representative).

Data controller

The data controller/controller is, according to the Data Protection Directive 95/46/EC, the natural or legal person who alone, or jointly with others, determines the purposes and means of the processing of personal data. The data controller is liable for the legality of the processing and the fulfilment of the obligations towards the national data protection authority and the patients. The hospitals/investigators participating in the CHIC project (data providers) are data controllers with regard to the collection of Patient Data and their transmission to CHIC, whereas CDP is the data controller with regard to the data stored in the CHIC infrastructure. Finally the CHIC end-users are in the position of data controllers with the obligation to ensure full confidentiality and security of the data they receive from the CHIC infrastructure and repositories.

Data processor

Data processor shall mean a natural or legal person, public authority, agency or any other body which processes patient data on behalf of the controller, such controller being liable for the legality of the processing and the fulfilment of the obligations towards the national data protection authority and the patients.

Data subject

The data subject is the subject of personal data, meaning an identified or identifiable person the data refers to. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. As a rule the patient, whose data are collected and processed for CHIC will be the data subject, when his/her personal data are processed.

Disclosing

Disclosure is a processing operation in which patient data are provided by a controller to a third party. The data controller must only disclose data to third parties if permitted by law or by the data subject´s consent. In CHIC, data are only shared among CHIC end users who have each signed a special agreement that forbids any disclosure of data received via CHIC to any third party.

Hospital

Hospitals are health institutions where patients are treated and their personal data are collected for the purpose of the CHIC project.

Investigator

The legal or natural person who gathers and manages the patient's data from the hospitals, laboratories etc. and maintains and controls the trial/study database.

Legal representative of the patient ("legal representative"):

The legal representative(s) of the patient is/are the person(s) who has/have the power by law or legal decision to decide for a minor patient (or equivalent status such as mentally disabled patients).

Necessary processing

When deciding which data will be collected and further processed, the controller must limit these data to the extent necessary to achieve the purpose of processing. This means that personal data will only be processed when it is necessary for the project.

Patient:

Patient means the person treated in a hospital. Certain data collected in the hospitals will upon the patient´s consent and/or the obtaining of appropriate ethics body approval be transferred to the CHIC infrastructure where they will be used for the purposes of scientific research in (de facto) anonymous form.

Personal data

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Therefore a set of data collected under a certain number or sign "patient xxx", "tissue YYY" can be personal data, if the patient concerned can still be identified by other means than his/her name.

Physician

The physician is the natural person who is in charge of the patient's treatment.

Publish

The controller and the processors will refrain from publishing personal data or otherwise making them public, unless specific consent from the patient concerned is obtained.

Purpose

The purposes for processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The purposes must be specified, explicit and legitimate. Personal data must not be further processed in a way incompatible with those purposes. The purpose for the collection, transfer and use of the data within CHIC is to create cancer models and hypermodels in accordance with the objectives of the project.

Secure Deidentification

To securely deidentify a data set means to employ a state of the art deidentification tool, which replaces the patient's name and other identifying characteristics with a coded label and performs such further appropriate operations (eg, suppressing and/or perturbing other dataset values) in order to preclude re-identification of the patient or to render such re-identification disproportionately difficult.

In CHIC the hospital/investigator acting as data providers will carry out deidentification on-site before sending deidentified patient data to CHIC; the data will then be subject to a further round of encryption by the CDP, prior to transfer to the CHIC infrastructure. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the sensitive data to be protected.

The CHIC TTP alone holds the key necessary to re-link a given coded and deidentified data set with the second coded label (generated by the CDP during secondary encryption), to the original code attached to the data set by the data provider.

Sensitive (personal data)/Special categories of data

Sensitive personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health (including genomic data) or sex life. The processing of sensitive data is only allowed in case of certain exceptions explicitly stated by the national laws of the Member State.

Storage

Storage of personal data is allowed by the Data Protection Directive 95/46/EC. But when the purpose of processing is achieved and the data are not required any more for that particular purpose, personal data must be rendered anonymous or must be destroyed. Most national laws allow personal data to be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics. Nevertheless, some national laws impose supplementary conditions or formalities in order to allow longer storage.

Technical and organisational measures

Organisational measures, together with technical measures, must ensure an appropriate level of security of the data processing, taking into account the state of the art and the costs of their implementation relative to the risks inherent in the processing and the nature of the data to be protected. Appropriate organisational measures shall be taken by the controller against accidental loss, destruction or alteration of, or damage to, personal data and against unauthorised or unlawful processing of personal data in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The controller must, where processing is carried out on his/her behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures. Such appropriate organisational measures to ensure the confidentiality, integrity and accuracy of processed data should include for example:

control of the entrance to installations

control of data media

memory control

control of utilization

access control

control of communication

control of data introduction

control and securing of data transmission

availability control

Such technical and organisational measures have to be taken by all the CHIC-participants processing patient data; other relevant required measures are set out in Annex B of the CHIC End User Agreement.

Third Party

A third party is a natural or legal person, public authority, agency or any other body other than the patient, the controller, the processor or persons who, under the direct authority of the controller or the processor, are authorised to process the data. With regard to CHIC, third parties will be all the other persons and bodies who have no authorisation from the CDP to process the data.

Transfer

Transfer of data means the transmission of CHIC data from one data controller to another.

Trusted Third Party

The role of Trusted Third Party in CHIC is performed by the CHIC TTP, an independent security authority, which has no interest in the content of the processed data and can therefore be trusted by all participants of the CHIC project. The Trusted Third Party will hold the pseudonymisation key (cross table) needed to link the double-encrypted CHIC data set to the initial deidentified data sets provided by the data providers. The involvement of the TTP guarantees that a CHIC data set can only be linked back to the original patient by the data provider institution treating the patient, in the exceptional circumstances defined in these Framework Terms.

Appendix 3 – End User Agreement

CHIC End User Agreement

(Version 1.0, March 2014)

between

the Center for Data Protection ("CDP")

Rempart de la Vierge, 5, Namur, Belgium 5000

hereinafter "CDP"

and

_____

("CHIC end user")

_____
(address and country of establishment)

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

Preamble

The Computational Horizons In Cancer (CHIC) project is a EU-financed FP7 project that aims to create an infrastructure for the development of a number of integrative multiscale cancer models and hypermodel oncosimulators. These will be clinically adapted and partly validated, a process which will involve sharing of clinical and genomic data of patients within the project. At the same time each of the partners recognises as a priority the imperative need to respect the fundamental interests and rights of patients, including the need to preserve the security and privacy of personal data involved in the project.

Therefore the Infrastructure of CHIC is embedded in the CHIC Data Protection Framework, which guarantees compliance with current European data protection legislation, primarily by de facto anonymising the patient data. Due to the diverse participation of researchers in the project, it is of high importance to process patient data in compliance with all applicable laws and regulations, including without limitation, privacy and medical secrecy laws applicable to the activities of the parties.

To fulfil the objectives of the project, the data will be de-identified, using secure state of the art pseudonymisation/de-identification tool (eg, CATS), on-site by the respective data providers to the project, before it is subject to a second round of encryption by the Center for Data Protection (CDP) and transferred to secure, access-controlled data repositories within the CHIC infrastructure. The CDP will transfer the original (data provider) code to an independent trusted third party, and the latter alone will retain the pseudonymisation key (cross table) needed to link the double-encrypted CHIC data set to the initial deidentified data sets provided by the data providers. This shall enable the project's partners to exchange patient data as end users, within a closed community, in which each of the

partners is contractually bound to implement all necessary technical and organisational safeguards to protect the data. Pursuant to the CHIC description of work, the CDP operates as the central data controller for the CHIC infrastructure.

This agreement is needed to state the conditions and obligations under which the CHIC end-users (scientific and technical partners, including modellers and tool developers) will process data within the said infrastructure.

Clause 1:   Definitions

For the purposes of this agreement, the terms used in these clauses shall have the same meaning as attributed to them in the General Framework Terms in Annex A to this agreement.

Clause 2:   Scope and responsibility

1.   This Agreement sets out the terms and conditions for the CHIC technical partners, including modellers and component developers working in the project (end users) to access, use, and share patient data within the CHIC infrastructure.

2.   The CDP is responsible as data controller for the management of the CHIC infrastructure, while the CHIC end user is responsible for the data it accesses and uses from the infrastructure within its own organisation.

Clause 3:   Obligations of the CDP

The **CDP** warrants and undertakes:

1.   to grant to the end user a non-exclusive right to access and use the data in the CHIC data infrastructure (hereinafter the CHIC data) for the purposes of the end user's work within the CHIC project, subject to the provisions of this agreement;

2.   that it is entitled to grant access to the CHIC data to the end user as aforesaid;

3.   to put in place procedures to ensure that prior to transfer to the CHIC infrastructure, CHIC data are collected and processed in accordance with the laws applicable to the data provider, including by entering into the 'CHIC Data Provider Agreement' with relevant data providers;

4.   to have in place appropriate technical and organisational measures to protect patient data within the CHIC infrastructure against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, including by entering the 'CHIC Trusted Third Party Agreement' with the CHIC TTP.

Clause 4:   Obligations of the CHIC end user

The **CHIC end user** warrants and undertakes:

1.   to process the CHIC data in compliance with applicable data protection regulation and the terms of this agreement; and where it cannot provide such compliance for whatever reasons, it agrees to inform promptly the CDP of its inability to comply, in which case the CDP is entitled to suspend access to the data and/or terminate the contract;

2.   to process the CHIC data only for the purposes of its work within the CHIC project;

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

4.   that it will ensure that where CHIC data is stored within its own organisation, such data is technically and organisationally separated from other data;

5.   that it will retain the CHIC data within a secure database or network system at such standard as would be reasonably expected for the storage of sensitive/confidential data;

6.   that it shall not attempt to identify any patient from the CHIC data either by external matching of the data or by any other means;

7.   that it shall not disclose or publish the CHIC data to any third party, which for the avoidance of doubt includes any of its subcontractors or party with which it has an equivalent arrangement, without seeking and obtaining the specific written authorisation of the CDP;

8.   that in the event of inadvertently identifying any patient, it will notify the CDP immediately setting out (in reasonable detail) the circumstances by which this occurred. In such a case it further undertakes not to make any use of the identifying information for any purposes and to take all necessary steps to protect the interests of the patient including so far as possible restoring the de-identified status of the patient;

9.   to ensure that each of its employees who has contact with the CHIC data is made aware of, and will be bound by, the terms of this Agreement, and such an employee will complete Annex C to this Agreement;

10.   to inform the CDP immediately, should the CHIC data, while in the hands of the end user be threatened with seizure or confiscation through bankruptcy or settlement proceedings, or through any other circumstances including the actions of a third party.

11.   that if it becomes aware that it is necessary or desirable, in the exceptional circumstances identified Annex A to this agreement, for the CHIC data to be re-linked to the data subject it shall contact the CDP only, so that the latter can initiate the re-identification process with the help of the Trusted Third Party that holds the key to link the de-identified data sets in respect of the subject concerned;

12.   to deal promptly and properly with all inquiries from the CDP relating to its data processing and data security measures;

13.   that upon reasonable request by the CDP, it will submit its data processing facilities, data files and documentation needed for reviewing, auditing and/or certifying by the CDP (or any independent or impartial inspection agents or auditors, selected by the CDP and not reasonably objected to by the CHIC end user) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The same obligations apply in case a supervisory authority demands auditing;

14.   to provide the CDP with contact details of the person responsible for data protection in its organisation.

Clause 5:   Cooperation with supervisory authorities

1.   The CDP agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable regulation.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the CHIC end user which has the same scope and is subject to the same conditions as would apply to an audit of the CDP under the applicable regulation.

Clause 6:   Liability and indemnity

1.   Each party shall be liable to the other party for damages it causes by any breach of these clauses. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

the parties promptly notifying each other of a claim; and

each party is given the possibility to cooperate in the defence and settlement of the claim.

2.   The parties agree that each party shall be liable for patient's damages it caused by any negligent violation of data protection legislation or any analogous provisions of national or international law.

Clause 7:   Penalty

1.   The parties agree that subject to the exception in clause 7.3 below, a party in wilful or negligent breach of clause 3 or 4 of this agreement shall pay a penalty of 10.000 (ten thousand) EUR. The enforcement of this clause shall be subject to the finding of wilfulness or negligence by the court under Clause 9 below.

2.   The penalty shall be paid to the CHIC Consortium and can be used for specific project purposes which will be determined by the Consortium. A user account approved by the whole CHIC Consortium will be supplied for this purpose.

3.   In the event that the breach or series of breaches does not lead to the identification of any data subject, then provided that the party in breach timeously corrects the breach in accordance with the terms of clause 8.2 below, it shall escape the liability set out in this clause.

4.   The above provision shall be without prejudice to the parties' right to terminate the contract, to seek compensation for damages or to enforce any claims under this agreement.

Clause 8:   Termination and obligations of the parties after the termination

1.   This agreement will terminate, if not otherwise superseded or amended by new provisions extending it, at the latest by 31st March 2017.

2.   In case of breach of clauses 3 or 4 by one of the parties, the other party is entitled to give written notice requiring the party in breach to be repair the breach within 72 hours, after which time if the breach remains outstanding it may terminate this agreement.

3.   Without prejudice to the foregoing provisions, any party may terminate this agreement for good cause, giving the reason for such termination.

4.   Each party shall inform the other party by prior written notice in case of termination of the agreement.

5.   The parties agree that on the termination of the provision of data processing services, the CHIC end user shall, at the choice of the CDP, return all the CHIC data and the copies thereof to the CDP or shall destroy all the data and certify to the CDP that it has done so, unless legislation imposed upon the CHIC end user prevents it from returning or destroying all or part of the data transferred. In all cases, the CHIC end user warrants that it will continue to guarantee the confidentiality of the data and will no longer actively process the data.

Clause 9:   Governing law and Jurisdiction, miscellaneous

1.   This agreement shall be governed by Belgian Law. The courts of Brussels/Belgium shall have exclusive jurisdiction. This shall also apply to disputes on the validity of this clause.

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

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

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

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

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

_____   _____

(Place, Date)   (Signature of Nikolaus Forgó (president of the CDP)

_____   _____

(Place, Date)   (Signature [CHIC end user])

Annex:

A.   General Framework Terms - version 1.0 (March 2014)

B.   Technical and organisational measures

C.   Access authentication form

Annex A (General Framework Terms)

[Identical to Annex A of Data Provider Agreement (see Appendix 2) and omitted here for reasons of space.]

Annex B

Technical and organisational measures

(Version 1.0, March 2014)

The CDP and the CHIC end user will take appropriate technical and organisational measures to protect the CHIC data against misuse and loss, in accordance with European data protection rules, including all necessary and reasonable precautions:

- to prevent unauthorised persons from gaining access to data processing systems with which the data are processed or used (physical access control),

- to prevent data processing systems from being used without authorisation (denial of use control),

- to ensure that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that the data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage (data access control),

- to ensure, including through use of secure encryption, that the data cannot be read, copied, modified or removed without authorisation during electronic transmission, transport or storage and that it is possible to examine and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transmission control),

- to ensure that it is possible retrospectively to examine and establish whether and by whom the data have been inputted into data processing systems, modified or removed (input control),

- to ensure that the data being processed on commission are processed solely in accordance with the directions of the controller (contractual control),

- to ensure that the data are protected against accidental destruction or loss (availability control),

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

Annex C - ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned ……………………….............................., (title) born on the ……………..................., in………………...................... and working on the project called CHIC on behalf of ……………………………….. (name of relevant CHIC partner institution) declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ……………………………….

Date and Place: ……………………………........................

Appendix 4 – Trusted Third Party Agreement

CHIC Trusted Third Party Agreement

(Version 1.0, March 2014)

between

the Center for Data Protection ("CDP")

Rempart de la Vierge, 5, Namur, Belgium 5000

hereinafter "CDP"

and

_____

("CHIC TTP")

_____
(address and country of establishment)

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

Preamble

The Computational Horizons In Cancer (CHIC) project is a EU-financed FP7 project that aims to create an infrastructure for the development of a number of integrative multiscale cancer models and hypermodel oncosimulators. These will be clinically adapted and partly validated, a process which will involve sharing of clinical and genomic data of patients within the project. At the same time each of the partners recognises as a priority the imperative need to respect the fundamental interests and rights of patients, including the need to preserve the security and privacy of personal data involved in the project.

Therefore the Infrastructure of CHIC is embedded in the CHIC Data Protection Framework, which guarantees compliance with current European data protection legislation, primarily by de facto anonymising the patient data. Due to the diverse participation of researchers in the project, it is of high importance to process patient data in compliance with all applicable laws and regulations, including without limitation, privacy and medical secrecy laws applicable to the activities of the parties.

To fulfil the objectives of the project, the data will be de-identified, using secure state of the art pseudonymisation/de-identification tool (eg, CATS), on-site by the respective data providers to the project, before it is subject to a second round of encryption by the Center for Data Protection (CDP) and transferred to secure, access-controlled data repositories within the CHIC infrastructure. The CDP will transfer the original (data provider) code to an independent trusted third party, and the latter alone will retain the pseudonymisation key (cross table) needed to link the double-encrypted CHIC data set to the initial deidentified data sets provided by the data providers. This shall enable the project's partners to exchange patient data as end users, within a closed community, in which each of the partners is contractually bound to implement all necessary technical and organisational safeguards to

protect the data. Pursuant to the CHIC description of work, the CDP operates as the central data controller for the CHIC infrastructure.

This agreement is needed to state the conditions and obligations under which the CHIC TTP shall fulfil its function referred to above.

Clause 1: Definitions

For the purposes of this agreement, the terms used in these clauses shall have the same meaning as attributed to them in the General Framework Terms in Annex A to this agreement.

Clause 2: Scope and responsibility

1. This Agreement sets out the terms and conditions under which the CHIC TTP may securely retain the cross table / pseudonymisation key (hereafter "the key") and assist the CDP in allowing a data provider to re-link CHIC data to a relevant patient subject to the feedback procedure described below.

2. The CDP is responsible as data controller for the management of the CHIC infrastructure, while the CHIC TTP is responsible for the retention and security of the key as aforesaid.

Clause 3: Obligations of the CDP

The **CDP** warrants and undertakes:

1. to grant to the CHIC TTP a right to retain the key, in order that it may fulfil its responsibilities as set out in clause 2 of this agreement;

2. to put in place procedures, including in particular by entering into a contractually binding "CHIC Data Provider Agreement" with each data provider, to ensure that, prior to upload to the CHIC infrastructure, all patient data has been subjected by the provider to a thorough and secure de-identification process.

Clause 4: Obligations of the CHIC TTP

The **CHIC TTP** warrants and undertakes:

1. to retain the key in a secure manner, protected by state of the art access security, and to deploy the said key only in the strict circumstances set out in the present Clause;

2. that it shall not disclose the key to any third party, which for the avoidance of doubt includes any of its subcontractors or party with which it has an equivalent arrangement, without seeking and obtaining the specific written authorisation of the CDP;

3. that except as specifically provided for in clause 4.5 below, it shall take no measures that may conduce by any means to the re-identification of the patients who are subjects of the codes contained in the cross table making up the key;

4. that if it is contacted by any CHIC data end user that, through analyzing the CHIC data, has acquired information of potential importance to the original patient subject, and which requests it to deploy the key to enable re-linking of the CHIC data to the patient in question, it shall refer the request to the CDP;

5.   that only if so instructed by the CDP, it shall take the steps in this sub-clause to comply with the request: first it will ask the end user for the code attached to the data set following the second round of encryption; second it will deploy its key in order to discover the original code attached by data provider; third it will notify the CDP of the original code so that the CDP can alert the data provider where the patient is treated that there is new information pertaining to the patient. In this case, the responsible physicians may if the patient has signalled a desire to be informed, identify and contact the patient;

6.   to ensure that each of its employees who has contact with the key is made aware of, and will be bound by, the terms of this Agreement, and such an employee will complete Annex B to this Agreement; .

7.   to deal promptly and properly with all inquiries from the CDP relating to its data security measures and faithfully follow the instructions of the CDP;

Clause 5:   Cooperation with supervisory authorities

1.   The CDP agrees to deposit a copy of this agreement with the supervisory authority if it so requests or if such deposit is required under the applicable regulation.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the CHIC TTP which has the same scope and is subject to the same conditions as would apply to an audit of the CDP under the applicable regulation.

Clause 6:   Liability and indemnity

1.   Each party shall be liable to the other party for damages it causes by any breach of these clauses. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

the parties promptly notifying each other of a claim; and

each party is given the possibility to cooperate in the defence and settlement of the claim.

2.   The parties agree that each party shall be liable for patient's damages it caused by any negligent violation of data protection legislation or any analogous provisions of national or international law.

Clause 7:   Termination and obligations of the parties after the termination

1.   This agreement will terminate, if not otherwise superseded or amended by new provisions extending it, at the latest by 31st March 2017.

2.   In case of breach of clauses 3 or 4 by one of the parties, the other party is entitled to give written notice requiring the party in breach to be repair the breach within 72 hours, after which time if the breach remains outstanding it may terminate this agreement.

3.   Without prejudice to the foregoing provisions, any party may terminate this agreement for good cause, giving the reason for such termination.

4.   Each party shall inform the other party by prior written notice in case of termination of the agreement.

5.   The parties agree that on the termination of the provision of data processing services, the CHIC TTP shall destroy the key and certify to the CDP that it has done so, unless legislation imposed

upon the CHIC TTP prevents it from so doing. In all cases, the CHIC TTP warrants that it will continue to guarantee the security and confidentiality of the key.

Clause 8:   Governing law and Jurisdiction, miscellaneous

1.   This agreement shall be governed by Belgian Law. The courts of Brussels/Belgium shall have exclusive jurisdiction. This shall also apply to disputes on the validity of this clause.

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

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

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

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

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

_____   _____

(Place, Date)   (Signature of Nikolaus Forgó (president of the CDP)

_____   _____

(Place, Date)   (Signature [CHIC TTP])

Annex:

A.   General Framework Terms - version 1.0 (March 2014)

B.   Access authentication form

Annex A (General Framework Terms)

[Identical to Annex A of Data Provider Agreement above and omitted here for reasons of space.]

Annex B

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned …………………………............................, (title) born on the …………….................., in……………….................... and working for the p-medicine TTP declare by this Access Authentication form, I am authorised to have access to the p-medicine pseudonymisation key.

I have read, I understand and I agree to observe the conditions as stated in the p-medicine Trusted Third Party agreement (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ……………………………….

Date and Place: ……………………………........................

Appendix 5 – CHIC model IPR Memorandum of Understanding

In supplement to the Consortium Agreement, version 4 of January 18, 2013

Memorandum of Understanding on disposal of Intellectual Property Rights in CHIC ('CHIC IPR memorandum')

(Version 1.0 as of May 2014)

Between the Parties to the Consortium Agreement, version 4 of January 18, 2013, as identified in the Consortium Agreement

relating to the Project entitled

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

Preamble:

WHEREAS, given the importance of safeguarding against the possible loss of economical and scientific interest of the Project research and development as a consequence of sharing creativity, and in course of fulfillment the tasks in course of Project implementation the Parties have identified that certain practical scenarios in place are not always fully covered by the default rules set out in the fp7 GA (Annex II) and provisions of the CA;

WHEREAS, the Parties accordingly believe that further augmentation or clarification of the default rules set out in the fp7 GA (Annex II) and provisions of the CA may be desirable, the Parties wish to provide and agree on the rules which shall govern the exercise and disposal of Intellectual Property Rights (IPRs) in the Project;

WHEREAS, pursuant to Article 11.4 of the Consortium Agreement, amendments and modifications to the text thereof, unless explicitly listed in Article 6.3.1.2 require a separate agreement between all Parties;

In supplementation to the provisions laid down in Grant Agreement and the Consortium Agreement, the Parties conclude this Memorandum on disposal of Intellectual Property Rights in CHIC as follows:

1.   Section 1: Definitions

1.1.   Definitions

For the purposes of this Memorandum, the terms beginning with a capital letter shall have the meaning, as defined in Article 1.1 of the   Consortium Agreement.

1.2.   Additional definitions

In addition to Article 9.8.1 of the Consortium Agreement, the Parties define the "software preparatory design materials" as follows:

"Software preparatory design materials" mean materials produced in various stages of software development which are capable of leading to the reproduction or the subsequent creation of the Software and are covered with the software rights, in particular: problem description, description of method, description of the main stages of the software execution and steps to be taken in execution of the stages.

2.   Section 2. Responsibilities of Parties

2.1.   Involvement of third parties

In addition to the obligations set out in Article 4.3 of the Consortium Agreement, each Party, which enters into a subcontract or otherwise involves third parties (including but not limited to Affiliates) in

the Project, shall procure the rights on use of the contributions made by such third parties into the Project (either by an assignment or license of the rights with the right to sublicense executed in writing) and provide for the scope of rights as sufficient for the performance of tasks assigned to the commissioning Party and other Parties under the Project and for the grant of Access Rights, either for Implementation and/or for Use, to the other Parties as well.

Where, in fulfillment of a task assigned to it under the Project, a Party commissions the development of Software from one or more third parties, it shall procure the rights in the Software contributed by those third parties in the scope as needed for the Project Implementation and for Use of the Foreground by the commissioning Party and other Parties to the Project. In particular, the commissioning Party shall have the rights in the Software in the required scope, as laid down in Articles 9.8.3 and 9.8.4 of the Consortium Agreement with the right to sub-license to the other Parties and to the end-users and shall be able to provide access to the Source Code pursuant to Article 9.8.3 of the Consortium Agreement (either by the license or an escrow agreement).

Other provisions of the Consortium Agreement relating to involvement of third parties into the Project and responsibility of each Party for supervision of its Subcontractors remain in full effect.

3.   Section 3: Foreground

3.1.   Employee´s rights

Supplemental to the obligations set out in Article 8.5 of the Consortium Agreement, each Party shall designate the employees which are engaged in the work under the Project, provide instructions on their duties under the Project and make them familiar with the provisions on Non-disclosure of information, as set out in Section 10 of the Consortium Agreement.

Each Party shall ensure that it holds the rights in the works created by its employees under the Project, either by operation of law or by contract, to the full scope and extent as is required for the Project Implementation and for Use of its own Foreground and for Use of the Foreground by the other Parties as well.

3.2.   Joint Ownership

Pursuant to obligations set out in Article 8.2 of the Consortium Agreement, the Joint Owners shall agree the license(s) under which they will release the Foreground into the Project and ensure that the components and programs used inside the Foreground are used in such a way that no compatibility issues arise either as between the licenses of the components and programs with each other or with the license of the Foreground as a whole.

3.3.   Composite Ownership

Pursuant to Article 8.2 of the Consortium Agreement, the Parties agree as follows:

If the work generating particular Foreground is carried out by or on behalf of more than one Party and if the contributions to or features of such Foreground are separately identifiable, but are inter-dependent, or if a number of contributions, constituting separate and independent works in themselves are assembled into a collective whole which constitutes such Foreground, then all patents and other registered IPRs issued thereon, and any other copyrights and IPRs protecting such Foreground, shall be jointly owned by the Parties as Joint Owners.

Ownership in the Foreground, generated pursuant to the above paragraph, shall be without prejudice to and not affect in any way ownership in the separate contributions collected in it.

The other provisions laid down in Article 8.2 of the Consortium Agreement shall continue to apply as before.

The Joint Owners shall agree the license(s) under which they will release the Foreground into the Project and ensure that the components and programs used inside the Foreground are used in a way

that no compatibility issues between the licenses of the components and programs with each other and with the license of the Foreground as a whole appear.

4. Access Rights

4.1. Inability to grant Access Rights due to third parties rights

Supplemental to the obligations set out in Article 9.2.2 of the Consortium Agreement when a Party considers that it is unable because of third parties rights to grant Access Rights to the other Parties, or that there might be a limitation to the granting of Access Rights or any other restriction which might substantially affect the granting of Access Rights, such Party shall enter its objection to granting the Access Rights concerned in Attachment 3 to this Memorandum.

The Parties agree and understand that one or more items listed in Attachment 3 may still be used to develop the Foreground of a Party and that Access Rights to such Foreground shall be subject to the terms and conditions of the respective right holder.

4.2. Access Rights for Use

In supplementation to the terms of Article 9.4 of the Consortium Agreement, the Parties agree that Access Rights to Foreground for Use shall be granted pursuant to the procedure, as laid down in Article 9.4.2 of the Consortium Agreement.

If pursuant to Article 9.2.6 of the Consortium Agreement the Granting Party makes the grant of Access Rights conditional on the acceptance of specific conditions, the Parties shall agree the terms on granting of the Access Rights most adequate to the rights and interests of the Parties concerned.

5. Access Rights to Software

5.1. Access to Software

In addition to Article 9.8.3 of the Consortium Agreement, the Parties who are willing, when granting the Access Rights to Software, to grant Access to the Source Code and/or who introduce open source Software, which is not subject to Controlled License Terms, pursuant to Article 9.8.6 of the Consortium Agreement, may do so by entering such Software into Attachment 2 to this Memorandum.

5.2. Access Rights for Implementation

Supplemental to the terms of Article 9.3 of the Consortium Agreement the Parties agree that the Access Rights to Software which is Background or Foreground for Implementation shall cover the right to use the Software in all modes and means as Needed for performance of the tasks assigned to the recipient Party under the Project, including but not limited to the right of the permanent or temporary reproduction of Software by any means and in any form, in part or in whole, such as by loading, displaying, running, transmission or storage; the translation, adaptation, arrangement and any other alteration of the Software and the reproduction of the results thereof, making available to the public, and other modes of Software use, as Needed for the Project Implementation.

5.3. Foreground – Rights to grant sublicenses to end-users

Supplemental to the terms of Article 9.8.4.1.2 of the Consortium Agreement, the Parties agree that a sub-license to the end-users shall include the right to use the Object Code for making a back up copy and error correction to the extent technically necessary for use of the Software in accordance with its intended purpose.

5.4. Foreground – Access to the Source Code to the end-users

In addition to and pursuant to Article 9.8.4.2.2 of the Consortium Agreement, a Party which, upon request from another Party, grants Access Rights to Source Code which is Foreground for Use may make such grant conditional upon proof by the Requesting Party that without access to the Source Code, adaptation, error correction, maintenance and/or support of the Software by the end-user would

be technically impossible. Access to the Source Code for the end-user shall be provided to the extent, technically necessary.

5.5. Open source Software

In addition to the obligations set out in Article 9.8.6 paragraph (i) of the Consortium Agreement, each Party shall ensure that the components and programs used inside the Software or Work which it introduces into the Project are used in such a way that no compatibility issues between the licenses of the components and programs with each other or with the license of the Software or Work as a whole arise.

6. Miscellaneous

6.1. Attachments, inconsistencies and severability

This Memorandum consists of this core text together with:

Attachment 1 (Request for Access Rights)

Attachment 2-A (List of Software with Access to Source Code granted for Access Rights)

Attachment 2-B (List of Software open source, not subject to Controlled License Terms)

Attachment 3 (Access Rights impaired by the third parties rights)

Attachment 4 (Request for approval on use of Software/Works under Controlled License Terms).

In case the terms of this Memorandum are in direct conflict with the terms of the Consortium Agreement or EC-GA, the terms of the latter shall prevail. In case of conflicts between the attachments and the core text of this Memorandum, the latter shall prevail.

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

This Memorandum is subject to the provisions of the Consortium Agreement and EC-GA. To the situations, rights and obligations of the Parties, which are not provided for in this Agreement, the provisions laid down in the Consortium Agreement shall apply respectively.

7. Signatures of the Parties

....

....

....

....

CHIC IPR memorandum_Attachment 1

To the Agreement on disposal of Intellectual Property Rights in CHIC

Contents of requests for Access Rights pursuant to Article 9.2.6 of the Consortium Agreement

Each Request for Access Rights shall include, as a minimum, the following:

1. Full name of the Requesting Party, as identified in the Consortium Agreement.

2. Full name of the Granting Party, to which the request for Access Rights is made, as identified in the Consortium Agreement.

3. The identity of the Foreground or Background requested, including name, version number, etc.

4. Reasons why Access Rights are needed:

    4.1. Access Rights for Implementation: specification of tasks assigned to the Requesting Party in the Project the performance of which without Access Rights would be impossible, significantly delayed or require significant additional financial or human resources;

    4.2. Access Rights for Use of the Foreground: specification of the Requesting Party´s Foreground the use of which without the Access Rights would be technically or legally impossible;

5. Additionally for request of Access Rights to the Software:

    5.1. Scope of Access :

        5.1.1. Object Code;

        5.1.2. Object Code and API, if API is required for use of the Object Code;

        5.1.3. Source Code: reasons, why execution of the tasks of the Requesting Party under the Project or Use of its own Foreground would be technically or legally impossible without access to the Source Code (with attachment of supporting materials, e.g. technical parameters, etc.); extent of the Source Code requested.

    5.2. Scope and modes of use to which the Software will be put.

    5.3. Rights to use of the Software as requested.

    5.4. Rights to sub-license, if requested, with indication of reasons and potential sub-licensees (e.g. end-users).

    5.5. An acknowledgement to comply with the software license terms.

6. An acknowledgement to comply with the terms under which the Access Rights will be granted.

7. Request to grant Access Rights.

8. Date, place, signature of the representative of the Requesting Party.

CHIC IPR memorandum_Attachment 2-A

List of Software in respect of which the Parties in addition to as provided for under the terms of Article 9.8.3 of the Consortium Agreement are willing and agree, when granting the Access Rights, to grant Access to the Source Code

CHIC IPR memorandum_Attachment 2-A

CHIC IPR memorandum_Attachment 2-B

List of Software which pursuant to Article 9.8.6 of the Consortium Agreement is introduced into the Project under open source licenses, not subject to the Controlled License Terms

CHIC IPR memorandum_Attachment 3

List of Access Rights which pursuant to Article 9.2.2 of the Consortium Agreement a Party is unable because of third parties tights to grant Access Rights to the other Parties or when, if granted, the exercise of Access Rights by the other Parties would be substantially impaired by the terms subject to the third parties rights

CHIC IPR memorandum_Attachment 4

Required contents of Requests for approval relating to Software and Works subject to Controlled License Terms pursuant to Article 9.8.6 Paragraph (iii) of the Consortium Agreement

   i.   Official name of the Party, proposing use of the Software/Work subject to Controlled License Terms;

   ii.   Identity of the Software/Work concerned, including name, version number;

   iii.   Copy of the license terms, including the Controlled License Terms under which the Software/Work is licensed by the right holder (author, contributor, source, right holder, etc.);

   iv.   The identity and contact coordinates of the author (contributor, source, etc.);

   v.   Description of the intended purpose and functions of the Software/Work;

   vi.   Reasons why use of the Software/Work would contribute to achieving the goals of the Project;

   vii.   List of alternative Software/Works considered alternative to the proposed Software/Work;

   viii.   Reasons why the contributing Party believes that use of the proposed Software/Work would contribute to achieving the goal of the Project better than any other alternative Software/Works;

   ix.   Use, modes and scope of use of the Software/Work in the Project;

   x.   Request to approve the use of the proposed Software/Work in accordance with the stated license terms and within the scope of use, as specified in paragraph viii);

   xi.   Request to approve that Access Rights to the Software/Work includes the right to sublicense the Software/Work upon Controlled License Terms; or

   xii.   Acknowledgement by the proposing Party that Access Rights to the Software/Work includes the right to sublicense the Software/Work upon Controlled License Terms;

   xiii.   Acknowledgement by the proposing Party, if the other Parties agree to approve the use of the proposed Software/Work in accordance with the stated license terms and the scope of use, specified in paragraph viii), such Software/Work may only be used only in accordance with the license terms and within the scope of use, as specified in paragraph viii);

   xiv.   Date, place and signature of the proposing Party.

Appendix 6 – Ethics Committee Approval obtained by KU Leuven in respect of provision to the CHIC project of additional glioblastoma image data

FACULTEIT GENEESKUNDE
COMMISSIE VOOR MEDISCHE ETHIEK/KLINISCH ONDERZOEK
U.Z. GASTHUISBERG E330
HERESTRAAT 49
3000 LEUVEN (BELGIUM)

KATHOLIEKE
UNIVERSITEIT
LEUVEN

Prof. S. Van Gool
Kindergeneeskunde - UZ Leuven

ONS KENMERK: ML6285 (BD-nr 3 dd. 17 maart 2014)
LEUVEN: 14 april 2014

A phase IIb prospective placebo-controlled double blind randomized clinical trial for the treatment of patients with newly diagnosed glioblastoma multiforme with tumor vaccination as "add-on therapy" to standard primary treatment.HGG-2010.

Eudract: 2009-018228-14
StudieReferentie: S52111

AMENDEMENT/BIJKOMENDE STUDIEDOCUMENTEN

DEFINITIEF GUNSTIG ADVIES

Geachte collega,

De Commissie Medische Ethiek van de Universitaire Ziekenhuizen KU Leuven heeft vermeld protocol initieel goedgekeurd op 1 maart 2010.

Met betrekking tot vermeld protocol werden bijkomende documenten ingediend bij de Commissie Medische Ethiek van de Universitaire Ziekenhuizen KU Leuven.

Bij het beoordelen van dit amendement werd rekening gehouden met alle aan dit amendement gerelateerde documenten die ingediend werden op 19 maart 2014.

Het amendement werd goedgekeurd op 7 april 2014.

Dit gunstig advies betreft o.m.:

- Amendement op Protocol
    Nederlandstalige samenvatting versie 4 20140317
    HGG-2010 protocol versie 4 20140317

De Commissie bevestigt dat ze werkt in overeenstemming met de ICH-GCP principes (International Conference on Harmonization Guidelines on Good Clinical Practice) en met de geldende wetten en regelgeving.

De Commissie bevestigt dat in geval van belangenconflict, de betrokken leden niet deelnemen aan de besluitvorming omtrent het amendement.

SECRETARIAAT: Tel. +32-16 34 86 00   Fax. +32-16 34 86 01   ec@uzleuven.be   www.uzleuven.be/ec

Vervolg blz. 2 van het advies voor Amendement mbt. ML6285

ONS KENMERK: ML6285
LEUVEN: 14 april 2014

Een ledenlijst wordt bijgevoegd.

De opdrachtgever is verantwoordelijk voor de conformiteit van de anderstalige documenten met de Nederlandstalige documenten.

Aandachtspunten: (indien van toepassing)

Indien er een Clinical Trial Agreement is, kan de studie in ons centrum pas aangevat worden wanneer dit Clinical Trial Agreement goedgekeurd en ondertekend is door de gedelegeerd bestuurder van UZ Leuven.

Studies met geneesmiddelen en sommige studies met "medische hulpmiddelen" dienen door de opdrachtgever aangemeld te worden bij het FAGG.
Studies met geneesmiddelen mogen slechts aanvangen op voorwaarde dat de minister (FAGG) geen bezwaren heeft kenbaar gemaakt binnen de wettelijke termijnen zoals beschreven in art.13 van de Belgische wet van 7/5/2004 inzake experimenten op de menselijke persoon.
Voor bepaalde studies met medische hulpmiddelen gelden eveneens wettelijke termijnen (zie KB van 17/3/2009).
Voor meer informatie hieromtrent verwijzen we naar de website van het FAGG www.fagg-afmps.be.

Onderzoek op embryo's in vitro valt onder de wet van 11 mei 2003. Voor dergelijk onderzoek is er naast een positief advies van het Ethisch Comité ook een goedkeuring van de Federale Commissie voor medisch en wetenschappelijk onderzoek op embryo's in vitro noodzakelijk vooraleer dit onderzoeksproject kan doorgaan.

Gelieve ook rekening te houden met de regelgeving van het ziekenhuis betreffende weefselbeheer en met de beschikkingen van de wet van 19 december 2008.

Dit gunstig advies van de Commissie houdt niet in dat zij de verantwoordelijkheid voor de geplande studie op zich neemt. U blijft hiervoor dus zelf verantwoordelijk. Bovendien dient U er over te waken dat uw mening als betrokken onderzoeker wordt weergegeven in publicaties, rapporten voor de overheid enz., die het resultaat zijn van dit onderzoek.

U wordt eraan herinnerd dat bij klinische studies iedere door U waargenomen ernstige verwikkeling onmiddellijk zowel aan de opdrachtgever (desgevallend de producent) als aan de commissie medische ethiek moet worden gemeld, ook al is het oorzakelijke verband met de studie onduidelijk.

Indien de studie niet binnen het jaar beëindigd is, vereist de ICH-GCP dat een jaarlijks vorderingsrapport aan de commissie wordt bezorgd.
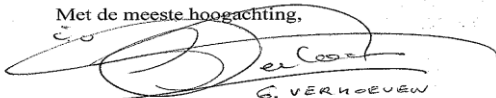
Tenslotte verzoeken wij U ons mee te delen indien een studie niet wordt aangevat, of wanneer ze wordt afgesloten of vroegtijdig onderbroken (met opgave van eventuele reden). Gelieve het (al dan niet vroegtijdig) stopzetten van een studie binnen de door de wet vastgelegde termijnen mee te delen en een Clinical Study Report aan de Commissie te bezorgen.

| SECRETARIAAT: | Tel. +32-16 34 86 00 | Fax. +32-16 34 86 01 | ec@uzleuven.be | www.uzleuven.be/ec |

Vervolg blz. 3 van het advies voor Amendement mbt. ML6285

ONS KENMERK: ML6285
LEUVEN: 14 april 2014

Met de meeste hoogachting,

G. VERHOEVEN

Prof. dr. W. Van den Bogaert
Voorzitter Commissie Medische Ethiek van de UZ KU Leuven

Cc. aan:
FAGG (Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten) - Departement R&D;
Victor Hortaplein 40, bus 40 1060 Brussel
UZ Leuven - Gasthuisberg - Clinical Trial Center
UZ Leuven - Neurochirurgie

SECRETARIAAT: Tel. +32-16 34 86 00   Fax. +32-16 34 86 01   ec@uzleuven.be   www.uzleuven.be/ec

Appendix 7 – TrueCrypt Tutorial: Create an encrypted volume

This tutorial instructs on how to use TrueCrypt to create an encrypted volume.

1. If not already installed, download and install TrueCrypt (www.truecrypt.org).

2. If not already launched, launch TrueCrypt (TrueCrype.exe)

3. You should now see the TrueCrypt main window on screen.
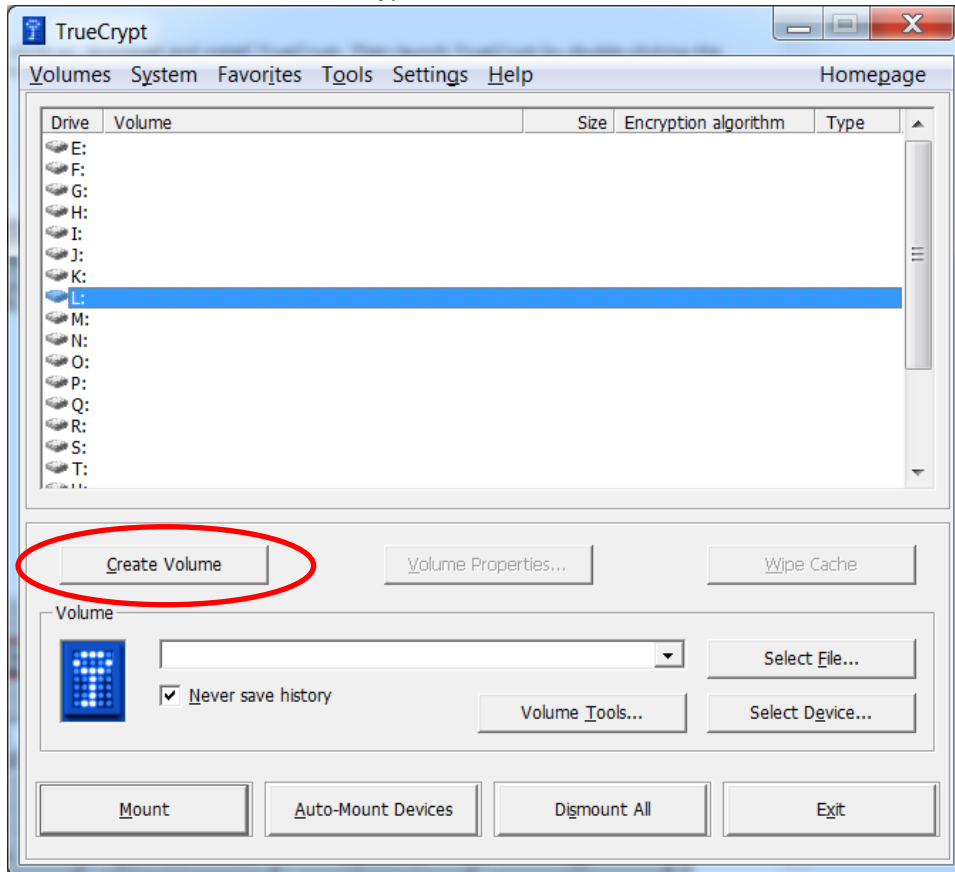
To start a new TrueCrypt volume, click on „Create Volume".

4. The „Truecrypt Volume Creation Wizard" should now be visible.
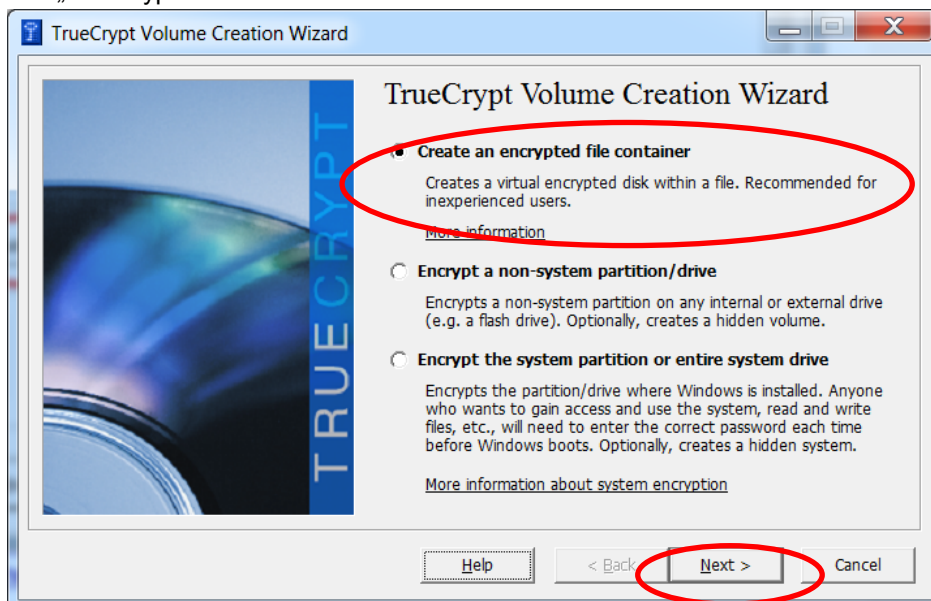
The type of TrueCrypt volume you wish to create should now be choosen. You can either create a virtual volume within a file (encrypted file container), create an encrypted non-system partition on any internal or external drive or encrypt the whole system partition or drive.

In this tutorial with wish to create an encrypted file container. Click on „Next" to go on.

5. You can either create a standard or hidden volume. Please select „Standard TrueCrypt Volume" and click on „Next" to go on.
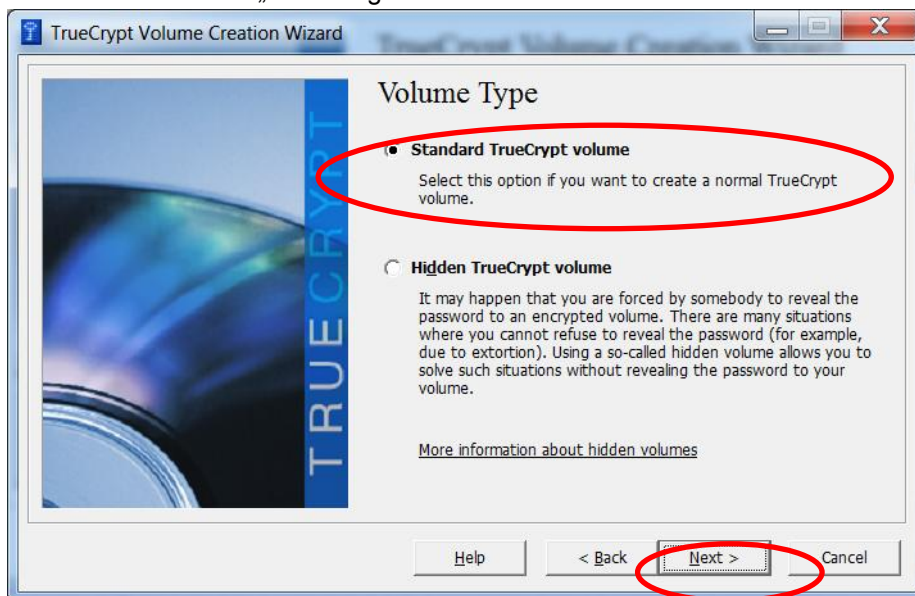
6. Next you should select where the TrueCrypt Volume (which is just a normal file) should be created.
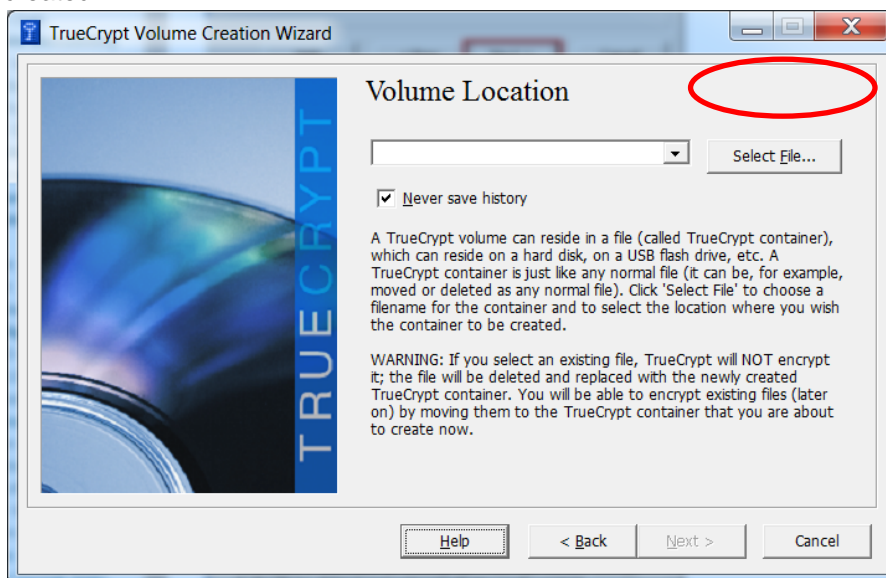
Open through „Select File" the OS File Wizard through which you can choose where the encrypted file container should be created.
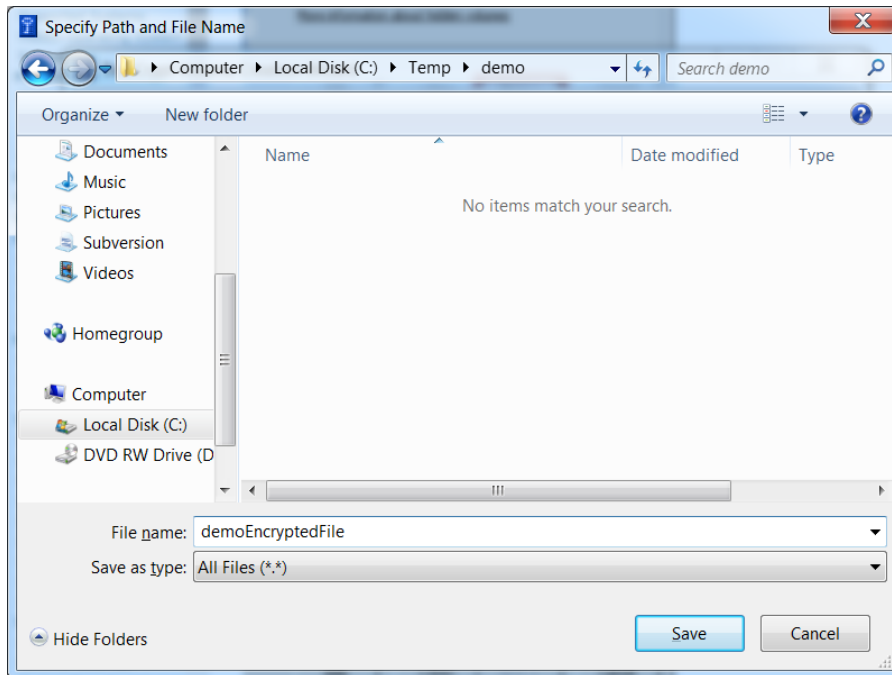
TrueCrypt will not encrypt exising files. If the provided file already exists it will be overriden.
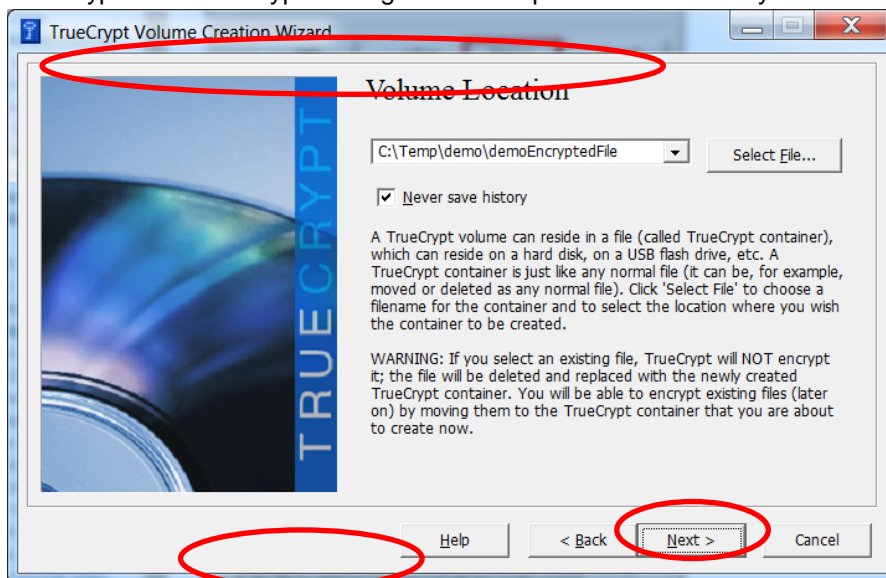
Click on „Next" to finalise the file selection.

7. The „Encryption Options" are now rendered. Choose „AES" as encryption algorithm and „SHA-512" as hash algorithm.
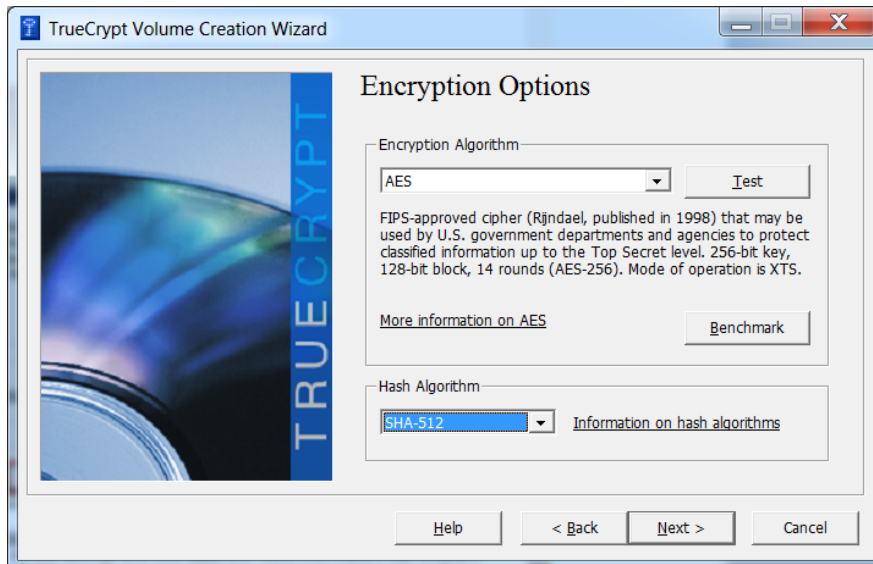
Click „Next" to confirm and continue;

8. Here you can choose the container size, for this demo we will create one that can contain 100MB. Click „Next" to continue.
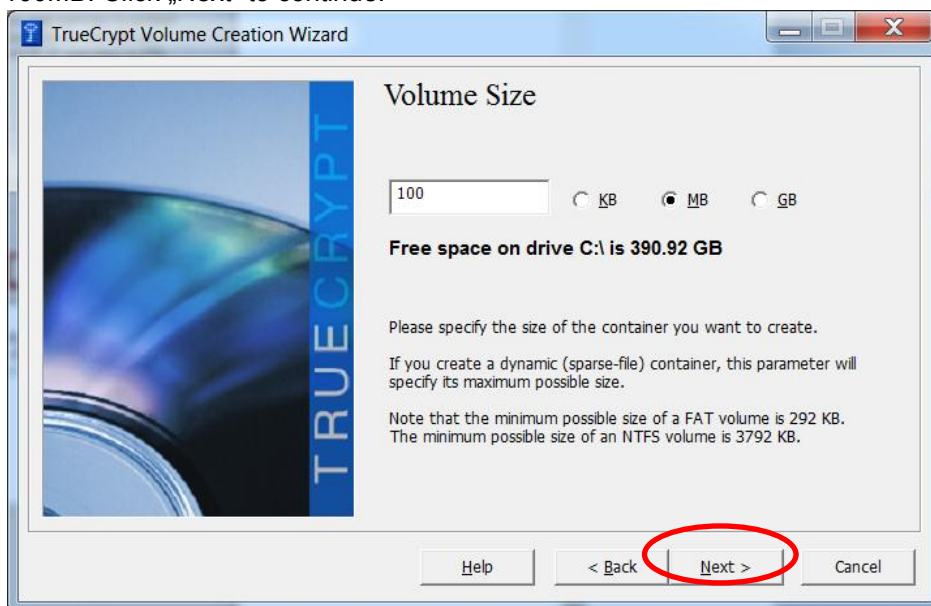
9. Next you should choose your encryption password. Please choose a strong random password containing at least 20 characters. The better the password the more secure the encryption. Click „Next" to continue.
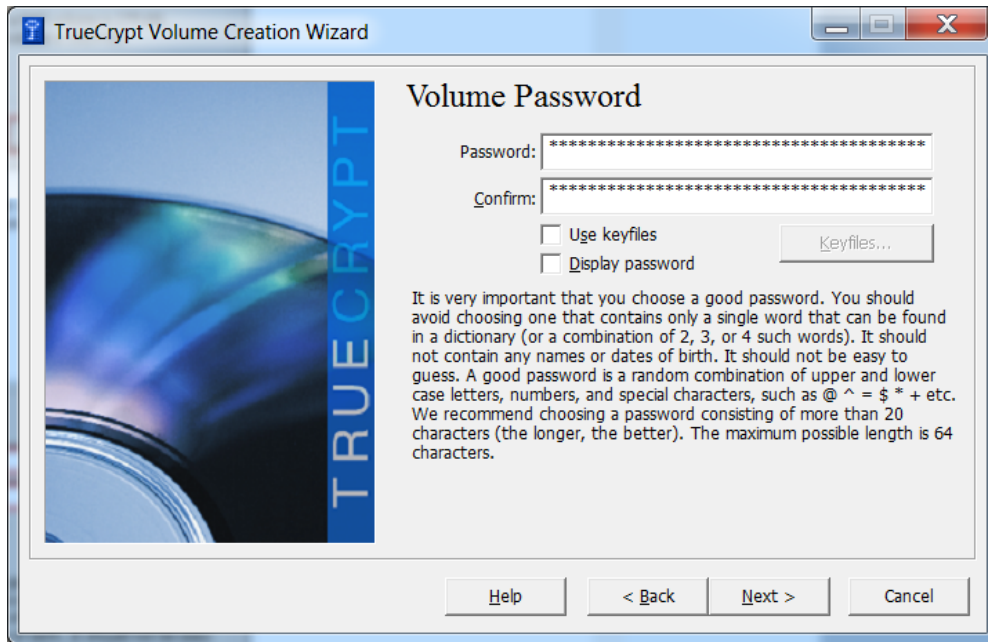
10. Move your mouse around for at least 30 seconds to generate a random seed and click on "Format". This will initiatie the volume creation.
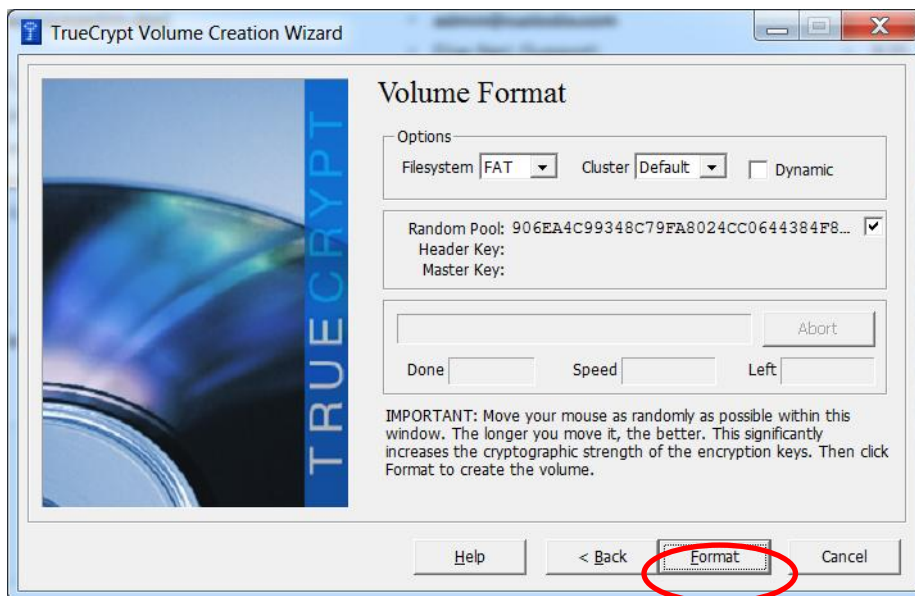
11. Once volume creation completed a success popup will be rendered.
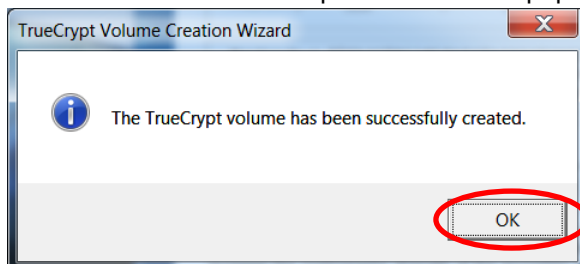
You can then click on „OK" in dialog and „Exit" in the Wizard.
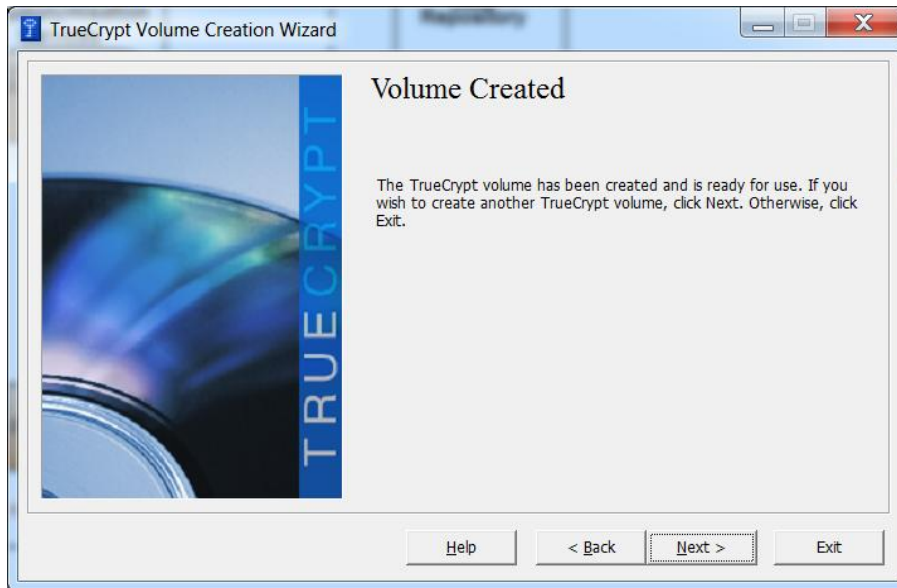
Now you are ready to use the encrypted volume. Appendix 8 explains how an existing encrypted volume can be mounted and used.

Appendix 8 - TrueCrypt Tutorial: Use an encrypted volume

This tutorial instructs on how to use TrueCrypt to create an encrypted volume.

1. If not already installed, download and install TrueCrypt (www.truecrypt.org).

2. If not already launched, launch TrueCrypt (TrueCrype.exe)

3. You should now see the TrueCrypt main window on screen.
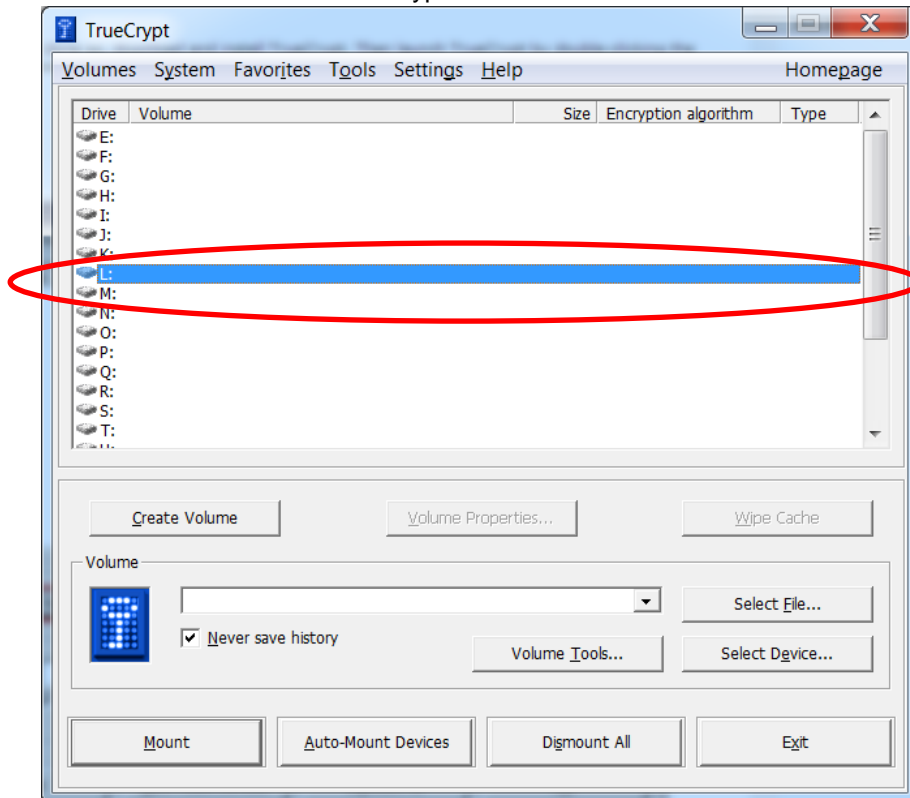
First you should choose the drive letter to which the TrueCrypt container should be mounted.

4. Next you should select the encrypted file container to be mounted through „Select File" and the OS File Wizard that pops up.
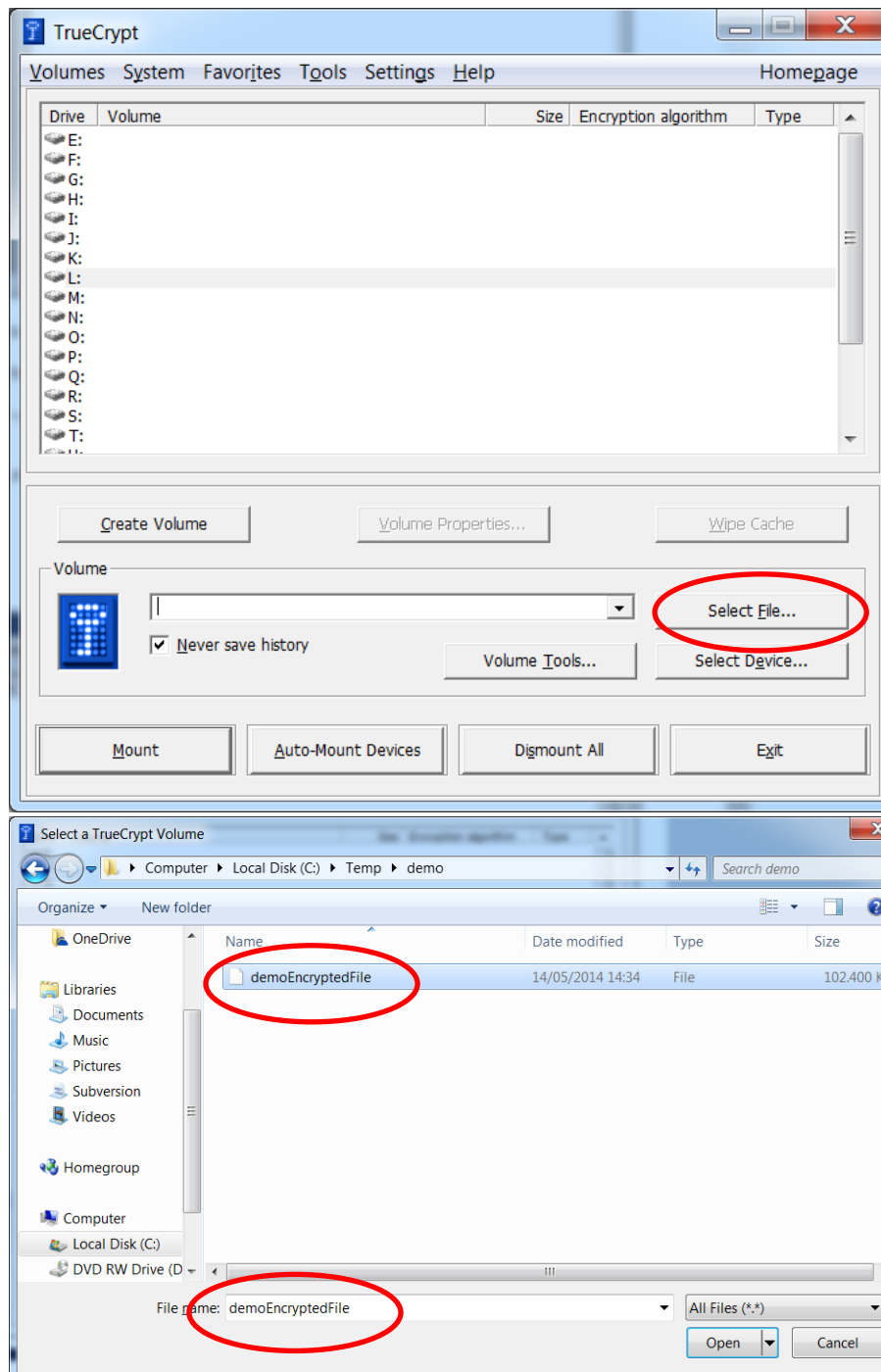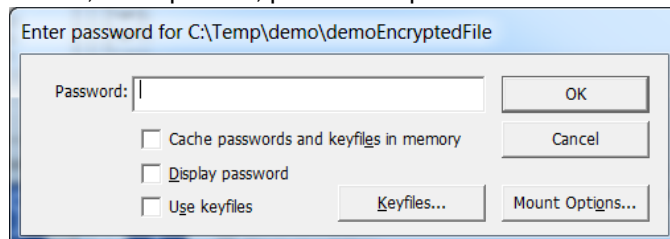
Click „Open" in the file wizard to select a given file and then on „Mount" in the main window to
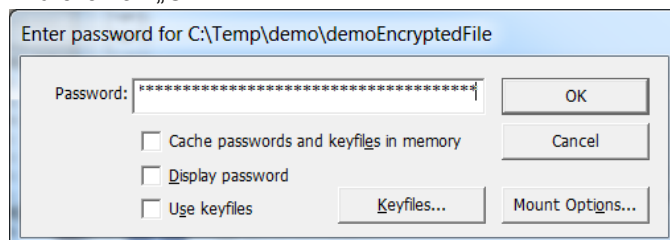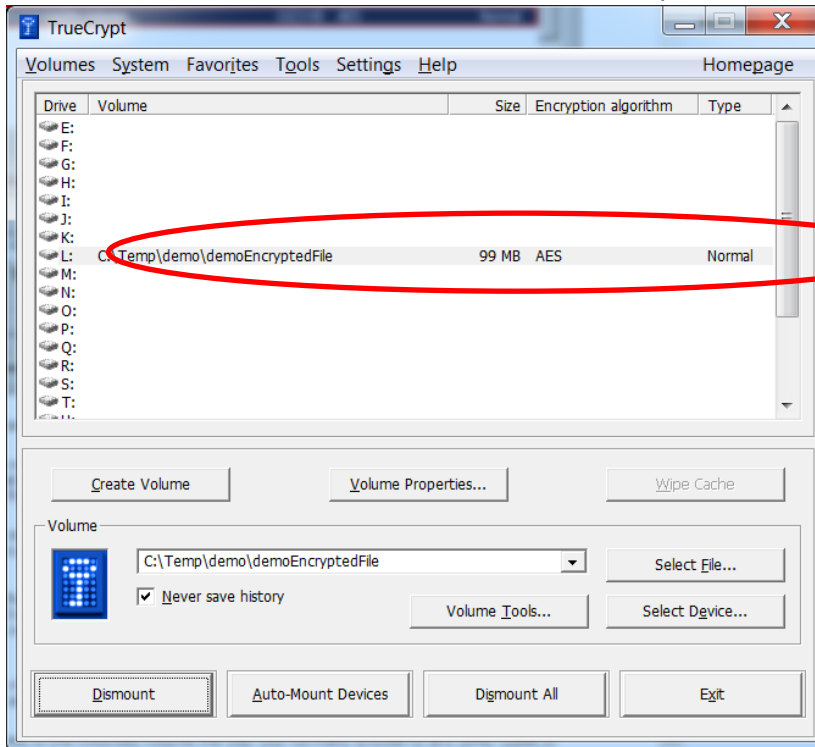
start the mounting of the file.
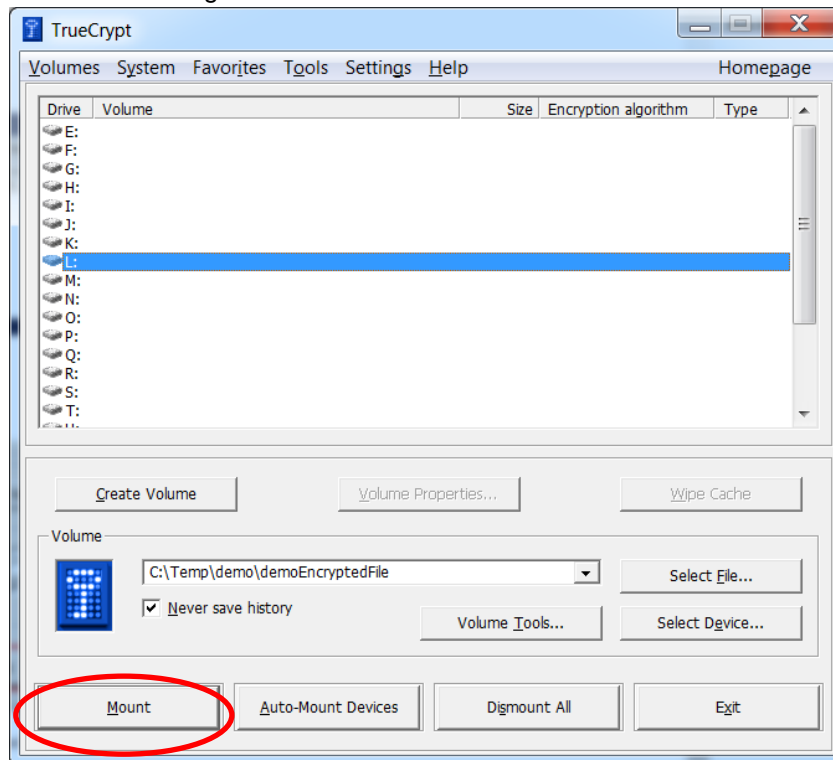
5. Please, as requested, provide the password needed to decrypt the file.

And click on „OK".

If successful the main window will be updated with mounted file information.

You can now access the mounted drive as you would with any other internal or external drive.