

A Data Protection Scheme for Medical Research Networks

Review after Five Years of Operation

K. Helbing¹; S. Y. Demiroglu¹; F. Rakebrandt¹; K. Pommerening²; O. Rienhoff¹; U. Sax^{1,3}

¹Department of Medical Informatics, University Medical Center, Georg-August-University, Goettingen, Germany;

²Institute for Medical Biostatistics, Epidemiology, and Informatics, University Medical Center, Johannes-Gutenberg-University, Mainz, Germany;

³Information Technology, University Medical Center, Georg-August-University, Goettingen, Germany

Keywords

Clinical trials, biomedical research, computer security, databases, pseudonyms

Summary

Background: The data protection requirements matured in parallel to new clinical tests generating more personal data since the 1960s. About ten years ago it was recognized that a generic data protection scheme for medical research networks is required, which reinforces patient rights but also allows economically feasible medical research compared to “hand-carved” individual solutions.

Objectives: To give recommendations for more efficient IT infrastructures for medical research networks in compliance with data protection requirements.

Methods: The IT infrastructures of three medical research networks were reviewed with respect to the relevant data manage-

ment modules. Recommendations are derived to increase cost efficiency in research networks assessing the consequences of a service provider approach without lowering the data protection level.

Results: The existing data protection schemes are very complex. Smaller research networks cannot afford the implementation of such schemes. Larger networks struggle to keep them sustainable. Due to a modular redesign in the medical research network community, a new approach offers opportunities for an efficient sustainable IT infrastructure involving a service provider concept. For standard components 70–80% of the costs could be cut down, for open source components about 37% over a three-year period.

Conclusions: Future research networks should switch to a service-oriented approach to achieve a sustainable, cost-efficient IT infrastructure.

ment modules. Recommendations are derived to increase cost efficiency in research networks assessing the consequences of a service provider approach without lowering the data protection level.

Results: The existing data protection schemes are very complex. Smaller research networks cannot afford the implementation of such schemes. Larger networks struggle to keep them sustainable. Due to a modular redesign in the medical research network community, a new approach offers opportunities for an efficient sustainable IT infrastructure involving a service provider concept. For standard components 70–80% of the costs could be cut down, for open source components about 37% over a three-year period.

Conclusions: Future research networks should switch to a service-oriented approach to achieve a sustainable, cost-efficient IT infrastructure.

dressed the question of adequate patient data protection as one key element to gain a high acceptance in the population to participate in these huge trials. Prominent results of these efforts are the Boston-based i2b2-project [2], the security framework of the National Institutes of Health (NIH) and National Cancer Institutes (NCI)-funded cancer Biomedical Informatics Grid (caBIG) research collaboration [3, 4], and the TMF (Technology, Methods, and Infrastructure for Networked Medical Research)^a. Internationally, the importance of data protection is reflected by the fact that the International Medical Informatics Organization (IMIA)^b implemented a working group dealing exclusively with data protection in health information systems [5]. Furthermore, the American Health Insurance Portability & Accountability Act (HIPAA) as well as the Austrian MAGDALENA framework for the use of informatics in the health care system both describe the importance of data protection and security of medical and identifying data of patients [6]. Moreover, in the context of medical research the Clinical E-Science Framework (CLEF) sponsored by the Medical Research Council of the United Kingdom is very similar to the TMF data protection scheme. Both frameworks include a physical and organizational separation of identifying patient data from the clinical and also the biomaterial data, and the use of pseudonyms [7–9].

The German TMF data protection scheme is continuously being updated, but the main focus of this scheme are not cost-efficiency and sustainability. Therefore, the

Correspondence to:

Krister Helbing
Georg-August-University Goettingen
University Medical Center
Department of Medical Informatics
Robert-Koch-Strasse 40
37075 Goettingen
Germany
E-mail: khelbing@med.uni-goettingen.de

Methods Inf Med 2010; 49: 601–607

doi: 10.3414/ME09-02-0058

received: December 14, 2009

accepted: April 30, 2010

prepublished: July 20, 2010

1. Introduction

The principles of data protection in medicine with respect to IT were originally formalized in Sweden and quickly adopted by several western countries [1]. However, it took another ten years until specific issues in medical research were discussed and

first solutions emerged. In the late 1980s the US National Science Foundation (NSF) and the German Ministry of Education and Research (BMBF) – amongst others – launched a series of big collaborative medical research projects and analyzed their performance, problems, and efficiency. One of the pivotal aspects of those trials ad-

^a <http://www.tmf-ev.de>

^b <http://www.imia.org>

authors put an emphasis on an efficient and sustainable data protection infrastructure for medical research networks. This infrastructure has to be affordable for smaller networks and has to offer a possibility for larger networks to sustainably operate their infrastructure with decreasing funds.

Our experience with data protection schemes is derived from three different research collaborations: The Competence Network for Congenital Heart Defects (KN AHF)^c as a multi-site research network consisting of centers all over Germany, the German Competence Network Multiple Sclerosis (KKN MS)^d as a similar construct, and the Clinical Research Unit (KFO) 179^e as a rather small interdisciplinary research unit within the University Medical Center in Goettingen. The KN AHF and the KKN MS are funded by the BMBF since 2003, respectively 2009. They are combining fundamental, clinical, and health services research with a strong translational component. One important difference, however, is that the KN AHF is already in its third funding period focusing on the sustainability of its IT infrastructure, whereas the KKN MS is just in the first funding period focusing on the setup of its IT infrastructure. The KFO 179 is funded by the German Research Foundation (DFG) since 2007 and aims at an individualized therapy for rectal cancer [10, 11].

2. Objectives

The experiences from three medical research networks regarding their data protection schemes are reviewed and recommendations for a sustainable and efficient data-protective IT infrastructure are given. The recommendations take the TMF data protection schemes [7, 9, 12, 13] as a basis. As the data protection schemes mainly focus on the legal requirements, we add the efficiency and sustainability point of view.

^c <http://www.kompetenznetz-ahf.de>

^d <http://www.kompetenznetz-multiplesklerose.de>

^e <http://www.kfo179.de>

3. Methods

3.1 TMF Data Protection Schemes

The requirements of an IT infrastructure for data protection are derived from the generic solutions for data protection in medical research networks [7, 9] and the generic data protection scheme for biobanking [12, 14]. These references focus on an organizational and physical separation of data to avoid their unauthorized linking (Chapter 4.1). As an effect of the TMF privacy models the IT infrastructures of the Competence Networks are designed along the requirements of the 2002 data protection schemes. Therefore, the IT infrastructure of the KN AHF, the KKN MS, and the KFO 179 were designed accordingly. However, the latest network, the KKN MS, incorporates a new approach for the implementation of its IT infrastructure. The KKN MS assigns several IT service providers to operate its IT components. This approach promises to be more cost-efficient than the approach of previously funded medical research networks like the KN AHF.

3.2 Calculation of the Costs for the Single IT Components

The costs of the service providers are compared to the regular costs of acquisition and operation for each IT component of the KKN MS. In this context, a service provider is a nonprofit institute, which is funded by public institutions like BMBF, DFG, and the government. This means the service provider fee includes only additional expenses for their service (like additional personnel, etc.) and not all expenses (e.g. backups, already existing IT infrastructure, etc.), because they were already funded by other projects.

The comparison includes the costs of acquisition and operation for a time span of three years. The calculations related to the acquisition and the operation of the IT components are based on the strength of past experience in other projects. The calculation includes the acquisition of software and hardware, and personnel costs. The authors calculate personnel costs for IT-

administration, setup, and testing. Other personnel costs such as form-building of the electronic case report forms (eCRFs) are not included. The rate of inflation is not taken into consideration at all.

3.3 Outline of the Paper

In this paper, we first generically introduce the components of the IT infrastructure of medical research networks. This is followed by a description of the data protection concept involving these IT components. In a second step, we characterize the three medical research networks with regard to the projects, the number of patients, research partners, clinical trials, service providers, and IT components. The third step involves a cost calculation for the single IT components. For this purpose, the costs of the single components of the IT infrastructures of the KN AHF and the KFO 179 are analyzed and compared with the costs of a service provider. For the review we consider the following components: 1) Identity management, 2) clinical trial database, 3) registry, 4) biomaterial database, and 5) imaging database (► Fig. 1). As the service provider seems to be the most cost-efficient for the KKN MS, we discuss in how far this approach could be applied to the other medical research networks. Finally, we discuss the advantages and disadvantages of both approaches and give recommendations for setting up the IT infrastructure for future medical research networks.

4. Results

4.1 The IT Infrastructure of a Medical Research Network from a Data Protection Point of View

The individual components of an IT infrastructure of a medical research network and their interactions are shown in ► Figure 1 as derived from the data protection requirements in Germany.

The essential components of the IT infrastructure are: 1) The identity management, 2) the clinical trial database, 3) the registry, 4) the biomaterial database, and 5) the imaging database. The data protection

schemes of the TMF [7, 9, 12–14] give detailed leads on some of these aspects.

The identity management module generates and handles the patient pseudonyms. It contains all identifying data of a patient, such as name, address, and date of birth. The data of the identity management module have to be physically and organizationally separated from the databases containing the medical data of the patients, which is similar in the UK [8] and other countries. The clinical trial database and the registry both contain medical patient data, e.g. medical history of a patient, or laboratory data, e.g. blood pressure or blood test results. These data should be physically and organizationally separated from the biomaterial database containing management data of the patients' biomaterial [12]. The biomaterial database contains information about the samples of a patient, e.g. the exact position in a freezer or the type, provenance, and concentration of a specific sample. The identifier of a sample should be different from the pseudonym generated by the identity management. The imaging database contains medical imaging data of patients, e.g. MRTs, CTs, and X-rays. These data should likewise be physically and organizationally separated from the identity management containing the identifying data of the patients.

4.2 German Competence Network Multiple Sclerosis (KKN MS)

The KKN MS represents a research-centered trial-based collaboration structure with about 1400 patients, one open clinical trial, and about 49 research partners. Moreover, it is planned to exchange data with two international registries. The infrastructure currently contains five IT components at four different service providers (► Table 1). KKN MS is funded since 2009 (first of three funding periods – maximum funding duration is 12 years). The IT infrastructure of the KKN MS consists of an identity management, a clinical trial database, a biomaterial database, a registry, and an imaging database. The identity management was handed over to a provider and is therefore physically and organizationally

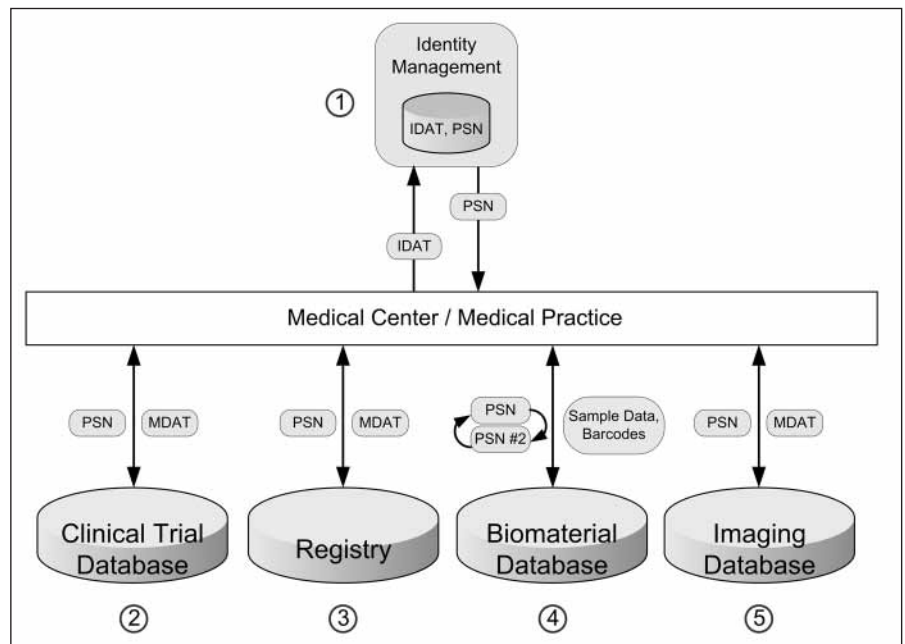


Fig. 1 Generic IT infrastructure of a medical research network with individual components and their interactions. 1) The physically separated identity management module generates the patient pseudonyms (PSN) based on the identifying data of patients (IDAT). It hosts the PSN and the IDAT. The PSN is used by the medical center and medical practices to capture medical data of a patient. 2) In the clinical trial database and 3) the registry clinical and medical patient data (MDAT) are stored with the pseudonym provided by the identity management. 4) The biomaterial database contains administrative biomaterial sample data, e.g. the barcode of the tubes containing the biomaterial. For data protection reasons the identity management PSN has to be transformed into another pseudonym (PSN #2) not listed in the identity management. 5) The imaging database contains pseudonymized imaging data of the patient.

separated from all other databases. Neither additional costs for hardware or software nor for experienced personnel was generated. The clinical trial database and the biomaterial database are managed by another provider. No additional investments into hardware, software, and experienced personnel were necessary. The imaging database and the registry are operated by two more providers.

4.3 Competence Network for Congenital Heart Defects (KN AHF)

The KN AHF was one of the first competence networks being funded in 2003 (2nd period 2007, 3rd and last period 2009–2012). The IT infrastructure was built centrally. The 12 clinical trials include more than 40,000 patients and about 290 research partners. The infrastructure currently contains six IT components at two

different service providers (► Table 1). The high number of patients is effected by the national AHF registry, the high number of research partners is based on one study, which aims to register all newborns with a congenital heart defect. There are several international projects, for example the Heart Failure and Cardiac Repair, the Euripides Registry, and a MRT project. The IT infrastructure of the KN AHF consists of an identity management, two clinical trial databases, a biomaterial database, a registry, and an imaging database. The identity management is physically separated from the databases containing the medical data. For the identity management module, new hardware had to be obtained and employees needed to be trained leading to costs for setup and operation. The clinical trial databases are operated at different locations. Here, the network could hark back on existing systems, thus no new hardware and personnel were required. In terms of the

Table 1 Key figures for the reviewed medical research networks concerning patients, research partners, clinical trials, research projects, and the corresponding IT infrastructure

Name	KN AHF	KKN MS	KFO 179
Patients	>40,000	>1400*	300*
National research partners	~290	41	8
International research partners	>3	8	2
Clinical trials	12	1	0
Research projects	8	28	8
IT provider	2	4	1
Identity management (PID) modules	1	1	0
Clinical trial modules	2	1	1
Registry modules	1	1	0
Biomaterial modules	1	1	1
Imaging modules	1	1	0

* expected

registry, hard- and software had to be financed, and personnel had to be trained. The registry is situated at the same location as one of the clinical trial databases and the imaging database. For the imaging database, new hardware and software was obtained as well as personnel was trained.

4.4 Clinical Research Unit (KFO) 179

The KFO 179 is a clinical research unit located at the University Medical Center Goettingen since 2007 (first funding period until 2010, second funding period expected from 2010 to 2013). Its aim is to investigate molecular mechanisms of rectal cancer so as to be able to deduce an effective therapy for each patient. This study is performed by ten project partners, eight from Goettingen and two from the US. About 300 patients should be included into the study to get sufficient biomaterial and clinical data for all eight research projects. The IT for this network is positioned at one single location and comprises the clinical trial database and the biomaterial database. Additionally, the infrastructure of the KFO 179 contains an identity management, which is physically and organizationally separated from the other databases and handled manually.

The clinical trial database and the biomaterial database are administered by one provider. Both databases were set into operation without new investments regarding software and hardware.

4.5 Summarizing Comparison of the Introduced IT Infrastructures

The presented IT infrastructures represent a) a highly flexible research network with multiple locations using generic components (KKN MS), b) a trial-based research network with many specific components like a registry and biomaterial database as early adopter (KN AHF), and c) a smaller-scale research-oriented network with few locations (KFO 179).

The IT infrastructures do not differ greatly in their single components but in the way they are operated. Early adopters generate high costs for the acquisition of hardware, software, consulting, and personnel compared to using a service provider offering a new software instance on an existing operating infrastructure.

The KKN MS transferred all of its IT components to four service providers offering the IT components as services.

The KN AHF handed over some standard components to a service provider but also invested into new equipment and per-

sonnel for the remaining IT components of its infrastructure.

The smaller KFO 179 just concentrated on one service provider offering a service involving existing hardware and software solutions for the clinical trial database and the biomaterial database.

4.6 Calculation of the Cost-efficiency of the Service Provider Approach of the KKN MS

To point out the cost-efficiency of the service provider approach with regard to the KKN MS, the costs of the service providers are compared to the regular costs of acquisition and operation for each IT component of the KKN MS (►Table 2) as described in the Methods section.

4.6.1 Identity Management

The calculation of the costs of acquisition and operation for the identity management is based on the costs of the KN AHF. Both medical research networks are using a TMF tool, which is free of charge [15]. The total amount the KN AHF spent for the identity management can be split into 27% for hardware and 73% for personnel. In comparison, the KKN MS was able to save 37% of costs by assigning a service provider for the identity management.

4.6.2 Clinical Trial Database

The calculation of the costs of acquisition and operation for the clinical trial database is based on the costs for software including service and updates. All reviewed networks are using the same software. The total costs for the clinical trial database consist of 88% for software, 3% for hardware, and 9% for personnel (this calculation is based on the costs of another project, which was operated by the authors' institute). In comparison, the KKN MS was able to save 70% of costs by assigning a service provider for the clinical database (since the authors have no specific data for this service, they calculate with their service fee for a clinical trial database), assuming the actual service provider calculations has four projects

Table 2 Cost relation of the single modules in % of the overall costs of the IT infrastructure (columns 2–4) compared to the service provider approach (column 5) of the KKN MS. The overall costs of the IT infrastructure include personnel on the base of actual costs of the components and personnel for the operation of the systems with the conventional approach. Concerning open source software, a service provider approach could cut down costs by 37%; using commercial software, the overall costs could be cut down by 70–80% in the presented network types.

Module	Acquisition of software [% of overall cost]	Acquisition of hardware [% of overall cost]	Personnel [% of overall cost]	Savings using a service provider approach [% of overall cost]
Identity management module (PID) (open source)	0	27	73	37
Clinical trial, registry, biomaterial modules	88	3	9	70
Imaging module	91	4	5	80

(one registry and three clinical trial databases).

4.6.3 Registry of MS Children

The registry is provided by a service provider in Munich. Since the authors have no specific costs for this service, they calculate with their service fee for a registry, which is included in the calculation of the clinical trial database.

4.6.4 Biomaterial Database

The biomaterial database is implemented using the clinical trial software and is integrated into the clinical trials. No additional costs for acquisition and operation arose.

4.6.5 Imaging Database

The calculation of the costs of acquisition and operation for the imaging database is based on the amount the KN AHF spent for the system including an annual service fee. The KN AHF and the KKN MS are using the same software. The authors had to recalculate the costs for the software, because the KKN MS uses fewer functionalities of the imaging database. The total cost for the imaging database are made up from 91% for software, 4% for hardware and 5% for personnel. Compared to these numbers the KKN MS was able to save 80% costs by assigning a service provider.

4.7 What Effect Would the Service Provider Approach Have on a Large-scale Fully Equipped Network (Like KN AHF)?

4.7.1 Identity Management

The analysis in Chapter 4.6 and ►Table 2 show that it is more cost-efficient to assign a service provider for the identity management. Since this calculation is based on the costs of the KN AHF for their identity management, the service provider approach should be more cost-efficient regarding this IT component for the KN AHF.

4.7.2 Clinical Trial Database

In the first funding period the clinical trial database and the eCRFs were implemented by the manufacturer – for lack of a service provider and functionalities of the software (like a form builder). In the second funding period the KN AHF assigned a service provider for the clinical trial database. Thus, the KN AHF already applies the service provider approach for this IT component.

4.7.3 Registry and Biomaterial Database

The registry of the KN AHF uses highly specialized software, including three databases: an identity management database, a biomaterial database, and a database for clinical data. This concept allows for the addition of several projects without additional costs. Thus, the KN AHF became a

service provider for other medical research projects. In this case the acquisition of the soft- and hardware is economically justifiable, because their registry perfectly fits to their needs. Additionally it becomes a major tool for their sustainable funding as they also offer this registry as a service for other projects. Thus, for the registry and the biomaterial database, assigning a service provider is not the best option.

4.7.4 Imaging Database

According to the analysis in Chapter 4.6 and ►Table 2 it is more cost-efficient to assign a service provider for the imaging database. Since this calculation is based on the costs of the KN AHF for their imaging database, the service provider approach should be more cost-efficient for this IT component of the KN AHF.

4.8 What Effect Would the Service Provider Approach Have on a Dynamic, Time-restrained, Smaller-scale Network (Like KFO 179)?

4.8.1 Identity Management

The KFO has an identity management, which is handled manually. Due to the expected number of patients and partners this might be the most cost-efficient solution, and the KFO does not need an IT component at all.

4.8.2 Clinical Trial Database

The clinical trial database is already hosted by a service provider, so that the KFO choose the most cost-efficient solution.

4.8.3 Biomaterial Database

The biomaterial database is hosted by the same service provider. The software for the biomaterial database is an adaption of the software for the clinical trial database. Due to its performance and functionality, this software is inferior to professional software for biomaterial databases, but on the other hand, no additional costs emerged. A second service provider could supply higher functionality and performance and moreover would increase the data protection level.

5. Discussion

The service provider approach seems to be very cost-efficient for all IT components of the KKN MS, given that all providers are nonprofit institutes, as mentioned in the Methods section.

A medical research network is designed for several decades and has to be able to adapt its IT infrastructure flexibly to its current and future needs. This means new IT components have to be adapted or acquired or older IT components need to be removed. The flexibility of the service provider approach advantaged this proceeding, because the research network is able to negotiate a new and/or annul a current contract with a service provider. Especially, if the research network uses approved IT components like a clinical trial database or imaging database (see KKN MS).

If a medical research network decides to implement innovative IT components, which are not yet offered as a standard IT component by service providers, like biomaterial software or research databases, it may decide to become a service provider themselves and offer the IT component for other research networks. The KN AHF established their registry as a service for others, thus keeping their IT infrastructure sustainable. Implementing one's own

IT components, however, offers the advantage of a solution tailored to specific needs.

For smaller research networks with a time constraint (like the KFO 179) the service provider approach seems to fit perfectly, because they do not have to invest in hard- and software nor personnel. Due to their small size and limited number of projects, they may not even need IT support for handling all their functional components, e.g. the identity management. Albeit, the operation of the identity management with a manually managed patient list turns out to be disadvantageous, as new patients can only be added using the single patient list, resulting in dependence on single persons.

Nevertheless, we calculated with few (one to four) projects per IT component, considering there are research networks with a lot more projects (ten and more) it might be cheaper to implement and operate their own IT components.

For the IT infrastructure of the KN AHF and the KFO 179 with just one or two IT providers, almost no laborious coordination is necessary and potential errors occurring during the coordination process involving several providers can thus be avoided. The many-provider approach of the KKN MS necessitates more coordination.

Overall, the service provider approach on the one hand does involve more communication and coordination effort than a single-provider solution. On the other hand, due to the experience and expertise of these providers, the effort to set up a generic IT infrastructure is comparatively low. As the interfaces between the standard components should be up and running, just another instance of application software has to be set up with roles and rights.

Another advantage of the many-provider approach from a data protection point of view is that the different types of medical patient data are distributed to several locations and providers. Thus, an unauthorized disclosure combining different sources of medical data of a patient can be prevented.

6. Conclusions

The service provider approach seems to be a good choice concerning standard components like a clinical trial database from the efficiency point of view especially for smaller, time-constrained or highly flexible research groups. Concerning sustainability it seems to be favorable to host one or two newer IT components within the research group. These should be components like biomaterial software or a research database, which are not as yet often offered by service providers.

However, the following needs to be considered: 1) A limited number of providers should be selected, which should have pre-specified and interoperable software systems and interfaces. 2) An experienced chief information officer (CIO) must be chosen for the coordination of the setup, operation, and extension of the IT infrastructure for the overall research network. 3) It should be ensured that not all data of one type, e.g. the identifying data of all German medical research networks, are hosted by one provider. Such a collection might prompt unnecessary high risks of unauthorized access.

As all presented medical research networks include international partners, the results of this review can be transferred to other projects in Europe and the US, as the privacy rules are comparable. Nevertheless, this result only can be achieved due to the efforts made to design a modular data protection concept and to discuss this concept with the relevant privacy officers.

Acknowledgments

This work was supported by the Deutsche Forschungsgemeinschaft (KFO 179). The Competence Network for Congenital Heart Defects was funded with grant no. 01GI0601 and the German Competence Network Multiple Sclerosis with grant no. 01GI0910 by the Federal Ministry of Education and Research (BMBF).

References

1. Rienhoff O. Zur Beurteilung der "Richtigkeit" patientenbezogener Daten in der medizinischen Dokumentation. In: Reichertz PL, Kilian W, editors. *Arztgeheimnis – Datenbanken – Datenschutz*. Berlin: Springer-Verlag; 1982. pp 196–203.
2. Murphy SN, Mendis M, Hackett K, Kuttan R, Pan W, Phillips LC, et al. Architecture of the open-source clinical research chart from Informatics for Integrating Biology and the Bedside. *AMIA Annu Symp Proc* 2007. pp 548–552.
3. Langella S, Oster S, Hastings S, Siebenlist F, Phillips J, Ervin D, et al. The Cancer Biomedical Informatics Grid (caBIG) Security Infrastructure. *AMIA Annu Symp Proc* 2007. pp 433–437.
4. Manion FJ, Robbins RJ, Weems WA, Crowley RS. Security and privacy requirements for a multi-institutional cancer research data grid: an interview-based study. *BMC Med Inform Decis Mak* 2009; 9: 31.
5. Lun KC. Challenges in medical informatics: perspectives of an international medical informatics organization. *Methods Inf Med* 2002; 41 (1): 60–63.
6. Duftschmid G, Wrba T, Gall W, Dorda W. The strategic approach of managing healthcare data exchange in Austria. *Methods Inf Med* 2004; 43 (2): 124–132.
7. Pommerening K, Sax U, Müller T, Speer R, Ganslandt T, Drepper J, et al. Integrating eHealth and Medical Research: The TMF Data Protection Scheme. In: Blobel B, Pharow P, Zvarova J, Lopez D, editors. *eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge*. Berlin: Akademische Verlagsgesellschaft Aka GmbH; 2008. pp 5–10.
8. Kalra D, Singleton P, Milan J, Mackay J, Detmer D, Rector A, et al. Security and confidentiality approach for the Clinical E-Science Framework (CLEF). *Methods Inf Med* 2005; 44 (2): 193–197.
9. Reng C, Debold P, Specker C, Pommerening K. *Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin*. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft; 2006.
10. Garman KS, Acharya CR, Edelman E, Grade M, Gaedcke J, Sud S, et al. A genomic approach to colon cancer risk stratification yields biologic insights into therapeutic opportunities. *Proc Natl Acad Sci USA* 2008; 105 (49): 19432–19437.
11. Ghadimi BM, Grade M, Difilippantonio MJ, Varma S, Simon R, Montagna C, et al. Effectiveness of gene expression profiling for response prediction of rectal adenocarcinomas to preoperative chemoradiotherapy. *J Clin Oncol* 2005; 23 (9): 1826–1838.
12. Simon JW, Paslack R, Robiński J, Goebel JW, Krawczak M. *Biomaterialbanken – Rechtliche Rahmenbedingungen*. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft; 2006.
13. Simon J, Paslack R, Robiński J, Cooper DN, Goebel JW, Krawczak M. A legal framework for biobanking: the German experience. *European Journal of Human Genetics* 2007; 15 (5): 528–532.
14. Kiehntopf M, Böer K. *Biomaterialbanken – Checkliste zur Qualitätssicherung*. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft; 2008.
15. Faldum A, Pommerening K. An optimal code for patient identifiers. *Comput Methods Programs Biomed* 2005; 79 (1): 81–88.