Deliverable No. 4.1

Initial analysis of the ethical and legal requirements for the sharing of data

Grant Agreement No.:	600841
Deliverable No.:	D4.1
Deliverable Name:	Initial analysis of the ethical and legal requirements for the sharing of data
Contractual Submission Date:	30/09/2013
Actual Submission Date:	30/09/2013

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.:	D4.1
Document name:	Initial analysis of the ethical and legal requirements for the sharing of data
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	RE
Version:	1.0
Actual Submission Date:	30/09/2013

Editor: Nikolaus Forgó
Institution: Leibniz University Hannover
E-Mail: nikolaus.forgo@iri.uni-hannover.de

ABSTRACT:

This deliverable describes an initial analysis of the ethical and legal requirements for data sharing in the CHIC project. The complex nature of the infrastructure being developed in the project requires the use of real patient data - retrospective and prospective data - and demands that careful measures be taken to protect such data, not only as a legal obligation, but also as an ethical requirement. This initial report centers on the data protection framework of the project during the development phase of the infrastructure. As one of the key safeguards with respect to the data usage in this phase, it proposes to adopt a safety net, where data will be processed in "anonymised" form within a closed network of researchers, with well defined rules and contractual

[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)

obligation to maintain data anonymity. In addition to the organizational framework, a layer of security framework that is made up of the use of a trusted third party to secure the pseudonymisation key, encryption, etc, will also be adopted. Overall, an approach is taken whereby the fragmented EU Member States national data protection laws are analysed and interpreted in a manner consistent with achieving the intention of the Data Protection Directive.

KEYWORD LIST:

Data Protection, Data Security, Ethical Requirements, Data Reuse, Anonymisation, Pseudonymisation

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 600841.

MODIFICATION CONTROL			
Version	**Date**	**Status**	**Author**
0.1	01/07/2013	Draft	Nikolaus Forgó Iheanyi Nwankwo Marc Stauch Johannes von Zastrow
0.2	29/08/2013	Draft	Nikolaus Forgó Elias Neri Iheanyi Nwankwo Marc Stauch Johannes von Zastrow
0.3	02/09/2013	Draft	Marc Stauch
0.4	05/09/2013	Draft	Elias Neri Iheanyi Nwankwo Marc Stauch Johannes von Zastrow
0.5	10/09/2013	Draft	Nikolaus Forgó
0.6	13/09/2013	Draft	Elias Neri Iheanyi Nwankwo Marc Stauch Johannes von Zastrow
0.7	21/09/2013 27/09/2013	Internal Review Internal Review	Norbert Graf (USAAR) Dimitra Dionysiou (ICCS)

0.8	22/09/2013	Draft	Nikolaus Forgó
0.9	24/09/2013	Draft	Iheanyi Nwankwo Marc Stauch Johannes von Zastrow
1.0	30/09/2013	Final version	Nikolaus Forgó Elias Neri Iheanyi Nwankwo Marc Stauch Johannes von Zastrow

List of contributors

- Nikolaus Forgó (LUH)
- Marc Stauch (LUH)
- Johannes von Zastrow (LUH)
- Iheanyi Nwankwo (LUH)
- Elias Neri (Custodix)
- Norbert Graf (USAAR - Internal Reviewer)
- Dimitra Dionysiou (ICCS –Internal Reviewer)

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, which brings into focus the legal and ethical requirements for the processing of sensitive health data.

On the one hand, the complex nature of the requirements for processing sensitive health data under the European legal regime is understandably founded upon the need to protect data subjects who may be adversely affected when privacy of such data is breached. This is seen clearly in the leading provisions of the Data Protection Directive 95/45/EC. On the other hand, it is very important that medical data be used for research that will better the conditions of patients and advance medical science as is being proposed in the CHIC project. This calls for balancing the equation so as permit the research to occur without unreasonable hindrance, but importantly not sacrifice the patients' fundamental privacy interests in the process. In CHIC, Work Package (WP) 4 of the project has been dedicated to carrying out this task, which necessitates this initial analysis.

In order to remove the barriers usually faced by researchers in getting access to and sharing data - mostly as a result of legal and ethical requirements, this deliverable proposes to establish a **network of trust** within a community of researchers involved in the project for data sharing. The data protection framework proposed here aims at taking care of the project development in **two broad phases** – the **development/validation** phase and the **exploitation** phase. The analysis in this report is mainly focused upon the former phase, and takes as its baseline the applicable provisions of the Data Protection Directive, the Clinical Trials Directive and applicable national implementation of the relevant Directives.

In the main, two domains have been identified in the data flow of the project- the **care** domain (hospitals) and the **research** domain (CHIC research platform). These domains will be separated from each other to maintain privacy and the required control mechanism. Data in the research domain will be pseudonymised twice to secure a high level of anonymity. In addition to this, the following pillars will be further used to ensure anonymity:

- Research data sets will be **stripped of any direct identifiers**;

- Confidentiality obligation will be imposed on the users by **binding contracts**;
- A trusted third party will be used for the **second pseudonymisation** process before data is used within the CHIC research domain;
- A **data protection office** will be re-used for the project;
- **Access** to the research domain will be **limited**/restricted to only authorised persons from each partner institution;
- **Technical security measures** such as traceability/logging capabilities, encryption, etc, will be maintained;
- There will be **no publication of personal identifiers** in the research results generated.

Moreover, as the project develops, this framework will be **reviewed**, and **updated** to take care of the validation aspects of the development phase as well as the exploitation phase of the project.

2 Introduction

This Deliverable aims to evaluate the legal and ethical requirements relating to the use of health data within the CHIC project. As will be described in Chapter 4, clinical and other research data is to be made available to the project, by a number of project partners, which will be used in a collaborative manner to generate tools, models and hypermodels for cancer and other medical conditions for effective care and treatment. Within this context, secondary use of data is envisaged, and ultimately shall contribute to the development of software tools and infrastructure to facilitate future medical treatment throughout the whole medical healthcare system. The relevant processing, insofar as the data qualifies as personal data, will be governed by the legal rules founded in Directive 95/46 /EC (Data Protection Directive), its national transpositions and other relevant international and national regulations. The Data Protection Directive has to be examined in particular because it specifies a fundamental rights framework for data protection, which in turn provides the required basis for national implementation, given the legal nature of a European Directive. The national regulations contain the directly applicable rules that apply at domestic law level, and thus have direct influence on the processing of medical data for research in individual member states. The diverse domestic laws at issue contain variations which pose a challenge in terms of finding a single framework for CHIC that implements all the relevant Member States laws.

In addition, ethical requirements must be observed when determining the permissibility of measures to be taken within the CHIC project. Compliance with the relevant laws and ethical norms is therefore a primary task of the legal/ethical WP in CHIC. The framework developed here takes work undertaken in research projects like Advancing Clinico Genomic Trials on Cancer (ACGT), p-medicine and EURECA as a baseline. The data protection and data security framework set up for those projects is adapted and further developed here and special emphasis is at the same time laid upon recent developments within technical aspects of data protection as well as the current review of the Data Protection Directive.

This WP Deliverable is to be seen as providing an initial analysis only, and will be therefore extended at a later stage, including – still at an early point within the overall lifetime of the CHIC project – in Deliverable D4.3.1, to be submitted in M14. Moreover an advance in technical understanding and potential opening up of other data applications is to be expected throughout the project's progress, that will substantiate the need for ongoing legal advice.

3 Structure

3.1 Structure of the Deliverable

This deliverable describes the initial analysis of the ethical and legal requirements for data sharing in CHIC. The remainder of the deliverable is divided into five main parts. Chapter four gives an overview of the data processing to be carried out in CHIC. Here on the basis of partner responses to a questionnaire developed and circulated by LUH, the sources and envisaged manner of usage of data by the project are enumerated. Chapter five then looks at the general legal principles and requirements for data protection and data security within the European legal system. Emphasis is laid on the current Data Protection Directive 95/46/EC and various national implementations of the Directive, especially as they pertain in the countries of CHIC data providers and users to the processing of sensitive personal data such as on health. The provisions off the Clinical Trials Directive 2001/20/EC, Good Clinical Practice Directive 2005/28/EC and Medicinal Products Directive 2001/83/EC are also analysed.

Chapter six then continues the analysis by considering the ethical requirements that are relevant, in addition to the legal data protection rules, for carrying out medical research using health data. On the basis of the overall evaluation of the relevant legal and ethical norms, Chapter seven then proposes a preliminary data protection and security framework for CHIC. Finally, Chapter eight provides a summatory conclusion to the deliverable.

4 Overview of data processing in CHIC

The high level aim of the CHIC project is to develop hyper-models of diseases and normal physiology for comprehensive exploitation of human multiscale biological data.[3] This will in the end lead to the development of a suite of tools, services and secure infrastructures that will support accessibility and reusability of VPH mathematical and computational hypermodels. In developing this infrastructure, a number of open source features and tools will be used, while some other tools will be developed from scratch, tested and validated. Clinical data obtained from the clinical partners will be used in the project. Test cases will be from cancer diseases, and cancer hypermodels to be developed will be tested with clinical data from three different cancer types - Wilms tumor, glioblastoma multiforme (GBM) and non small cell lung cancer (NSCLC). 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, molecular data, metadata, annotations, added semantic information to data and model/hypermodel configuration parameters.[4]

It is proposed that data from these cases will be stored within the infrastructure of CHIC in a secure and – wherever possible – anonymized way according to the legal and ethical framework of CHIC. It is of utmost importance to understand where the data come from, where they are transferred to for which purpose and who is entitled to do what with the data. The steering of this process requires technical, in particular security related, means and a network of legally binding agreements that clarify who may do what with the data at stake. The setup of this network is a key requirement for D 4.3.1.

4.1 CHIC Questionnaire

In order to gain a more detailed understanding of the data that will be provided and utilized within the CHIC project, WP 4 developed and circulated a questionnaire to the relevant clinical and technical partners: the questionnaire is appended to this Deliverable as Appendix 3. The questionnaire consisted of 14 questions aimed at eliciting details on which partners will provide data for the project, what will the status of the data be – personal, pseudonymised, anonymised, whether data will be prospective (collected in the future) or retrospective (already collected), whether informed consent covers the use of the data in CHIC, whether real data will be required to test the tools and models to be developed in the project, and (of relevance to IPR issues in forthcoming

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

deliverables) details of licenses under which the tools and models to be used in the project development were released.

So far, twelve partners have responded to the questionnaire. These include importantly all five data providers in CHIC, namely the clinical partners, USAAR, KU Leuven, and UNITO, which will make available clinical and research data in Workpackage 3; UBERN, which will provide brain image data in Workpackage 6, and UPENN which will provide Non-clinical Data from computational analysis. The other responses are from seven of the technical partners, namely BED, CUSTODIX, SCS-SCR, UOXF, ICCS, FORTH and USFD. Responses are pending from three further technical partners, namely PHILIPS, TEI-C, and UCL

Subsequently, on the basis of the information from the preliminary questionnaire, and taking account of the development and refinement of the use cases in Workpackage 2, a set of further 'tailor-made' questionnaires (i.e. containing specific additional questions for each partner) will be developed in Workpackage 4. These secondary questionnaires will be distributed to the relevant project partners by M11 so that their responses may be incorporated into the first iteration of the CHIC data privacy and copyright framework (D4.3.1) in M14.

In the next sections of this Chapter, we will elaborate on the nature of the data to be provided to and processed in CHIC. Later, on the basis of this evaluation together with the legal and ethical analyses presented in Chapters five and six, we outline in Chapter seven the key technical, organisational and legal safeguards that will be deployed within the integrated CHIC Data Protection Framework in order to protect it.

4.2 The planned provision to and processing of data within CHIC

As noted above, five partners, USAAR, KU Leuven, UNITO, UBERN, and UPENN will provide data to the CHIC project. From the responses of these partners to the preliminary WP 4 questionnaire, it is apparent that this is planned to occur as follows:

(1) USAAR

USAAR will make available retrospective and prospective data relating to nephroblastoma (Wilms tumour) patients participating in former and current SIOP trials for nephroblastoma and non small cell lung cancer (NSCLC) trial. The data will be stored in the ObTiMA data management system developed for the p-medicine FP7 project, and includes clinical data, imaging data and biological data. This will be provided to CHIC in a securely de-identified form in line with the p-medicine framework: thus the data will be doubly pseudonymised, with the second keycoding carried out by a trusted third party and according to the terms and condition relevant for the p-medicine project. It might be the case but is yet undecided that USAAR will not transfer data that is to be seen as

completely anonymised data in the legal sense. The reason for using this approach rather than irreversible anonymisation, in which no keycode is kept, is to allow the possibility to revert to the patient in case of incidental findings relevant to the individual patient's wellbeing in p-medicine and (possibly) also in CHIC after the initial phase of the project's setup.

USAAR has **informed consent** for the research use of the retrospective SIOP and NSCLC trial data, though – as the data collection predated the project – this does not expressly mention use for CHIC. USAAR has thus in addition applied for and obtained the **approval of its ethics committee** to the use of the data in the project. In the case of the **prospective** data, the informed **consent** forms are to be **modified** by USAAR to also mention CHIC as one of the project-purposes for which the data may be used. Copies of USAAR's existing consent form and the ethics committee approval to the use of the retrospective data for CHIC are appended in Appendix 4 of this deliverable.

(2) KU Leuven

KU Leuven is to provide clinical, radiological and pathological data of patients with glioblastoma, treated with surgery, radiochemotherapy and dendritic cell vaccination. This includes retrospective data from a longitudinal follow-up study (HGG-2006) to monitor patients treated with immune therapy as well as prospective clinical, radiological and immunological data of patients included in a currently running clinical trial (HGG-2010). Patient informed consent was obtained from participants in the study. A copy of the consent form developed for the HGG-2010 trial is appended in Appendix 4 of this deliverable.

In accordance with its local ethics committee guidelines the data from the previous study (HGG 2006) will be provided to CHIC in anonymous form. Similarly, the data provided from the HGG-2010 will be anonymised so that when used to develop the CHIC models relevant data cannot be linked to the patient. The relevant patient consent and ethical approval in respect of the HGG-2010 trial that is currently running are appended in Appendix 4.

(3) UNITO

UNITO will make available to CHIC retrospective clinical and pathological data from prostate cancer patients from a multi-centric observational follow up study on prognostic factors after radical prostatectomy or radical radiotherapy. The data was provided to UNITO by over a dozen Urology and RT Units across North-West Italy and is being used by it to develop a personalized mathematical model concerning prostate cancer relapse risk. The data relates to around 4500 patients going back over fifteen years and is held by UNITO – and will be made available by it to CHIC - in coded, irreversibly anonymous form for the purposes of developing the CHIC models. The relevant ethics approval in relation to the provision of this data is appended as Appendix 4. Although, the respective

Urology and RT clinics retain keys for their own purposes, these will not be made available to the CHIC project.

(4) UBERN

UBERN is to make available image data to CHIC in the form of multimodal MRI images corresponding to the BRATS Brain Tumor Segmentation challenge. The data is retrospective, having been obtained for the Miccai 2012/2013 research challenge and, apart from the brain tissue images themselves, include no other individuated data regarding the patients from whom they came. In this regard, we are of the view that currently there probably are no reasonably available means to link back the data to the patient. However, giving possible future development which might enable such image linking to specific individuals, it is important that the image remain protected and will only be made available within the secure CHIC data protection framework.

(5) UPENN

UPENN is to make available non-clinical data from computational analysis to CHIC. The data will be harvested from the execution of multiscale simulations, analysed and processed before provision to the project. In this regard, no personally identifying information will be transferred. In addition, "raw" data – data that has not been analyzed and processed, can be transferred on-demand to specific partners that might need it.

In addition to the above data from partners, literature and open sources will also be processed within CHIC. It is not possible at this stage to conclusively enumerate and analyze the nature of data to be obtained from these sources. However, there is a high chance, in accordance with standard research publication practice, that these may be anonymised, i.e. the original data controllers would have stripped the data of all personal identifiers as required by European data protection law. In many cases, given that the focus of scientifically valid research is on general connections rather than the individual and anecdotal, the data is likely to be aggregated data (i.e. true for multiple patients), not individual microdata. Accordingly, fewer privacy concerns arise; however, this may not entirely be the case, particularly for data originating from jurisdictions where there are not strict requirements as seen in Europe.

On provision to CHIC, it is planned that all relevant data will pass though a further de-identification process[5] and then securely stored in the data repositories developed in Workpackage 8. These include the CHIC data repository, the multiscale data repository, the in silico trial repository, and the distributed RDF repository to store metadata from each partner, including the corresponding

[5] As further described in Chapter seven.

interfaces for annotating and querying.[6] Data provided in the project will be used by the technical partners for the development of models and hypermodels within Workpackages 6 and 7. This will involve the creation of integrated models that seek to simulate and thus to allow differential prognostics (based on alternative possible therapies) for the key tumour types addressed by CHIC. They will function by synthesising separate bioprocess models of the various complementary mechanisms at play in the progress of the relevant disease-type. The resulting hyper-models will subsequently undergo numerical analysis and at least partial clinical adaptation and validation using pertinent multiscale data to be provided by the CHIC clinical partners and/or mined from literature and/or provided by experimental or clinical collaborators of modellers. The hypermodels will thus serve as demonstrators of the implementation of the concept of hypermodelling in the cancer domain.

In terms of privacy implications, the fact that hypermodelling combines different models under a common roof means that insofar as the models use real data, the merging of this data could lead to facilitating patient re-identification. In this regard, hypermodels could be seen as offering a new, advanced data-linking and –mining technique. At the same time, a full examination of specific additional risks posed by the technique will have to await the crystallisation of specific use scenarios later on in the project. At this stage though, a further potential legal and more especially ethical implication deriving from the use of the relevant hypermodels should be highlighted, in terms of their anticipated enhanced predictive power compared to contemporary models. Thus it may prove possible with much greater accuracy than hitherto to inform a cancer patient with a tumour of the type under study of their detailed prognosis with or without a given therapy. This should be reflected in the terms of the informed consents for prospective studies or trials run by partners contributing data to CHIC as well as future users of the infrastructure, so that the patients participating are put on notice as to the greater possibility of information disclosure (and allowed to opt out from receipt of it, if they wish). This is a matter that will require to be kept under close review over the further course of the CHIC project.

One of the planned CHIC repositories to be developed in Workpackage 8 is for the storage of metadata from each partner, and will include interfaces to facilitate data annotation and querying. This is at present a developing technical field and uncertainties remain as regards the legal standing of metadata in the context of personal data processing. In a computerized world it is apparent that the information might relate both to the substantive contents, or to data that describes the content (meta-data or “data about data”). Meta-data are included for instance in catalogues and libraries for automation reasons (e.g. search, statistical analysis). The American Health Information Management

[6] DOW, p A 31.

Association defines metadata as, "[d]escriptive data that characterize other data to create a clearer understanding of their meaning and to achieve greater reliability and quality of information."[7] This systematic method of describing a resource is key to facilitating and improving its retrieval in information systems.

In information science, metadata can be divided into at least three categories - structural metadata, descriptive metadata and administrative metadata.[8] Metadata could be created by the maker of the content data, others (users of the data) or by computer algorithm. This underlies the fact that it is sometimes not possible to distinguish between content and metadata.[9] Especially in digital storage, data may be augmented with metadata. To understand the use of the term in the medical context, much depends on the structure of the data involved and the platform upon which it is used. For example, it could include metadata about the patient's identity, metadata about the clinical description/value of the file, metadata about its provenance, metadata about the person who granted access to it in the past, when and for how long, metadata about what changes were made and the successive versions in which it was previously presented, metadata about the creation of the file, etc. In the context of CHIC, a further investigation will be carried out when these metadata are generated to ascertain their status.

The other partners who responded to the questionnaire, were Universities and technical partners – USFD, UOXF, CUSTODIX, SCS SRL, UBERN, ICCS, FORTH and UPENN. All but one of these respondents indicated that they will require either real data for the validation of the tools or models to be developed in the project, or will handle real data in the course of their work. In particular this is relevant for testing and validation of the in silico predictions of outcome provided by the hypermodel simulations as against real world patient outcomes. In this regard the in silico trial repository developed in Workpackage 8 will store the input data (the original state of the patient), the simulation scenario (the in silico treatment) and the output data (the state of the patient after in silico treatment). This data will then be available for evaluation, comparison and validation.[10] This suggests that neither synethetic, nor real but irreversibly anonymised data will be sufficient for the purposes of the project.

4.3 Initial summary and implications

In our assessment of the responses, the data that will be transferred to the CHIC research domain will not contain any direct identifiers of the data subjects. Broadly speaking, they could be

[7] AHIMA, "Rules for Handling and Maintaining Metadata in the EHR", http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050177.hcsp?dDocName=bok1050177
[8] Jeffrey Pomerantz, "Metadata: organising and discovering information", Lectured delivered on coursera.org.
[9] Article 29 Data Protection Working Party, Opinion 7/2007, p. 7.
[10] DOW, p A 31.

categorised into two types of datasets - irreversibly anonymised datasets, where direct identifiers of patients have been stripped and replaced by a unique, irreversible code; and reversibly anonymised (pseudonymised) datasets, where the direct identifiers are similarly stripped, but a key remains in the hands of the provider institution that allows it to re-establish the link between a given coded dataset and the previously stripped identifiers (i.e. the patient's name, etc). The legal implications are as follows:

- The irreversibly anonymised data are, subject to all further necessary safeguards being taken to prevent re-identification, such as strict access control, logging, and binding obligations on users to foreclose misuse, no longer personal data, and will not be subject to the data protection law of the state where the data provider is located.
- The pseudonymised data (due to the need to follow up patients) is seen as personal data,[11] even though the personal identifiers have been removed. This will require additionally stringent safeguards under the European data protection law in order to be legally processed as well as maintain the anonymity required for medical research.

As stated, the preliminary questionnaires on which the present Chapter is based provide an initial picture that will be further refined and completed through the use of directed, partner specific questionnaires to be distributed in M11. However, already from the above it appears clear first that highly sensitive individuated data will be required in the CHIC project infrastructure. Although the datasets will be provided in irreversibly anonymised form for developing the hypermodels, given their high level of granularity, they may have the potential to be re-identified by data-matching, if it is accessed in an unauthorised manner and/or misused, and thereby cause grave harm to the privacy and other fundamental interests of the relevant patient subjects. It will therefore be necessary to accompany the technical solutions developed by a framework of contracts between data providers and technical partners in order to clearly distinguish legitimate from illegitimate use of data and to protect patients' privacy by anonymisation wherever possible. Secondly, it appears at least provisionally likely that to validate the hypermodels and other tools in the validation part of the development phase of the project in Workpackage 11 (from M36), an updated architecture will be needed that allows in some cases the partners which provided data to link this back to the individual sources. Two messages are important here: First, it is advisable and will be undertaken if technically and legally possible to process anonymous data only in the technical setup of the infrastructure. Second, the health data at issue will most probably qualify as personal data for the purposes of data protection law at least from month 36 onwards so that all data protection rules will apply. WP 4 will therefore need to monitor closely whether personal data is processed, avoid this wherever possible,

[11] See chapter 5 below for fuller analysis.

set up a framework of trust guaranteeing anonymity in an early stage and a second framework of trust for the proper processing of personal data, if needed, in the later stages of the project.

We next proceed in Chapters five and six to examine further the relevant legal and ethical rules that will apply to the data to be used within CHIC, before returning in Chapter seven to outline the concrete safeguards that will be called for to allow data use in a secure justified and controlled framework. This will require especially the data providers and users in CHIC to implement all necessary and appropriate steps, in the form of sound technical and organizational measures, to ensure a sufficient level of data security, in particular to prevent unauthorized disclosure of the data, with the patient risks described above. The initial analysis presented in Chapter seven will later form the starting point for the CHIC data privacy and copyright framework - first iteration (D4.3.1).

5 Processing of personal data – general legal requirements

5.1 Legal requirements for data processing – theoretical analysis and timeline

The protection of personal data is considered a fundamental human right in the European legal framework, and as such, it is the subject of a complex and comprehensive network of legislation. Historically, over the course of the past century, Europeans became acutely familiar with the dangers posed by unrestricted access to personal information.[12] The increase in the use of computers in processing of personal data and the need to facilitate cross-border transfer of data for economic activities has prompted concerted efforts in data protection all over Europe. The European Convention of Human Rights of 1950 ("ECHR") represents one of the first efforts to extend protection to personal data on a regional scale through the provision of its Article 8: "[everyone has the right to respect for his private and family life, his home and his correspondence." It further provides that interference with the right by governments is prohibited except where necessary for the proper functioning of a democratic society.[13] Building on ECHR provisions, the Council of Europe passed Resolutions 73/22[14] and 74/29[15] on the protection of individual privacy on electronic data banks, setting out some basic principles on personal data processing in both the private and public sector respectively.[16] This paved the way for individual legal systems in Europe to legislate on data protection in the early 1970s in reaction to perceived dangers of automated data processing.[17]

The concept of privacy was further outlined in the Organization for Economic Cooperation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("Guidelines") in 1980.[18] The Guidelines represented efforts to reduce barriers to the free flow of information that arose from divergent national laws, built on the several basic principles for the protection of personal data as well as for the free flow of information among member states. These

[12] H. Kaplan, M. Cowing and G. Egli, "A primer for data-protection principles in the European Union", 2009, http://www.shb.com/attorneys/CowingMark/APrimerforDataProtectionPrinciples.pdf

[13] European Convention on Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf

[14] Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, http://www.giodo.gov.pl/237/id_art/216/j/en/.

[15] Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, http://www.giodo.gov.pl/237/id_art/215/j/en/

[16] S. Rudgard, "Origins and historical context of data protection law" in E. Ustaran (ed) *Law and Practice for Data Protection Professionals*, IAPP, 2012, https://www.privacyassociation.org/media/pdf/publications/European_Privacy_Chapter_One.pdf.

[17] Ibid.

[18] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

principles include: collection limitation and notice, purpose limitation, data quality, data security, disclosure, data subjects rights and accountability.[19]

However, the OECD recommendations were not binding, so a full harmonisation was not achieved. The OECD recommendations were followed by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981.[20] As technology moved on again, the EU Data Protection Directive 95/46/EC was passed in order to harmonize existing data protection laws and to ensure a free and secure flow of data among Member States. The Directive is currently under review, and likely to be replaced by a Regulation in the near future.[21]

5.2 Legal sources on data protection

In a multilevel legal system, like the European Union (EU), it is necessary to identify the relevant legal sources at each level. According to the norm pyramid and the primacy of EU law, special focus is to be set on the EU provisions on data protection which is regulated by a Directive EU law establishes a framework, as addressed to the member states (e.g. art. 34 Directive 95/46/EC), and requires implementation through national legislation. Hence every single national legal system has to be included in the analysis. This, while giving member states a margin of discretion in how they choose to transpose detailed aspects of the parent Directive so as to cohere with their own law, creates some potential for conflict between primacy of EU law and the differential, and sometimes restricted, manner it may be implemented within a given national legal system. By implication, both the Directive itself and the national transposition have to be taken into account, as outlined above.

In the context of the CHIC project, the national legal systems of all member states, where a relevant consortium partner resides should be analysed. This applies to both the data provider and the data user partners. In addition fundamental rights influence the interpretation of all legal sources, as to be found under the Charter of Fundamental Rights of the European Union and the national legal system's constitutions like the German Constitution (Grundgesetz). Although an international multilateral contract in its origin, the European Convention on Human Rights has to be considered as well, as to its possible direct effect within legal systems of the EU and different member states according to the principle of “monism” or its international law friendly transformation into national law, like in Germany.

[19] Ibid.

[20] See http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[21] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Within CHIC project consortium however, partners are not limited to the member states of the EU, as two partners reside in Switzerland and the United States, respectively. Both of these countries are not member of the EU, although bilateral international contracts might influence both legal requirements on the transnational use of personal data. Nevertheless it is envisaged to briefly analyse both national legal system for their requirements on processing personal health data and in respect of the "safe harbour" requirements for cross border transfer of personal health data.

Besides legal sources ethical requirements for processing personal health data can be found under international declarations, such as the Helsinki Declaration. One question will be, in what extent these declarations should be followed as sources of binding or persuasive norms as well.

5.2.1 Data protection and fundamental rights

Fundamental rights are the foundation, from which all data protection regulations stem. This involves a consideration and weighing up of the various interests in data use, not only of the persons from whom personal data is collected, but also of those persons who wish to use and/or may otherwise benefit from the use of the data in question. The last point (i.e. the potential benefit to persons suffering from serious, and presently only limitedly treatable diseases) counts especially when one considers data use for the purposes of medical research. In addition medical research might be seen in the public interest, to be balanced with the fundamental rights on privacy.

In the area of data protection, the existence of fundamental rights at both levels, the European and the national, need to be examined, given that, as noted, Member States have the duty to transform the European law into national law. In this regard, in transposing and interpreting the provisions of the Directive, Member States have a certain range for choosing the appropriate means of implementation, so as to reflect the scope of their national fundamental rights as well. In line with this, Recital 2 Directive 95/46/EC stresses, that: "data processing systems are designed to serve man; [...] they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, in particular the right to privacy".

5.2.1.1 Fundamental Rights and the European Union

On the level of the European Union, the Charter of Fundamental Rights is a key instrument of fundamental rights to be recognised according art. 6 (1) EU-Treaty.[22] The Charter of Fundamental Rights guarantees "Everyone [...] the right to the protection of personal data concerning him or her" under art. 8 (1). As a fundamental basis of the protection of the individual, this right is to be

[22] See [http://www.consilium.europa.eu/documents/treaty-of-lisbon?lang=en].

restricted only so far as necessary and proportionate in order to protect the fundamental rights of others or legitimate public interests. Applied to medical research the right to limit the protection of personal data could arguably be premised upon the right to science as laid down in art. 13 ("… scientific research shall be free of constraint. Academic freedom shall be respected") as well as the public interest in an effective health care system. As to the allowable manner of limiting the protection of personal data, art. 8 at the same time insists that "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified" and "Compliance with these rules shall be subject to control by an independent authority." The framework stipulated by the Charter of Fundamental Rights give the basis of the protection of personal data to everyone. Any limitation to this right requires the data to be processed fairly and for a specific purpose and a legal bases or the consent of the person concerned. In addition, on the level of the Charter of Fundamental Rights, the right to access and to rectification of stored data is laid down as a precondition to be fulfilled to process personal data lawfully within the European Union. Even if Fundamental Rights bind the state only and have no direct effect as between citizens, the organs of the European Union are obliged to establish an appropriate legal base to protect the Fundamental Rights of an individual on a horizontal level as well. In that respect, each individual institution conducting medical research will be affected by art. 8 Charter of Fundamental Rights of the European Union at least indirectly and via the relevant domestic law to concretize this fundamental rights framework.

5.2.1.2 European Convention on Human Rights

On the European level, in addition to the Charter of Fundamental Rights, the EU is bound to the European Convention for the Protection of Human Rights and Fundamental Freedoms under art. 6 (3) EU-Treaty.[23] In comparison the relevant text of the Convention is much shorter than that of the Charter of Fundamental Rights, restricting itself (under art 8(1)) to "Everyone has the right to respect for his private and family life, his home and his correspondence" without special reference to "personal data". The principle of permitting limits to this fundamental right only in a proportional and balanced way exists for the European Convention the same way as for the Charter of Fundamental Rights, as outlined in art 8(2): "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." In contrast to the Charter of Fundamental Rights, here the

[23] Ibid.

public interest is explicitly mentioned as a legitimate basis for limiting the fundamental right, but with no difference in outcome. Medical research could also be seen as part of the "protection of health", that is recognized as legitimate purpose under art. 8 (2) European Convention on Human Rights.

5.2.1.3 Fundamental Rights under national constitutions

Fundamental right to data protection is also seen in national constitutions of European countries, including those of CHIC consortium partners that will be providing data to the project. Thus, under the Belgian Constitution, of applicability to KU Leuven, data protection is guaranteed as part of the right to privacy, that "everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law"[24]. Under the Dutch Constitution (relevant to Philips) personal data is addressed under art. 10 (2) Dutch Constitution, which states: "Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data."[25] Here in addition, a right to access and rectification is stipulated by art. 10 (3), in a similar manner as under the Charter of Fundamental Rights: "Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament." Under the German Constitution, and of application to USAAR, a fundamental right concerning the privacy of a human being is established by the jurisdiction of the federal constitutional court (Bundesverfassungsgericht) only, which merged art. 1 and 2 German Constitution to a single fundamental right with different expressions. The German federal constitutional court held that under the conditions of modern data processing, the protection of the individual is covered against unlimited collection, storage, use and disclosure of personal information by the general right of art. 2 (1) in conjunction with art. 1 (1) of the Constitution. The fundamental right guaranteeing to that extent the right of the individual to determine in principle the disclosure and use of personal data is essential[26]. This right is to be restricted only by overriding public interest and on the basis of a Parliamentary act. In addition safeguard measures are to be taken, that will prevent the risk of infringements to the "right of informational self-determination". The Greek Constitution, which will apply to processing by FORTH and TEI-C, restricts itself to the principle that "the private and family life of the individual is inviolable." As regards United Kingdom law (relevant to BED, UOXF and UCL), while it lacks a formal written constitution as such, the fundamental rights from the European Convention on Human Rights

[24] Unofficial translation of the Belgium Constitution:
http://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/grondwetEN.pdf
[25] Unofficial translation of the Dutch Constitution:
http://legislationline.org/documents/section/constitutions/country/12
[26] BVerfG, *Urt.* vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 = LMRR 1983, 56 ff.

have been implemented into national law by the Human Rights Act 1998, so that they may be relied on directly in front of domestic courts.[27]

Ultimately, in all the above member states, a similar fundamental rights framework can be found, which is relevant in determining how to proceed when carrying out medical research using health data. When it comes to preconditions of processing personal data, the Charter of Fundamental rights seems to be the most precise and detailed instrument. Preconditions to be satisfied are that the processing in question is fair and proportional, occurs for a legitimate purpose, and is subject to various necessary safeguard measures.

5.2.2 Legal requirements according the Data protection Directive (Directive 95/46/ EC) and its transformation into national law

As discussed in Chapter 4, within the CHIC project it is envisaged to develop "a robust, reproducible, interoperable and collaborative hyper-model of diseases", that consists of a "hypermodel-driven clinical data repository, a distributed metadata repository and an in silico trial repository".[28] These different repositories consist of various information, and as indicated in Chapter Four above, not all data in the repository (as least during the project development phase) will be fully anonymised, meaning that fall under legal regulations, such as the Data Protection Directive. By its nature the Directive, has been transposed separately into diverse national legal systems, we consider the test for determining under which jurisdiction a particular case will fall (Territorial application). This is relevant in the light of the fact, that CHIC project partners are located in a number of different member states. According to its art. 1, Directive 95/46/EC pursues two purposes: on the one hand to allow the free flow of data within the EU in order to prevent the Member States from blocking cross border data flows on grounds of data protection within the EU; and on the other hand to establish in accordance with the fundamental rights and freedoms a minimum level of data protection throughout all Member States. In that respect the Data Protection Directive 95/46/EC seeks to harmonize data protection within the European Union in order to establish a clear and straightforward legal framework for personal data protection and data security throughout the Union.

5.2.2.1 Territorial application

According to art. 4 (1) a) the application of the transposed national law is to be based on the *territoriality principle*. This principle is outlined as follows by the Directive, namely "that every

[27] See: http://www.legislation.gov.uk/ukpga/1998/42/contents.
[28] See the CHIC Description of Work (DoW)

Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable". Within CHIC, both the clinical partners (as data providers) and the technical partners (as data users) will be processing data. Hence the crucial criterion is where they are respectively. This rule is added to by art. 4 (1) c) Directive 95/46/EC, which provides that national law shall apply also where, "the controller is not established on Community territory and, for purpose of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." It follows that the place, where the processing takes place is relevant to the decision what national law is applicable as an exemption only, in cases no controller is situated within any Member State of the EU. As far as a controller is located in one of the 28 Member States, all processing of personal data "in the context of the activities of an establishment of the controller" will fall under the national law of this specific Member State. And in case a controller runs establishments in different Member States the same time, the respective establishments must comply with the national law of each Member State in which the relevant particular establishment is located. The CHIC consortium partners within the EU are located across six Member states, namely Belgium, Greece, Germany, Italy, the Netherlands and UK. In this regard, each respective CHIC project partner will have to comply with the relevant national implementation of Directive 95/46/EC in its Member State.

5.2.2.1 Impact of anonymisation/psuedonymisation on data processing

Directive 95/46/EC applies only to "personal data", as stipulated under art. 3 (1). Under the Directive the legal definition of "personal data" as "any information relating an identified or identifiable natural person ("data-subject")" is to be found under art. 2 a) Directive 95/46/EC. By this data is excluded from the scope of application of the directive, insofar as it is or has been rendered anonymous[29]. The criterion to distinguish between personal and anonymous data is whether there is a link between the data and the data-subject such that the latter is identified or identifiable. It is not straightforward and for these purposes also unimportant to distinguish between identified and identifiable data. This is because "personal data" exists in both cases. Hence the only question for the purposes of applying the relevant statutory norms is whether one is dealing with "personal data" or "anonymous data". This discussion is particularly important in the context of clinical trials and other

[29] See Article 29 Data Protection Working Party, Opinion 4/2007.

medical research because anonymisation without any possibility of re-linking the data to a particular person may be difficult to achieve (for example, when it relates to genetic data); moreover, irreversible anonymisation may not always serve the best interests of the data subject (for example, where a new successful treatment is proved, and/or it is important to monitor patients' reactions to the treatment. In such cases, it may well be desirable to maintain a possibility to link the data back to the patient.[30]

The easiest solution, would be for all data to be anonymous, because it would on the face of things remove all obligation laid down in the Directive 95/46/EC. Therefore first of all the criteria of personal data in contrast to anonymous data should be examined. "Anonymous data" will become "personal", in case of a linkage to a person. The criterion, for when this linkage is to be imputed, turns out though to be one of the most controversial questions in data protection regime worldwide, at least in course of the last ten years[31]. The provisions of the Directive itself refers to "factors specific to [the data subject's] physical, physiological, mental, economic, cultural or social identity" as relevant for determining the possibility of re-identification. However, this enumeration of connecting factors is not to be regarded as being exhaustive, as clarified by the use of the phrase "in particular" before. Hence the concept of "personal identifiable information" may be seen as inherently context-specific and open-ended. An exception where one could argue uncertainty does not arise, concerns the identification of a person by name or a number; but this relates to when data will definitely be personal, not the converse case of definite anonymity. When it comes to the latter, such certainty is precluded by the **contextual approach**, involving reference to the possibility of "indirect" identification, as mentioned in art. 2 a) Directive 95/46/EC. First of all indirect identification might occur in respect of information such as an image alone, but most of the time will likely require several identifiers, that will single out a person in combination. In a computerized world for identification reasons both the content as well as meta-data has to be taken into account. To exclude the possibility that several identifiers together may allow identification is not a matter that can be decided in general, but needs to be **verified in every individual case**. It similarly is impossible to say in advance what "identifiers" may help to indirectly identify a data-subject, as relevant identifiers could include information one would have classified as useless at the beginning[32]. Such information could help to identify in connection with other sources that were meant to be kept apart[33]. "The idea

[30] M. Arning, N. Forgó, R. Kollek, T. Kruegel, "Data protection in grid-based multicentric clinical trials: killjoy or confidence-building measure?", Phil. Trans. R.Soc. A 2009 367, pp. 2729-2739.

[31] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), pp. 1716, 1719-1720.

[32] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), p. 1723.

[33] Ibid, pp. 1704-1705.

that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned"[34]. But for a starting point, it can be argued that "data can be either useful or perfectly anonymous but never both"[35]. With the amount of data available and the data stored in a single data base, when it comes to "big data" it will increase the likeliness of re-identification[36]. An underlying tension is thus apparent, when balancing the fundamental rights of the data-subject against the right of science and public interest: every regulation will either, by increasing privacy, cause the data to less useful, or conversely, by increasing the utility of data, cause privacy to decrease[37]. To give an image, it is like a pair of scales every movement of one scales will automatically cause the opposite to the opposite scale. Although one could assume, that "even the modest privacy gains require almost complete destruction of the data-mining utility"[38]. In the end, this balance between useful and anonymous data is to be regarded as never being perfect, as "long as data is useful, even in the slightest, then it is also potentially re-identifiable"[39].

This conflict of interests reappears again in relation to the determining the most appropriate measures to achieve anonymisation, in short how to anonymise personal data. The simplest solution would be to suppress all identifiers that could link data to a data-subject. As pointed out already, though, it has proven impossible to determine a priori, what identifiers should be deleted, because of indirect identification bases of information that in itself may appear innocuous as not conducing to identification. Moreover, suppressing data aggressively to try and guarantee privacy may cause the data to become useless for the purpose for which the controller wishes to use it[40] A second possibility to be taken into account is that of generalizing data, so that specific information within datasets are rendered less detailed, such as by using age instead of the concrete day of birth of a given person. This faces the same problems as deleting data, however, because it will often be difficult to decide, when generalization will be enough to avoid possible re-identification. A third measure would be to merge data sets to produced aggregated, statistical conclusions. A fourth method would be to alter or exchange parts of a dataset. In the last cases it is doubtful how far, when generalizing or merging datasets, the value of the underlying information can be preserved at the same time[41]. In the worst case, any change in raw data designed to anonymise it, may cause the

[34] Ibid, p. 1732.
[35] Ibid, p. 1704.
[36] Ibid, pp. 1746, 1766.
[37] Ibid, pp. 1705-1706.
[38] Ibid, p. 1753.
[39] Ibid, pp. 1751, 1755.
[40] Ibid, p. 1714.
[41] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), p. 1756.

wrong answer to an investigation, possibly without knowing it[42]. This illustrates the above mentioned problem concerning the decreasing utility of data, when it comes to measures to secure privacy.

It is also a controversial question, what efforts can be deployed for verification of a de-identification. As noted above, the main criterion appearing in this definition is that of the ability to identify, meaning the potential of information to enable identification of an individual[43]. This "potential in identification" has to be ascertained to decide the scope of application of the Directive 95/46/EC. In this context the Article 29 Data Protection Working Party[44] states in its Opinion 4/2007 that the relevant factors for assessing the question of means likely reasonably to be used were cost, intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality) and technical failures[45]. Health data is to be regarded as highly interesting for e.g. insurance companies or employers. Hence it is reasonable to assume that there may parties, who have a significant interest in, as well as resources to devote to, re-identification. One additional factor that makes estimating identification problematic is that the technical means for data-linkage are in fluctuation, especially given improvements in computer science and decreasing costs (in this respect see further the discussion under "security" below). Moreover data sources that may reasonably be used may be increasingly available via the World Wide Web, and it is to be expected also that computer science will improve its capabilities in using social media as a source of identification[46]. Under these circumstances the criterion of time, duration of storage, might be a crucial point, in deciding whether a data-subject should be regarded as identifiable or remains anonymous. Whether data was rendered anonymous must ultimately then, be determined on a case-by-case basis and on detailed information only[47]. This also affects security measures to be taken, as outlined later on.

A relevant processing operation on the path to achieving anonymous data might be to pseudonymise data, because of its intent to prevent re-identification by others. In that respect it may be questioned, whether pseudonymisation, a term used under e.g. German law (§ 3 (6) BDSG), will lead to data to be regarded as anonymous. "Pseudonymous data" is to be seen as personal identifiable

[42] Ibid, p. 1757.

[43] See also Kuner, European Data Protection Law, rec. 2.74.

[44] The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. For further information please see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

[45] Article 29 Data Protection Working Party, Opinion 4/2007, p. 15.

[46] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), pp. 1719-1720, 1724-1725.

[47] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), p. 1744.

information that is altered in such a way that a third party would be unable to re-identify it. But under German law "pseudonymous data" is still considered to be "personal data"[48]. It is true that this need not automatically be the same position at the European level, because of the principle of norm pyramid. Nevertheless "pseudonymous data" has been subject to the legal discussion at the European level as well and according to the Article 29 Data Protection Working Party classification as personal or anonymous depends on whether two-way encryption is used with a key being retained for decrypting, or one-way encryption without a key is undertaken[49]. One-Way (irreversible) encryption is estimated to lead to "in general anonymised data"[50]. Hence "pseudonymised data" exists in case of two-way encryption only. Consequently, according to the Article 29 Data Protection Working Party, two-way encrypted data will lead to "retraceable pseudonymised data [that] may be considered as information on individuals which are indirectly identifiable" and therefore "data protection rules apply" to it[51]. The Working Party later considers how far one could argue Directive 95/46/EC will not apply due to the fact of anonymous data only, when data within medical research has been pseudonymised before its transfer by the physician[52]. The Working Party refutes such an argument convincingly though by referring to recital 26, where it is stipulated as relevant factors "all the means likely reasonably to be used"[53]. The purpose of two-way encryption is precisely to allow the re-identification and it "would be sheer contradiction in terms", if this purpose is disregarded while determining the data being anonymous[54]. This interpretation is underlined by recital (26) of the Directive 95/46/EC: a person is to be regarded as "identifiable", by "all the means likely reasonably taken to be used either by the controller or by any other person to identify the said person". As to the wording of "any person" it is to be assumed, that it is irrelevant who might be the person to re-identify. In addition there is no reason, if re-identification is not within the purpose of the recipient, "pseudonymised data" needs be transferred instead of "anonymous data". In other word, to the extent that no re-identification is required, one-way encryption should always be chosen over two-way encryption. Therefore if two-way encrypted data, i.e. "pseudonymised data" is to be transferred a second, one-way encryption process should be used in addition, to achieve anonymous data. Nevertheless it still has to be verified, if it will result in "anonymous data", which as pointed out before may be very difficult in practice. No exemption exists for metadata in this respect, as meta

[48] Dammann, Simitis et. all, BDSG Kommentar, § 3, rec. 222.
[49] Article 29 Data Protection Working Party, Opinion 4/2007, p. 18.
[50] Article 29 Data Protection Working Party, Opinion 4/2007, p. 18, by this, the term of "pseudonymous data" is diluted in that extend, that distinction with "anonymous data" is undermined, while equalizing "pseudonymous" and "anonymous data" when it come to one-way encrypted data.
[51] Article 29 Data Protection Working Party, Opinion 4/2007, p. 18.
[52] Ibid, p. 15, 16.
[53] Ibid, p. 16.
[54] Ibid.

data is to be seen as part of a dataset, that is linked to a data-subject in a whole and may even facilitate re-identification.

Within the CHIC project, as outlined above already, various types of data will be used. This data is not completely specified at the moment, so a decision on single case basis is not possible right now. However, of considerable importance in tending to reduce the possibility that data may be re-linked, is not only the technical way de-identification was originally achieved (e.g. through full or partial anonymisation, with or without aggregation or perturbation), but steps taken thereafter to strictly control access, penalize any misuse, etc. Here organizational and legal measures, including the use of binding contracts to establish a network of trust, have a vital role to play in allowing the data to be regarded as de facto anonymous. The measures envisaged in this regard for CHIC, including the use of an independent intermediary (CDP) to enforce the relevant contractual framework, will be discussed in Chapter seven.

Concerning imaging data personal linkage might depend on the outline of the data itself or added metadata as well. Even annotations to data might help for re-identification. Right now, one can doubt whether model/hypermodel configuration parameters could be seen as personal data, though at this stage it can not to be excluded. An important fact to be taken into account is, that one consortium partner indicated the need to process pseudonymized data for possible re-identification, that will lead to the conclusion, that personal data is to be used within the CHIC project. Re-identification within a hypermodel envisaged might follow the amount of data besides classic personal identifiers too. A detailed analysis of each data set will be carried out, commencing in Deliverable D.4.3.1, due in M14, and added to and updated subsequently.

5.2.2.2 General requirements for the legal processing of personal data

A number of different general requirements, in addition to the specific legal ground on processing personal data, can be found under Directive 95/46/EC.[55] These requirements include in particular the need for “purpose limitation”, “proportionality” of data use, “transparency”, “security” and “control” while processing personal data.

5.2.2.2.1 Purpose limitation

The first general requirement for the processing of personal data is its limitation to the original purpose of its collection. Art. 6 b) Directive 95/46/EC states in this regard, that all “personal data must be: b) collected for specific, explicit and legitimate purpose and not further processed in a way incompatible with those purpose”. This is further explained in Recital 28 of Directive 95/46/EC. As to

[55] See for example art. 6 of the Data Protection Directive.

the criteria of a legitimate processing, its conditions differ depending on the legal ground and it is discussed below under specific requirements of processing data.

The purpose limitation itself requires the data to be collected specific and explicit to the purpose of processing in question. An exemption is expressly mentioned, however, for the "further processing of data for historical, statistical or scientific purposes [in case] Member States provide appropriate safeguards" under 6 b) Directive 95/46/EC. The purpose limitation principle has two components: on the one hand, the data controller must specifically inform the data subject of the purposes for which data are being collected, and on the other hand, once they have been properly collected, the data must not be used for further purposes incompatible with the original purposes. In general the further processing of data will only be found to be compatible if it is closely connected to the original purpose[56].

First of all, the purpose of data processing should be clarified. Applied to medical research on health data, two main situations may be distinguished. On the one hand, personal data could be collected as a preliminary work just for the medical research in question. Here the precondition would be, that the research is made as concrete as possible, so as to satisfy the requirement of a specific and explicit purpose. This applies to the aim of the medical research as well as to the methods planned to be used in performing it. It is doubtful though, whether this criterion should be applied as strictly as in the field of commercial data processing for example. After all, it is inherent to medical research on health data that it may expand into previously unthought-of fields of data use. One purpose of research in general is to find new purposes and methods, for instance. Nevertheless research starts from established milestones that have to be taken as providing the purpose for subsequent research, and which should be defined to be specific and explicit.

On the other hand medical research could make use of personal data, that had previously been collected for other purposes, such as in many cases the direct treatment of care provided to a patient for the particular illness they are suffering from. Medical research as part of scientific research may benefit from the Directive's exemption (from the purpose limitation principle) for this kind of further processing of personal data, provided the relevant Member State has implemented appropriate safeguards measures into national law. This will be relevant for medical research on EHRs provided by physicians, or personal data collected in previous and distinct research projects, for instance. Within CHIC project data that is derived from previous clinical treatment will be used. Concerning the purpose limitation, this is an extension to its original purpose, the data is collected for. In general the original purpose will limit the legitimate processing of data, for scientific research an exemption

[56] Kuner, European Data Protection Law, rec. 2.90.

applies though. This exemption found both under Directive 95/46/EC and its national transformations as seen in the six Members States where the CHIC partners are established will serve as a legal basis for further processing of personal data within CHIC project.

5.2.2.2.1.1 Data reuse for research under the Data protection Directive

In the age of information technology, there is an ever-increasing demand for patient health data for 'secondary purposes', that is, uses not related to the treatment and care of the patient.[57] With the increasing potential in data analytical tools, new discoveries are possible when existing data is mined. In medical research for instance, data collected during past treatment of patients could be revisited in order to discover new outcomes and variables. However, secondary use of data may have implications in terms of privacy, and abuse could lead to unintended consequences. Generally, data processing beyond the purpose of collection is permissible under the Data Protection Directive if Member States institute suitable safeguards, and such further processing is not incompatible with the original purpose.[58] In practice, different approaches have been adopted by Member States to ensure data privacy remains safeguarded in the context of secondary purposes such as research.

As explained above, Art 6 (1b) of the Directive contains provision relating to the reuse of data for research provided that safeguards are in place. However, it remains uncertain though what these safeguards should consist in. The Directive here does not provide a specific privacy standard that has to be met when processing sensitive health data for secondary research purposes. In this way it leaves significant interpretational latitude on this matter. However, the Article 29 Working Party has recently provided guidance at European level to enhance and bring legal certainty to the application of the purpose limitation principle, including in relation to the further processing of data for research purposes.[59] The Opinion also outlines factors that should be considered when doing a compatibility assessment for secondary use of data. In its analysis the Working Party notes that the purpose limitation principle consists of two elements or building blocks – that personal data must be collected for specified, explicit and legitimate purposes (purpose specification) and that such personal data shall not be further processed in a way that is incompatible with those purposes (compatible use).[60] This principle has a direct bearing on data reuse.

To determine compatibility, a case by case assessment is necessary, and common factors to consider as stipulated by the Working Party include:

[57] Marc Stauch, "The Draft Data Protection Regulation and the secondary use of patient data for research: prospects and concerns", Journal of Professional Negligence, vol. 29,No 2 2013

[58] See for example Art 6 (1b) of the Directive.

[59] WP Opinion on purpose limitation. See also WP opinion on the PSI

[60] Ibid

a. the relationship between the purposes for which the personal data have been collected and the purposes of further processing;

b. the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;

c. the nature of the personal data and the impact of the further processing on the data subjects;

d. the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[61]

Regarding further use for historical, statistical or scientific purposes, these have been adjudged as compatible with initial purpose of data processing, as long as the controller implements appropriate safeguards, and in particular, by ensuring that the data will not be used to support measures or decisions regarding any particular individuals. Appropriate safeguards could thus, in principle, serve as 'compensation' for a change of purpose or for the fact that the purposes have not been specified as clearly in the beginning.[62] This might require technical and /or organizational measures to ensure functional separation (such as partial or full anonymisation, pseudonymisation, and aggregation of data), privacy enhancing technologies, as well as other measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals.[63]

5.2.2.2.1.2 Data reuse under the proposed General Data Protection Regulation

Under the proposed Regulation, processing of personal data for other purposes shall only be 'allowed where the processing is compatible with the collection purposes, in particular where the processing is necessary for historical, statistical or scientific research purposes'.[64] If the purpose is incompatible with the initial purpose, consent of the data subject for this purpose is required. In addition and if consent cannot be obtained, processing may be legitimate if European law or national Member State law provides legitimate grounds. Furthermore, the Regulation addresses health data processing in Art 9. Processing is legitimate if the patient has given informed consent (Art 9 (2a)), or processing is necessary for health (Art 9 (2h) and Art 81) or scientific (Art 9 (2i) and Art 83) purposes.

A closer look at Art 81 and 83 of the Regulation shall be taken. Art 81 outlines the legitimate processing of health data under the regulation. Health data is defined as 'in particular all data pertaining to the health status of a data subject; information about the registration of the individual

[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Draft Data Protection Regulation, Recital 40.

for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test'. The legislator states that processing of personal health data deserves higher protection. It may be 'justified due to a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare'. Data subjects shall have access to their personal data concerning health, as may be contained in personal health records, diagnosis, examination results, and assessments by treating physicians etc.

Processing of health data is legitimate under the Regulation for 'the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies', Art 81 (1a), or 'reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices', Art 81 (1b). Public health means all elements relating to health, namely 'health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality'. Data processing on the grounds of public interest shall not result in the processing of personal health data by third parties.

It is debatable whether data processing for clinical care and clinical research processing, as will be performed in the CHIC project, is covered by Art 81 (1a) or (1b). This would be the case, if the project is carried out for the purposes of preventive or occupational medicine or to improve medical diagnosis. Since the CHIC project is especially designed to optimize the development of hypermodels to be used in the diagnosis and treatment of cancer, the aim might be said to improve the efficiency of clinical care as well as research, i.e. a dual purpose of the project could be identified: it aims at optimizing future medical treatment, but at the same time feeds research results back to clinical care

systems to optimize present medical diagnosis. For this reason, data processing carried out in the CHIC project may well be considered to be covered in part by Art 81 (1a) in addition to the requirements of Art 83 of the Regulation. Accordingly, data processing within the project would then need to comply with both provisions of the Regulation. At present, the detailed rules within the relevant provisions remain subject to ongoing discussion and reform, but it is clear that their final conception will be of vital significance for the manner in which the data privacy framework in CHIC is developed. Accordingly, the present legislative process leading up to the adoption of the regulation will be subject to intense and continuing monitoring from LUH as the project unfolds.

A further point, at least as the draft Regulation stands in its present form, is that the Commission will be invested with powers to further specify the criteria set out in Art 81 and 83 through delegated acts: see Art 81(3), 83 (3) and 86 of the draft Regulation. Again, as regards the putative exercise by the Commission of these powers, this is a matter that requires ongoing monitoring to ensure the proposed health data processing within the CHIC project remains compatible with the relevant rules.

5.2.2.2.2 Proportionality

The next principle of processing personal data is the test of “proportionality”. Under art 6 c) Directive 95/46/EC this principle is described as meaning that personal data must be “adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed”.

First of all, the data must be adequate to the purpose, which means the data needs at least to facilitate the purpose aimed at in processing the data. Therefore everyone conducting medical research on personal data is obliged to show what benefit the use of that data will potentially produce. Given the difficulties for scientific research in general, mentioned above, the researcher will have to specify, by reference to the present state of scientific knowledge in the area, that his research hypothesis, and the method chosen for testing it, is plausible and prima facie requires the processing of personal data.

Next the personal data needs to be relevant to the purpose. Relevance as an aspect of proportionality pertains to the necessity of the given measure, when compared to the purpose aimed at. The principle of “relevance” is complied with only, as long as the purpose cannot be achieved by adopting other measures that are less burdensome to the interests affected. Applied to medical research this means that an accurate investigation should confirm that the effectiveness of the research will indeed depend on the use of personal data. Here, as an intermediate possibility, it might be shown that for performance of the medical research pseudonymized data is sufficient; if

that is so, then proportionality would require the use of such merely indirectly identifiable data (albeit, as discussed earlier, it is still personal data) in preference to directly identified data. Data irrelevant to the purpose must not be collected or, in case of being collected must be suppressed[65].The same goes for data, where the use purpose has expired and the data is not required any more[66].

Last but not least the processing of personal data must not be excessive in relation to the purpose. In order to meet the principle of proportionality the purpose needs to be balanced to the harm and infringements to anyone concerned by the processing. As a part of this all appropriate measures will need to be taken to lower the risks to those affected. One measure that could be taken would be to provide for the participation of a Trusted Third Party to limit the actual medical research to the use of the minimum information needed, but to retain the possibility of re-identification in previously defined necessary cases as well.

Even if personal data is allowed to be processed at the outset, this could alter over a period of time. Under art. 6 (1) e) Directive 95/46/EC "Member States shall provide that personal data must be: e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use." The underlying principle is, that all personal data is to be anonymised later on, as soon as the purpose of retaining it no longer requires it to be held in personal form. Concerning the proportionality of data use, on the one hand the improvement of medical treatment and its capabilities is to be seen as an important purpose for data use[67]. On the other hand, personal health data is to be seen as very sensitive, when it comes to privacy of the data-subject. Proportionality within CHIC project therefore will be achieved with safeguard measures only to be described later on.

5.2.2.2.3 Data security

The processing of personal data requires security measures to prevent any accidental disclosure or unauthorised access to the data. Data security is an integral part of data protection that focuses on maintaining the confidentiality, integrity and availability of information. Though much emphasis has been laid on the technical aspect of data security, laws and regulations have contributed immensely in this respect, and mandatory rules have been prescribed when personal data is processed. Art. 17

[65] Article 29 Data Protection Working Party, Opinion 7/2007, p. 6.
[66] Article 29 Data Protection Working Party, Opinion 7/2007, p. 6.
[67] See DOW Part B, p. 3.

(1) Directive, states that "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected." This is also reflected in Recital 46 of the Directive. Read together, it is apparent that the preconditions to be taken into consideration include state of the art security measures. This might be a series of different measures that will function independently or be combined in certain circumstances. When deciding what security measures should be deployed, the key criteria are the fundamental rights and interests of the data-subject and the risk of harm. Systematically all "special categories" of personal data are to be treated as requiring a higher standard of security measures. Therefore medical research given its usage of sensitive health data, faces stricter requirements for securing the processing of personal data.

As Recital 46 of the Data Protection Directive points out, the duration of time for which the data are to be held will also be a relevant factor, as the level of security that can be guaranteed depends inter alia on technical developments in the computerized industries. Here again, as with the criterion of anonymisation, data protection is subject to the underlying time scale in terms of its interpretation. Taking into account that medical research is often designed as a process that will subsist for a longer period of time, the time scale might be an important factor, demanding particular vigilance on the part of the data controller to ensure that security remains adequate in the light of new techniques for processing data. The same Recital also requires that these appropriate technical and organizational measures shall be taken, both at the time of the design of the processing system and at the time of the processing itself (a 'privacy by design' approach).

Under recital (25) of the Directive "[…] the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out." According to this, security is achieved through obligations imposed on the data controller. In the event that personal data is needed for medical research, the use of a Trusted Third Party may be one of these measures. In addition, it may be useful to think about contractual penalties as well as to appoint a "personal data protection official" as foreseen under art. 18 (2) Directive 95/46/EC. The desirability of such an approach has recently been confirmed by the Article 29 Working Party in its Opinion on purpose limitation where it comments:

"Among the appropriate safeguards which may bring additional protection to the data subjects, the following could be considered:

- taking specific additional security measures (such as encryption);

- in case of pseudonymisation, making sure that data enabling the linking of information to a data subject (the keys) are themselves also coded or encrypted and stored separately;

- entering into a trusted third party (TTP) arrangement in situations where a number of organisations each want to anonymise the personal data they hold for use in a collaborative project;

- restricting access to personal data only on a need-to-know basis, carefully balancing the benefits of wider dissemination against the risks of inadvertent disclosure of personal data to unauthorised persons. This may include, for example, allowing read only access on controlled premises. Alternatively, arrangements could be made for limited disclosure in a secure local environment to properly constituted closed communities. Legally enforceable confidentiality obligations placed on the recipients of the data, including prohibiting publication of identifiable information, are also important. It is important to note that in high-risk situations, where the inadvertent disclosure of personal data would have serious or harmful consequences for individuals, even this type of access or restriction may not be suitable."[68]

At the same time, the Data Protection Directive itself does not specify what constitutes appropriate level of data security. It merely states the legal requirement to be met, leaving the implementation approach to Member States and data handlers - controllers/processors. This indicates that there is no "one size fits all" solution to information security on European level already. Arguably at least, access control and data logging might be expected,[69] even if their implementation in practice is unlikely to ever provide perfect security.[70] As also noted by the Article 29 Working Party Opinion on purpose limitation, when it comes to the use of sensitive data, one might also consider the option of not transferring the data to the researcher, but merely allow him to have access to the data requiring "physical presence and in-person analysis at the site where the data is hosted"[71].

5.2.2.2.3.1 Security under national law

The requirement of data security has been implemented nationally in various forms such as in Section 9 of the German Federal Data Protection Act (BDSG), the Danish Executive Order on Security, Article 16 of the Belgian Privacy Act, etc. Arguably, the expectation that member states would

[68] Article 29 Working Party, Opinion 03/2013 on purpose limitation, wp 203 [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf], at p. 32.

[69] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), pp. 1756.

[70] Ibid, p. 1757.

[71] Ibid, p. 1770.

provide the necessary guidance was the reason why no reference was made to any concrete security standards in the Directive. Most national implementation of the directive followed this approach, but member states have gone further in providing guidance and recommendations on a number of occasions. The Belgian DPA has for instance, issued three different documents/guidelines on information security.[72] The German Federal Data Protection Act equally defines eight specific data security goals in the annex to section 9.

A common feature in all these recommendations is that personal data handlers must have a precise data security strategy, including features to forestall and mitigate potential threats to personal data being processed without authorization, which strategy should be constantly reevaluated. This entails undertaking a risk assessment of the proposed data processing, and a documentary approach to protective measures. Technical measures generally will include measures such as data encryption, data segregation, data destruction, access control, user authentication, access logs, audit trail, backups, etc., which are geared towards the prohibition of unauthorized login and access to data.[73] Where data is transmitted through a network, there will be a need too for technical safeguards to protect the network from intrusion from virus and malware through the use of VPN, firewalls, antivirus, intrusion detection/prevention systems. Security incident management and recovery plan should also be defined and documented in the technical aspect of the information security.[74] A number of recommendations have made reference to existing information security standards such as the ISO/IEC 27000 series. The German Federal Office for Information Security developed the "IT-Grundschutz Methodology" based on ISO 27001.[75]

Organizational measures indicate a defined responsibility and management process regarding data security as integrated into the functioning of the organization or infrastructure. This includes securing the physical security of the premises and systems where person data is being processed. It should be noted that there is no strict definition of what amounts to state of the art in information security. It is an open-end approach. However, reference to well-recognized standards such as the ISO 27000 series, may be a persuasive factor when deciding whether an implemented security measure is of state of the art. Currently, there is no harmonized framework of information security standards in Europe.

[72] W. Nauwelaert, "The Belgian Privacy Commission's New Guidance on Information Security", World Data Protection Report, Vol. 13, No. 5, 2013

[73] Martin Meints, "The Relationship between Data Protection Legislation and Information Security Related Standards", http://link.springer.com/chapter/10.1007%2F978-3-642-03315-5_19#page-1

[74] Ibid.

[75] Ibid.

Various DPAs have published distinct documents and procedures to guide those using personal data for health research, which in most cases address the general data protection issues without specific emphasis on data security. Here the practice of two data protection authorities, though for countries not directly concerned in the CHIC project, may be cited as offering useful indicative guidance. First, the Irish Data Protection Commissioner's guidelines on research in health sector for example, focus on data protection requires, but only make reference to the security aspect by indicating the importance of putting in place appropriate safeguards such as anonymisation/pseudonymisation and access control mechanisms.[76] Secondly, the Danish Data Protection Agency for its part maintains a notification and authorization scheme where the any research involving individuals' sensitive information must be authorized by the Agency prior to the data processing.[77] In this scheme, a number of conditions, in addition to the general provisions of the data protection law, must be observed when conducting the research project, including but not limited to:

a) Facilities used for storage and processing of the data must be organized and fitted up in order to prevent unauthorized access.

b) Data processing must be organized in such a manner that data are protected against accidental or unlawful destruction, loss or impairment.

c) If results from the project are published, this must be done so that it is impossible to identify individual persons.

d) Identification data must be encrypted or replaced by a code number. Alternatively, all data can be stored encrypted. Encryption keys, code keys etc. must be stored securely and separate from the personal data.

e) Access to project data must only be obtained through the use of a confidential password.

f) If data identifying individuals are transferred over the Internet or other external network, necessary security measures must be taken to ensure that the data do not come to the knowledge of any unauthorized third parties. As a minimum, the data must be encrypted during transmission.

g) When using internal networks, it must be ensured that unauthorized persons are unable to obtain access to the data.

h) Storage media, safety copies of data etc., must be stored securely and under lock and key to prevent unauthorized access.[78]

[76] http://www.dataprotection.ie/viewdoc.asp?DocID=1091

[77] Datatilsynet, "Private research and statistics projects", http://www.datatilsynet.dk/english/health-research-and-statistics-projects/private-research-and-statistics-projects/

[78] Datatilsynet, "Requirements of clinical drug trials, clinical testing of medical equipment, and mandatory safety monitoring of medical products and medical equipment, in accordance with the Danish Act on Processing of Personal Data", http://www.datatilsynet.dk/english/health-research-and-statistics-projects/the-medical-products-and-medical-device-industry-etc/requirements-of-clinical-drug-trials-clinical-testing-of-medical-equipment-and-mandatory-safety-monitoring-of-medical-products-and-medical-equipment-in-accordance-with-the-danish-act-on-processing-of-personal-data/

In addition to guidelines provided by such national DPAs, the Article 29 Working Party has, as noted above, recently provided helpful clarification of security mechanism when conducting health research with personal data in its opinion on purpose limitation.[79] While this opinion has no binding force, it provides a valuable source of best practice and practical application on the subject. In essence, it provides that all relevant circumstances and factors must be taken into account when deciding what appropriate safeguards to implement in a research involving personal data. Functional separation which is a measure to ensure that data used for research purposes are not used to 'support measures or decisions' that are taken with regard to the individual data subjects concerned (unless specifically authorized by the individuals concerned) could be introduced in this regard to guarantee the security of the data.[80] The use of anonymisation (partial or full, depending on individual cases), complemented with other safeguards such as encryption, appropriate key management including the use of trusted third parties, access restriction, and legally enforceable confidentiality obligation have been suggested by the Working Party.[81]

Further guidance on what are appropriate technical and organizational measures are provided in section 9 of the Council of the Europe committee of ministers on the protection of medical data Recommendation No. R (97) 5.[82] In essence, the following measures should be taken:

a. to prevent any unauthorised person from having access to installations used for processing personal data (control of the entrance to installations);

b. to prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);

c. to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (memory control);

d. to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (control of utilisation);

e. with a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of identifiers and data relating to the identity of persons, administrative data, medical data, social data and genetic data (access control);

[79] Art. 29 Working Party, Opinion on Purpose Limitation, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[80] Ibid.
[81] Ibid.
[82] http://www1.umn.edu/humanrts/instree/coerecr97-5.html

f. to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);

g. to guarantee that it is possible to check and establish a posteriori who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction);

h. to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport);

i. to safeguard data by making security copies (availability control).

Applied to the CHIC project, security measures should thus lay special emphasis on access control and all technical aspects necessary to secure full protection of the data within the model repositories from the risk of any unauthorised processing of any kind. At the moment it can be doubted in this regard, whether security measures offered by a cloud infrastructure (whether public or private) will be suitable to use given the acute sensitivity of the data at issue in CHIC. This is the more so in the light of recent revelations of the inherent vulnerability of networked data even when encrypted (as discussed in Chapter 7). At the same time, this is ultimately an empirical question that will need to be kept under review and revisited in the light of overall technical developments and experience gained with the general social usage of the relevant technology.

5.2.2.2.4 Transparency

Transparency consists of various rights of the data-subject. A major part is the data-subject's right to information and access to the information processed about him. Provisions differ according to whether the information is collected directly from the data-subject himself, or not. Art. 10 Directive 95/46/EC applied to the former case, and art. 11 to the latter. These rights are clarified under recital (38), stating “whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection.“ Recital (39) adds: “Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party.” So in principle the data-subject has to be informed about the identity of the controller, purpose of the processing and his rights to obtain information and to rectify. In medical research this might cause difficulties because of the number

and the age of the data-sets. Therefore art. 11 (2) Directive states an exemption, "Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards."[83]

Out of this recital an exemption concerning medical research limits the efforts required to make processing transparent, in cases where huge number of data-subjects are involved. As a compensatory measure again a Trusted Third Party might be seen as desirable to secure the data-subject's interest to privacy. By enhancing data security, the correlative need for transparency and control by the data-subject himself arguably becomes less necessary.

The same goes for the data-subject's right to access the data stored and processed about him. In principle it is the right of the data-subject to ask for information about the personal data about him pursuant to art. 12 a) Directive 95/46/EC. If so, he should be given, "without constraint at reasonable intervals and without excessive delay or expense - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1)." At the same time, an exemption removes this right to access in cases of scientific research. In this regard art. 13 Directive 95/46/EC stipulates as follows: "2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics."

Concerning CHIC project it will depend on the amount of data-subjects and the duration of time from its collection, whether information it to be regarded as disproportionate. Of the data providers indicated that its retrospective data has involves a large number of subject (about 4500) and has been collected over 15 years back. For such data, the need for information and access may no longer be envisaged. In case data-subjects already gave their consent for medical research on their health data, information is to be regarded as not necessary anymore.

[83] See also Recital 40

5.2.2.2.5 Control

Control, based on transparency, on the one hand concerns the right of the data-subject himself, which comprises the right to rectify the personal data, or to require the personal data to be erased or to be blocked, art. 12 b) Directive 95/46/EC. This is further outlined under recital (41) "Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;" At the same time it has to be admitted, that in practice due to the exemptions referred to, the desired transparency, and control by the data-subject are often limited or even excluded.

On the other hand, and particularly in the light of this last factor, control by third parties becomes more relevant. The internal control suggested under art. 18 (2) Directive 95/46/EC is that the data controller "appoints a personal data protection official". However, this is to be seen as a partial response only. In all other cases there is the obligation to notify the supervisory authority under art. 18 Directive 95/46/EC: "1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes."

5.2.2.3 Specific requirements for legitimacy of processing personal data

Legitimacy as a specific requirement to process personal data can be divided into two limbs. On the one hand, consent of the data-subject is capable to give permission for the performance of processing. On the other hand, a legal ground may mandate such processing under law without a decision of the data-subject.

5.2.2.3.1 Consent

5.2.2.3.1.1 Consent under Directive 95/46/EC

A legal ground to process personal data, in accordance with the autonomy of the data-subject and his fundamental rights, is first of all the consent of the data-subject himself. In art. 2 h) Directive 95/46/EC a consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". Out

of this requirements for a consent to be found in general are the consent to be given “freely” and under “specific” and ”informed” conditions. The insistence on the need for consent to be given “freely” excludes any expression of wishes based on violence executed on the data-subject or fraud to gain the consent. The latter is added to by the requirements that the consent be specific and informed. The first of these aspects may be seen in systemic terms as a reference to the purpose limitation principle as part of the general requirements of processing personal data. Building on this, an informed consent requires a positive knowledge about the planned processing of personal data as set out by the specific purpose as a *sine qua non* (causal) basis for the consent.

The general requirements stipulated under art. 2 h) Directive are added to by art. 7 and 8, depending on the kind of personal data to be processed. The general provision to legitimate the processing of personal data by the data-subject's consent is to be found under art 7 a) Directive 95/46/EC. This provision provides a legal ground for the processing of personal data based on an “unambiguously given […] consent” by the data-subject. However, this provision is displaced by art. 8 (1) Directive 95/46/EC for “processing of personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, and processing of data concerning health or sex life”. In the event that a series of different information is to be processed, the provision governing the most strict element has to be applied, as long as the data are to be processed together. While medical research might be based both on general data like sex or age and on data about diseases and health conditions of the patient, the requirements under art. 8 Directive 95/46/EC will thus have to be met for all. According to art. 8 (2) a) Directive 95/46/EC consent concerning the processing of special categories of personal data may serve as a legal basis if “the data-subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that prohibition referred to in paragraph 1 may not be lifted by the subject's giving his consent”. In this context it could be argued, that the main criteria of consent to the processing of special personal data is that the consent be “explicit”. However, the wording is less clear than may appear at the first glance. On the one hand the wording of “unambiguous” and “explicit” of art. 7 and 8 Directive 95/46/EC leads to the conclusion, that “explicit” requires a more precise reference to the purpose of the data processing, as expressed by the data-subject himself. On the other hand it is doubtful, whether “unambiguous” should be regarded as the outcome of a consent to be given “explicitly”. In that sense “explicit” would be the method and “unambiguous” the outcome, rather than being alternatives. Systematically the interpretation is no clearer. On the one hand, it may be argued that, given the whole provision of art. 8 Directive applies to more sensitive data compared to art. 7, the requirements similarly need to be more strict. On the other hand, in medical research it often is difficult to inform the data-subject in detail about the proposed data use at the beginning of the

research. Here possibly, "specific" could be seen as a synonym for "explicit" and as far as no written form is required by the word "explicit"[84]; indeed the explicit consent under art. 8 (2) a) Directive 95/46/EC is sometimes described as "specific". An informed consent, making the subject of the key intentions of the researchers with regard to how the data will be used to achieve the research goals, and what the implications may be for the subject, should lead to an explicit consent at the very least.

5.2.2.3.1.2 Consent under national law

Here, for CHIC, we focus on the implementing laws of the countries of the clinical data providers, which will provide clinical data of patients to the project. For the other partners it is apparent that, absent any individual contact with the patient (which should be conclusively ruled out by the fact they only see securely pseudonymised data), obtaining consent directly is not an option.

First, in relation to KU Leuven, Belgian law in line with the Directive requires sensitive data to be treated under special regulations under art. 7 (1) of the Belgian Law on Privacy Protection: "The processing of health-related personal data shall be prohibited" and only allowed under sub-paragraph 2 of art. 7. In addition, and here differently to the Directive, consent has to be in written form under art. 7 (2) a) Belgian Law on Privacy Protection. As regards scientific research, consent might be seen as the only possibility to process health-related data under Belgian law by persons other than physicians and health-related personal, according art. 7 (4): "Health-related personal data shall only be processed under the responsibility of a health professional, except for the written consent of the data subject or if the processing is necessary for the prevention of a concrete danger or for the suppression of a specific criminal offence".

Secondly, as applicable to UNITO, the Italian Personal Data Protection Code section 23 (3), provides that any consent "shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13 and in writing if the processing concerns sensitive data."

Third, under the German Federal Data Protection Act relevant to USAAR, health data is dealt with under "Special categories of personal data" that "shall mean information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life" under section 3 (9). In principle consent has to be given in written form too, under section 4a (1), but with an exemption to scientific research: "In the field of scientific research, a special circumstance as referred to in subsection 1 third sentence shall be deemed to exist if the defined purpose of research

[84] Article 29 Data Protection Working Party, Opinion 7/2007, p. 9.

would be seriously affected if consent were obtained in writing. In this case, the information referred to in subsection 1 second sentence and the reasons the defined purpose of research would be seriously affected shall be recorded in writing". Additional requirements to be followed when processing "special categories of personal data) are, that "the consent must also refer specifically to these data" under section 4a (3) German Federal Data Protection Act.

To summarize the requirements under national law as they relate to consent as a basis for processing health data for the research envisaged in CHIC, in some member states the consent has to be given in written form. Other member states restrict themselves to a mere use of the wording of the Directive itself. In the case of Germany, while the written form is the default option, a special scientific research exemption to this is also foreseen. Accordingly, it is advised to have consent in written form, even if exemptions might be applicable to medical research, as most of the national implementations require so. Additionally consent in written form is advisable for evidentiary reasons as well. The consent necessary has to be given specifically and special emphasis will need to be put on informing the data-subject about the processing and aims of the medical research and, where relevant, its implications for the data-subject as an individual.

5.2.2.3.2 Processing of sensitive personal data on another legal basis

5.2.2.3.2.1 Processing of sensitive personal data on legal bases under Directive 95/46/EC

In cases the consent of the data-subject is not obtained, or is not obtained in a valid form, the processing of data might nonetheless be possible by reference to a separate legal basis. The potential legal bases in question are to be found both under art. 7 and 8 Directive 95/46/EC, though as regards medical research only the exemptions permitted under art. 8 Directive 95/46/EC will apply as outlined above already.

A first exemption, under art. 8 (2) b) Directive 95/46/EC, applies to "processing […] necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far it is authorized by national law providing for adequate safeguards". A connection with health data is not to be seen at the first glance, though an employer may need information about the employee's health, when it comes to preconditions to work. However, given the very different underlying context between employment and scientific research, this exemption would appear of little or no application to medical research.

A second exemption laid down in art. 8 (2) c) Directive 95/46/EC applies, where the "processing is necessary to protect the vital interest of the data-subject or another person where the data-subject is physically or legally incapable of giving his consent". It could be argued, that medical research

would be in the "vital interest" of the data-subject and its medical treatment as a patient. This interpretation though is curtailed by the provision's wording, requiring that the data subject is "incapable" to give his consent. A further systematic ground for denying the relevance of this provision points to the fact that medical treatment is more specifically regulated by art. 8 (3) Directive 95/46/EC (see below), which may be argued to be of exclusive application

As just foreshadowed, an exemption most appropriate to process personal health data is to be found under art. 8 (3) Directive 95/46/EC, according to which the prohibition of processing personal health data "shall not apply where processing of the data is required for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy." At the first glance this provision may also seem appropriate to cover research, as the latter aims at advancing capabilities in medical diagnosis and treatment. The specific wording of the Directive in this respect is to be seen as rather vague. Seen the medical diagnostic and treatment as part of the health-care system, because of the reference to preventive medicine and the management of health-care services, this purpose of this provision has to be seen for the concrete medical treatment of the data-subject only. This is underlined by the principle of restrictive interpretation of exemptions[85]. Applied to medical research, the purpose is different to medical treatment of the data-subject himself. While medical research aims at to improve knowledge about diseases in general and accidental benefit to the data-subject, any processing of personal data under medical treatment is meant for data-subject's specific health-care only. This interpretation of art 8(3), which denies its application to medical research, has also been taken by the Article 29 Working Party in its 2007 Working Document on the processing of personal data relating to health in electronic health records (EHR).[86]

Accordingly, no specific exemption for medical research can be based directly on the provisions of the current[87] Directive 95/46/EC. Nevertheless an open exemption under the Directive permits Member States to implement further exemptions under national law. Thus, according to art. 8 (4) Directive 95/46/EC and "subject to the provision of suitable safeguards, Member States may, for reason of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority." Hence the question is, whether medical research is to be classified as a "reason of substantial public interest". As

[85] Article 29 Data Protection Working Party, Opinion 7/2007, p. 10.
[86] Article 29 Data Protection Working Party, Opinion 7/2007, p. 16.
[87] This situation is to be changed probably under future European Regulation in data protection.

outlined above, medical treatment depends on advancement in medical knowledge. It may well be regarded therefore as in substantial public interest to improve the quality of medical treatment, and the knowledge that the health-care system is based on. Besides this general argumentation, it is noteworthy that recital 34 of the Directive specifically refers to medical research as an "important public interest, to derogate from the prohibition on processing sensitive categories of data". In conclusion medical research on personal health data may, in cases that consent is not obtained, be based on the national law implementation of an exemption under art. 8 (4) Directive 95/46/EC in the current state. This is also the view of the Article 29 Working Party in its 2007 Working Document, where it at the same time issues a reminder as to the importance of taking necessary safeguards: "Processing of EHR-data for the purposes of medical scientific research…could be allowed…, provided that all these exceptions are in line with the Directive (cf. Article 8 (4) and the corresponding Recital 34: they must therefore be foreseen by law for previously determined, specific purposes under special conditions to guarantee proportionality ("specific and suitable safeguards") so as to protect the fundamental rights and the privacy of individuals".[88]

5.2.2.3.2.2 Processing of sensitive personal data on legal bases under national law

These bases will be potentially relevant to all data processing that will occur in CHIC, i.e. also the processing carried out by the data users partners following provision to CHIC. Accordingly we consider the national law in each member state where a CHIC partner is based. First, under Belgian Law on Privacy Protection, any processing of health-related personal data is allowed under the exemptions of art. 7 (2) only. Like the Directive itself, most of these exemptions do not refer to medical research on health data. The first exemption of potential relevance is to be found under art. 7 (2) d) Belgian Law on Privacy Protection, where processing of health-related data is allowed, "if the processing is necessary for the promotion and protection of public health, including examination of the population." Medical research could be seen as part of protection public health. More clearly and specifically, though, scientific research is recognized under art. 7 (2) k) Belgian Law on Privacy Protection. Under art. 7 (2) processing of health-related personal data is allowed, "if the processing is necessary for scientific research and carried out under the conditions established by the King in a decree agreed upon in the Council of Ministers after advice of the Commission for the protection of privacy." Systematically this leads to the conclusion, that the protection of public health deals with the concrete treatment of the diseases and scientific research covers any processing of health data in a more abstract form. Hence medical research may occur subject to the exemption under 7(2)(k) only. Additional safeguard measures under the Belgian law directly are that "health related personal data shall only be processed under the responsibility of a health professional, except for the written

[88] Article 29 Data Protection Working Party, Opinion 7/2007

consent of the data subject" and the King is to decide, "which categories of persons are to be considered health professionals in the meaning of this law" under art. 7 (4). Last but not least: under art 7 (4) "the health professional and his appointees or agents shall be obliged to secrecy with regard to the processing of personal data referred to in the first section."

In cases where processing of sensitive personal data will fall under Italian jurisdiction, section 26 has to be taken into account. Most of the exemptions requires authorisation by the supervising authority (Garante) under section 26 (4) Italian Personal Data Protection Code. No reference is to be found, that will allow scientific research as an exemption to process sensitive personal data. The only exemption for scientific research data to be processed without the consent of the data-subject in section24 (1) i) does not apply according to the principle of *lex specialis* concerning section 26. This means that "data disclosing health may not be disseminated" without an exemption to be found under section 26 (5) Italian Personal Data Protection Code.

Under the German Federal Data Protection Act, use of data is allowed "for the purpose for which the data was collected" under section 14 (1). Again most of the given exemptions to process special categories of personal data do not apply to medical research on health data. Special categories of personal data are allowed to be processed where "necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort". Safeguard measures are found under section 4d (5) German federal Data Protection Act, which states: "(5) Where automated processing operations present special risks to the rights and freedoms of data subjects, these operations shall be examined before the start of processing (prior checking). Such prior checks shall be carried out in particular:

1. if special categories of personal data (Section 3 (9)) are to be processed, or

2. the processing of personal data is intended to assess the data subject's personality and his/her abilities, performance or behaviour, unless a statutory obligation applies, the data subject's consent has been given, or the collection, processing or use is needed to create, carry out or terminate a legal obligation or quasi legal obligation with the data subject."

Under German law, secrecy is required in processing special categories of personal data, when it comes to "preventive medicine, medical diagnosis, the provisions of care or treatment or the management o health-care services" according art. 14 (6) together with art. 13 (2) no. 7) of the German Federal Data Protection Act.

In the Dutch Data Protection Act "medical research" is not expressly mentioned; however, an explicit

exemption concerning scientific research is provided. Scientific research as a broader term comprises "medical research" as well, with both being undertaken in the interest not only of the data-subject, but also the interest of the people in general and other persons in similar particular circumstances. Two provisions of the Dutch Data Protection Act refer to scientific research concerning "sensitive personal data" on health. First, the most applicable accurate provision concerning processing health data, might be that in the art. 21 (3) b) Dutch Data Protection Act, depending of its interpretation. On the one hand, one could understand the provision as an exemption in processing "other" personal data than intended in art. 16 Dutch Data Protection Act. This is the way it is translated in the unofficial version mentioned above. This interpretation runs into the systematic objection that art. 21 is meant to be an exemption only to art. 16 Dutch Data Protection Act. Accordingly, there would be room for this provision to apply to "other" data. In other words, there is no need to allow the processing of data in exemption to art. 16 Dutch Data Protection Act, given that is not within the scope of the prohibition in the first place. On the other hand, another interpretation of art. 21 (3) Dutch Data Protection Act could be that the provision provides an exemption to processing the data "of others". This is reinforced by a second requirement of the same paragraph. Art. 21 (3) Dutch Data Protection Act, which allows the processing of the data in addition to a medical treatment. This interpretation though is at variance with the need for the processing of data to occur in order for a proper treatment of the data-subject himself. Ultimately, then, it remains unclear what specific cases art. 21 (3) Dutch Data Protection Act applies to.

The second exemption that allows the processing of sensitive personal data without the consent of the data-subject can be found in § 23 Dutch Data Protection Act. In this regard art. 23 (2) c) dispenses with consent where obtaining it proves impossible or would require a disproportionate effort. Further preconditions here, under art. 23 (2) Dutch Data Protection Act, are that the research serves a public interest, the processing of the information is necessary to the research and safeguard measures guarantee that the data subject's privacy is not infringed excessively. A second possibility under § 23 Dutch Data Protection Act is for a special exemption to be granted by the "college" (the Dutch data protection authority), or by law. Additional requirements here are a substantial public interest and that safeguard measures to protect the privacy of the data-subject are taken: § 23 (1) e) Dutch Data Protection Act. An additional safeguard measure under art. 27 Dutch Data Protection Act is the prior notification to the "college", while processing data fully or partly automatically. For scientific research an exemptions from this duty of notification is established by art. 44 Dutch Data Protection Act, if safeguard measures guarantee that the personal data are processed for the research purpose in question only. The Directive 95/46/EC open for the processing of sensitive personal data without the consent of the data-subject only, but Italy seams not to have implemented

this optional exemption when it comes to sensitive data. This should be taken into consideration, when to decide, whether processing will be done with at least additional consent of the data-subject within CHIC project. The same goes for the Belgian implantation that could cause interference with the law concerning the technical partners that could not be regarded as professional healthcare personal. All other national implementations provide for an exemption to process sensitive personal data without the consent of the data-subject, though in some cases additional safeguard measures have to be taken into account. Most of all, an additional safeguard measure is the duty to notify the supervising data protection authority or prior check, when processing comprise sensitive personal data.

5.2.2.4 Parties processing personal data

Different parties might be involved in the processing of personal data. Apart from the data-subject mentioned above already, as the person the data is linked to, two more parties to data processing are defined under the Directive itself. Art. 2 Directive 95/46/EC mentions the "controller" on the one hand and the "processor" on the other. "The controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determine the purpose and means of the processing of personal data" under art. 2 d) Directive 95/46/EC. "The processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" under art. 2 e) Directive 95/46/EC. Controller and processor are distinguished by the way the purpose of the processing is decided. The controller is able to determine the purpose himself (or jointly with others). By contrast, the processor is subordinated to the controller and subject to his directions concerning the processing of personal data. Every other person not involved directly in the processing, is termed a "third party", defined under art. 2 f) Directive 95/46/EC as "any natural or legal person, public authority, agency or any other body other than the data-subject, the controller, the processor and the person who, under the direct authority of the controller or the processor, are authorized to process the data". Last but not least the Directive mentions the "recipient" as being any entity, whether a third party or not, "to whom data are disclosed" under art. 2 g) Directive 95/46/EC.

Last but not least, a further question to be answered is whether the data protection regime only applies where the data subject is still living, or extends to protect the data of deceased persons. Admittedly, the Directive 95/46/EC on its face applies to "natural persons", which has generally been interpreted as covering living persons only. Accordingly, where a patient has died one could argue that this "former" personal data falls outside the ambit of the Directive. On the other hand, it is apparent that results from medical research may have implications for other persons than the

patient such as family members.[89] Thus, depending on the information collected, conclusions might be drawn concerning diseases to be inherited and by this linked to relatives of the persons as well. In single cases it even might be difficult to ascertain, if a data-subject has died. Hence under these circumstances it is arguably preferable to regard all persons as putative data-subjects and for the use of their data be treated as subject to data protection rules.

To understand the controller processor relationship within CHIC project appears to be complicated. Firstly, it has to be distinguished between the transfer of data to the CHIC repositories and then, the use of these repositories during the CHIC project. The clinical partners (data providers) are to be regarded as controllers, while they transfer data to the CHIC repositories.

When the health data is transferred to the CHIC data repository, a first thought might be to think the consortium as a whole will be the controller. This conclusion is not sustainable because of the fact, that the consortium lacks legal personality. However, where one particular partner manages the repositories, one could think of that partner being the controller. The other project partners could then be seen as processors in the sense of Directive 95/46/EC. This argument is forceful because the decision as to which data is to be stored, the way access or anonymised is under control by the partner managing the repository. On the other hand, another interpretation could be that the other partners remain joint-controllers under art 2(d) of the Directive, together with the partner managing the repository. This would be the case, when the repository is open to all CHIC partners without further decision of the managing partner. Ultimately, given the division of responsibilities, with the repository-managing partner responsible for some processing decisions, and the other CHIC project partners for others, this appears the most likely conclusion..

Concerning the CHIC project partners they could be seen as controller, as they provide for a individual legal personality. Additionally, the individual researcher, who is responsible for the CHIC project within the organisation of the project partners, might be regarded as a controller. One argument for the researcher being regarded as the controller is based on the principle of freedom of science as part of their fundamental rights enjoyed by each scientist. From this perspective one may need to distinguish between partners that are universities where researchers are to be regarded as capable to claim this freedom of science, and the other partners that are industrial partners. Their employees should arguably be seen as working on behalf of the legal body only, within the direction of the legal body and part of the organisation. Because of this, they are less likely to be controllers in their own right.

[89] Article 29 Data Protection Working Party, Opinion 4/2007, p. 22.

Furthermore, the controllers will include (as regards the relevant processing in order to ready the data for transmission and the transmission operation itself) the physician who transfers the data to the CHIC repositories. Concerning the technical project partners, these themselves should be regarded as controllers, in so far as they process personal data, e.g. for creating or evaluation of the research outcome.

5.2.2.4.1 Conclusions

In summary, rendering data anonymous would leave them outside the scope of regulation by the Directive 95/46/EC. But what necessary measures are to be taken, so that data may be regarded as anonymous is difficult to decide, because every reasonable possibility to re-link them will keep data personal. In this regard, all aspects of a given dataset must be taken into account, including metadata. Moreover, following the opinion of the Article 29 Working Party, it appears reasonably clear in relation to pseudonymous data, using reversible, two-way encryption, that such data remains personal data in any event. When processing personal data, the general requirements are purpose limitation and proportionality of data use. Most of these requirements are transposed fairly closely (sometimes more or less verbatim) into national law; the same goes for data security, transparency and control as further preconditions for processing personal data. Concerning the processing of sensitive data, exemptions to the prohibition to process are to be found in slightly different terms under different national implementations. Thus “explicit” consent as found under Directive 95/46/EC, which is not necessarily meant to be written, is transformed into a precondition to have it in writing in some of the evaluated countries, albeit not all. According art. 8 (4) Directive 95/46/EC a legal basis for processing sensitive data for medical research purposes could be introduced, subject to the provision of suitable safeguards, under national law. All member states evaluated and implemented such an exemption apart from Italy. However, explicit additional safeguard measures, besides access control and notification to a supervising authority are to be found only in Belgian law, which also requires secrecy obligations for all personnel involved in medical research.

5.3 Processing of personal data outside the territorial application of EU law and the Directive 95/46/EC

In CHIC two of the project partners providing data are based outside the EU, namely UBERN from Switzerland, and UPENN from the US. Accordingly, in this section we provide an analysis of the salient data protection rules, especially as regards the research use of health data, applicable in those jurisdictions.

5.3.1 Legal requirements for processing personal health data under Swiss law

In Switzerland the data protection law is mainly governed by the Federal Act on Data Protection (FADP) of 1992.[90] In addition, further data protection statutes are also found at individual canton level. The rules determining the applicable legal forum, especially as regards entities with a public law dimension, such as universities, are in fact relatively complex. Accordingly, in the prospective case within the CHIC project of data processing to be carried out by the partner from the University of Bern, confirmation will be sought from its legal department as to whether the immediately applicable law is the FDAP or that of the Canton of Bern. In any event the canton-level rules are modelled closely on the federal instrument. Focusing thus for the present on the FADP, its main aim is to protect the privacy and the fundamental rights of persons when their data are processed.

Compared to the EU Data Protection Directive, the FDAP's scope of application is broader, as it covers data on legal bodies as well. Thus according to art 2, para 1 the FADP applies to the processing of (personal) data pertaining to natural persons and legal persons by both, private entities and federal bodies. When it comes to the definition of data, the provision found in art. 3 a) stipulates it as "any information" similar to the Directive 95/46/EC and its member state transpositions. Similarly, personal data is defined in equivalent terms: "personal data (data) [means] all information relating to an identified or identifiable person", but again with no further reference to the way to determine the criteria of "identifiable.

According to art 3 (c), sensitive personal data are data on religious, ideological, political or trade union-related views or activities, as well as on health, the intimate sphere or racial origin, social security measures, administrative or criminal proceedings and sanctions. Accordingly data in the context of medical care and research containing information about the health of the data subject will almost certainly fall under this category under Swiss data protection law. Within the general principles for the processing of data (art 4) it is stated, that personal data must be processed lawfully. The processing must be effected in good faith and must be proportionate. Furthermore it is stated the collection of personal data and in particular the purpose of its processing must be evident to the data subject. In case the consent of the data subject is required, such consent is valid only if it is given voluntarily and based on adequate information. For its part, under art. 3 e) FDAP, processing means: any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data;" Under at. 4 (3) FDAP a purpose limitation principle is to be found, including the statement that, "Personal data may only be processed for the purpose indicated at the time of collection, that is evident from

[90] Unofficial English translation: http://www.admin.ch/ch/e/rs/2/235.1.en.pdf.

the circumstances, or that is provided for by law." The principle of proportionality is set out under art. 4 (2), albeit without further explanation. However, given that proportionality requires the use of personal data to be necessary and reasonable, it appears that wherever possible pseudonymized data should be preferred instead.[91] Similar to the Directive 95/46/EC, the FDAP also provides legislatively for controls to exist over the use by the data controller of the data he has collected. This consists firstly of the control of the data-subject himself. Thus "Any data subject may request that incorrect data be corrected" under art. 5 FDAP. This is added to by public authority control, namely that "The Commissioner maintains a register of data files that is accessible online. Anyone may consult the register" under art. 11a 5 FDAP. This control by the Commissioner is exercised over both public and private persons, pursuant to art. 27 FDAP.

Art. 7 FDAP explicitly refers to data security and required safeguard measures. According to this provision "personal data must be protected against unauthorised processing through adequate technical and organisational measures." The responsibility for laying down measures in detail is left to the Swiss data supervising authority: "The Federal Council issues detailed provisions on the minimum standards for data security. " These provisions refer to Appendix A of ISO 27001, referring to ISO 2002 itself, concerning data security measures[92].All these measures are in common, to prevent unauthorized access to personal data and protect the data against any misuse or unauthorized alteration. The security measures to be taken in a single case correspond to the degree of sensitivity of the personal data processed[93].Transparency is achieved under Swiss law by a right to information according art. 7a (2-3) FDAP, which comprises the duty to notify the data-subject, similar to art. 10 Directive 95/46/EC. An explicit duty to inform the data-subject is found under art. 14, when it comes to sensitive personal data.

According to art 12 FADP, the person processing personal data must not disclose sensitive personal data or personality profiles to third parties without justification (breach of privacy). A relevant justification may be provided by the consent of the data subject, by the law, or by an overriding private or public interest. Such an overriding interest of the person processing the data shall in particular be considered if that person processes personal data in direct connection with the conclusion or the performance of a contract and the personal data is that of a contractual party (art

91 Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, p 5
http://www.edoeb.admin.ch/org/00828/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdX58hGym162epYbg2c_JjKbNoKSn6A--

92 Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, p 9
http://www.edoeb.admin.ch/org/00828/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdX58hGym162epYbg2c_JjKbNoKSn6A--

93 Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, p 9
http://www.edoeb.admin.ch/org/00828/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdX58hGym162epYbg2c_JjKbNoKSn6A--

13 (a)). Accordingly this exemption might cover e.g. the processing of patient data in the course of medical treatment, whereas it would not apply to the processing of data for the purposes of scientific research. However, Swiss data protection law allows for the processing personal data for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics and publishes the results in such a manner that the data subjects may not be identified.

Thus the use of data for the purposes of research by a private entity could be based on the consent of the subject. Furthermore data may be processed for research purposes without the consent of the person concerned when the data are used for purposes not relating to that person and the results are published in anonymised form. As noted, in art 14 the FADP provides for an information duty for the procurement of sensitive data. This duty to inform also applies, when the data are obtained from third parties. The person concerned must be informed at least about the owner of the data collection (a), the purpose of processing (b), and the categories of data recipients, if disclosure of data it is planned (c). If the sensitive data is not obtained from the data subject, the data subject must be informed not later than the storage of the data or if the data is not stored, with their first disclosure to third parties. This duty to inform does not apply if the data subject has already been informed, or the storage or publication of data is expressly provided for by the law, or if information cannot be provided without disproportionate effort.

As well as general data protection law, specific provision has been made under Swiss criminal law to allow the non-consensual transmission of confidential health data for research purposes, subject to safeguards. Thus whereas such a disclosure is prima facie an unlawful breach of professional secrecy contrary to art 321 (1) of the criminal code, art 321 (2) permits this subject to approval by an expert commission. The commission will need to be satisfied that the interest in research outweighs the privacy risks to the data subject and that the obtaining of consent would be disproportionately onerous.[94]

Concerning the transfer of personal data beyond the territory of Switzerland, this is prohibited under art. 6 (1) FADP in general. Exemptions are foreseen for countries that guarantee an adequate and comparable level of protection of personal data. This adequate level of protection is reached because of the ratification of "Bilateralen II", which associate Switzerland with the Schengen-treaty and the Dublin-system. Consequently, one of the legal acts of the EU to be applied in Switzerland is Directive 95/46/EC itself[95]. By this the adequate level of data protection is established *per se* between Switzerland and the EU, and by this serves as a basis for the transfer of personal data from

[94] See: http://www.admin.ch/ch/d/sr/311_0/a321bis.html.

[95] Bilateralen II, Appendix (Anhang) B: http://www.admin.ch/opc/de/classified-compilation/20042363/index.html

Switzerland to every Member State of the EU under art. 6 (1) FADP. By this UBERN, as a CHIC project partner is allowed to both send personal data cross border and receive it when it comes to all project partners located within the EU.

The transfer of personal data to countries that offers no adequate level of data protection is allowed only in case sufficient guarantees are given to protect personal data abroad or the data-subject gave his consent for the transfer. These might be the only exemption, when it comes to a transfer of data to UPENN that is located in the United States.

5.3.1 Legal requirements for processing personal health data under US law

In the United States, the use of health data for research purposes is potentially governed by two distinct but overlapping regimes: the first is found under the Health Insurance Portability and Accountability Act (HIPAA) 1996, whose relevant data privacy provisions ('Privacy Rule') of which entered force in 2003.[96] This covers the processing of health data in general (including for research use). In the second place, there are federal level regulations, agreed in 1991 by a number of federal agencies involved in research on human subjects, which have come to be known as the 'Common Rule', and which lay down protections, inter alia, in relation to the use of information pertaining to such subjects.[97]

First, as regards the Privacy Rule, this applies to personally identifiable health information held by so-called 'covered entities', broadly organizations and businesses involved in financing, brokering or providing health care. This will include hospitals, insofar as they transmit health information electronically in connection with certain financial and administrative transactions. For the purposes of the Privacy Rule, such health information is known as "protected health information" (PHI), and it may not be disclosed or used unless this is allowed for under the Rule. "Disclosure" and "use" are defined widely, with the effect that "a covered entity cannot look at or "touch" protected health information within its own organization, or divulge or provide access to the information to any outsiders, except as the Privacy Rule permits or requires".[98] In principle PHI can include information as to deceased patients; however in this analysis we shall focus on the rules as they pertain to the PHI of the living.

[96] US Department of Health and Human Services (HHS), *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82798 (Dec. 28, 2000) and 65 Fed. Reg. 82944 (Dec. 29, 2000), codified in Title 45 of the Code of Federal Regulations (CFR) Parts 160 and 164.
[97] HHS, Protection of Human Subject regulations at 45 CFR Part 46
[98] Ibid.; see also Gosfield, A (ed) Health Law Handbook (Current / 2011 Edition), § 8:7. HIPAA privacy rule framework.

The Privacy Rule does not by contrast apply to the use or disclosure of de-identified health information. In this context, two alternative methods for achieving such de-identification are presented within the rule itself.[99] The first is a 'check-list' approach (also known as the 'safe harbor' approach), which involves stripping datasets that contain health information of 18 specified identifiers. The latter include the patient, relatives or employer name and other associated individuating information (such as phone numbers, email addresses and social security or health insurance numbers). Further, all elements of dates except for the year (and for patients over 90 years, not even that) should be removed, as should geographical addresses apart from the first three digits of the regional zip code (provided the region has more than 20,000 inhabitants). Further, the covered entity must not have actual knowledge that the remaining information could be used alone or with other information to re-identify the patient.

The second and alternative route for the covered entity to use or disclose de-identified health information is that, though not all specified identifiers are removed as above, it obtains expert certification from a statistician to the effect that, applying generally accepted statistical and scientific principles, there is only a 'very small risk' of a recipient using the information, alone or with other reasonably available information, to identify the subject of the information. Importantly, though (both here and when using the 'safe harbor' approach), the covered entity may itself retain a coded link allowing it to re-identify the subject, provided the code is randomly generated (and so contains no clues itself to the subject's identity) and this is not disclosed to any other party.[100] Restated in European terms, this means that securely pseudonymised health data will also count as de-identified information (and hence not PHI) under HIPAA.

As noted the proposed use of health information in the US must also be in line with the Common Rule, which establishes more general protections for human research subjects and applies to most such research carried out in the US. The two key definitions under the Common Rule, determining its scope of application, are "research" and "human subject". The first is defined as a systematic investigation, testing and evaluation, designed to develop or contribute to generalizable knowledge, and expressly includes research development (i.e. the types of activity classified by HIPAA as 'preparatory to research').[101] Secondly, a human subject is "a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual or (2) identifiable private information...."[102]

[99] The methods are detailed in 45 C.F.R. § 164.514 (a)-(c).
[100] NIH, Protecting Personal Health Information in Research, note 5 above.
[101] HHS Protection of Human Subject regulations at 45 CFR 46.102(d); the full regulations are available at: [http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html].
[102] Ibid., 45 CFR 46.102(f).

In the case of non-interventional research where the researcher does not obtain data directly from the subject, the research will only count as "human subject research", and hence come within the Common Rule (or its FDA variant), if it involves the use of identifiable private information. As to this, the Rule – in contrast to the HIPAA Privacy Rule – does not use a check-list, but rather an open-ended approach (similar to the EU Data Protection Directive, but arguably somewhat less strict[103]): 'Individually identifiable' is defined to mean that "the identity of the subject is or may readily be ascertained by the investigator or associated with the information"; and 'private' that the individual "can reasonably expect [the information] will not be made public (for example, a medical record)".[104]

However, if the research will indeed make use of 'identifiable private information' there are two key requirements to be met under the Common Rule. These are first, that the subject gives full informed consent, and secondly that the research project is reviewed and approved by an Institutional Review Board (IRB). In addition, the research institution must be able to document its compliance with the regulations.[105] In certain circumstance an IRB may waive the requirement of informed consent. This may occur inter alia where the IRB finds that: (1) the research involves no more than minimal risk to the subjects; (2) the waiver will not adversely affect the rights and welfare of the subjects; (3) the research could not practicably be carried out without the waiver; and (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation.[106]

Transferring personal health data fall under the same Privacy Rules, regardless of whether the recipient is located within the United States or not.[107] This transfer has to comply with the above mentioned requirements about disclosure of personal data. For the non-clinical data from computational analysis that UPENN will make available to CHIC, it will be further investigated if the data qualify as PII for HIPAA to apply.

[103] As noted, for it to count as identifiable, the subject's identity must be 'readily' ascertainable by the investigator, or associated (by another) with the information. This on the face of it allows information to be considered unidentifiable even if, with moderate technical know-how, it could be linked back to the subject: see Greely, H, (2007) 8 Ann. Rev. Genomics Hum. Genetics (2007) 343–64.

[104] 45 CFR 46.102(f).

[105] F. Cate, Protecting Privacy in Health Research: The Limits of Individual Choice (2010) 98 Cal. L. Rev. 1765, 1784.

[106] 45 C.F.R. § 46.117(c); HHS, Protecting Personal Health Information in Research, note 11 above, 15.

[107] Frequently Asked Questions about HIPAA, http://www.ama-assn.org//ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/frequently-asked-questions.page

5.3.2 Safe harbor requirements concerning cross border transfer of personal data to the United States

Within the CHIC project, there is the potential for some clinical data subsequently to be required by UPENN in the United States to fulfil its task of building multiscale cancer models. Our present understanding is that this data will have been irreversibly anonymised by the data providers prior to transfer. However, if this position should change later in project lifetime, and UPENN require personal data, it is important to already consider the implications. One of the underlying objectives of the EU Data Protection Directive is to ensure that personal data lawfully processed within the EU/EEA remain within the area of jurisdiction of EU law in general. By contrast, the transfer of data to third (i.e. non-EU) countries is allowed only where an exemption applies, and subject to safeguard measures being taken. In view of the legal complications (outlined below) it will be important to clarify as early as possible the precise kind of data that it is envisaged that UPENN will process and check whether either synethetic or fully anonymised data may be used (in which there is no reasonable possibility of relinkage back to individual patients. This clarification will be achieved inter alia through the use of the tailored follow up questionnaires to UPENN and other relevant partners and will be reported on in Deliverable D4.3.1 in M14. However, in the event that the transfer of personal data outside the EU is indeed needed, this could in principle be permitted under the Directive on three broad bases:

i) where the country has been assessed by the EC as having an adequate level of data protection, [108] or a special framework such as the US Safe Harbor policy is in place;

ii) where further safeguards are put in place by the transferor, such as where the EC approved Standard Contractual Clauses are used in the contract for the transfer in cases where a country's adequacy level has not been found; or where there is an approved Binding Corporate Rule in place within a multinational company; or the use of ad hoc contracts approved by the DPAs;[109]

iii) where any of the exceptions in Art. 26(1) of the Directive is relied upon for the transfer. The most relevant exemption, when it comes to medical research, that allows the transfer of personal data to countries with no adequate level of personal data protection, is envisaged under art. 26 (1) a) Directive 95/46/EC, when "the data subject has given his consent unambiguously to the proposed transfer".

[108] So far, the following countries have been assessed as having adequate level of data protection: Andorra, Faeroe Islands, Israel, Argentina, Guernsey, Jersey, Canada, Isle of Man, Switzerland, Uruguay, New Zealand.
[109] See arts. 25 and 26 of the Data Protection Directive

However, it should be noted that the framework for the international data transfers is under review following the revelations of government surveillance of international data. Currently, the German DPAs have suspended approvals for international data transfer applications, and the WP is reviewing the Safe Harbor framework with the US.[110] In principle, the United States is not recognised by the EU as having an adequate level of personal data protection; hence any transfer of personal data is prohibited in general. Two exemptions under Directive 95/46/EC that will apply nonetheless in the context of CHIC is that a transfer may be based on the consent of the data-subject, or the European Commission approved standard contractual clauses. Currently there are two decisions laying down standard clauses for the transfer of personal data to controllers outside the EU (Decisions 2001/497/EC and 2004/915/EC). In addition there is a decision of the European Commission on standard contractual clauses for the transfer of personal data to processors established in third countries (Decision 2010/87/EC).

In addition consideration may be given to obtaining safe harbour status for UPENN. Here, insofar as it is a "covered entity" under HIPAA, this would be a helpful factor given that it is already subject to significant US data privacy governance (see section 5.3.2). However, where there are discrepancies of protection as between the US and EU approaches, UPENN would need to show compliance with the EU standard if this is higher. The EU transferor of the data will be responsible for checking this:[111] In an earlier Opinion published by the Art. 29 Working Group it also suggested that transfer of sensitive data may be considered to fall outside the restrictions in the Directive if it is at least put in securely pseudonymised form prior to transfer, and subject to other strict organizational and technical safeguards so as to preclude the reasonable possibility of re-identification by the recipient outside the EU.[112]

5.4 Legal requirements according Directive 2001/20/EC – Clinical Trials Directive

Directive 2001/20/EC[113], also known as Clinical Trials Directive, states the requirements for the conduct of clinical trials in the EU. It is concretised by the Commission Directive 2005/28/EC[114], discussed hereafter.

[110] J. Bhatti, "In Wake of PRISM, German DPAs Threaten To Halt Data Transfers to Non-EU Countries", July 29, 2013, http://www.bna.com/wake-prism-german-n17179875502/.

[111] Article 29 Data Protection Working Party, Opinion 5/2012, p. 17.

[112] Article 29 Data Protection Working Party, Opinion 4/2007, p. 19.

[113] Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, published in Official Journal L 121, 1.5.2001, p. 34.

The question is, whether Directive 2001/20/EC applies to medical research on health data too. By adopting this Directive the European legislator aimed to facilitate the performance of multi-national clinical trials in Europe through the harmonisation of the regulatory procedures. Art 1 Directive 2001/20/EC stipulates the scope of the whole Directive "regarding the conduct of clinical trials, including multi-centre trials, on human subjects involving medicinal products as defined in Article 1 of Directive 65/65/EEC, in particular relating to the implementation of good clinical practice. This Directive does not apply to non-interventional trials."

The first precondition this Directive to be applied is, that a "clinical trial" is to be conducted. According to art. 2 a) Directive 2001/20/EC a clinical trial consist of "any investigation in human subjects intended to discover or verify the clinical, pharmacological and/or other pharmaco-dynamic effects of one or more investigational medicinal product(s), and/or to identify any adverse reactions to one or more investigational medicinal product(s) and/or to study absorption, distribution, metabolism and excretion of one or more investigational medicinal product(s) with the object of ascertaining its (their) safety and/or efficacy;". This requires investigational medicinal product(s) to be used on a subject. Under art. 2 i) Directive 2001/20/EC, the "subject is an individual who participates in a clinical trial as either a recipient of the investigational medicinal product or a control". Both definitions refer to the deployment of "investigational medicinal product(s)" as the crucial precondition for application. "Investigational medicinal product(s)" are defined under art. 2 d) Directive 2001/20/EC as "a pharmaceutical form of an active substance or placebo being tested or used as a reference in a clinical trial, including products already with a marketing authorisation but used or assembled (formulated or packaged) in a way different from the authorized form, or when used for an unauthorised indication, or when used to gain further information about the authorised form". The main criterion established is that an investigational medicinal product consists of an active substance (or placebo for reference). Thus Directive 2001/20/EC applies to trials on medicinal products, covering trials on pharmaceuticals, which are in development, and "investigational medicinal products" only. The Directive does not apply to other health related research, such as physiological research, research into medical devices, observational studies, research into tissue, organs or blood, or embryo research.[115] There needs to be a substantial impact on the subject. This outcome is underlined by recital 1 Directive 2001/20/EC, which requires that placing a medicinal product on the market should be "accompanied by a dossier containing particulars and documents relating to the results of tests and clinical trials carried out on the product", implying that the key

[114] Commission Directive 2005/28/EC of 8 April 2005 laying down principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products (Text with EEA relevance), published in Official Journal L 91, 9.4.2005, p. 13.

[115] Hervey/McHale, Health law and the European Union, p. 251.

rationale for the Directive is the need to supervise the launch of a medicinal product. Software in form of a hypermodels however, as contemplated in CHIC, will assist the physician in his decision only and cannot be seen as a medicinal product because of this.

5.5 Legal requirements according Commission Directive 2005/28/EC – Good Clinical Practice Directive

The Commission Directive 2005/28/EC (Good Clinical Practice Directive) was enacted under art. 1 lit 2 Directive 2001/20/EC, laying down principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products. As regards the scope of its application, the Commission Directive is based on Directive 2001/20/EC and remains within its sphere of application. Hence the Commission Directive 2005/28/EC equally will not apply to medical research on health data alone.

5.6 Legal requirements according Directive 2001/83/EC – Medicinal Products Directive

In addition the Directive 2001/83/EC on the Community code relating to medicinal products for human use should be taken into account. This Directive deals with the disparities between certain national provisions, in particular between provisions relating to medicinal products. A medicinal product is defined under art. 1 lit 2 Directive 2001/83/EC as “any substance or combination of substances presented for treating or preventing disease in human beings” or “any substance or combination of substances which may be administered to human beings with a view to making a medical diagnosis or to restoring, correcting or modifying physiological functions in human beings is likewise considered a medicinal product”. The Directive provides inter alia rules regarding the placing of medicinal products on the market, such as marketing authorisation, specific provisions applicable to homeopathic medicinal products, procedures relevant to the marketing authorisation. Furthermore the Directive regulates the manufacture and importation of medicinal products, their labelling and the package leaflet as well as the wholesale distribution of, and advertisement for medicinal products.

As regards this Directive, it too is ultimately of no application to the kind of data research (and later development of hypermodels) that will occur in the CHIC project. This is because, according to its art. 2, Directive 2001/83/EC applies only to “industrially produced medicinal products for human use intended to be placed on the market in Member States”. Art. 3 of the Directive also provides further limitations as to its scope. Accordingly the Directive inter alia does not cover medicinal products intended for research and development trials. Furthermore the Directive does not apply to whole

blood, plasma or blood cells of human origin. Hence this Directive does not apply to the use of medicinal products, if these products are merely used for research and development trials. Directive 2001/83/EC can be seen rather to be designed to apply only subsequent to a complete clinical trial as set up by Directive 2001/20/EC for the general use on the market for medicine products.

In addition, as with Directive 2001/20/EC, a further limitation on the scope of application of Directive 2001/83/EC is that it applies only to substances that will directly be used on a human being.

6 Ethical Requirements

6.1 Overview

Medical research has been an important aspect of human development. Though there have occasionally been some systematic practices which tend to put the life of the research subjects in danger, efforts have been made to prevent any recurrence of unethical conduct, especially as exhibited by physicians during the World War II (WWII). Ethical principles such as respect for persons, informed consent and confidentiality have been recognized as basic principles in the physician-patient relationship during care and research situations.[116] These principles are constantly updated and expanded as changes are being introduced in medical research. Greatly influenced by developments in human rights law as well, some ethical principles have been codified into law in some legal systems.

Research on health has been regarded as a special category of activity, requiring special arrangement to protect the subject because of the sensitive nature of the human physiology and the data associated with health status. Apart from the requirement of a well defined protocol, data management practices have also been evolving over the years. Core principles such as purpose limitation and compatibility of further processing with the original purpose, conservation of medical data, informed consent, etc. appear to have crystallized. Difficult circumstances have equally been balanced in certain instances with exceptions on certain rules as may be seen in a number of legislations and guidelines.

It has also been ethically established that medical research studies involving human subjects must be preceded by careful assessment of predictable risks and burdens to the individuals and communities involved in the research. It is necessary for the researcher to demonstrate that the risks to the research subjects are not unreasonable or disproportionate to the expected benefits of the research.

[116] WHO, *Ethical issues in patient safety research interpreting existing guidance*, Geneva, 2013.

Paragraph 20 of the Declaration of Helsinki (DoH) requires researchers to adequately assess these risks and be sure that they can be managed. If the risk is entirely unknown, then the researcher should not proceed with the project until some reliable data are available, for example, from laboratory studies or experiments on animals.

At the global level, the World Medical Association (WMA) has set forth a broad range of ethical statements aimed at protecting patients, and these are revised as advances in medical science and technology raise new ethical issues that cannot be answered by traditional medical ethics. With respect to medical research involving human subjects**,** the WMA's Declaration of Helsinki (DoH) has provided valuable guide and principles, one of which is that "In medical research involving human subjects, the well-being of the individual research subject must take precedence over all other interests."[117] While the DoH is a concise summary of research ethics, other much more detailed international documents have been produced in recent years such as the International Ethical Guidelines for Biomedical Research Involving Human Subjects, 1993, revised in 2002), and on specific topics in research ethics (e.g., Nuffield Council on Bioethics [UK], The Ethics of Research Related to Healthcare in Developing Countries, 2002).

In Europe, the European Convention on Human Rights, Council of Europe Recommendation (R (81) 1) on automated medical data bank; Recommendation (R (97) 5) on the Protection of Medical Data, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (Convention on Human Rights and Biomedicine), Clinical Trials Directive among others play significant roles.

Furthermore, other local or municipal laws apply to medical research depending on the location of the research. It should be noted however, that new technologies have reshaped data processing (easy linking, failure of anonymization) necessitating new rules for data management in health research.[118] Data security requirements have also been emphasized on a number of occasions in reaction to data breaches witnessed in the health sector. In the following sections we will look at some of the requirements that have crystallized in medical research, though with minor variances in term of scope and geographical application, that are relevant for the CHIC project.

6.2 Informed consent

Informed consent is a major and well known element of medical ethics and bioethics today. At its core stands the principle that 'any preventive, diagnostic, or therapeutic medical intervention, is only

[117] Paragraph 6 of the DoH, http://www.wma.net/en/30publications/10policies/b3/
[118] See for example, WP 29 Opinion on purpose limitation.

acceptable with prior, free and informed consent of the person concerned, based on adequate information'.[119] Since medical treatment or medical research gives rise to risks to patients, they need to be given the opportunity to decide autonomously, if they are willing to bear the consequences in order to possibly profit from medical processes. Informed consent is an expression of patient autonomy and self determination in clinical daily routine. In standard clinical trials, informed consent is obtained in order to ensure that the patient's rights - including respect and autonomy - are not infringed. In informational research, the situation is – from an ethical point of view - less clear. If personal data is processed for scientific research purposes, the data processing operation should be bound to the will of the patient. This may be different if data is de-identified prior to further processing it for research purposes. The scope of consent can vary due to the design of the consent. Different models have been established in the ethical discourse.

One of the basic principles of the Nuremberg Code is that participation in medical research should be a voluntary choice of the research subject. This is reflected in other similar documents and human rights law. This principle requires, among other things, that the research subject "should have sufficient knowledge and comprehension of the elements of the subject matter involved, as to enable him to make an understanding and enlightened decision." Paragraph 24 of the DoH also reiterates the importance of voluntary and informed consent and specifies what the research subject needs to know in order to make an informed decision about participation in medical research. Research subjects who are unable to give consent, such as minor children, severely mentally disabled individuals, or unconscious patients, can still participate in medical research under restricted conditions, including obtaining the consent of a legal representative of such a person. Consent is best evidenced in writing, and the modern practice is to have the participants sign a consent form indicating their freedom of participation after being furnished with an explanation of the research processes. More importantly, research subjects should be informed about their right to withdraw their consent to participate in the research at any time, without suffering any harm or compromise of their healthcare as a result of such decision. And even when there is a valid consent, ethical preconditions consist of the responsibility of the physician or the health care professional to protect the rights and interests of the data-subject as laid down in paragraph 16, DoH.

This requirement is essential for CHIC to maintain compliance. In this regard, informed consent forms have been developed by the clinical partners, who will carry out prospective trials. However, WP 4 will review these forms to ensure their compliance with specific consent rules. Responses to the

[119] Forgó, Kollek et al., Ethical and Legal Requirements for Transnational Genetic Research, p.8.

questionnaire also indicate that informed consent was obtained for the retrospective data, and ethical committee approval, where required, had been obtained for its use in CHIC.

6.3 Right to withdraw

Consent may be withdrawn by the data subject at any time. This means that the research activities, including data processing in relation to the subject will no longer be legitimate. To respect the will of the data subject (and his or her right to free self-determination) is especially in (clinical) practice of utmost importance. The right to consent withdrawal requires the data subject to be sufficiently informed about data processing procedures. In this case, the physician must fully inform the patient which aspects of the care are related to the research. The refusal of a patient to participate in a study or the patient's decision to withdraw from the study must never interfere with the patient-physician relationship. Furthermore, smart IT solutions should be implemented to ensure that data is factually no longer processed after consent has been withdrawn. For CHIC, while the informed consent process should covers the right to withdraw, we will aim also at a technical solution to implement this (see chapter 7 below). It is necessary to point out that a refusal or withdrawal of consent to participate in a research project must not interfere with the medical treatment of patients.

6.4 Confidentiality

One other basic principle in medical research is that research subjects have a right to privacy and confidentiality with regard to their personal health information. Paragraph 23 of the DoH states that "Every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information and to minimize the impact of the study on their physical, mental and social integrity." As indicated by the WMA ethics manual, the nature of medical research requires in certain circumstance that information about the subjects be revealed to a third party. Here, consent is required to such disclosure, or Ethics Committee approval should be obtained where consent is not practicable. As a general rule in these circumstances, the information should be de-identified and should be stored and transmitted securely. The WMA Declaration on Ethical Considerations Regarding Health Databases enjoins: "Care must be taken to ensure that secondary uses of information do not inhibit patients from confiding information for their own health care needs, exploit their vulnerability or inappropriately borrow on the trust that patients invest in their physicians."[120] Safeguards must be in place to ensure that there is no inappropriate or unauthorised use of or access to personal health information in databases, and to ensure the authenticity of the data and secure transmission. Audit systems must keep a record of who has accessed personal health

[120] http://www.wma.net/en/30publications/10policies/d1/

information and when. People who collect, use, disclose or access health information must be subject to an enforceable duty to keep the information secure.

In CHIC, it is proposed that a confidentiality contract will be concluded by all researching that will be having access to the data in the CHIC repository. This will forbid matching data or doing anything that will reveal the identity of the data subject. In addition to the technical measures to be taken in this regard, publication of the result of the project will not reveal the data subjects.

6.5 Involvement of Ethics Committee

Paragraph 15 of the DoH stipulates that every proposal for medical research on human subjects must be reviewed and approved by an independent ethics committee before it can proceed. The reason for this is to have an independent and objective view of the research protocol to determine whether it is scientifically and ethically appropriate and justifiable. Such a review may result to modification of the protocol as well as a constant monitoring of the research in order to safeguard the subjects. Obtaining Ethics Committee approval could be complicated in some situations, especially when a multinational research is conducted. Each of the national ethics committee may have a different opinion concerning the research, and it is thus important for researchers to schedule sufficient time between applying for the review and execution of the proposed research activity.

In addition to ethical committee approval obtained by the clinical partners for their trials, it is also planned in CHIC to have an International Ethics Board to monitor ethical issues in the project due to the multinational nature of the consortium. This has not been finalized at this stage.

6.6 Feedback of information

In order for the data subject to validly make use of his rights, there is an obligation on the data controller to inform the data subject about data processing operations as well as potential results. The right to know can be considered as broadly recognized and constitutes an obligation to any person processing personal data to answer questions raised by the data subject which relate to data processing. Above all, Art 10 of the Data Protection Directive contains this obligation. From an ethical point of view it is still in question, how far reaching the right to know is. There may be a moral obligation to give contextual information and to explain the 'importance and relevance' of the proposed data processing operations to the data subject. This moral obligation may arise from the ethical principle of respect, which is a major issue in tissue research and might be extended to data subjects outside of genetic research.

This principle will influence the data management of the project. In the light of this, chic will not destroy the link to feedback information to patients. However, feeding back information will be directly to the patient in the CHIC framework, but to his physician as will be developed in the data protection framework to be established.

6.7 Retention and destruction of health information

One other ethical issue in medical research is how to balance the tension between privacy and the retention of data for a long period of time, to permit a therapeutic follow up of the patients or for future research. In some cases, long - term follow up for example, reveal that adverse effects of malignant disease and its treatment may manifest many years, sometimes decades, after treatment. In cancer cases for instance, it is important that details of chemotherapy and radiotherapy received be retained for a patient's lifetime. Premature destruction of such records may result in preventable harm or inappropriate subsequent treatment.[121] Similarly, retention of treatment records for children and young adults is also important to monitor their ailment in their adulthood. Apart from retaining data for treatment and research purposes, medical records may also be required for evidentiary purposes in legal proceedings.

There is currently no uniform legal or ethical instrument that addresses this issue, globally or regionally. Each state has developed its own rules on retention of health information, which varies depending on the type of health records involved. In the UK for example, the Records management NHS Code of Practice provides for the period of retention and destruction of medical related data. Child health record for instance should be retained until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment, or 8 years after death, and could even be retained for longer period under certain circumstance.[122] Retention periods for clinical trial records also vary in the UK depending on the nature of the trial.[123] Similar retention periods can also be found Germany.[124]

However, it has to be noted that the ICH GCP provides that the IRB/IEC should retain all relevant records (e.g., written procedures, membership lists, lists of occupations/affiliations of members, submitted documents, minutes of meetings, and correspondence) for a period of at least 3 years

[121] RCR, The Retention and Destruction of NHS and Private Patient Records: Updated Advice, http://www.rcr.ac.uk/docs/oncology/pdf/BFCO%2806%292_retention_of_records%282011%29.pdf, for a list of the minimum periods in the UK.

[122] See: DoH, Records Management NHS Code of Practice Part 2 (2nd Edition) www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf

[123] Ibid.

[124] See: http://www.gfhev.de/de/qualitaetsmanagement/aufwahrungsfristen.pdf

after completion of the trial.[125] In the context of CHIC, none of the retention rules apply to the project directly. Rather, clinical data providers as the original data source should adhere to the national data retention periods applicable to their institution.

7 Proposed Data Protection Framework for CHIC

7.1 Introduction

As shown in the Chapters four and five above, a proper development of the infrastructure intended in the CHIC project will require at least in later stages of the project real data which will involve personal data within the definition of the Data Protection Directive. The analysis in this chapter is intended to be part of the requirement elicitation process of the project, and is focused on data protection, data security and ethical aspects of the infrastructure. It is also intended to be incorporated with requirements from other work packages. Here, legal and ethical constraints as identified from the previous chapters will be elucidated and applied to the CHIC environment. Their potential impact will be assessed upon the functional and non-functional aspect of the infrastructure as it develops. With this in mind, a privacy-by-design approach is adopted here, which is informed by the Recital 46 of the current Data Protection Directive and art 23 of the proposed Regulation. This will mean that even when the Regulation comes into force, it will not radically affect the design of the infrastructure.

It should be noted at the outset, however, that the requirements specified below only reflect an initial analysis. They may be reviewed in future as the infrastructural design develops and practical lessons learned. So far, as described in Chapter four, input at this stage have been obtained from the DOW, responses to a questionnaire designed for WP 4, literature on medical research, data protection, data security, European and national legislations. As a result of the fact that the project use cases and scenarios are being developed, the requirements specified here appear generic. Workpackage 4 will be in close contact with other Workpages, including sending a follow up questionnaire to individual partners to gather the required information. In this regard, subsequent deliverable (D4.3.1) will contain a more specific analysis/framework that is tied to the scenarios.

[125] http://ethikkommission.meduniwien.ac.at/fileadmin/ethik/media/dokumente/rechtsgrundlagen/GCP.pdf

The privacy framework proposed for the project will be categorised into two (or possibly even three) phases – the development phase (that might not require personal data processing in an early stage, but will then work with anonymised data, but might later need to validate the technical solutions developed by use of personal data) and the exploitation phase. This is to reflect the changes in the data processing that will occur between the two phases. For example, while a limited set of institutions, notably the partners in the CHIC consortium will be involved in the development of the tools, a larger community of users is envisaged during the exploitation phase of the infrastructure. Similarly, the nature of the data that is processed in the former phase may be different from the latter.

7.2 Legal bases for data sharing in CHIC

As was analysed in Chapter five above, a legal basis to process data within the CHIC project will be necessary only, in case the data is not rendered anonymous. At least one of the project data providers indicated that its data is fully anonymous. This would lead to the consequence that no legal basis is required for such data. On the contrary, other providers showed that re-identification is envisaged in case of findings during the research project that will serve the data-subject. One of the providers even pointed out the fact that genetic data will be processed, which is to be seen as impossible to anonymise. So in the very end it cannot be excluded that a legal basis is required.

As discussed, an appropriate legal basis will need to be found in every member state a consortium partner is located that transfer or use CHIC repository data within the project. In addition the legal basis might depend on the data being retrospective or prospective. For the prospective data, there is the opportunity to ask the data subjects for their consent in advance. Consent forms have been developed by the partners intending to engage in prospective data collection. In this respect, these consent forms will be further evaluated by WP 4 to ensure their compliance with consent requirements.

When it comes to retrospective data, further processing might be more complicated. All the data providers envisage using data collected for previous research projects or within clinical setting. Hence CHIC project might be seen as further processing data, and as we saw in Chapter five, one ground for this further processing could be based on art. 6 (1) b) of the Directive, which permits further processing of personal data for scientific purposes, where appropriate safeguards are guaranteed. Safeguards adopted here include anonymising data where necessary, obtaining ethical committee approval, as well as implementing a second round of pseudonymisation before data is processed within the CHIC research platform. As deducible from the WP opinion on purpose limitation, these will be compatible under Directive 95/46/EC.

In addition, CHIC will implement a further safety net to protect the data under its control as will be outlined in the sections below. To put it in a nutshell, processing data within CHIC can rely on a multilevel bases and safety net. In the first stage data might be seen as anonymous falling outside the scope of legal regulation. In addition both consent as well as legally recognised basis for processing for scientific purposes can be relied upon for processing of both prospective and retrospective data.

7.3 Privacy framework in the project development phase

For the setting up of the CHIC infrastructure, the development phase of the project refers to the phase of building the platform with a set of technical tools and data. The tools will be tested with data obtained from the clinical partners, and for the development of fully functional tools for medical decision making support, a careful analysis of user needs will be focused. For this reason, access to real clinical data is needed. In the same vein, there is also the need to have a level of feedback to the data source as indicated in the responses to the questionnaire. This requires a level of flexibility in the de-identification process of the data so as to achieve this aim, while also ensuring a high level data protection. During this phase, datasets shall be provided by some project partners (data providers) and will be used by other partners (end users/researchers) within the CHIC infrastructure to develop models and tools. This will involve a data sharing arrangement, requiring a special care and attention (due to the sensitive nature of the data), and to ensure compliance with European data protection regulations, ethical rules as well as to safeguard the fundamental rights of data subjects as explained in the previous chapters.

7.3.1 Data flow

The initial understanding of the data flow and management in the project presented in Chapter four indicate that there will be prospective clinical trial data and retrospective trial data into the project.[126] The retrospective data were collected prior to the CHIC project and have either been "anonymised" or "pseudonymised". The prospective data will be collected in the course of the project and pushed to the CHIC data repository to be developed in Workpackage 8.[127] It is envisaged that access to the CHIC repository will only be given to the researchers within the project consortium at this development stage of the project.

Two possible domains could be identified from this data flow – the clinical domain and the research domain. While data will move from the clinical domain, it is not envisaged that data will flow back

[126] Responses to the questionnaire are on file.
[127] DOW, A 31.

from the research domain to the treatment domain at this stage. In this case, a clear separation of the two domains will be maintained.

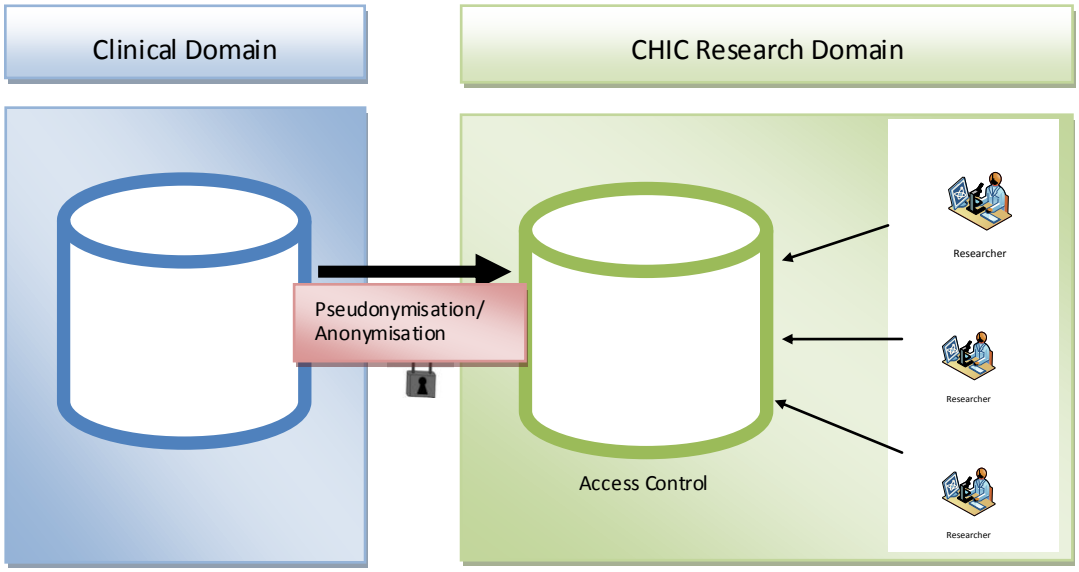


Figure 1: CHIC Domain separation framework

7.3.2 Clinical and research domain

When working with data for clinical research it is important to make a clear distinction between the treatment domain (at the source, e.g. a hospital) and the research domain (the CHIC infrastructure). This is because different privacy and data protection rules apply to the storage and processing of data for the purpose of medical care as opposed to for research. Thus, a clear separation of the hospital database from the research database will be maintained so as to reduce the risks of unauthorised access to each of the databases. This will ensure that the hospital data management system is not compromised, and the data exporters will actively initiate data transfer and retain control of their systems, while the research domain will be under the control of the CHIC project data management. (See fig.1 above)

7.3.2.1 Clinical Domain

Within the clinical domain such as hospital/trial centre, data is typically collected by treating physicians. This data contains medical information on the patient and is thus very sensitive. Usually in practice, hospitals store and process this data in a pseudonymous way whenever no direct identification is required by the physician. And pseudonymisation within this treatment domain is generally carried out by the local hospital's pseudonymisation tools using their own tool which is not uniform in all hospitals. Therefore, a second pseudonymisation will be introduced at the point of transfer into the research domain. This is to further decrease the possibilities of re-identification and maintain a high level of anonymity of the data within the research domain.

7.3.2.2 Research Domain

Within the research domain, where data is used for the purpose of scientific research, the data shall generally be used anonymously whenever possible. This implies in the first place that hospitals should strip all direct identifiers before exporting the data to the research domain. However, if the hospital would either directly export their internal pseudonym to a research domain or a badly generated irreversible anonymous patient identifier, there is a risk that someone with access to the hospital's data could then re-identify patients in the research domain.[128] To avoid this and to avoid the need to verify the reliability of all pseudonymisation tools used by hospitals as explained earlier, a second round of anonymisation/pseudonymisation should be performed by a (independent) Trusted Third Party (TTP) within the research domain. The TTP ensures that anonymous identifiers are irreversible and that pseudonyms can only be reversed under strictly supervised circumstances (e.g. to send back results relevant to a patient's treatment to the treating physician). Apart from this technical measure, other administrative measures will be in place such as strict access control and binding contract among the researchers using the data. In this case, it is arguable that the data within the CHIC research domain is by default anonymous (de facto anonymous) because of the reasonable effort it will take to identify individuals within the data set. This gives room for the flexibility required for processing this data for research purposes.

7.3.3 Safeguarding anonymity and mitigating data disclosure risks at the development stage in CHIC

As emphasised in the opinions of the Article 29 Working Party examined earlier in Chapter five, there could still be risks associated with the use of de-identified data, even when there is limited access disclosure of the data for research. This calls for adequate technical and organizational safeguards in mitigating the risks. In CHIC, we intend to establish a "safety net" using the following pillars to ensure anonymity:

- Research data sets will be stripped of any direct identifiers;
- Confidentiality obligation will be imposed by binding contracts;
- A trusted third party will be used for the second pseudonymisation process;
- A data protection office (CDP) will be re-used for the project;

[128] This will also be the case where a motivated attacker intends to re-identify data based on his prior knowledge about the data

- Access to the research domain will be limited/restricted to only authorised persons from each partner institute;
- Technical security measures such as traceability/logging capabilities, encryption, etc will be maintained;
- There will be no publication of personal identifiers in the research results generated.

7.3.3.1 Stripping data of any direct identifiers

As explained in 7.3.2, the de-identification of datasets will occur through a two step process: firstly the data exporters will pseudonymise their data in their individual system. Secondly, before providing data to the CHIC research platform (repository), a second pseudonymisation process will be performed, as a further safeguard to securing the anonymity of the datasets. In this case, it will require reasonable efforts to re-identify the individuals in the data set because the two sets of key are managed by separate entities – the initial data provider and CHIC's TTP.

However it has to be considered that in the light of the Data Protection Directive, the sole act of removal of direct identifiers does not make the data completely anonymised - non-personal, in the sense that there is no possibility at all of relating back to the original data.[129] Indeed, as indicated earlier, completely anonymised datasets will not serve the research purposes of the project. Besides, some of the particular datasets involved in the project will include genetic information, or body scans that even without direct identifiers, have a higher chance that they could still be re-identified.

In this regard, CHIC will not only process anonymous data. For the processing that involve pseudonymised data, a high level of anonymity will be maintained, including the double pseudonymisation process as explained above, in addition to other safeguards – legal, organisational and technical, that will limit the risk of data breaches. Furthermore, a standard framework for re-linking data within the project if (and only if) this proves strictly necessary will be proposed. In effect, this process will be subject to the control of the project data protection office and the TTP, and only the authorised persons within the data exporter's institute who require the information will be contacted (See fig. 3 below).

[129] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf

7.3.3.2 First Round Pseudonymisation at the source

Data exporters (as the institutional sources of the data) are responsible for pseudonymising their data locally on their site before exporting the data to the CHIC research domain to ensure that no explicit[130] or easily observable quasi[131] identifying information leaves the hospital. Such explicit and quasi-identifiers are amongst others:

- Identifiers such as a hospital number, insurance number, national security number.
- Patient demographics such as name, initials, contact information, date of birth.
- Other (non patient) demographics such as hospital (place of treatment) and physician contact information, names of relatives.
- Other specific individualised information (e.g. rare diseases and treatments, minority social and physical features, socio-economic data such as occupation, place of work, income and education) so far as unnecessary to pursue the CHIC research objectives.

As patient IDs are removed, these should be replaced by either an anonymous identifier or a pseudonym.

An anonymous identifier implies that the data exporter itself does not know which identifier was assigned to which patient. This can be implemented by assigning a random identifier to each patient without keeping track of it through a linking table.

A pseudonym implies that the source knows which pseudonym was assigned to which patient. This can be implemented, among others options, by using:

- a random identifier which is stored, locally at the source, in a linking table. Such a linking table links the local patient IDs with the issued pseudonyms.
- a secure hash (HMAC) generated from the local patient identifier.

CHIC will provide a default reference implementation of a first round client side pseudonymisation mechanism. This will allow sources who do not yet have an adequate tool of their own to use the reference implementation.

7.3.3.3 Second round of pseudonymisation and Use of Trusted Third Party

The Trusted Third Party (TTP) is in charge of the second pseudonymisation round. The TTP ensures, cryptographically, that it is not possible to go back to the original patient ID without the TTP's

[130] Explicit identifiers are attributes that clearly identify an individual (e.g. social security number, address and name).

[131] Quasi-identifiers are attributes whose values when take together can potentially identify an individual (e.g. zip-code, birth date and gender).

approval and intervention. Thus even when a source issues weak pseudonyms that can easily be linked to the patient, by adding the TTP we can be confident that the CHIC pseudonyms cannot easily be linked back to the original patient IDs.

It should be acknowledged that pseudonymisation per se does not stop re-identification attempts by using quasi identifying data fields within a given dataset. Quasi identifiers can result in the patient being re-identified, when combined with knowledge on the patient group, e.g. it is possible in a small population, when you know that some particular person is in that population, to deduct the real patient from his height, weight and diagnosis. As previously described, those quasi identifiers not strictly required for the CHIC research objectives will be removed by the data source; however, for those that remain (in order for the datasets retain research utility), key additional safeguards to preserve their security will take the form of strict technical, organisational and legal controls. These measures are described at 7.3.3.5 ff below.

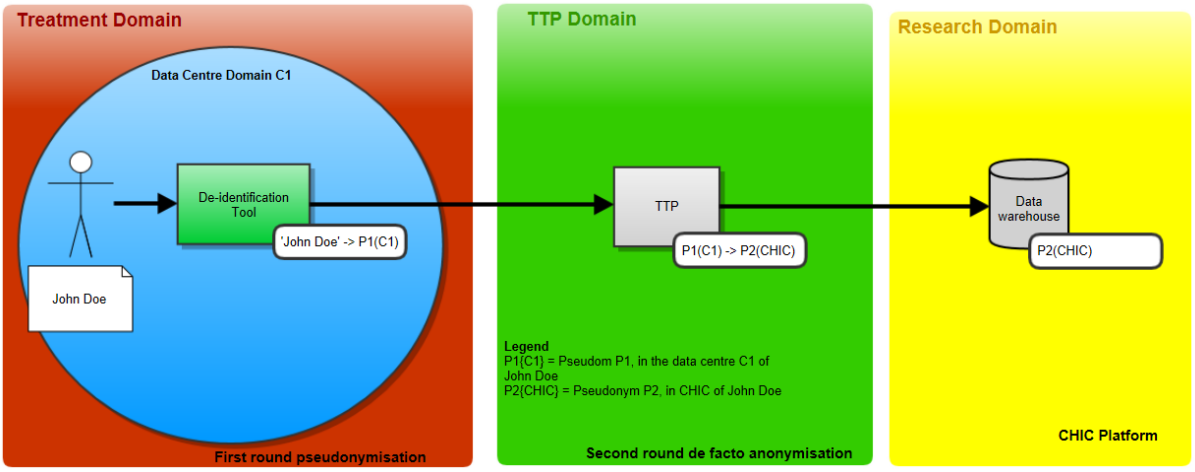


Figure 2: De-identification flow

The diagram above describes the flow of uploaded data from a data centre C_1 to CHIC. At the source C_1 an example patient "John Doe" is pseudonymised as P_1. This patient is then uploaded through the TTP into the CHIC data store. The TTP hereby cryptographically transform the pseudonym P_1 into a new pseudonym P_2. Within CHIC the patient is thus identified as P_2 while at the source he is identified as P_1.

7.3.3.4 Re-identification

Messages can be sent back from the research domain to the treatment domain through the TTP. The TTP will then re-identify the patient in the message. Such re-identification will only be allowed by the TTP under specific strict circumstances as defined by the legal requirements.

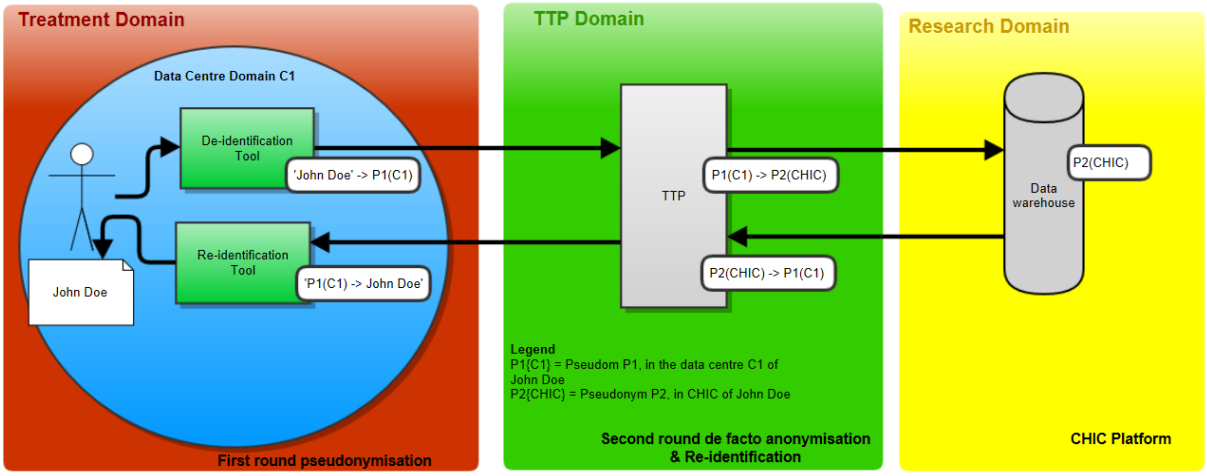


Figure 3: Re-Identification flow

7.3.3.5 Access restriction

One of the main safeguards upon which the concept of 'anonymity' rests is limiting the access to data. For this reason a closed user group shall be established – a "network of trust", consisting of a group of only authorised persons from each project partner who are fully committed to the strict rules of data access and disclosure as envisaged here. All of the "network of trust" members are obligated to firmly respect patients' privacy rights and follow data security rules. The compliance of institutional members, as well as of individual persons, to the rules of the "network of trust" is guaranteed through contractual obligations. This will minimize the risk of data being accessed by those who do not need it, even when they belong to partner institutions.

CHIC therefore needs an authentication and authorisation infrastructure, which will be proposed in an initial iteration in Deliverable D4.3.1. The authentication components should allow CHIC to ascertain the identity of the acting user while the authorisation components take the decision on whether a person has access to sensitive data.

7.3.3.6 Confidentiality obligation by contract

An end user contract that will bind the closed group of researchers to the use of datasets with the CHIC research domain will similarly be needed and presented in outline in Deliverable D4.3.1, due in M14. This framework will ensure that the context of anonymity is maintained during the project development phase, enhance trust as well as make data sharing between the users who require it easy. This contract will be concluded between the CDP which acts as the data protection office and end users (research institutions). A detailed description of the contract will be developed in D4.3.1.

7.3.3.7 Other elements to the data security framework

7.3.3.7.1 Traceability/logging capabilities (audit)

Audit services are an important part of a security infrastructure. Not only do they allow the detection of intrusions, but audit logs can also be used to support access control scenarios. Through policies access can be given to data under some rare circumstances, for example if re-identification data is needed to be able to provide important feedback to an individual patient. The relevant policies will be developed in WP 4 and presented in two iterations in Deliverables D4.3.1 and D4.3.2. For their part, audit logs can then be used afterwards to verify whether the person rightfully accessed the data. On the other hand audit logs can also be important from a patient's point of view to find out what happened with his data.

Auditing today is mainly focussed on Security Information and Event Management (SIEM). SIEM provides real-time analysis of security alerts originating from network, hardware and applications. Current SIEM applications mainly focus on low level logging and auditing such as network and operating systems. The challenge for CHIC is to integrate application level logging into SIEM and correlate those application events with low level system events.

General audit requirements:

- Audit logs should only be accessible by authorized users. Neither should audit queries reveal more information than the querying user is allowed to see.
- It should not be possible to tamper with audit logs without detection.

7.3.3.7.2 Encryption of data

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. Securing this data from interception will be an important security measure to be adopted in the project. It is thus really important to always encrypt sensitive data at any state to ensure confidentiality.

7.3.3.7.2.1 Encryption requirements

It is fundamental that secure algorithms are used when encrypting data. For this we refer to the example of the NHS[132] which has defined cryptographic guidelines[133] for NHS Informatics suppliers.

- For symmetric ciphers, which use the same key to encrypt and decrypt data, the NHS currently recommends the follow block ciphers and key sizes: AES[134] with a 256 bit key size.

[132] http://www.nhs.uk.
[133] http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/acs.pdf.
[134] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

- Twofish[135] with a 256 bit key size.

Symmetric keys are typically used to encrypt large amounts of data. It is not advisable to use any stream ciphers, but instead use the above block ciphers.

For asymmetric ciphers, typically used for key exchange, agreement and digital signature, the NHS advises that, if RSA is used, it should comprise at least 2048 bit keys.[136]

7.3.3.7.2.2 Encryption tools

Various open-source and commercial tools exist for on-the-fly disk encryption. Most OS's also provide disk encryption solutions. A reliable open-source encryption OS independent tool (Windows, Linux, MacOS) is TrueCrypt . TrueCrypt can be used to encrypt the whole hard drive or just external drives. A possible alternative is Microsoft's BitLocker.

7.3.3.7.2.3 Snowden Effects

Recent information[137] revealed that the NSA might have inserted secret back doors in many (encryption) tools and systems. It also revealed that the NSA uses encryption algorithm vulnerabilities and brute force attacks through super computers to decrypt encrypted data.

Modern encryption algorithms though use long key sizes (128 bit and more for symmetric cryptography, 2048 bit and more for public-key cryptography). Based on the available material it is unlikely to that the NSA has succeeded in fundamentally breaking existing cryptographic algorithms. However we can assume they have seriously reduced the key strength. Cryptography experts currently advise that increasing key lengths give sufficient protection.[138]

More worrying are the back doors the NSA supposedly inserted in encryption tools, operating systems and hardware. Such back doors would allow the NSA to intercept the data before it is encrypted.

As this is an ICT project, we have no choice but to be online and use software. CHIC also does not have the resources to develop its own hardware, operation systems and software. The best we can do is to use more encryption rounds and longer keys while using existing software, and encrypt all sensitive data with strong encryption algorithms.

7.3.3.7.3 Use of private cloud for storage and compute capabilities

The use of cloud computing in recent time has shown huge advantages in terms of cost reduction and the provision of high computing capabilities. However, from a legal point of view, such

[135] http://www.schneier.com/twofish.html.
[136] See the NHS guidelines for more requirement on other asymmetric cyphers, hashing algorithms.
[137] http://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/.
[138] http://www.wired.com/opinion/2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic-capabilities/.

computing models still have some data protection, security and compliance issues that are yet to be fully understood.[139] Among such issues is the transfer of control to third parties, the legal jurisdiction for the location of data, access to data by law enforcement agencies without judicial oversight, etc.

The prevailing view of the majority of experts is that of the three deployment models – private cloud, public cloud and community cloud, privacy and control is more easily retained in a private and community cloud. However, in terms of cost, a private cloud is more expensive to maintain. A community cloud on the hand is available to a closed community of users such as financial institutions or health practitioners, and could lead to cost reductions through its economy of scale.

As a result of the sensitive nature of data involved in the CHIC project, a private cloud will be recommended in order to retain control of the data being processed.

7.3.3.7.4 Backups

Next to protecting data from unauthorized disclosure, it is also important to protect the data from accidental loss because of system failure.

7.3.3.7.5 Prohibition on the publication of personal identifiers in the foreground

A check will be performed on dissemination materials such as article publications, conference presentations, etc, to ensure that personal identifiers are removed. This will reduce the risk of individuals being identified by a third party which attempted to match the dissemination data against other information in the public domain.

7.3.3.7.6 Respect for patients' informed consent

As discussed in chapters 4-6 above, implementing the informed consent of the patient is core to fulfilling ethical and legal requirements. Thus, opt out systems should be implemented so that when a given patient decides not to participate in the trial, his or her data will not be further processed. In addition, the sharing of data will be based on the purposes and consent for which they were collected and will not be further processed for any incompatible purposes. In case any further retention is needed for auditing purposes, then according to GCP criteria the data should be completely anonymized, so that no re-identification is possible any more.

7.3.3.8 Creating a data protection office for the project

To ensure that the members of the "network of trusts" strictly adhere to the principles of the framework, it is proposed that a central entity acting as a central data controller dedicated to the CHIC project will be put in place, which would have broad audit rights over the functioning of the framework. As the consortium itself has no legal personality, an independent entity would be used

[139] D. Marinescu, *Cloud computing, theory and practice*, Orlando, 2012.

for this which could act on behalf of the consortium. This entity would enter into binding agreements with all the data exporters and data users as the case may be.

Such a solution is simpler compared to concluding bilateral agreements between all data providers and end users. The Center for Data Protection (CDP), a non-profit legal entity established under Belgian law, could serve as a central data controller within the project framework.

The CDP has already proven its usefulness in a number of recent medical projects – it was founded in August 2007 as one of the outcomes of the ACGT project and after a positive evaluation is also being successfully used in the p-medicine and EURECA project.

The choice of the CDP as the central data protection authority will save time and resources in comparison to signing bilateral agreements between singular project partners, or establishing a completely new legal entity serving only the CHIC project.

7.3.3.9 Review of the framework

This framework will be reviewed as the infrastructure of the project is developed and adjusted where there is need for such, especially before the exploitation phase.

7.4 Privacy framework in the project exploitation phase

The exploitation phase of the project will be at the end of the project when the infrastructure has been set up and ready for use by a larger community. In this phase, the tools developed would have been deployed in either an open source or restricted platform or both. It may be too early at this stage to determine in detail how the infrastructure will look. However, the framework that has been developed during the first phase will still be relevant, though it may require some adjustments. In this regard, it is envisaged that:

- Data will remain securely de-identified during the exploitation phase to maintain privacy.
- Furthermore, access to the tools that contain de-identified data will be granted after the requester fulfils key requirements including signing an agreement to maintain anonymity.

The exploitation framework will be more fully developed in Deliverable D4.4.

8 Conclusion

In developing the CHIC research infrastructure, sensitive health data will be processed and therefore a strong data protection and data security framework has to be set up as proposed in this Deliverable. The use of personal data is regulated by the Data Protection Directive 95/46/EC, which sets out the rights of the data subject, establishes general rules on the lawfulness and fairness of the processing of personal data and states inter alia conditions for the transfer of personal data to third countries. Furthermore, the nature of the CHIC project also requires that other legal instruments applicable to medical research and ethics be considered to have a holistic view of the project requirements. In this respect, the Clinical Trials Directive, international and national laws and regulation on medical research were considered as well.

The special sensitivity of certain types of data, including information on the health of a person has been recognised under the European fundamental rights framework. Accordingly the Directive generally prohibits the processing of such sensitive data. However, it also introduces several exemptions to the general prohibition in Art. 8. For the processing of patient data within CHIC, two exemptions are relevant - the informed consent of the patient and national transposition of the exemption stated in Art. 8 (4) in case of “substantial public interest”. Medical research is assumed to be in this category.

For the prospective data used in the project, informed consent has to be relied upon, and should meet specific requirements of the Directive in order to be valid. The patient has to be provided with all information necessary for his/her decision. The information has to be comprehensive and understandable and should at least include the main intentions of the CHIC project and the range of possible uses of data, measures taken to protect patients’ personal rights, the possible risks and benefits, and further implications of participation. Further the consent has to be given voluntarily and the patient has to be capable to take decisions. The informed consent form to be used in CHIC is currently under development, and will be integrated in the tasks ahead. It is also a requirement that retrospective data has to be “anonymised” before they are transferred to the CHIC research domain. But in addition to this, all data in the CHIC domain will be secured with other technical and organisational measures to ensure anonymity throughout the life span of the project. A two-folded initial data privacy framework has been developed in this regard. The first applies to the development phase of the project, and will be updated to take account of the hypermodel validation towards the end of this phase. The second will apply to the exploitation phase, and will address the participation of CHIC users from outside the initial consortium. This is to achieve the flexibility needed for data sharing in the project.

As far as possible the project will utilise anonymised data. However, complete anonymisation may not provide a solution at every point because, for ethical reasons, there should be the possibility to contact the patient in the event that research findings could influence the treatment of a patient; furthermore to validate the hypermodels, some linkage to securely pseudonymised patient data may be required towards the close of the development stage. Accordingly, a solution is aimed at that will ensure the highest level of data protection while maintaining this flexibility. The framework for the development phase is based on a network of trust that enable efficient 'anonymous' data sharing for building the project infrastructure tools. This gives a guarantee that no user will re-identify the patient. All this shall be safeguarded by the data protection and data security framework that ensures that the data within the project is only accessible for researchers that are contractually bound to the data protection rules set up for CHIC. This will include: the use of a central data protection authority for the project - Center for Data Protection (CDP), the deployment of a Trusted Third Party (TTP) to secure the pseudonymisation key; strict access control, etc.

The privacy framework in the project exploitation phase will be built upon the initial development phase framework, but will be more open to a larger user network. The mechanism as to how this will operate, and in particular the necessary up-scaling of data privacy and security measures, will be the focus of ongoing analysis and attention as the project develops. By implementing this two-folded privacy framework, legal and ethical compliance, as well as a high level of data privacy will be ensured throughout the lifespan of the CHIC project.

9 References

AHIMA, "Rules for Handling and Maintaining Metadata in the EHR", http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050177.hcsp?dDocName=bok1050177.

Article 29 Data Protection Working Party, Opinion 7/2007 on the concept of personal data, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Data Protection Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf.

Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, p 5 http://www.edoeb.admin.ch/org/00828/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdX58hGym162epYbg2c_JjKbNoKSn6A--.

Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, p 9 http://www.edoeb.admin.ch/org/00828/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdX58hGym162epYbg2c_JjKbNoKSn6A--

C. Kuner, *European Data Protection Law: Corporate Regulation and Compliance, 2007*

CHIC Description of Work (DOW).

Council of Europe Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, http://www.giodo.gov.pl/237/id_art/216/j/en/.

Council of Europe Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, http://www.giodo.gov.pl/237/id_art/215/j/en/.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data, http://www1.umn.edu/humanrts/instree/coerecr97-5.html.

Council of the European Union, Treaty of Lisbon, http://www.consilium.europa.eu/documents/treaty-of-lisbon?lang=en.

Datatilsynet, "Private research and statistics projects", http://www.datatilsynet.dk/english/health-research-and-statistics-projects/private-research-and-statistics-projects/.

Datatilsynet, "Requirements of clinical drug trials, clinical testing of medical equipment, and mandatory safety monitoring of medical products and medical equipment, in accordance with the Danish Act on Processing of Personal Data", http://www.datatilsynet.dk/english/health-research-and-statistics-projects/the-medical-

products-and-medical-device-industry-etc/requirements-of-clinical-drug-trials-clinical-testing-of-medical-equipment-and-mandatory-safety-monitoring-of-medical-products-and-medical-equipment-in-accordance-with-the-danish-act-on-processing-of-personal-data/.

Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, published in Official Journal L 121, 1.5.2001.

Directive 2005/28/EC of 8 April 2005 laying down principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products, published in Official Journal L 91, 9.4.2005.

D. Marinescu, *Cloud computing, theory and practice*, Orlando, 2012.

Department of Health, Records Management NHS Code of Practice Part 2 (2nd Edition) www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf.

European Convention on Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

F. Cate, Protecting Privacy in Health Research: The Limits of Individual Choice (2010) 98 Cal. L. Rev. 1765.

Gosfield, (ed) Health Law Handbook (Current / 2011 Edition), § 8:7. HIPAA privacy rule framework.

Greely, H, (2007) 8 Ann. Rev. Genomics Hum. Genetics (2007) 343–64.

H. Kaplan, M. Cowing and G. Egli, "A primer for data-protection principles in the European Union", 2009, http://www.shb.com/attorneys/CowingMark/APrimerforDataProtectionPrinciples.pdf.

HHS Protection of Human Subject Regulations at 45 CFR 46.102(d), http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html.

Hervey/McHale**,** Health law and the European Union

Irish Data Protection Commissioner, "Data security guidance", http://www.dataprotection.ie/viewdoc.asp?DocID=1091

J. Pomerantz, "Metadata: organising and discovering information", Lectured delivered on coursera.org.

J. Bhatti, "In Wake of PRISM, German DPAs Threaten To Halt Data Transfers to Non-EU Countries", July 29, 2013, http://www.bna.com/wake-prism-german-n17179875502/.

M. Stauch, "The Draft Data Protection Regulation and the secondary use of patient data for research: prospects and concerns", Journal of Professional Negligence, vol. 29, No 2, 2013

M. Meints, "The Relationship between Data Protection Legislation and Information Security Related Standards", http://link.springer.com/chapter/10.1007%2F978-3-642-03315-5_19#page-1.

M. Arning, N. Forgó, R. Kollek, T. Kruegel, "Data protection in grid-based multicentric clinical trials: killjoy or confidence-building measure?", Phil. Trans. R.Soc. A 2009 367, pp. 2729-2739.

N. Forgó, Kollek et al., *Ethical and Legal Requirements for Transnational Genetic Research*, UK, VCH Beck, 2010.

NIH, Protecting Personal Health Information in Research

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", 57 UCLA Law Review 1701 (2010), pp. 1756.

Räther/Seitz, Übermittlung personenbezogener Daten in Drittstaaten Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, p. 425, 427.

RCR, The Retention and Destruction of NHS and Private Patient Records: Updated Advice, http://www.rcr.ac.uk/docs/oncology/pdf/BFCO%2806%292_retention_of_records%282011%29.pdf, for a list of the minimum periods in the UK.

S. Rudgard, "Origins and historical context of data protection law" in E. Ustaran (ed) *Law and Practice for Data Protection Professionals*, IAPP, 2012, https://www.privacyassociation.org/media/pdf/publications/European_Privacy_Chapter_One.pdf.

S. Dammann, Simitis et. all, BDSG Kommentar, § 3, rec. 222.

Unofficial translation of the Belgium Constitution: http://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/grondwetEN.pdf.

Unofficial translation of the Dutch Constitution: http://legislationline.org/documents/section/constitutions/country/12.

Unofficial English translation of the Federal Data Protection Act, Switzerland, http://www.admin.ch/ch/e/rs/2/235.1.en.pdf.

US Department of Health and Human Services (HHS), *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82798 (Dec. 28, 2000) and 65 Fed. Reg. 82944 (Dec. 29, 2000), codified in Title 45 of the Code of Federal Regulations (CFR) Parts 160 and 164.

W. Nauwelaert, "The Belgian Privacy Commission's New Guidance on Information Security", World Data Protection Report, Vol. 13, No. 5, 2013

WHO, *Ethical issues in patient safety research interpreting existing guidance*, Geneva, 2013.

WHO Declaration of Helsinki, http://www.wma.net/en/30publications/10policies/b3/.

Other Internet Resources:

http://www.admin.ch/ch/d/sr/311_0/a321bis.html.

http://www.wma.net/en/30publications/10policies/d1/.

http://www.nhs.uk.

http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/acs.pdf.

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

http://www.schneier.com/twofish.html.

http://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/.

http://www.wired.com/opinion/2013/09/black-budget-what-exactly-are-the-nsas-cryptanalytic-capabilities/.

http://ethikkommission.meduniwien.ac.at/fileadmin/ethik/media/dokumente/rechtsgrundlagen/GCP.pdf

http://www.gfhev.de/de/qualitaetsmanagement/aufwahrungsfristen.pdf

Appendix 1 – Abbreviations and acronyms

ACGT	Advanced Clinico Genomic Trials
BDSG	German Federal Data Protection Act
CHIC	Computational Horizons In Cancer
CDP	Center for Data Protection
ICT	Information and Communication Technology
D	Deliverable
DoW	Description of Work
DPA	Data Protection Authority
DoH	Declaration of Helsinki
EURECA	Enabling information re-Use by linking clinical REsearch and CAre
ECHR	European Convention of Human Rights
EU	European Union
EEA	European Economic Area
EHR	Electronic Health Record
FADP	Federal Act on Data Protection (Switzerland)
GBM	Glioblastoma Multiforme
HIPAA	Health Insurance Portability and Accountability Act
IRB	Institutional Review Board
MRI	Magnetic Resonance Imaging
NSA	National Security Agency (US)
NSCLC	Non Small Cell Lung Cancer
OECD	Organization for Economic Cooperation and Development
PHI	Protected Health Information"
SIOP	International Society of Paediatric Oncology
SSL	Secure Sockets Layer

SIEM	Security Information and Event Management
TTP	Trusted Third party
VPH	Virtual Physiological Human
WP	Work Package
WWII	World War II
WMA	World Medical Association

Appendix 2 – Draft CHIC position paper

CHIC_Position Paper on the Draft Data Protection Regulation and Health Data Use for Research_LUH_ June 2013

Introduction

In this short position paper we should like to focus our discussion on the original form in which the Commission proposed to address the matter of health data processing for research, notably in articles 81 and 83 of the draft Regulation (dDPR) as published in January 2012.

Beginning first with the status quo ante under Directive 95/46/EC, in our view the three key problems that have remained unresolved for medical researchers wishing to use health data for research can be summarized as follows:

- Terminological and factual difficulties in deciding if some given data qualify as personal or not, so that the legal data protection framework applies notionally or not (a related ambiguity concerns how far processing of such data by anonymising or key-coding them are themselves operations that trigger the full legal obligations under that framework);
- Independent of the above, difficulty in deciding when the patient data subject should be approached for consent to data use, and if so what would count as appropriate consent in a given case;
- Independent of the above, difficulty in deciding when it would be appropriate or even mandatory to approach a review body of some kind, e.g. an ethics committee or data protection authority, for authorization of the proposed research using the data.

The first of these problems may be attributed to vagueness or lack of clarity in the Directive; however, the second and third issues, while contributed to by the Directive's shortcomings, are in our view at least as much a product of the confusing plethora of other norms which confront researchers in different countries in their daily practice on the ground, including professional and ethical 'best practice' guidance from a multitude of bodies and organizations.

In the light of this we believe that, as well as providing specific solutions to the above problems, the rules in the Regulation must at the same time 'make sense' in ethical and professional terms to researchers and other actors in the research community (such as ethics committees). Only then will they have a chance of being accepted by such actors as offering an authoritative unified model that deserves to be followed by them in practice (in preference to inconsistent soft-law norms). One aspect of this is that, besides providing a framework for facilitating medical research with health data, the rules must always be mindful of the values that animate professional and ethical guidance in this area, in terms of the protection so far as practical of patient privacy, dignity, and autonomy.

Articles 81 and 83 of the original dDPR

A *novum* in the draft Regulation is that "health data" are parceled off from other sensitive data and their processing made subject to additional provisions set out in article 81 of the draft. That article in its second paragraph provides in turn that health data processing for research is to be governed by the rules (applicable to processing data in general for research) found in article 83.

As we read this article, it seeks to distinguish between the 'processing' and the 'publishing' of personal health data for research purposes. The former is covered by 83(1), and may reasonably be interpreted as applying to controlled 'internal' uses of such data – e.g. by a limited number of

specified partners within a given research project. By contrast, 'publishing', which is governed by 83(2), appears to mean the disclosure or dissemination of personal health data to the world at large.

Consent is retained as a basis for legitimizing the latter activity, subject to being valid in line with the conditions set out in article 7 dDPR. However, consent is no longer mentioned as a requirement for the internal research use of data under article 83(1). In its place two other jointly necessary conditions are specified, namely that (a) it is not possible to do the research using non-personal data; and (b) the data is protected by pseudonymisation (key-coding) so far as this is consistent with fulfilling the research aim.

Subsequently, under article 83(3), the Commission is empowered to concretize in delegated legislation further conditions and circumstances in which the research processing of the data may occur. At the same time, such processing also remains subject to the more general data security requirements (under article 30 dDPR) and to safeguards under the 'data protection by design and default' provisions of article 23. Moreover, given its putative status as an operation of 'specific risk' under article 33(2)(b), the data controller will, before using the health data, probably need to conduct a data privacy impact assessment (and potentially refer the matter for prior checking under article 34).

Evaluation

We shall now consider the effectiveness of the above features as responses to the three key problems for researchers using health data that were identified in the introduction to this paper. In this regard we would make the following points:

(i) The problem of deciding if data is personal or not

- The general approach from the Directive, of using a standard of reasonable likelihood of re-identification, is continued in the Regulation. While noting that this by its nature makes it difficult for researchers on the ground to draw the line, we endorse this as a pragmatic and technology-neutral solution, but would however appreciate further discussion whether the "all or nothing approach" chosen (data is either personal or not – with nothing in between) is still the best way to go. We believe there are good arguments that some protection might also be needed for non-personal data as well as some reliefs might be appropriate for data on not directly identifiable subjects.

- Here article 83 (1)(b) would help researchers in any case by (as we understand it – the wording could be clearer…) telling them they can use data provided it has been pseudonymised/key-coded so far as possible. As noted above, our assumption is that what is here at stake is 'internal' uses of data within a closed team of partners to a particular research project; this is again something that should be spelt out more clearly.

- Art 83(1) appears also to allow that identified health data may be processed, i.e. by implication, insofar as neither anonymisation (under 83(1)(a)) nor pseudonymisation (under 83(1)(b)) are feasible for fulfilling the relevant research purpose. Here (and arguably already for 83(1)(b)) we believe a clause should be added setting out a further necessary condition for such data use, namely that the data controller adopts appropriate technical, organizational and legal safeguards to ensure access to the data is limited to researchers concerned in the relevant research project and bound by appropriate professional rules.

- As regards article 83(2) this in some circumstances allows publication of personal health data used in research to the world at large, e.g. where the subject has consented. We believe more thought should be given to this clause – arguably, even with subject consent, such data

should not be published if it is not really necessary (indeed this follows straightforwardly from the data-minimization principle). So at the very least, 83(2)(a) and (b) should be presented as jointly necessary conditions, i.e. connected by an 'and'.

(ii) Difficulties in relation to obtaining consent

- As noted, artide 83(1) would dispense with subject consent. Here, while noting the practical (logistical) and conceptual difficulties with the consent concept – which indeed may be added to if article 7(4) is adopted – we do not believe it should be abandoned entirely. Doing so is in any case likely to be of little effect, as practitioners on the ground (whose views, as argued in the introduction, should be taken account of) would continue to seek some form of subject agreement anyway as a key aspect of their perceived ethical and professional duties. At worst the effect may be to diminish practitioner and public confidence in the legal rules in this area.

- While thus wishing patient agreement to be retained, we would argue that in this context it needs to be re-thought. Indeed there is a growing consensus that full informed consent (in terms of specific detailed knowledge by research subjects as to each possible use of their data) does not provide a workable approach: we would thus suggest a provision is added clarifying that, wherever practical, some different and less onerous form of subject agreement / assent is obtained as necessary and sufficient for data processing for research.

(iii) The involvement of review bodies

- As in the case of subject consent, in our view the European legislator should begin with the reality that researchers on the ground for a variety of professional, ethical, and prudential reasons often wish to obtain some form of review and approval to their use of health data for research (even where the data is not obviously linkable to individual subjects, and/or where the subjects have agreed to the use). Indeed the need for such review – certainly if there are doubts as to subject consent - is set out in key international ethical documents, e.g. the Declaration of Helsinki (clause 25). But the existing position for researchers – especially those in trans-European research projects is here complicated by the proliferation of different ethical and professional review bodies, leading to delay, and inconsistency.

- In our view (despite paradoxically at first sight appearing to impose a further restraint on research), a great practical contribution could be made by article 83 if it were to institutionalize the need for research projects using health data to undergo such review (as presently drafted, it is possible prior-checking may be triggered under articles 33 and 34, but this remains somewhat unclear). Thought would need to be given to the details, e.g. establishing fast- and medium-track procedures where data is putatively anonymous, pseudonymous, etc. But if done well, this would lead to uniform, transparent and stream-lined procedures, improving confidence among researchers and the public alike. It would then be of utmost importance to how to achieve European standard procedures to regulate how Ethics Committees would deal with such requests.

Appendix 3 – CHIC WP 4 questionnaire

Please indicate the name of your institution

……

1. Will your institution be supplying data for the CHIC Project? ……..

2. If yes, please describe the nature and source of the data

……

……

3. If the data is retrospective, i.e. data that you previously collected or obtained, please describe:

   (i) the circumstances in which this occurred:

……

……

   (ii) the purposes for which the data was obtained/collected:

……

……

   (iii) (where the data relates or related to identifiable individual persons) whether those individuals ('data subjects') consented to the collection or transfer of their data [NB: in this case please also append a copy of the relevant consent/information sheet]:

……

……

4. If the data is prospective, i.e. to be collected or obtained in the future for the purposes of CHIC, please describe how this process is planned to occur:

……

……

……

5. Has the data been or will it be subject to any process of modification (e.g. aggregation, addition or removal of attribute fields, etc, before its provision to the Project? If so, please describe:

……

……

……

6. In the form that the data will be provided to the Project, will it in your view be:

   (i) Personally identified (i.e. contain one or more identifiers that alone or together directly single out the data subject);

   (ii) de-identified, but reasonably re-identifiable (i.e. the data still contains potential identifiers that do not directly single out the data subject, but where someone who has access to the data could make the linkage with relative ease)

   (iii) de-identified, and not reasonably re-identifiable

   Please explain briefly your reasons for holding this view:

   ……

   ……

   ……

7. Where measures have been or will be taken to de-identify the data, was/is this by means of pseudonymisation (where a key remains that would allow de-identified datasets to be officially re-linked to named data subjects) or full anonymisation (where there is no such key)

8. Do you think that the purpose of the CHIC Project can be achieved if the data is fully anonymised? Please briefly give your reasons:

……

……

……

9. Do you envisage any situation where re-identification of the data subject will be necessary?

   ……

   If yes, please briefly explain such situation:

   ……

   ……

10. Will your institution require data (personal or anonymised) to test the model or tool you are developing? ……

11. Please list the models, tools, software, etc that your institution will be using for developing your model/tool and indicate the licenses under which they were released:

SN	Models/Tools	Licenses

12. Will your institution be conducting a clinical trial within the CHIC Project?

……

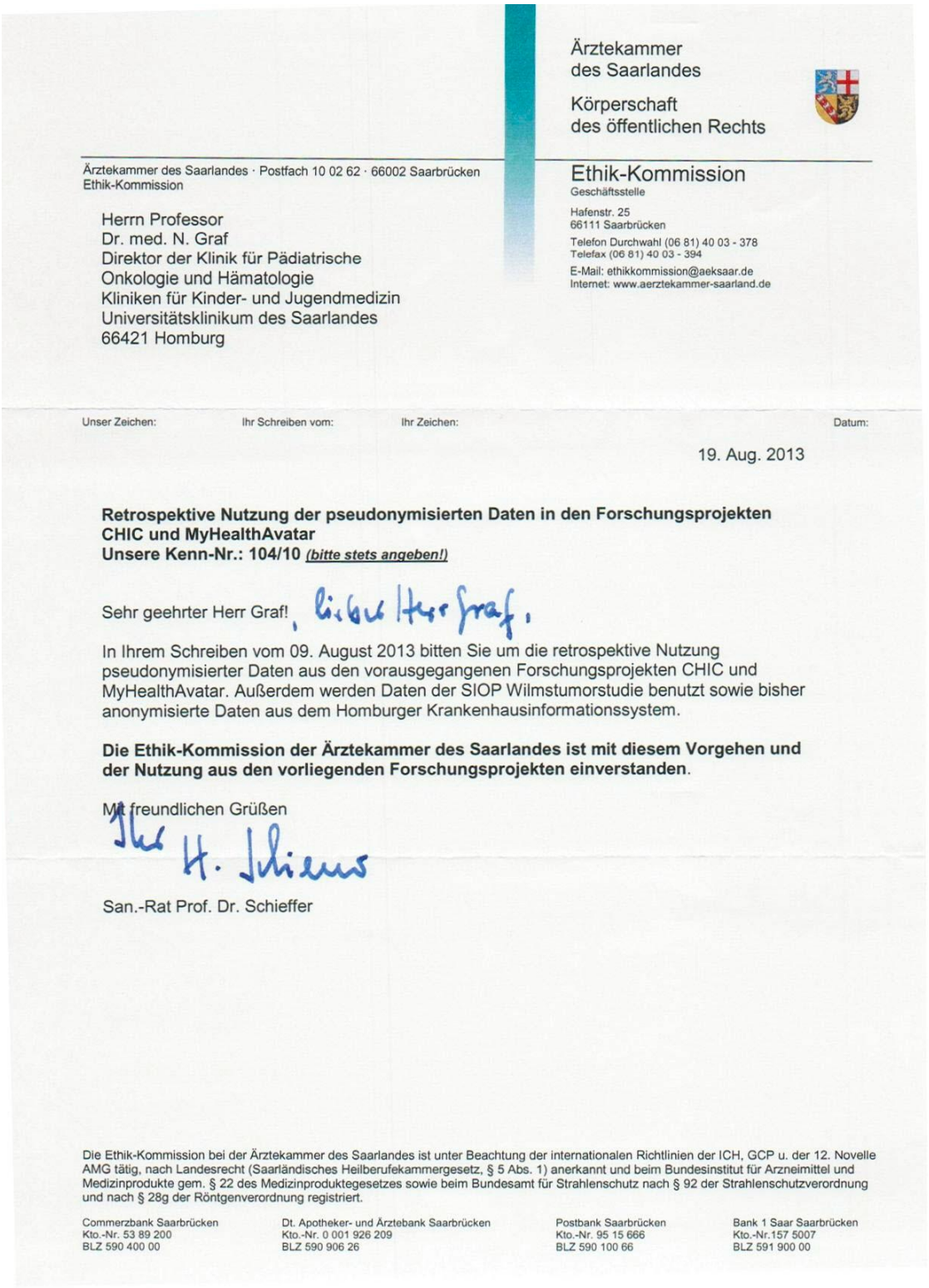
13. If yes, do you have an informed consent form developed for this clinical trial?

……

14. If yes, please append a copy of the consent form

Appendix 4 – Copies of Applicable Informed Consents and Ethics Approval for Data Provider Partners

01. Ethics Approval USAAR



Ärztekammer
des Saarlandes

Körperschaft
des öffentlichen Rechts

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

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

Ethik-Kommission
Geschäftsstelle

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

Unser Zeichen: | Ihr Schreiben vom: | Ihr Zeichen: | Datum:

19. Aug. 2013

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

Sehr geehrter Herr Graf! Lieber Herr Graf,

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

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

Mit freundlichen Grüßen

Ihr H. Schieffer

San.-Rat Prof. Dr. Schieffer

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

Commerzbank Saarbrücken
Kto.-Nr. 53 89 200
BLZ 590 400 00

Dt. Apotheker- und Ärztebank Saarbrücken
Kto.-Nr. 0 001 926 209
BLZ 590 906 26

Postbank Saarbrücken
Kto.-Nr. 95 15 666
BLZ 590 100 66

Bank 1 Saar Saarbrücken
Kto.-Nr.157 5007
BLZ 591 900 00

02. Consent Form KU Leuven

UZ LEUVEN | KINDERGENEESKUNDE

Professor Dr. Stefaan Van Gool
Kliniekhoofd Kinder-hemato/neuro-oncologie
Stefaan.Vangool@uz.kuleuven.ac.be
Tel. 32-(0)16-34 38 67
Fax. 32-(0)16-34 38 42

Professor Dr. Steven De Vleeschouwer
Adjunct-kliniekhoofd Neurochirurgie
Steven.Devleeschouwer@uz.kuleuven.ac.be
Tel. 32-(0)16-34 46 10
Fax. 32-(0)16-34 42 85

http://www.uzleuven.be **Universitaire Ziekenhuizen Leuven, Herestraat 49, 3000 Leuven** http://www.kuleuven.be
www.oliviafund.be, www.hmrf.be

Formulier Geïnformeerde Toestemming voor het HGG-2010 protocol

Een fase IIb prospectieve placebo-gecontroleerde dubbel blinde gerandomiseerde klinische studie voor de behandeling van patiënten met Hoog-Gradig Glioma graad IV met tumor vaccinatie als toegevoegde therapie aan de standaard behandeling

Opdrachtgever: UZ Leuven

Uitleg en verklaring tot akkoord

voor een behandeling volgens het protocol Hoog-Gradig Glioma-2010

Geachte mevrouw, geachte heer,

Uw behandelende geneesheer stelt u voor om deel te nemen aan een studie waarbij het effect van een experimentele immuuntherapie voor de behandeling van een kwaadaardige hersentumor wordt onderzocht. De kwaadaardige hersentumor heet hooggradig glioma graad IV of glioblastoma multiforme.

Doel van de behandeling

Het doel van dit onderzoeksprotocol is het aantonen dat de immuuntherapie als experimentele interventie in dit protocol een verbetering van de 6 maanden ziekte-vrije overleving kan induceren bij patiënten met een hooggradig glioma. Met het oog hierop wordt gepoogd om de groei van de tumor af te remmen door het afweersysteem (een andere naam is: immuunsysteem) van de patiënt te stimuleren tegen de tumor. Mogelijks kan ook een verkleining van minimaal resterend tumorweefsel bekomen worden. Natuurlijk wordt bij de evaluatie van een nieuwe therapie ook gekeken in welke mate de therapie verdragen wordt. Vanuit de studie van deze behandeling bij patiënten die een herval vertonen van een hooggradig glioma weten we reeds dat in die situatie de therapie zeer goed verdragen wordt, en dat bij sommige patiënten er gunstige klinische effecten zijn met langere overleving als gevolg.

Patiënten die in aanmerking komen voor de experimentele immuuntherapie

De patiënten die voor dit protocol in aanmerking komen zijn patiënten bij wie de diagnose van een hooggradig glioma graad IV voor het eerst wordt vastgesteld, waarbij de chirurg in staat is geweest om de tumor (sub)totaal te kunnen verwijderen, en waarbij voldoende weefsel kon bewaard worden voor de productie van de vaccinaties. Bovendien dienen de patiënten te voldoen aan de vooropgestelde criteria in deze studie (vb. serologie, leeftijd,…).

Achtergrond

Hooggradige glioma's, die ook wel hooggradige astrocytomen worden genoemd, zijn hersentumoren die snel groeien, die in het gezonde hersenweefsel infiltreren, en die kunnen uitzaaien vooral binnen de schedeldoos. Volgens hun agressief verloop worden ze verder ingedeeld in graad III glioma of anaplastisch astrocytoma en graad IV glioma of glioblastoma multiforme.

De behandeling van hooggradige glioma's blijft extreem moeilijk, ondanks maximale therapie met chirurgie, radiotherapie en chemotherapie.
De standaard behandeling van een patiënt met een hooggradig glioma bestaat uit een heelkundige ingreep, wat nodig is om het ruimte-innemend proces in de hersenen zo volledig mogelijk en veilig te verwijderen en om onder de microscoop naar het weefsel te kijken teneinde de juiste diagnose te kunnen stellen. Na de chirurgie volgt dan een periode van 6 weken radiotherapie in combinatie met het innemen van chemotherapie (het medicament noemt Temozolomide met als handelsnaam Temodal®). Enkele weken later wordt dan overgegaan tot een onderhoudschemotherapie met inname van Temozolomide gedurende 5 dagen, en dit om de 28 dagen gedurende 6 maanden (zes 5/28 dagen cycli).
De radiotherapie en chemotherapie zijn therapievormen die biologisch niet heel specifiek gericht zijn, enkel tegen de tumor. Bij andere tumoren evenwel is de medische wereld erin geslaagd om tegen de tumor gerichte actieve specifieke immuuntherapie te ontwikkelen, met gunstige klinische resultaten als gevolg. We weten dus dat tumor-specifieke immuuncellen, die we T cellen noemen, kunnen geactiveerd worden tegen sommige tumoren. Daarbij speelt uiteraard het soort tumorweefsel een rol, en meer bepaald de eiwitten die zich op het celoppervlak van de tumor situeren.
Hoe is de interactie tussen de hersentumor en het afweersysteem ? Belangrijk in een dergelijke interactie zijn de zogenaamde tumorantigenen. Dit zijn eiwitten die door de tumorcellen op het celoppervlak gebracht worden, maar die door het tumorale karakter van de cel verkeerd gebouwd zijn, en dus eigenlijk lichaamsvreemd zijn. We weten dat in deze soort tumoren, de T cellen ook zonder actieve specifieke immuuntherapie in het tumoraal weefsel binnendringen (Tumor-Infiltrerende Lymfocyten of TIL). Bij hooggradige astrocytomen is het eveneens zo dat er TIL te zien zijn bij pathologisch onderzoek. Maar uit literatuurgegevens weten we dat de tumorcellen cytokines produceren (dat zijn hormonen maar met een zeer gelokaliseerde werking enkel op de cellen in de buurt), die de T cel functie onderdrukken. Dus, hoewel de T cellen de tumor herkennen via hun antigeen, en de tumor zouden willen doden, worden zij in hun werking onderdrukt.
Er is nog een ander probleem. Vooraleer T cellen adequaat geactiveerd worden, moeten ze niet alleen de tumorantigenen herkennen als lichaamsvreemd, maar zijn er ook andere signalen nodig. Als het ware zijn er bijkomende sleutels en schakelingen nodig om de motor op gang te krijgen. De cel die beschikt over de capaciteit om antigenen te presenteren en terzelfdertijd de nodige bijkomende signalen op gang kan brengen is de dendritische cel (kortweg DC). Deze cellen zijn de krachtigste cellen om het immuunsysteem te activeren. Hoewel deze cellen in sommige tumoren kunnen binnendringen om antigenen te gaan oprapen, geraken zij niet bij hooggradige astrocytomen, waarschijnlijk ondermeer omwille van de bloed-hersen-barriere.
Dankzij een combinatie van verschillende vooruitgangen binnen de basiswetenschappen kunnen we het volgende realiseren met het oog op actieve specifieke immuuntherapie, ook wel therapeutische tumor vaccinatie genoemd. Het tumorweefsel kan in het laboratorium tot een lysaat gemaakt worden, waarin de tumoreiwitten of tumorantigenen aanwezig zijn. We kunnen uit het bloed van de patiënt bepaalde witte bloedcellen isoleren, en deze in het labo laten uitrijpen tot DC. We kunnen in het labo dan deze DC beladen met tumorlysaat, opdat deze DC de tumorantigenen op een immunologisch juiste manier aanbieden aan de T cellen. De beladen DC kunnen we in de huid inspuiten opdat zij zich zouden verplaatsen, zoals zij dit in gewone omstandigheden steeds doen, naar de lymfeknopen, om daar de T cellen te activeren tegen het antigeen, in dit geval dus het tumorantigeen. Deze geactiveerde T cellen tegen de tumorantigenen kunnen in het bloed circuleren, en naar de tumorcellen gaan om deze kapot te maken. Daar een overaanbod aan tumorcellen de werking van de geactiveerde T cellen zou kunnen tegenwerken, wordt dit principe bij voorkeur toegepast, wanneer er na de operatie hoogstens een minimale tumorrest aanwezig is.
Het principe om een antitumorale therapie toe te passen door middel van met tumorantigenen beladen DC is reeds aangetoond bij patiënten met huidkanker (melanomen), nierkanker (niercel carcinoom) en prostaatkanker. Ook bij lymfeklierkanker en borsttumoren zijn er gelijkaardige therapieconcepten in ontwikkeling. Voor hersentumoren is er een bijkomend probleem dat de bloed-hersen-barriere mogelijkerwijze de hersenen afsluit van immunologische reacties. Maar precies in het tumoraal weefsel zijn er voldoende aanwijzingen dat de bloed-hersen-barriere ter plaatse verstoord is. Bovendien tonen experimenten op proefdieren aan dat immuuntherapie via DC wel degelijk een tumor binnen de hersenen kan bereiken.
Bij de mens zijn er slechts enkele groepen die een gelijkaardige strategie ontwikkelen. De rapporten vanwege de groep van Los Angeles betreffende de verdraagzaamheid van de therapie en onze eigen ervaringen leren ons dat er geen majeure neveneffecten zijn. Over de doeltreffendheid van de therapie kan op dit moment geen uitspraak gedaan worden. Deze belangrijke vraag is het onderwerp van het u voorgestelde studieprotocol HGG-2010. De grote ervaring in UZ Leuven bevestigt wel dat de behandeling geen majeure toxiciteit induceert, en dat met deze technologie de levensverwachting van sommige patiënten kon verbeterd worden bij wie de tumor teruggekomen was na de standaard radio- en chemotherapie.

Elementen in de behandeling

1. Radiotherapie. Dit is een standaard behandelingstechniek gedurende 6 weken voor de behandeling van hooggradige gliomen. Uw radiotherapeut zal u alle uitleg verstrekken. Omdat deze behandeling reeds gecombineerd wordt met chemotherapie, noemen we deze fase van de behandeling radiochemotherapie. De nevenwerkingen van radiotherapie zijn

voornamelijk zichtbaar op langere termijn. Er kunnen hormonale stoornissen optreden wanneer de stralenbundel eveneens een centrale klier in de hersenen (de hypofyse) raken. Deze hormonale stoornissen kunnen perfekt opgevangen worden door een arts-endocrinoloog. Door radiotherapie kunnen er minimale cognitieve functiestoornissen zich voordoen. Tenslotte merkt men soms op dat de haargroei op de plaats van de intrede van de stralenbundel verminderd is.

2. Chemotherapie. Chemotherapie heeft als doel om cellen met een ongecontroleerde celdeling (tumorale celdeling) te vernietigen, terwijl gezonde cellen kunnen herstellen. Temodal®.is een standaard medicament voor de behandeling van hooggradige gliomen. Temodal® wordt dagelijks genomen tijdens de radiotherapie (radiochemotherapie), en nadien gedurende 5 dagen om de 4 weken als onderhoudschemotherapie (zes 5/28 dagen cycli). Uw medisch oncoloog zal u alle uitleg verstrekken. De nevenwerkingen van chemotherapie zijn voornamelijk zichtbaar tijdens de therapie periode, en zijn multipel. Op niveau van comfort van de patiënt is vooral de chemotherapie-geïnduceerde misselijkheid de belangrijkste. Evenwel zijn er nieuwere medicaties die op deze vorm van misselijkheid heel sterk inwerken, zodat deze tot een minimum kan herleid worden. Bij sommige patiënten is er een beperkte haaruitval. Verder kan de aanmaak van de verschillende bloedcellen in het beenmerg dalen. Door de te lage rode bloedcellen zal de patiënt bleek zien en vermoeid zijn. Een eventuele transfusie van rode bloedcellen kan hieraan verhelpen indien de arts dit noodzakelijk acht. Door de te lage bloedplaatjes zal de bloedingsneiging iets vergroten. Indien de bloedplaatjes te laag zijn, zullen bloedplaatjestransfusies gegeven worden. Op basis van eerder opgedane ervaring met het toedienen van Temodal® weten we dat de nood aan transfusies uiterst zeldzaam is. Door de te lage witte bloedcellen zal de patiënt meer vatbaar zijn voor infecties. Daarom worden er voor alle patiënten preventiemaatregelen ingesteld om maximaal infecties te voorkomen, zoals het nemen van 1 antibioticum tijdens de radiochemotherapie.

3. Tumor vaccinatie

- **Tumorantigenen.** De tumor wordt op steriele wijze verwerkt tot een lysaat. De aanwezige tumoreiwitten of tumorantigenen worden gebruikt om de DC te beladen. Het is absoluut uitgesloten dat er levende tumorcellen nog aanwezig zijn in het verwerkte lysaat.
- **DC.** De DC worden gekweekt uit monocyten, een bepaalde soort witte bloedcellen, die circuleren in het bloed. De benodigde witte bloedcellen zullen afgenomen worden via een toestel, reeds voor de radiochemotherapie. Deze procedure noemen we leukaferese. Bij een leukaferese wordt bloed uit de patiënt genomen via een intraveneuze toegangslijn. Het bloed wordt in het toestel gecentrifugeerd, en op deze manier kunnen de witte bloedcellen er selectief uitgehaald worden. De bloedplaatjes, de rode bloedcellen en het plasma worden daarna via een andere intraveneuze toegangslijn aan de patiënt terug gegeven. Alles gebeurt op een steriele wijze. De totale procedure duurt ongeveer 4 uren. Het betreft hier een zeer gekende techniek, die bij heel veel patiënten voor verschillende redenen wordt toegepast. De ervaring met deze techniek leert dat er nagenoeg geen complicaties voorkomen. Deze witte bloedcellen zullen in het laboratorium ingevroren worden. Voor het aanmaken van elk vaccin zullen een gedeelte van de witte bloedcellen ontdooid worden, om de monocyten eruit te halen, die dan verder gedurende een cultuurperiode van 1 week met cytokines worden bewerkt tot ze omgevormd zijn tot onrijpe DC. Deze onrijpe DC worden dan vervolgens beladen met de tumorantigenen uit het tumorlysaat, en worden verder gerijpt door toevoegen van stimulerende cytokines.
- **Vaccinatie met DC.** De beladen rijpe DC worden door middel van 4 wekelijkse injecties (afhankelijk van het aantal cellen die uit de cultuur bekomen werden) in de huid van de bovenarm (intradermaal) ingespoten. Elke intradermale injectie gelijkt erg op de manier van inspuiten tijdens de Mantoux proef om TBC op te sporen. Deze verschillende injecties die op 1 ogenblik worden ingespoten vormen 1 vaccin. Vier wekelijkse vaccins worden voorzien na de radiochemotherapie. Na elke vaccinatie wordt u een vragenlijst aangeboden waar gepeild wordt naar de graad van zelfredzaamheid en naar de kwaliteit van leven onder de therapie. Deze vragenlijsten zijn gevalideerd en internationaal erkend voor de evaluatie van zelfredzaamheid en kwaliteit van leven bij patiënten met hersentumoren.
- **Vaccinatie met lysaat.** Na de eerste 4 vaccinaties met DC wordt gestreefd naar een onderhoud van de immuun reactiviteit. Om het immuun systeem alert te houden worden om de maand in totaal 3 zogenaamde "boost" vaccinaties gegeven met lysaat, en een vierde na 3 maanden. Hierbij zullen telkenmale twee spuitjes in de huid gegeven worden. In functie van de hoeveelheid materiaal dat ter beschikking is, kan het zijn dat de derde boost niet kan gegeven worden, of eveneens dat er meerdere boost kunnen worden ingespoten dan de 4 geplande. De boost vaccins worden gepland op dag 8 van de 5/28 dagen cycli 1, 2, 3 en 6.
- **Imiquimod crème (Aldara ®).** Om de maturiteit van de DC en de reactiviteit tegen het Lysaat te versterken moet de avond voor de vaccinatie met DC of Lysaat de crème Aldara aangebracht worden op de huid op de plaatsen waar de inspuitingen zullen gegeven worden. Deze plaatsen zullen door uw arts zorgvuldig uitgelegd worden. Voor het aanbrengen van de crème dienen de handen zorgvuldig gewassen te worden. De crème moet in een dun laagje aangebracht worden tot de crème geheel is ingedrongen. Er mag geen verband of pleister nadien gebruikt worden om de plaats te bedekken. Na toediening van de crème dienen de handen terug zorgvuldig gewassen te worden. De crème blijft gedurende de gehele nacht ter plaatse (een tiental uur). 's Morgens wordt de plaats gewassen met zeep en water. Ook de avond na de vaccinatie en de daaropvolgende avond moet opnieuw Aldara aangebracht worden. Dit wil dus

zeggen dat per vaccinatie de avond voordien en twee avonden nadien behandeld wordt met Aldara. Voor elke toediening dient een nieuw zakje gebruikt te worden, dus 3 zakjes voor 3 nachten per vaccinatie moment. In de verpakking zijn er 12 zakjes. Er zijn mogelijks enkele nevenwerkingen te verwachten, die gekend zijn bij gebruik van Aldara®: lokale huidreacties, waaronder roodheid, huiderosie, schilfering, vervelling en huidzwelling. Verharding, verzwering, korstvorming en vorming van blaren zijn minder te verwachten. De meeste huidreacties die werden geobserveerd na het gebruik van Aldara® voor andere indicaties waren licht tot matig van ernst en verdwenen binnen twee weken na het staken van de behandeling. Een aantal systemische reacties, waaronder hoofdpijn, griepachtige symptomen en spierpijn, werden eveneens beschreven bij patiënten die behandeld werden met imiquimod crème.

- **Immuunmonitoring.** Immuunmonitoring wil zeggen: het meten in het lichaam of er een reactie van het afweersysteem is opgewekt tegen de tumor antigenen. De immuunmonitoring zal gebeuren op vastgelegde tijdstippen. Er zullen speciale bloednames uitgevoerd worden, waarbij in het laboratoratorium dan verder zal onderzocht worden of de witte bloedcellen, die genomen worden op verschillende tijdstippen tijdens de vaccinatie, in toenemende mate reageren tegen de tumor antigenen.

Schema van het HGG-2010 protocol

In het HGG-2006 protocol dat afgesloten werd in februari 2009, werd immuuntherapie reeds geïntegreerd in de multimodale standaardbehandeling voor patiënten met een eerste diagnose van glioblastoma multiforme. Op basis van het doorvoeren van dit protocol kunnen we stellen dat de gezamelijke therapie goed haalbaar is, en de toxiciteit door de immuuntherapie niet wordt versterkt.
De toegevoegde waarde van actieve specifieke immuuntherapie kan enkel nagegaan worden indien in een en hetzelfde protocol een experimentele behandelingsgroep patiënten de standaardbehandeling met de immuuntherapie krijgt, terwijl een standaard behandelingsgroep patiënten enkel de standaardbehandeling zonder de immuuntherapie krijgt, doch wordt ingespoten met een placebo product. Beide groepen patiënten zullen volledig vergelijkbaar zijn rekening houdend met de gezamelijke gegevens van leeftijd, graad van zelfredzaamheid (Karnofsky index), mentale status en uitgebreidheid van resectie (de RPA klassificatie). De al dan niet aanwezigheid van immuuntherapie in het totale behandelingstraject zal onbekend blijven voor u, voor de radiologen die de status van de tumor radiologisch opvolgen, en voor de dienst psychodiagnostiek die de zelfredzaamheid en de kwaliteit van leven opvolgen. Een scanner na de zesde cyclus Temodal® bij elke patiënt bepaalt het resultaat van de interventie ten opzichte van de controle. Op dat moment wordt immers gekeken naar het % ziektevrije patiënten in de experimentele behandelingsgroep ten opzichte van de standaard behandelingsgroep.
Beide groepen patiënten zullen een leukaferese ondergaan, en de witte bloedcellen zullen ingevroren worden. Deze witte bloedcellen zullen naar een vaccin verwerkt worden na de radiochemotherapie enkel voor de patiënten die behoren tot de experimentele groep en niet tot de standaard behandelingsgroep. Na de zesde cyclus Temodal® en de daaropvolgende controle scan, wordt vermeld of de patiënt al dan niet gevaccineerd is geweest. De patiënten die tot de standaard behandelingsgroep behoorden zullen op dat moment opstarten met actieve specifieke immuuntherapie. Bij hen zullen op dat moment de ingevroren witte bloedcellen naar een vaccin verwerkt worden. Hiermee wordt bekomen dat ook deze controle patiënten toch de 4 therapie modaliteiten (chirurgie, radiochemotherapie, chemotherapie en immuuntherapie) bekomen. Hiermee wordt een tweede vraag in het protocol beantwoord, met name of er een betere immuunrespons na chemotherapie kan bekomen worden dan tijdens chemotherapie. Dit laatste is dan weer belangrijk voor het uittekenen van combinatie therapieën in latere behandelingsprotocollen.

Controle van de behandeling

Naast regelmatig klinisch en neurologisch onderzoek zijn regelmatige controles voorzien via een scanner, ook wel kernspintomografie (KST) of magnetische resonantie (MRI) genoemd. Hierbij wordt gekeken naar het volume van de tumorale massa, alsmede naar het peritumoraal oedeem. Een PET scan (Positron Emission Tomografie) zal eventueel uitgevoerd worden op indicatie van de behandelende arts om eventuele locale processen ter hoogte van de tumorstreek optimaal te kunnen interpreteren.
De immunisatie zal opgevolgd worden via bloednames en gespecialiseerd laboratorium onderzoek.

Risico's en Nevenwerkingen

Bij de herhaalde injecties kan er roodheid en zwelling optreden ter hoogte van de injectieplaats. Eveneens kunnen de lymfeknopen zwellen en licht pijnlijk worden door de immuun activering. Deze nevenwerkingen bleken tot hiertoe dermate minimaal te zijn dat er geen specifieke behandeling nodig was.
Allergische reacties zijn niet te verwachten gezien de bloedcellen van de patiënt zelf afkomstig zijn, en gezien er geen substanties van andere mensen of van dieren (lichaams-vreemde eiwitten) gebruikt worden.

Auto-immuun reactie is een groot *theoretisch* risico. Met name stimuleren we het immuunsysteem tegen de hersenentumor, maar is er het risico dat er ook tegen eiwitten die op de normale hersencellen aanwezig zijn een immuunrespons geïnduceerd wordt. Daarbij zouden theoretisch alle mogelijke en zelfs vitale hersenfuncties kunnen aangetast worden. In geval zich zo'n situatie voordoet moeten onmiddellijk sterke ontstekingsremmende medicamenten toegediend worden, voornamelijk een hoge dosis cortisone. Er moet evenwel opgemerkt worden dat deze nevenwerking tot heden niet werd waargenomen in de dierexperimenten, bij de gerapporteerde behandelde patiënten in de medische literatuur, en bij de in Leuven behandelde patiënten tot hiertoe.

Duur van de behandeling

Het behandelingsprotocol duurt in totaal 74 weken.

Opvolging na de behandeling

Na de behandeling zal een klassieke oncologische opvolging gebeuren. Voor het eerste jaar opvolging na de vaccinaties zal om de 3 maanden een klinisch onderzoek uitgevoerd worden. Om de 3 maanden is eveneens een kernspintomografie voorzien.
De controles zullen progressief minder frequent worden gedurende de verdere jaren opvolging, op indicatie van de behandelende geneesheer.

Onderzoeksgroep

De eerste **pre-klinische faze** van het onderzoek, met name de bewijsvoering dat humane T cellen kunnen geactiveerd worden tegen glioblastoma tumor cellen door stimulatie met beladen DC, en dat deze T cellen de groei van de glioblastoma tumor cellen dan afremmen, werd uitgevoerd in het Laboratorium Experimentele Immunologie, dat geleid wordt door Professor Dr. Jan Ceuppens, binnen de onderzocksgroep van Professor Dr. Stefaan Van Gool, kinderneuro-oncoloog. De pre-klinische experimenten werden uitgevoerd door Dr. Steven De Vleeschouwer en mevrouw Martine Adé.
De **piloot fase van de klinische toepassing** werd opgezet door Dr. Stefan Rutkowski onder supervisie van Professor Dr. Joachim Kühl, in de Universitäts-Kinderklinik te Würzburg en Professor Dr. Stefaan Van Gool. Professor Dr. Ecki Kämpgen van de universiteit te Erlangen is mee betrokken als onderzoeker.
Het **klinisch protocol HGG-IMMUNO-2003 voor patiënten met een herval van een hooggradig glioma** werd vervolgens ontwikkeld door Professor Dr. Stefaan Van Gool, in samenwerking met de dienst neurochirurgie en de dienst medische oncologie van UZ Leuven, en in samenwerking met de universiteiten van Würzburg en Regensburg.
Het **klinisch protocol HGG-2006 voor patiënten met een eerste diagnose van hooggradig glioma graad IV** en waarbij de immuuntherapie werd geïntegreerd in de multimodale standaardtherapie werd uitgevoerd onder leiding van Professor Dr. Steven De Vleeschouwer van de dienst neurochirurgie in UZ Leuven. De verantwoordelijkheid voor het deel immuuntherapie berustte bij Professor Dr. Stefaan Van Gool.
Het voorliggende **klinisch protocol HGG-2010 voor patiënten met een eerste diagnose van hooggradig glioma graad IV** werd ontwikkeld door Professor Dr. Stefaan Van Gool en Professor Dr. Steven De Vleeschouwer (de onderzoekers), in samenwerking met de dienst neurochirurgie (Professor Dr. Frank Van Calenbergh, Professor Dr. Jan Goffin), de dienst medische oncologie (Professor Dr. Paul Clement) en de dienst radiotherapie (Professor Dr Johan Menten).

Behandelende artsen

De verantwoordelijkheid van de chirurgie berust bij uw neurochirurg. De verantwoordelijkheid van de radiotherapie berust bij uw radiotherapeut. De verantwoordelijkheid van de chemotherapie berust bij uw medisch oncoloog. Volgens organisatie ter plaatse in uw ziekenhuis zal 1 van deze collega's ook de coördinatie van de totaal zorg en de communicatie naar het studiecentrum in Leuven op zich nemen.
De verantwoordelijkheid voor de globale uitvoering van het behandelingsprotocol HGG-2010, in het bijzonder de controle op de correcte toediening van de verschillende therapie onderdelen zoals voorzien in het protocol alsook de integratie van de vaccinatie als vierde onderdeel van uw totale behandeling zal berusten bij Professor Dr. De Vleeschouwer. Professor Dr. Stefaan Van Gool is verantwoordelijk voor de productie van de vaccinaties en de praktische uitvoering van de immuuntherapie.
Stalen, die overblijven na therapie, kunnen geanonimiseerd verder gebruikt worden voor strikt wetenschappelijke onderzoek in immuuntherapie met dendritische cellen, tenzij de patient zich hiertegen verzet.
De verantwoordelijke onderzoekers zullen de gegevens gebruiken voor wetenschappelijke mededelingen en discussies, met uitzondering van die gegevens die zouden toelaten om de patiënt te identificeren.

Kosten en verzekering

Alle kosten, eigen aan de vaccinatietherapie, zullen gedragen worden door de onderzoeksgroep. Hierin zijn gevat: de aferese en zo nodig hiervoor de plaatsing van een diepe veneuze catheter, de virologische screening, de productiekosten voor het aanmaken van de vaccins (minimum 4000 euro, in functie van het aantal gekweekte dendritische cellen) en de honoraria voor klinische opvolging op de ogenblikken van vaccinatie toediening. Bijkomende klinische en technische onderzoeken op indicatie van de neurochirurg, radiotherapeut of medisch oncoloog vallen niet onder deze regeling.
Conform de Belgische wet van 7 mei 2004 inzake experimenten op de menselijke persoon, is de opdrachtgever zelfs foutloos, aansprakelijk voor alle schade die de deelnemer en/of zijn rechthebbenden opgelopen en die rechtstreeks dan wel onrechtstreeks verband houdt met de proef. De opdrachtgever van de studie HGG-2010 heeft een verzekering afgesloten die deze aansprakelijkheid dekt. Indien U schade zou oplopen ten gevolge van uw deelname aan deze studie zal de schade bijgevolg worden vergoed conform de Belgische wet van 7 mei 2004.

UNIVERSITAIRE ZIEKENHUIZEN LEUVEN

Professor Dr. Stefaan Van Gool
Kliniekhoofd Kinder-hemato/neuro-oncologie
Stefaan.Vangool@uz.kuleuven.ac.be
Tel. 32-(0)16-33 22 11; zoeker 43345
Fax. 32-(0)16-34 38 42

Professor Dr. Steven De Vleeschouwer
Adjunct-kliniekhoofd Neurochirurgie
Steven.Devleeschouwer@uz.kuleuven.ac.be
Tel. 32-(0)16-33 22 11; zoeker 44802
Fax. 32-(0)16-34

http://www.uzleuven.be **Universitaire Ziekenhuizen Leuven, Herestraat 49, 3000 Leuven** http://www.kuleuven.be

Verklaring tot akkoord voor deelname aan het HGG-2010 behandelingsprotocol

- *Ik ben over de immuun therapie met dendritische cellen, die in het laboratorium beladen werden met tumorantigenen, voldoende geïnformeerd.*
- *Ik ben volledig op de hoogte van het experimentele karakter van de therapie, en begrijp volledig de theoretische achtergrond die heeft geleid tot de ontwikkeling van deze therapie.*
- *Ik ben op de hoogte van de ingrepen en maatregelen ten gevolge van de therapie.*
- *Ik ben op de hoogte van de mogelijke nevenwerkingen.*
- *Ik heb de gelegenheid gehad om al mijn vragen uitvoerig te stellen, tot ik de antwoorden erop volledig begrepen heb.*
- *Het nut van de experimentele immuun therapie werd overwogen in het licht van de mogelijke risico's.*
- *Ik geef WEL/GEEN * toestemming om de stalen die overblijven na therapie te gebruiken voor wetenschappelijk onderzoek voor immunotherapie met dendritische cellen.*
- *Ik ben op de hoogte dat de medische gegevens zullen gebruikt worden voor wetenschappelijke mededelingen en discussies, met uitzondering van die gegevens die zouden toelaten om mij als patiënt te identificeren.*

- Ik heb het recht ten allen tijde te stoppen met verdere vaccinaties, zelfs zonder dat redenen dienen geduid te worden, en heb de absolute garantie dat dan opnieuw door de verantwoordelijke professoren zal gezocht worden naar gepaste behandelings-modaliteiten in deze omstandigheden.

Leuven, _____/_____/_____

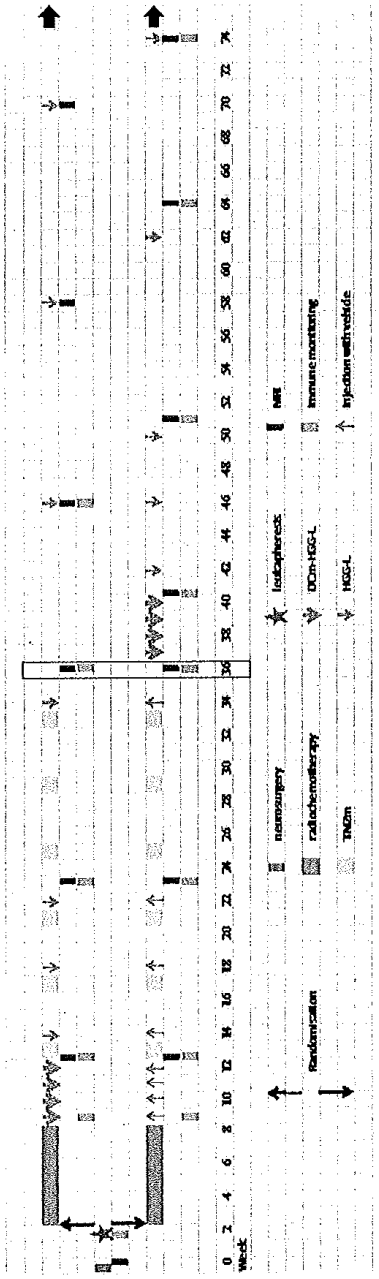
Patiënt *Onafhankelijke getuige*

Professor Dr. Stefaan Van Gool *Professor Dr. Steven De Vleeschouwer*

**Schrappen wat niet past*

HGG-2010 outline

8



03. Ethics Approval KU Leuven

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 1 dd. 23 augustus 2011)
LEUVEN: 5 september 2011

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 K.U.Leuven heeft vermeld protocol initieel goedgekeurd op 1 maart 2010.

Op 1 september 2011 werden bijkomende documenten met betrekking tot bovenvermeld protocol ingediend bij de Commissie Medische Ethiek van de Universitaire Ziekenhuizen K.U.Leuven:

- Patient information sheet and IC
  HGG-2010; ICF amendment 20110822

Deze documenten werden onderzocht en goedgekeurd op 3 september 2011.

Met de meeste hoogachting,

p/o Dr. J. WILDIERS
Internist
Jagersdreef 5
3210 LUBBEEK-LINDEN
1.02117.24.580

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

UZ LEUVEN
COMMISSIE VOOR MEDISCHE ETHIEK
KLINISCH ONDERZOEK

SECRETARIAAT: **H. HUYGHE** **M. LEYS** **N. OPDEKAMP** **M. SAELENS** **D. VAN MOLL** **M. VERBEECK**
Tel. +32-16 34 86 00 Fax. +32-16 34 86 01 ec@uzleuven.be ec-submission@uzleuven.be www.uzleuven.be/ec

04. Ethics Approval UNITO]

FONDAZIONE PIEMONTESE
PER LA RICERCA SUL CANCRO
ONLUS

COMITATO ETICO

Candiolo, 9 luglio 2013

Dott. Pietro Gabriele
Responsabile U.O.A.
di Radioterapia
IRCC CANDIOLO

OGGETTO: Valutazione "Studio osservazionale retrospettivo multicentrico per la definizione di modelli prognostici sul cancro prostatico in pazienti operati – European multicentric Retrospective Study evaluating prognostic factors on prostate K (CAncer) in prostatectomysed patients " – EUREKA-1

Le comunico che nella seduta dell'8 luglio 2013 il Comitato Etico dell'Istituto, esaminato e discusso il protocollo in oggetto, ha espresso **parere favorevole.**

Si fa presente che:
La sperimentazione va condotta nel rispetto della normativa vigente e dei regolamenti dell'istituzione presso la quale deve essere svolta, secondo i principi etici fissati nella Dichiarazione di Helsinki e della buona pratica clinica (D.M.S. 15.07.1997).
Si fa, inoltre, presente che lo sperimentatore ha l'obbligo di comunicare la data di inizio della sperimentazione.
Il responsabile della sperimentazione ha l'obbligo di riferire immediatamente al Comitato Etico indipendente:

- le eventuali variazioni del protocollo;
- tutte le reazioni avverse da farmaci soprattutto se serie ed inattese;

segue

Indirizzo Strada Provinciale 142, Km 3.95, 10060 Candiolo (TO) **T** 011.9933.380 - **F** 011.9933.389 **c/c Postale** 410100 - **C. F.** 97519070011 **UniCredit IBAN** IT 64 T 02008 01154 000008780163 - **Intesa Sanpaolo IBAN** IT 07 O 03069 01000 100000516980 - **web** www.fprconlus.it - **e-mail** fprc@fprconlus.it

Riconoscimento della Regione Piemonte: D.G.R. 22/07/1986 n° 3-6673 - Iscrizione anagrafe Onlus prot. n. 9882440 del 19/06/1998

2)

- ogni nuova informazione che possa incidere negativamente sulla sicurezza dei soggetti e sulla conduzione dello studio.

Lo sperimentatore deve dare comunicazione sulla conduzione dello studio al Comitato Etico ogni anno e, comunicare senza ritardo, l'esito della sperimentazione.

Con i migliori saluti

Il Presidente
(Carlo Luda di Cortemiglia)

Prot. C.E. 0171/2013

brl/CLC

FONDAZIONE PIEMONTESE
PER LA RICERCA SUL CANCRO
ONLUS

COMITATO ETICO

Candiolo, 9 luglio 2013

Dott. Pietro Gabriele
Responsabile U.O.A.
di Radioterapia
IRCC CANDIOLO

OGGETTO: **Valutazione** "Studio osservazionale retrospettivo multicentrico per la definizione di modelli prognostici sul cancro prostatico in pazienti radio trattati" EUREKA-2

Le comunico che nella seduta dell'8 luglio 2013 il Comitato Etico dell'Istituto, esaminato e discusso il protocollo in oggetto, ha espresso **parere favorevole.**

Si fa presente che:
La sperimentazione va condotta nel rispetto della normativa vigente e dei regolamenti dell'istituzione presso la quale deve essere svolta, secondo i principi etici fissati nella Dichiarazione di Helsinki e della buona pratica clinica (D.M.S. 15.07.1997).
Si fa, inoltre, presente che lo sperimentatore ha l'obbligo di comunicare la data di inizio della sperimentazione.
Il responsabile della sperimentazione ha l'obbligo di riferire immediatamente al Comitato Etico indipendente:

- le eventuali variazioni del protocollo;
- tutte le reazioni avverse da farmaci soprattutto se serie ed inattese;

segue

ISTITUTO DI CANDIOLO

Indirizzo Strada Provinciale 142, Km 3.95, 10060 Candiolo (TO) **T** 011.9933.380 - **F** 011.9933.389 **c/c Postale** 410100 - **C. F.** 97519070011 **UniCredit IBAN** IT 64 I 02008 01154 000008780163 - **Intesa Sanpaolo IBAN** IT 07 O 03069 01000 100000516980 - **web** www.fprconlus.it - **e-mail** fprc@fprconlus.it

2)

- ogni nuova informazione che possa incidere negativamente sulla sicurezza dei soggetti e sulla conduzione dello studio.

Lo sperimentatore deve dare comunicazione sulla conduzione dello studio al Comitato Etico ogni anno e, comunicare senza ritardo, l'esito della sperimentazione.

Con i migliori saluti

Il Presidente
(Carlo Luda di Cortemiglia)

Prot. C.E. 0172/2013

brl/CLC