Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, 11-13 November 2012

Legal and Ethical Issues in Integrating and Sharing Databases for Translational Medical Research within the EU

Iheanyi Nwankwo, Stefanie Hänold, Nikolaus Forgó
Institute for Legal Informatics, Leibniz Universität Hannover
nwankwo; haenold; forgo @iri.uni-hannover.de

Abstract— **Apart from technical challenges, legal and ethical issues form part of the considerations when pooling together and sharing databases for translational medical research. Questions referring to data protection, data security and intellectual property rights, which are even made more complex because of the transnational aspect of such research, have to be addressed in order to make data sharing legally compliant. Additionally, medical research brings along ethical requirements such as protecting the autonomy and the well-being of the patients. In all, a wide net of rules has to be considered, and in most cases this may hinder the flexibility needed for clinical researches. This paper aims to give an overview of these issues and an insight of the p-medicine's approach at navigating these requirements, which can serve as a guide to similar projects, especially within the EU.**

Keywords—Database sharing; translational medical research; data protection; legal and ethical issues

I. INTRODUCTION

Advances in medicine and information technology have revolutionalised the way in which medical care and research are being performed. Today, personalized medicine has been recognized as the key towards solving complex medical issues. Thus, it is necessary to find ways of quickly translating the discoveries about human genetics made by laboratory scientists into tools that physicians can use in making decisions about the best ways to treat patients [1]. Translational research is best suited for this purpose: for it links basic laboratory study to clinical data in order to discover new patters of healthcare delivery.

The European Union is currently funding a lot of projects in this area under the 7th Framework Programme. However, one area that has not drawn much attention is on the legal and ethical issues that may arise in integrating or sharing databases for these translational medical researches. This is important, because combining clinical research and clinical care activities into a unified system requires integrating a substantial body of regulatory requirements [2]. This sharing of databases will involve institutions within the EU, but also third countries in view of the international cooperation going on in this area of research. Most importantly, these databases will contain sensitive data and will be accessed or shared among many participating research institutions.

One of such ongoing collaborative translational research is the p-medicine project, partially funded by the EU that aims at developing an IT infrastructure - a toolkit and VPH models, to accelerate the steps to be taken to achieve advanced personalized medicine [3]. In this project, data from various participating institutions will be integrated into a p-medicine database and mined for the purposes of the research.

While there are technical aspects of this data integration as well as sharing, in this paper, we will mainly focus on the legal and ethical challenges that may arise in pooling together sensitive databases (e.g. hospital databases) for research purposes. The solution adopted in the p-medicine scenario will be explained and could serve as a model for similar projects.

II. DATABASE INTEGRATION AND INTEROPERABILITY

Typically, the aim of data warehousing is to integrate data from a multitude of original databases into one comprehensive intelligence platform [2]. Various forms of such integration exist in clinical research domain. Piwowar et al (2008) identified models such as centralised, federated and distributed data sharing frameworks and systems [5]. In the centralized model, multiple datasets are hosted at a single location in a common format. In a federation, information technology is used to provide a virtual common dataset, while the data sets are stored physically separated. Each of these models has its merits and demerits, but that is beyond the scope of this paper.

However, one identified major challenge in integrating and sharing databases in translational medical research is their interoperability. This stems from the fact that each hospital is free to use its own format in the absence of a harmonized global standard in the area of EHR. The lack of standardized mapping of clinical terminologies, communication standards and clinical research ontologies have affected multicentric research and data exchange in clinical trials [2]. So far, there is no common standard for GCP-compliant data management and IT Infrastructure [4]. The GCP requirements on data management from applicable regulations such as the EU Directive 2001/20/EC, EU Directive 2005/28/EC, Annex 11 of the Rules Governing Medicinal Products in the EU as well as the ICH Topic E 6 (R1) Guideline for Good Clinical Practice are mostly unspecific on technical requirements [6]. To fill this lacuna, the European Clinical Research Infrastructures

Network (ECRIN) was founded. Its objective is to harmonise clinical research in Europe by defining minimum requirements for GCP and best practice to be used for quality management, validation process, preparation of audits etc [6].

Besides the variety of formats, conceptual and semantic equivalence has to be considered when integrating databases. Especially, where a multitude of languages is involved, accurate translation will be needed to safeguard the validity of the data [7]. Genuine semantic interoperability requires that any particular language in a dataset is unambiguous and has the same meaning for any subsequent user of the system [8].

Apart from the technical issues of standardization and interoperability, institutions participating in clinical research that intend to integrate and share their various databases will also need to comply with certain legal and ethical requirements in terms of data protection and data security. This is especially important in view of the sensitive nature of health-related records. These legal pre-conditions as applicable in clinical environment within the EU stem from diverse sources, ranging from directives and national laws, to medical practice regulations and guidelines. We approach the issues of data protection and security separately below. Thereafter, intellectual property issues will be considered.

III. LEGAL PRECONDITIONS

Health-related data are part of the general personal data protected under the Data Protection Directive (Directive 95/46/EC) which is the basic document regulating personal data processing at EU level, and had to be implemented into national law by the Member States.

A. Data Protection

An integrated medical research database will ordinarily contain data of the trial participants obtained from the trial centres. Where the data reveal information concerning the health status, racial or ethnic background of the participant, it is specially protected under Article 8 of the Data Protection Directive. If so data processing steps are only permitted if the strict processing borderlines of the national laws of the Member States implementing Article 8 of the Directive are observed. For example, obtaining informed consent of the data subject, and other applicable rules as established by the Directive, including the general principles mandating the data controller to: limit data use to the purpose for which it was collected (purpose principle); ensure data quality (relevancy and accuracy principle); limit data retention (and not further process the data for incompatible purposes provide individuals with data collection information and access to the information collected (with rights of correction); and provide appropriate data security measures.

Apart from the initial legal challenge of obtaining personal data in compliance with the above stated principles, the subsequent conduct of the research would also need to comply with data protection legislation, particularly, in relation to access to and security of the data. Therefore, it is usually preferable to limit the application of the data protection rules in the research domain since compliance with such rules often hinders the smooth operation of the research. Especially, where retrospective data are involved, for which specific consent may not have been obtained. The general thinking in this regard is to render data anonymous as soon as possible, so that those cannot be linked to an identifiable person. From a privacy perspective, this is desirable. However, there is still a legal conundrum as what makes a health-related personal data anonymous in the strict sense of it. The EU prescribes no uniform criteria relating to anonymisation of personal data which has resulted to divergent anonymisation rules among the Member States, although there has been a tendency to the "reasonable efforts" approach [9]. In most cases, key-coded data increasingly appear to be considered as personal data, either because of the amount of data available to the sponsor, the characteristics of the (regulatory) environment in which trials are conducted, or the investigator's ability to reverse the code [10], [11].

Germany for instance has adopted the 'disproportional effort' approach where data is to be regarded as anonymised if a re-link to the data subject is impossible at all, or if an unreasonable effort of time, costs and labour would be required to attach the data to a certain individual (§ 3 VII BDSG). Here an objective consideration for every single case has to be taken, but still if it is planned to identify the data subjects, then the data has to be regarded as personal data [12]. In contrast to this the Irish data protection authority requires an irrevocable anonymisation in order to put data out of the data protection requirements [13]. Where this is not possible, data can only be regarded as pseudonymised (personal data), requiring that certain data protection measures be in place, for example that the data controller should not disclose data to third parties without fulfilling data protection requirements such as consent of the data subject. Other Member States such as France, Belgium, Italy and Sweden regard the issue of anonymisation and pseudonymisation as a consequence of Article 17 of the Directive, and never a condition for the related data not to be considered personal data [10].

This discuss is particularly important in clinical trials because absolute anonymisation without any possibility of re-linking the data to a particular person may be impossible (e.g. when it comes to genetic samples), or may not serve the purpose of the research (e.g. where a new successful treatment is proved, and it may be desirable to contact the patient(s) and/or monitor patient(s) reactions to the treatment) [9]. Furthermore, even when personal data are strongly de-identified, the advancements in data mining technologies could make re-identification of the persons possible. What has been regarded currently as 'irrevocably anonymised' or as 'unreasonable efforts', may not be seen so in the light of future technologies. Additionally, medical data sets are often rich in content and very likely to occur in unique combinations and often come from hospitals which have corresponding data sets [14]. It may be a mirage to assume that 'anonymisation' has solved the problem.

Our argument here is that in view of the uncertainties surround anonymisation, such mechanism may not on its own accord the required safeguards in respect of health related information used for research. Incidents have been recorded

where patients were identified by third parties with reference to so called anonymised data sets discarded from an insurance company that appeared in public domain [15]. A more holistic framework has been proposed in [9] where a 'safety net' involving building up a 'network of trust' within participating research partners, with supporting mechanisms such as an independent data protection authority overseeing the data, legally binding contracts and a trusted third party forming further safeguards.

Furthermore, where a translational research involves international collaboration with partners from a non-EU state, the uncertainty described above may raise an issue as to the legal basis for granting access to or transfer of data to such a third country. This is relevant because under the Data Protection Directive, transfer of personal data to a third country is prohibited except such a country provides adequate level of personal data protection, or any of the legal exceptions is invoked for such transfer. The Article 29 Working Party has recognised this problem and suggested that in such cases, data may be transferred "in anonymized or at least pseudonymized form" [4]. However, this suggestion does not settle the complexities on the issue of anonymisation and pseudonymisation, thus necessitating further contractual safeguard, such as the use of standard contracts issued by the European Commission. This may be complex in certain Member States where authorisation and notification requirements exist for such contracts.

In addition to the Data Protection Directive, specifications for the conduct of clinical trials within the EU are regulated under the framework of the EU Clinical Trials Directives – Directive 2001/20/EC and Directive 2005/28/EC. These Directives are to be considered when establishing a database for medical research because they also lay a framework for safeguarding clinical trial subjects. Their scope borders on good clinical practice, which is defined "as a set of internationally recognised ethical and scientific quality requirements which must be observed for designing, conducting, recording and reporting clinical trials that involve the participation of human subjects". It is envisaged that compliance with this good practice will provide assurance that the rights, safety and well-being of trial subjects are protected, and that the results of the clinical trials are credible. While Directive 2001/20/EC did not specifically elaborate on the data protection issues in integrating databases used in clinical trials, it however provides that clinical trials may be undertaken only if *inter alia*, the rights of the trial subjects to physical and mental integrity, to privacy and to the protection of the data concerning them in accordance with Directive 95/46/EC are safeguarded. It can be deduced from this that the Directive recognises the pre-eminence of the Data Protection Directive in safeguarding personal data, even when processed in clinical trials.

Directive 2005/28/EC on its part lays down principles and detailed guidelines for good clinical practice in respect to investigational medicinal products for human use. It supplements Directive 2001/20/EC and does not also deal with specific data protection requirements for integrating databases for medical research. However, it provides in its Article 5 that: "All clinical trial information shall be recorded, handled, and stored in such a way that it can be accurately reported, interpreted and verified, while the confidentiality of records of the trial subjects remains protected." This indicates that the handling and storage of data in a medical research database should protect the confidentiality of the data. This requires technical and organizational measures as will be discussed in the next section.

B. Data Security

An often profound issue to be addressed by data controllers in medical research is the security of the data they are processing. Obtaining the consent of trial participants in clinical trials is not an end in itself, but also requires putting in place appropriate safeguards to ensure that patients data are only used for the specified purpose(s) for which they are supplied, and can only be accessed or further disclosed to those persons to whom it is intended. The Data Protection Directive in its Article 17 requires the Member States to provide that the controller/processor 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". Though these terminologies were not defined in the Directive, technical measures generally deal with practical methods implemented to secure the data being processed. They include the use of encryption, secure connections, firewalls or access by biometric identification or similar methods. Organizational measures on the other hand refer to a set of rules to enable data security by regulating authorization and authentication procedures, such as access policies and identity management for the IT system processing the data as well as physical access control.

Furthermore, Recommendation No. R (97) 5 and the WMA Declaration have recommended some security models that are very relevant for any integrations of medical databases. These documents, in addition to their ethical guidance, also reflect on necessary security measures that should be in place in a health database. In a nutshell they include: a) Access control; b) Management system for the database; c) Secure transmission; d) Audit or log system; e) Anonymisation or psudonymisation of data; f) Constant review of the security mechanism; g) Conservation of data.

Apart from the above, where the integrating infrastructure for storing and accessing the database is an open network infrastructure such as cloud computing, it will be also relevant to carry out a risk assessment of such technology vis-à-vis the sensitive nature of the data involved. While it is still debated whether critical information should be stored in the cloud, it is beyond the scope of this analysis to delve into such discussion. However, issues such as loss of data control, jurisdiction, security breaches and vendor lock-in etc. should be thoroughly weighed when using the cloud for clinical research [14]. It may be important to consider using a private cloud infrastructure where data control will not be completely relinquished to a third party.

IV. ETHICAL CHALLENGES

The accelerated development in IT-technology enables researchers to collect and evaluate huge numbers of data sets containing sensitive health information. Therefore the use of such databases demands cautions from researchers because disclosure of the data can have serious negative impacts on the life of the concerned data subject when they become identified, e.g. refusal of health or life insurance or job loss. It is also important to respect the trial participants and their autonomous decisions as secured from their informed consent. A major challenge therefore in integrating medical databases is how to reflect each and every trial participant's wishes.

A. Informed Consent

The most important ethical requirement for the collection and further processing of data in clinical trials is prior, free and informed consent of the trial subjects which aims at ensuring their right of self-determination and autonomy [16]. Where prospective data are collected in view of a future trial, there is usually not much controversy in integrating and sharing such data where they are covered by the requisite informed consent. However, ethical issues arise in respect to the re-use of participants' data which have been collected in previous trials and stored in a database for another purpose. Karp *et al* (2008) reviewed these complications, pointing out that retrospective data stored in medical research databases, may have been collected without authorisation that meets today's standards for informed consent [17]. Research participants may not have consented to the inclusion in genetics databases specifically, or to the use of their samples in genetic analyses that were unanticipated at the time samples were collected, or may not have consented to "secondary uses" of those data for unrelated research, or for the use by third parties.

There is an interest to reuse data because it may be inefficient and contrary to the public good to collect new similar data at public expense, especially, in the field of genetic studies that require retrospective data [17], [18]. However, this raises ethical issues such as the risk of re-identifcation of not only individual participants, but also their families and groups. This calls for a strong ethical consideration and oversight before integrating retrospective data into future research databases. One very costly solution would be to re-contact the data subjects and ask for their permission, but this would also be time consuming, and in some cases the subjects might simply not be interested in re-consenting, or might have changed their contact address or be deceased [16], [19]. A more practical way would be to have an oversight procedure done by an ethical committee to clarify whether the original consent covers the new research [17].

Karp et al (2010) have suggested in order to facilitate the procedure of secondary uses of data, the consent process should concern future uses of the data [17]. While there is still a divide in opinions among authors regarding the legal validity of broad and unspecified consent between as against a specific consent [16], a middle course is developing which enables the trial participant to choose between various alternatives with varying degrees relating to the use of the data [18], [20]. For example, if the data could be stored, used for only specified research topics [16] or shared with researchers not belonging to the original researcher team [18]. It remains to be seen which model will achieve most acceptance.

B. The Right to Be Forgotten

A similar issue to be considered in this case will be how to effectively erase a participant's data when consent is withdrawn, not only from the data warehouse, but also from other places where copies may have been made [21]. While this is still a controversial concept in the legal domain [22], it is nevertheless part of the informed consent principles that the trial participants should be free to withdraw at any time in a clinical trial without suffering any harm to their privacy. How to enforce this right should be a factor to be considered when integrating and sharing databases.

V. INTELLECTUAL PROPERTY

Ownership of the intellectual property in a medical research database and associated rights therein has been subject of controversy over the years. Many hospitals consider the records in their systems to be their property, whereas patients argue that their medical information ought to belong to them. This scenario becomes more complicated when many institutions are involved in a medical research, with multiple interests, such as the funders and researchers in a project. While a clear resolution of the issues raised here can be made by contract involving the parties, policies or regulations on these issues may differ substantially in different states.

Interesting arguments have been going over the years as to who should posses the intellectual property rights of data used in clinical trials – patients, hospitals, sponsors of the trial, researchers/participants in the project, the public, etc [23]. In deciding this issue, a lot of factors would have to be considered, including for example the fundamentals of trial design, protocol management and regulatory oversight. Equally relevant here will be how to control these data if too many persons are involved in their management. While there may be divergent opinions as to who should have proprietary rights in medical research databases, it is settled that patients should have the right of access to their medical records, even when used for research purposes [24]. By virtue of Article 12 of the Data Protection Directive (subject to the derogations in Article 13), data subjects have the right to access to their data. This right has even been associated with the right to private and family life under Article 8 of the ECHR as indicated in *Roche v UK* [25] and *KH v Slovakia* [26]. In these cases, the court ruled that there is a positive obligation on the hospital to make available to the patients copies of their data file.

The notion that hospitals should own medical databases has on the other hand received some legal and legislative backing. In *R v Department of Health ex parte Source Informatics Ltd* [27], the English appeal court ruled that a patient had no proprietary claim to the prescription form or to

the information it contained and had no right to control the way the information was used provided only that his privacy was not put at risk. Rodwin (2009) has argued against such private ownership of patients' data, insisting that it would preclude downstream invention and benefit for individual owners and the society at large [28].

Although according ownership right of medical research databases to patients will not usually be problematic on its face value, provided that the data are managed and processed by researchers to suit the research purposes, giving proprietary rights to the sponsors of the trial has also been considered. This is in view of the efforts and financial investment they made in the collection of the data and the trial as a whole. It follows then that where clinical trials are funded with public money, the data generated from such trials should be public property. Rodwin reiterated this argument, insisting that "core values of medical professionalism – the promotion of patients' interests, medical knowledge, and public health also support public ownership" [28]. Suggesting that sponsors will likely own the data in clinical trials, Drazen (2002) pointed out that ownership could be specified in the informed consent form, where patients would agree to give up ownership of data to sponsors, even when such may be used for commercial purposes [29]. He however adds that such right should not be exclusive. It should at least permit dissemination of data by participating investigators for non-commercial uses such as re-analysis of findings and publication in per-reviewed journals. But it is contentious whether data should be in public domain when sponsored by public authorities in view of the risk of violating patient's privacy where they could be identified from such data. Although Drazen's analysis did not consider ownership rights between sponsors and investigators or participants in the clinical trial, it does suggest that such ownership rights could be spelt out contractually.

The EU has however, addressed this intellectual property rights issues in relation to EU Seventh Framework Programme (FP7) projects. In this respect, the EC Guide to Intellectual Property Rules for FP7 Projects, the EC Grant Agreement Annex II, and the FP7 Regulation (EC) No. 1906/2006 have addressed how to handle the background and foreground property in EU funded projects. "*Background"* means "information which is held by participants prior to their accession to the grant agreement, as well as copyrights or other intellectual property rights pertaining to such information, the application for which has been filed before their accession to the grant agreement, and which is needed for carrying out the indirect action or for using the results of the indirect action". "*Foreground*" on the other hand means the results, including information, whether or not they can be protected, which are generated by the indirect action concerned. Such results include rights related to copyright, design rights, patent rights, plant variety rights or similar forms of protection. Thus, foreground includes the tangible and intangible intellectual property results of a project.

From the above definitions, each participating partner will continue to have the intellectual property rights it holds in its database even when such data has been integrated into a common database. However, the resultant foreground generated from the processing of this background information either in isolated units or in conjunction with other such information in the database may have a different outcome. In the first place, the foreground shall be the property of the participant carrying out the work generating that foreground. But where several participants have jointly carried out work generating the foreground and where their respective share of the work cannot be ascertained, they shall have joint ownership of such foreground. The parties shall establish an agreement regarding the allocation and terms of exercise of that joint ownership; in the absence of which a default rule applies to the foreground.

VI. P-MEDICINE APPROACH

As could be deduced from our discussion above, the regulatory environment upon which translational medical research is conducted is complex, resulting into a multitude of laws and ethical guidelines on the European and national levels. It may be, for instance, particularly difficult to apply all the EU Member States data protection laws in an integrated databases containing data from each of these states. These complexities were examined in ACGT, and the participating partners devised practical means involving a combination of technical, organisational and legal measures aimed at navigating the identified problems [30]. ACGT thus became a forerunner for the p-medicine framework. While no common database platform was adopted in ACGT, p-medicine incorporated a data warehouse (federated architecture) as a repository platform for securely storing and processing data from diverse sources; integrated semantically to enable reporting and analysis. For p-medicine, establishing a database for integrating large amount of data needed for a translational medical research seems essential, and could serve as a foundation for a knowledge discovery system. Such a repository is more beneficial when heterogeneous data from various sources are seamlessly integrated, so as to produce a predictive result when mined appropriately with the use of information technology.

In order to enhance privacy in the whole p-medicine project structure, a clear separation between the treatment and the research domain is maintained. Within the treatment domain, medical data are collected in the course of the patients' treatment. At this stage personal health data are processed since the clinical trial record and biomaterials are linked to the patient and informed consent serves as a legal basis for the processing as required by Article 8 of the Data Protection Directive. After this first stage of collection, the hospitals pseudonymise the patients' data as kept in their database. Thereafter, the pseudonymised data is pushed to the common p-medicine database (research domain). Before coming into the research domain, a second pseudonymisation procedure is automatically performed using Custodix Anonymisation Tool Services (CATS). The identification key of this second pseudonymisation is kept by a trusted third party (TTP) [31]. This process is also legally based on the consent of the patient.

Apart from the above technical measures, organisational policy is also put in place. In addition to the domain separation, a data protection authority is particularly set up to oversee the data processing in the database - the Centre for Data Protection (CDP). The CDP concluded contractual agreements with the consortium partners in which they declare to comply with data protection and data security standards in the project. These standards entail the prohibition of re-identification with penalty clause for any breach. If there is a need to re-identify the patient for example, a new successful treatment is discovered, the CDP is contacted which will send a request to the TTP for the key if the patient has agreed on such re-identification in the consent procedure.

P-medicine, which is following the "reasonable efforts" approach, does not rely solely on technical measures, but optimises the security level with a contractual framework thereby reducing the risk of re-identification to an absolute minimal level. This translates to the data in the research database being regarded as 'de facto anonymised' and outside the scope of the directive and the implementing national laws. However, this must not lead to the assumption that the participants data are no longer protected afterwards. For the mining activities in the database, a privacy preserving technology has been established using a combination of k-anonymity and l-diversity constraints. A data processing and mining guideline is also put in place indicating the access policy and the security framework in a fine-grained manner.

VII. CONCLUSION

Navigating through the various legal and ethical hurdles in translational medical research is very essential in achieving an integration of valuable databases that can help translational research in many ways: from patient recruitment to developing health care decision support tools. We have shown the legal and ethical complexities, and the growing need to integrate heterogeneous databases for translational research purposes. In p-medicine, we have tried to identify and closed this gap by instituting a 'safety net' within the project, which relaxes the application of the Data Protection Directive to achieve the flexibility needed, and also at the same time, protect the sensitive data processed in the project.

ACKNOWLEDGMENT

The research leading to these results has received funding from the EU's FP7 (FP7/2007-2013) under Grant Agreement No 270089. The work is part of the on-going p-medicine project funded under the FP7 framework of the European Union. The content of this article reflects the views of the authors and not necessarily those of the project consortium.

REFERENCES

[1] N. Graf, C. Desmedt, F. Buffa, et al, "Post-genomic Clinical Trials: The Perspective of ACGT", eCMS, vol.2, no. 66, pp. 1-17, 2008.

[2] H.U Prokosch, and T. Ganslandt, "Perspectives for Medical Informatics Reusing the Electronic Medical Record for Clinical Research", Meth. Inf. Med., vol. 48, pp- 38-44, 2009.

[3] www.p-medicine.eu.

[4] W. Kuchinke, C. Ohmann, Q. Yang, et al, "Heterogeneity prevails: the state of clinical trial data mangement in Europe – results of a survey of ECRIN centres", Trials, vol. 11, no. 79, pp. 1-10, 2010.

[5] H. A. Piwowar, M. Becich, H. Bilofsky, R.Crowley, "Towards a data sharing culture: recommendations for leadership from academic health centers", PLoS Med, vol. 5, no. 9, pp. 1315-1319, 2008.

[6] C. Ohmann, W. Kuchinke, S. Canham, et al, "Standard requirements for GCP-compliant data management in multinational clinical trials", Trials, vol. 12, no. 85, pp. 2-9, 2011.

[7] ECRIN, Deliverable 10, GCP-compliant data management in multinational clinical trials, version 1, final, 2008.

[8] European Commission, "Connected Healths: Quality and Safety for European Citizens, Belgium, p.22, 2006.

[9] 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, vol. 367, no. 1898, pp. 2729-2739, 2009.

[10] K. V. Quathem, "Controling personal data in clinical trials", Covington & Burling, 2009.

[11] K. V. Quathem, "Controling personal data: the case of clinical trials", Covington & Burling, 2005.

[12] P. Gola, R. Schomerus, Kommentar zum Bundesdatenschutzgesetz, 11. Aufl., § 3 Rn. 43 ff., 2012.

[13] Irish Data Protection Commissioner, Data Protection Guidelines on Research in the Health Sector, 2007.

[14] European Network and Information Security Agency, Cloud computing: benefits, risks and recommendations for information security, pp. 1-125 2009.

[15] P. Ohm, "Broken promise of privacy: responding to the surprising failure of anonymisation", UCLA Law Review, vol. 57, pp. 1701-1777, 2010 .

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

[17] D. Karp, S. Carlin, R. Cook-Deegan, et al, "Ethical and Practical Issues Associated with Aggregating Databases", PLoS Med, vol. 5, no. 9, pp. 1333-1337, 2008.

[18] R. Watson, E. Kay, D. Smith, "Integrating biobanks: addressing the practical and ethical issues to deliver a valuable tool for cancer research", Nat. Rev. Cancer, vol. 10, no. 9, pp. 646 -651, 2010.

[19] Art. 22 of the Draft Recommendation Rec (2006) of the Committee of Ministers to member states on research on biological materials of human origin Draft explanatory memorandum.

[20] T. Caulfield, R. Upshur, A. Daar, "DNA databanks and consent: A suggested policy option involving an authorization model", BMC Medical Ethics, vol. 4, no. 1, pp. 1-4, 2003.

[21] See Commission Proposal for a Regulation of the European Parliament and of the Council, art. 4(2), COM (2012) 11 final (Jan. 25, 2012).

[22] J. Rosen, "The right to be forgotten", STAN.L.REV.ONLINE, vol. 64, pp. 88-92, 2012.

[23] C. Hinds, M. Jirotka, M. Rahman et al, "Ownership of intellectual property rights in medical data in collaborative computing envrionments", Ncess, 2005.

[24] Art. 26 of the Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, 2005.

[25] Roche v. The United Kingdom [2005] ECHR 32555/96.

[26] K.H. and others v. Slovakia [2009] 32881/04.

[27] R. V. Department of Health ex parte Source Informatics Ltd [2000] 1 All ER 786 .

[28] M. Rodwin, "The case for public ownership of patient data", JAMA, vol. 302, no. 1, pp. 86-88, 2009.

[29] Jeffrey Drazen, 'Who owns the data in a clinical trial?', Sci.Eng.Ethics, vol. 8, no. 3, pp. 407 – 411.

[30] See ACGT Deliverable 10.2, The ACGT ethical and legal requirements 2007.

[31] See P-medicine Deliverable 5.1, Setting up the data protection and data security for p-medicine, 2012.