Clinical Record Systems in Oncology. Experiences and Developments on Cancer Registers in Eastern Germany

Bernd BLOBEL
The Otto-von-Guericke University Magdeburg, Faculty of Medicine, Institute of Biometrics and Medical Informatics, Leipziger Strasse 44, D-39120 Magdeburg, Germany

Abstract. Healthcare information systems have to guarantee quality and efficiency of the medical maintenance. The basis of such information systems is an good medical and caring documentation. The labour-shared, cooperative care for cancer patients as "Shared Care" requires a complete, distributed cancer documentation, summarized in clinical cancer registers. The information of those registers are also a basis for a population-related epidemiological registry. Cancer registers must meet all demands in data protection.

This paper deals with the security architecture of distributed information systems. Organizational as well as technical problems are discussed. Essential attention is paid to security modelling and access rights. The actual structure of the regional Clinical Cancer Register Magdeburg/Saxony-Anhalt and the existing as well as the planned register security mechanisms are presented.

1. Introduction

The healthcare system in the former GDR was characterized by a centralized organization structure. From the year 1989 [8], the following facts demonstrate the achievements, problems, and difficulties of healthcare. The expenditure for healthcare and social welfare increased up to 6.9% of the state budget, but also the healthcare suffered from the inefficiency economics, the objectively small resources, and the low technical standard. The inpatient care was realized in 543 hospitals with 165,950 beds. Providing outpatient care, 117 outpatient departments have been faced with 1,625 state doctor's practices, 2,024 doctor's medical services, 5,509 district nurse's stations, 1,327 nurse's medical services, and only 367 registred doctors. Nearly 600,000 employees worked for the healthcare. For each 10,000 inhabitants, the care was performed by 25.0 doctors, 7.8 dentists, and 2.6 pharmacists.

After the German reunification the healthcare and social welfare in Eastern Germany was adapted to the conditions in the "old" German Federal Republic. Accompanied by huge expenditures, this process will occupy yet a lot of years. The buildings have to be renovated, the equipment and the care structure must be brought up to date. The number of beds per hospitals was decreased and the number of registred doctors was increased extremely.

The reorganization of the healthcare system is directed towards an efficient healthcare system and medical informatics has to help realize this, as it will be shown in this paper.

2. The National Cancer Registry

All newly reported malignant neoplasms that occured in the former GDR have been recorded and entered into the „Nationales Krebsregister“ (National Cancer Registry). This epidemiological register was one of the largest cancer registries of the world, founded in 1953. It was an population-based incidence register classified by place of residence. The cancer registration is based on the legal obligation of each doctor and dentist to declare all malignant neoplasms. Within a well developed cancer notification system, cancer control agencies for cancer patients were established in almost all of the more than 200 counties of the former GDR. Currently, the register includes detailed information of 2 million cancer patients, collected using an uniform questionnaire unchanged over the register's lifetime.

The major goals of the National Cancer Registry of the former GDR were

- the realization of medical statistics related to national cancer cases, supporting the decision-making by the State health authorities,
- the epidemiological research of malignant tumours.

The notification procedure ensures the recording of the tumor diagnosis, results of the first treatment, of additional measures, of follow-up and of autopsy in case of death. Each doctor or dentist was obliged by law to fill in a notification form and to transmit the form for evaluation to the National Cancer Registry through the local cancer control agencies performing quality assurance.

The registration was paper-based. For technical reasons in the eighthies only the centralized records were realized in a computerized manner.

The following details were recorded for each cancer case [27]:

- cancer patient's personal identification,
- tumour site,
- tumour histology, classified by the ICD-O,
- tumour stage,
- tumour diagnosis, related to the ICD9,
- tumour therapy,
- further treatment,
- follow up,
- individual history,
- family history,
- death, including autopsy results, if any.

These items correspond to sensitive personal and medical information.

The use of cancer documentation data was restricted and audited. Besides rules for the confidential doctor-patient relationship there were no security measures like encoding of records etc. From the technical point of view the National Cancer Registry was a closed system.

After the German reunification some cases of security offences, e.g. related to special patients' medical record, were announced, perpetrated in the GDR healthcare by the state security service. Such misdemeanours in relation to the cancer registry the author cannot verify, but also not exclude. Apart from dissidents or similarly evaluated persons, there were practically no social or related threats for patients within the GDR society, concerning e.g. the revelation of medical information by insurance companies or others.

About 99% of the malignant neoplasms were registered in the National Cancer Registry. Only <1% was recorded by death certificates only (DCO). Initially there were political restrictions for work with and interpretation of the information concerned with the cancer

register, but also technical problems hindered the successful use of that excellent scientific source.

In the former Federal Republic of Germany such registry was not available. Only the Saarland has created a comparable institution. After the German reunification the legal basis for the continuation of the National Cancer Registry was missing. Big efforts had to be made, to save the National Cancer Registry from extermination. First, the registry was adopted by the 5 "new" German Federal States and Berlin with an administrative agreement. By a quickly elaborated and passed law for saving the cancer register („Krebsregistersicherungsgesetz“ [6]) the continuation of registration and the restricted use of the cancer data for research was made possible until the December 31th, 1994. Since January 1st, 1995, the Cancer Registry Law („Krebsregistergesetz“) is legally valid, after having been discussed for more than 10 years and finally accelerated by the circumstances and legal problems with the National Cancer Registry [7].

The procedure of the population-based cancer registration is realized in two steps by two institutions. In the first stage, the Trusted Site accumulates the patient-related tumour data recorded by doctors, dentists, Follow-up Organization Centres or Clinical Cancer Registers (see later). Only few items about the cancer case, needed for a population-related cancer incidence register are recorded. The Trusted Site anonymizes the cancer patient’s personal data by an asymmetric procedure, e.g. a hybrid IDEA-RSA encoding. The identifying data will be encoded with an IDEA session key, generated accidentally. The IDEA key will be encoded by a public RSA key with a minimal length of 640 bit. To allow an unambiguous assigning of additional information to the correct patient record, a control number (a special kind of pseudonyms) will be generated, using different attributes of the personal data. That control number will be generated by the utilization of a one-way procedure (MD5) and a symmetrically cryptographic algorithm (IDEA). To allow the assigning of data from the different federal states, the control number procedure and key have to be united Germany-wide ("Linkage Format"). The Trusted Site transfers both the encoded patient-identifying data and the epidemiological plaintext data to the Registry Site. The Registry Site stores the record in the register database and brings together different registrations belonging to one patient. After the matching of data, an accidental number will be added to the control number and the result will be symmetrically encoded by IDEA ("Storage Format"). For the record linkage, the control numbers must be transformed from the "Storage Format" to the "Linkage Format". A corresponding security infrastructure (TTP services like key management) is necessary.

On request, the exploitation of anonymized register data is possible for scientific aims, restricted in time and number. In special medical cases a trustworthy advisory committee can also authorize the use of reidentified records. The procedure applied in the context of the epidemiological cancer registry was developed by *Appelrath* and *Michaelis* [11, 26].

In the context of reorganization and reformation of the Eastern Germany’s healthcare system and his adaption to the Western Germany’s conditions, there was a big chance to design the healthcare system with the latest technology and according to the actual requirements in industrial countries all over the world.

3. Background Conditions in Healthcare

The basic conditions of the future healthcare systems in the industrialized countries are characterized

- by the demographic development with an increasing number of multimorbid persons,
- by the rapid medical and technical progress as well as

- by increasing demands on the quality of life also regarding disease and suffering, disabilities and chronic diseases.

Taking these basic conditions into account, the industrial countries are trying to realize an efficient healthcare within the health policy framework [19], which is determined objectively as well as subjectively. The efficiency of healthcare must be evaluated by both the managerial and the economical efficiency (cost-benefit relation, outcome) **but also** by the quality of medical outcome. Regarding this

- specialization and shared labour in both healthcare and welfare as "Shared Care",
- communication and cooperation between the care givers, but also between providers and funding organizations, e.g. insurance companies, and/or other institutions directly or indirectly involved in healthcare as well as
- competition on the basis of corresponding transparency of achievements and flexibility

must be developed [19]. These processes are accompanied by an improvement in technology in health institutions, especially in information technology.

Traditionally, information systems support achievement-related (outcome-related) evaluation and compensation as well as an optimal interoperability between the different healthcare providers. The outcome evaluation is required for the ascertainment of an achievement-related reimbursement as well as for a corresponding transparency of costs and achievements. Internally such transparency is useful for an optimal arrangement and management of the processes. Externally it serves the productivity certificate facing the potential partners in cooperation or facing the funding organizations. Increasingly, the medical objectives, i.e. the direct care processes and their optimization, will become dominant. The information systems meeting these requirements must be established nearly real-time and process-oriented as well as patient-centred. The system architecture has to be designed according to the complex model of the real processes. Such an information system architecture is very demanding with respect to data security.

Also the care of cancer patients should be organized in an efficient manner. A specialized and labour-shared cancer care as well as a secure distributed tumour documentation meet these requirements.

4. Structure of Hospital Information Systems

Figure 1: General model of a Hospital Information System

The architecture of information systems corresponding to the described demands should be explained using the example of Hospital Information Systems (HIS) [4]. Figure 1 shows the streams of information and materials within a hospital as well as between hospital and its associated area (modified according to [1]). The representation formalizes the actual processes of labour-shared medical care within a hospital. If the general HIS model will be realized by actual application systems which are distributed in analogy to the underlying processes, this can be illustrated as shown in figure 2.

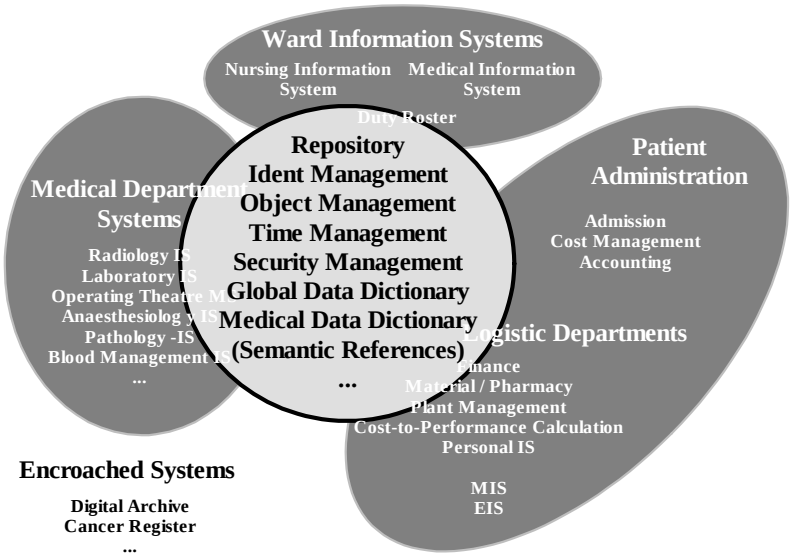

Figure 2: HIS characterized by applications

5. General System Structure

The systems associated with the individual work fields must copy and support the actual care process optimally by information. They must communicate or still better cooperate like in the real labour-sharing world. To guarantee a semantically determined communication and cooperation, different logically "centralized" functions are necessary. This includes extended identification management, object management ("Extended Object Directory") with indexation, time management for the supply of ressources without conflicts, security management, a global "Data Dictionary" for the navigation between (preferably database-based) applications, a medical "Data Dictionary" for the semantic reference as well as a complex "Repository".

These logical "centralized" functions will be realized in the HANSA project [1] for open, distributed, modular, networked healthcare information systems. Among other things [21], it deals with the "Identification and Authentication Manager", with the "Rule Manager", and with the "Security Manager". which will be processed by the Magdeburg team.

[1] The HANSA project (Healthcare Advanced Networked System Architecture) is funded by the European Commission within the fourth framework "Telematics Applications Programmme". It is coordinated by *Frabrizio Massimo Ferrara* (Rome).

6. Definition of "Shared Care"

Corresponding to [20] the "Shared Care" can be defined as
"a continuous and coordinated activity of
different persons in
different institutions under
employment of different methods at
different times
in order to be able to help patients optimally with respect to their
medical,
psychological and
social being".

The cancer care is a vivid example of the "Shared Care" concept in healthcare. From the first suspicion or ascertainment of a cancer disease, the diagnostics follows in specialized institutions (usually in hospitals, but also in special ambulances or in specialist's practices). Currently, the therapy is likewise accomplished in specialized sites (usually in hospitals, but also in special ambulances or in specialist's practices). However, also an increasing number of GPs take over these tasks themselves and/or at least organize or coordinate the care. The same is true more than ever for the follow up, where, in addition, also rehabilitation organizations, self-help groups and other "Shared Care" structures are entering.

The "Shared Care" concept requires an optimal design of informational relationships and information systems respectively. The convenient system for the documentation and information in medical care is the medical record. Consistently, a process-related and patient-centred information system dominated by medical and caring aspects is realized by an electronic patient record (EPR, electronic medical record, computerized patient record, ...) [19, 29]. Within healthcare delivery structures, which are organized labour-shared and distributed, the electronic patient record is the way to support the care.

For the support of area-covering evenly high-degree care of cancer patients, so called cancer centres or oncological centres were founded in Germany. With generous funding through the German Federal Ministry of Health, a network of about 20 such institutions was installed also in Eastern Germany [3, 4]. Apart from clinical cancer registers, epidemiological cancer registers are also very helpful for the investigation of some cancer-related questions, as mentioned in paragraph 2. In 1993, the "new" German federal countries and Berlin have decided to continue the common epidemiological cancer registration in Berlin, called „Gemeinsames Krebsregister". The clinical cancer registers are the dominant registration sites for the data flow to this Berlin registry. Following, I will restrict my presentation mainly to the regional Clinical Cancer Register Magdeburg/Saxony-Anhalt.

Within the cancer centres, which were founded

- to support the cooperation between the different institutions relating to the labour-shared care of cancer patients,
- to improve quality and efficiency of cancer care,
- to promote research and development in oncology,
- to improve training and education,
- to elaborate standards for care and quality assurance etc.,

the clinical cancer registers should support the authorized user to achieve these objectives by available, integer and consistent information at the right time and at the right place.

Logically, the regional Clinical Cancer Register Magdeburg/Saxony-Anhalt supports the "Shared Care" concept in Oncology.

7. The Legal Framework of Cancer Registers

The arrangement of processes in a society and therefore also in healthcare is bound to the legal framework, to professional regulations as well as to institutional instructions and guidelines. But especially in medicine, ethical criterias, psychological conditions and social consequences must be considered [15, 16, 23, 24].

The legal basis for the function of cancer registers are

- the general legislation of documentation in medicine,
- the regulations of the „Bundesdatenschutzgesetz“ (the federal data protection law) as well as the „Landesdatenschutzgesetze“ (the data protection laws of the different federal states),
- professional regulations for physicians, nurses and equivalent professionals in relation to medical processes and medical data (e.g. the obligation of secrecy),
- the orders of the criminal law.

Within the European Union, the EU Data Protection Directive, passed by the Council of Europe in the summer 1995, is also an attractive legal basis. But the transformation into the German legislation is rather unlikely due to the principle of subsidiarity [5].

Amongst all, the special legal framework for the function of epidemiological cancer registers are established in the already cited German Cancer Registry Law [7]. These general regulations will be specified by corresponding „Landes-Krebsregistergesetze“ (cancer register laws of the different German federal states), which will be extended to some instructions on clinical cancer registers.

The medical documentation and especially cancer registers must be carried out in such a way, that the patient’s right of informational self-determination is guaranteed and that hygenic, mental, social harm or even existential threats are kept away. But there are also objective aspects and constraints, determining record, storage and processing of patient information. Such aspects and constraints are in patient’s interest or absolutely necessary for the staging of medical care. In this context the civil rights of health professionals, which are defined in professional regulations or in the works constitution law for employed health professionals, are also noteworthy. Security measures in medicine should also improve the common legal security.

A basic condition of recording, processing and communication of personal data is in general the consent of the concerned, but at least his/her information. For implementation of patient-related documentation and information systems the three dimensions of security have always to be guaranteed [12]; i.e.

- integrity
- availability and
- confidentiality.

Currently the legal basis of recording, processing and communication of patient related oncological data is the patient consent.

8. The Security Background in the Magdeburg Department of Medical Informatics

The Magdeburg department is the medical informatics group with the most extended activities and experiences on data security in modern information systems in Germany. In 1993 the first hardware based solution for trusted communication in the German healthcare was implemented in the Clinical Cancer Register Magdeburg/Saxony-Anhalt. The research and development as well as the implementation of security measures in productive medical

information systems is realized in two organizational and technological phases. In the first phase, we have implemented secure communication and interoperability between different institutions, assumed as closed systems. Following, we have installed a secure external communication infrastructure. Within the organizations therefore, we have guaranteed traditional measures, like organizational instructions and rules, physical measures in the departments, password systems, audit, network security mechanisms etc. The internal infrastructure was considered secure. The second phase is characterized by trusted communication and cooperation in an insecure world. The challenge of such strategy is to overcome the implementation of security measure in both client and server systems. In this context we are currently incorporated into different projects, funded by the European Commission in the fourth framework "Telematic Applications Programme". The activities are addressed to the different views of security in medical informatics

- as the definition of general objectives and conditions and as the management of processes and measures [2],
- the development of security utilities, facilities, and services in modern healthcare information system architectures [3],
- the development, realization, and evaluation of trusted communication by secure authentication and Trusted Third Party services [4],
- the realization and evaluation of all these features in the context of some special applications in realistic healthcare environment, like "Shared Care", network based as well as chip card based heterogeneous information system architecture [5].

Therefore, the Magdeburg Department of Medical Informatics performs activities on all relevant topics of complex data security in medicine, demonstrated in a typical example of labour-shared and regional organized care.

9. General Guidelines for Development and Implementing of a Secure Clinical Cancer Register

In 1990/1991, we have started the development and implementation of an integrated hospital information system (HIS) at the Magdeburg University Hospital. Since then we have to realize all activities, covering the systems development, like specification, design, realization and testing of components of our HIS. The developed components have to be integrated in an existing organizational, functional and technical environment for production.

Since the introducing of IT-applications must be oriented on the objectives and processes of the concerned institution, the most important activity is a clear and complete description of the enterprice policy (objectives; measures; management, process and quality criterias). The second activity should deal with complex process analysis, including integration

[2]These activities run in the ISHTAR project (Implementation of Secure Healthcare Telematics Applications in Europe; coordinator: *Barry Barber*, Birmingham) as a part of the fourth framework “Telematics Applications Programme“, sponsored by the European Commission under use of the results of the SEISMED project of the third EC framework “Advanced Informatics in Medicine (AIM)“.

[3] These activities are running in the HANSA project.

[4]These works are accomplished within the TRUSTHEALTH1 project (Trustworthy Health Telematics) as part ot the fourth framework “Telematics Applications Programmme“, sponsored by the European Commission. The project is coordinated altogether by *Gunnar Klein* (SPRI Stockholm) and nationally by *Otto Rienhoff* (Göttingen).

[5]DIABCARD projects as parts of the third and/or. the fourth framework of the European commission (coordinator: *Rolf Engelbrecht*, Munich).

mechanisms. Then a general risk analysis of the system environment as well as the definition of threats and countermeasures have to be performed. Quality management and system evaluation as development results are often unsatisfactory, nevertheless they are essential.

A general prerequisite is a clear description of the responsibilities within the institution as well as in the supplier enterprice. We have good experiences with the appointment of a General Manager (preferably a specialist in organizational and IT issues) in the person of the Medical Informatics Department's head and with specialized responsibilities for each activity and topic respectively. In Germany the involvement of the works committee is subject to legislation. But also in countries without such regulations, such involvement should be done as early as possible, for instance by the inclusion of the concerned personnel. All activities must be documented and in the performing phase protocolled in detail.

For each step, the continuous propagation of high level security policy, the improvement of security awareness, and also the training and education of the management as well as the employees is very important. These aspects had always our special attention. It proved difficult, that the Medical Informatics staff could develop the whole concept, but that the components were realized both by ourselves and by external suppliers. That means, that the philosophy must be adopted to the different development environments and possibilities of the supplier in a compromizing sense, but preserving some basic principles.

In order that information systems are approximately as close to reality as possible, the different applications must be able to cooperate. To bring about cooperativity or interoperability of subsystems, the system has to realize the integration type "Integration" [17]. However this implicates that all functions and methods are defined at the database level. Only object-oriented databases have overcome this challenge.

We took the decision for INGRES as the application system database and the development environment. The choice was founded on the property of INGRES as the first relational DB to realize object-oriented features like the knowledge base, rule, trigger events and stored procedures. Meanwhile all dominant DBs have implemented such functions and possibilities and we have installed applications, based on different wide-spread databases, like Oracle, Informix, Sybase and so on.

10. General Security Architectures

The general architecture of distributed cooperating information systems is demonstrated in figure 3. The first requirement is to guarantee the communication of legitimated personnel in a trusted manner only. For this reason a corresponding security infrastructure must be established. In the following chapters this complex of trustworthy communication is described as communication security.

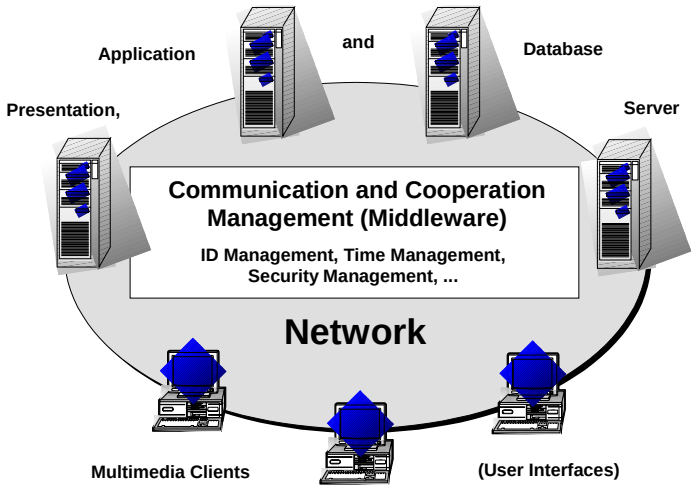

Figure 3: General architecture of distributed cooperating information systems

The authorities within the security infrastructure have to be trustees by their structure as well as in the authority's legal relation to the communication partners and their interests. This is the only way, by which the authorities as references can guarantee trustworth.
The main task of the security infrastructure in respect to the communication security is the provable guarantee of the communication partners' authentication amongst themselves as well as towards third persons or organizations. For this function and for the protection of information integrity one is using certified electronic signatures.

Another important prerequisite for the communication of medical (that means in general highly sensitive) data is the confidentiality of communication, which must work between the partners in the sense of addressed confidentiality without any functional or other restrictions (e.g. performance). Such confidentiality of the contents of information is realized by using cryptographic measures. Symmetric as well as asymmetric algorithms are implemented.

The second requirement for security architectures deals with the functional and data access restrictions for legitimated personnel. In the following chapters this complex of restricted functional as well as data access rigths is described as application security. The basis for application security management is the different position and function of the personnel within the healthcare. Especially, in this context the doctor-patient-relationship, privacy and confidentiality as well as the real process of medical treatment and care are essential.

11. Required Infrastructure for Communication Security

As pronounced, the installation of secure communication systems requires a security infrastructure, which is realized by trustworthy authorities in form of *T*rusted *T*hird *P*arty (TTP) services. Functions of the security infrastructure (TTP services) are for instance

- the generation, distribution and management of keys,
- the promotion and maintenance of name services (directories),
- the certification of keys,
- the time services (certified timestamps) and
- other notary's office functions.

Within a German model project for using health professional cards (HPC) [6] as a part of the TRUSTHEALTH project, we are preparing the development and implementation of the corresponding security infrastructure in the environment of the Clinical Cancer Register Magdeburg/Saxony-Anhalt. In this context it was remarkable, that not only natural persons (individuals), but also legal persons (organizations) should be able to communicate in a secure manner.

For the use of HPC as electronic identity cards and also as electronically vocational identification, the following trustworthy structure must be established. As a result of the German TRUSTHEALTH project group [10], we plan for the German model project the following authorities:

- for the personal authentication
  - the Naming Authority (NA),
  resulting in a personal distinguished name
  - the Registration Authority (RA),
  resulting in an authentic personal document
- for the professional authentication
  - the Qualification Authentication Authority (QAA),
  resulting in a qualification authentication
  - the Profession Authentication Authority (PAA),
  resulting in a profession authentication
  - the Professional Registration Authority (PRA),
  resulting in an authentic professional document
- for the professional certification
  - the Professional Certification Authority (PCA),
- for the professional class authentication
  - the Professional Class Definer (PCD)
  resulting in a professional class definition
  - the Professional Naming Authority (PNA),
  resulting in a professional class distinguished name
  - the Professional Class Registration Authority (PCRA),
  resulting in an authentic professional class document
- for the key certification
  - the Key Generation Instance (KGI)
  resulting in a public (and a privat) key
  resulting in a public (and a privat) class key
  - the Certification Authority (CA)
  resulting in a public key certificate

There is a common consideration of identity and profession within the context of the application in the case of cancer registers. Therefore, a general authority (C)A could be useful, which also certificates the keys. For general purposes chip cards, the separation of the CA for both the identity and the profession should be recommended. Figure 4 presents the planned structure of security infrastructure authorities in the regional cancer register.

[6] This German model project of the „Arbeitsgemeinschaft Karten im Gesundheitswesen“ is chaired by Otto Rienhoff (Goettingen) and includes also the HPC-use in an intensive care ward of the Goettingen University Hospital [2].

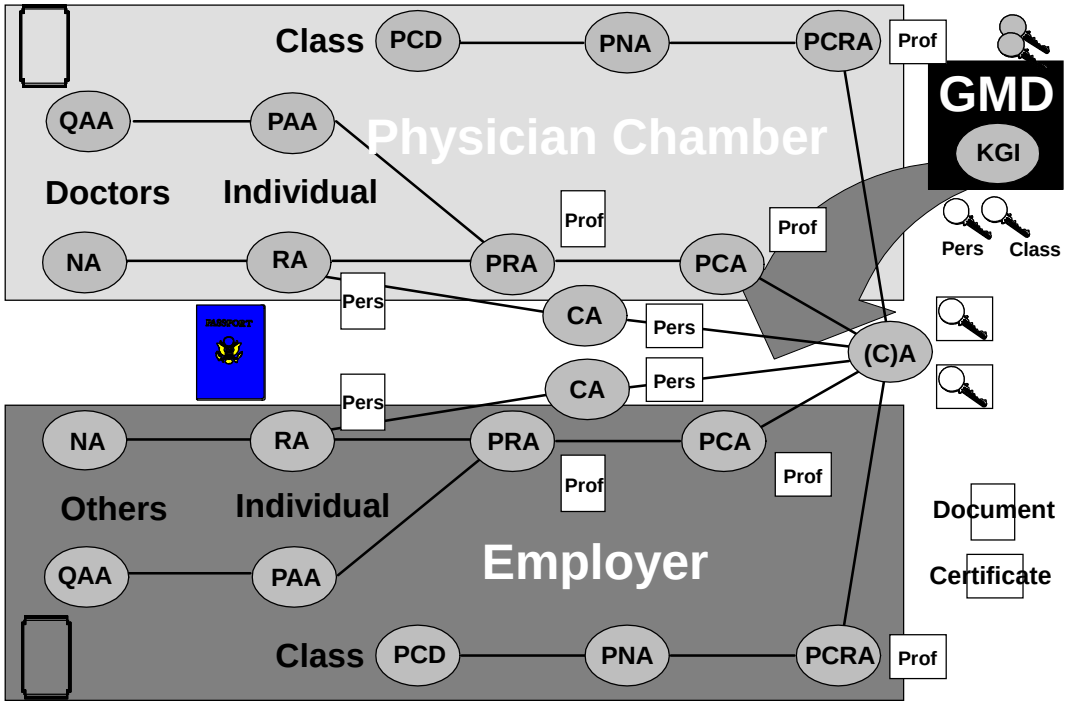

Figure 4: The planned structure of security infrastructure authorities

12. The Security Architecture of the Regional Clinical Cancer Register Magdeburg/Saxony-Anhalt

The foundation and further development of the Clinical Cancer Register Magdeburg/Saxony-Anhalt in 1992/1993 was persecuted to realize a regionally distributed EPR in Oncology, which is usable for all institutions and individuals, labour-shared involved in the cancer care. This pioneer achievement could only be realized with pioneer achievements on the data security domain. Therefore, the Magdeburg cancer register was the first medical institution in Germany, designing and realizing data security in medicine systematically. On account of our objectives, additional to the cancer register functions [19], the functionality of intra-institutional and inter-institutional communication by online-documentation as well as online-information has been forced.

Currently, 53 clinics of the Magdeburg University Hospital and of other important hospitals in the governmental district Magdeburg are involved in the regional cancer register. To establish the register as a continuous and patient-centred cancer documentation, the crucial breakthrough could be achieved with the integration of the Oncological Follow up Organization Centre for registered doctors into our cancer register. By the direct and secure connection of the Follow up Organization Centre LAN to the GTDS, also the GP's Follow up structures (registered doctors) could be involved into the syntactically and semantically unified form of documentation and information. In this context, the Oncological Follow up Organization Centre realizes both the function of a documentation place and the institution for follow up organization in mission of registered doctors (GPs). Figure 5 gives an overview of the geographic structure of the Clinical Cancer Register Magdeburg/Saxony-Anhalt. The catchment area of the register includes the north of our federal country (with a total 2.8 million inhabitants) with about 1.2 millions inhabitants.

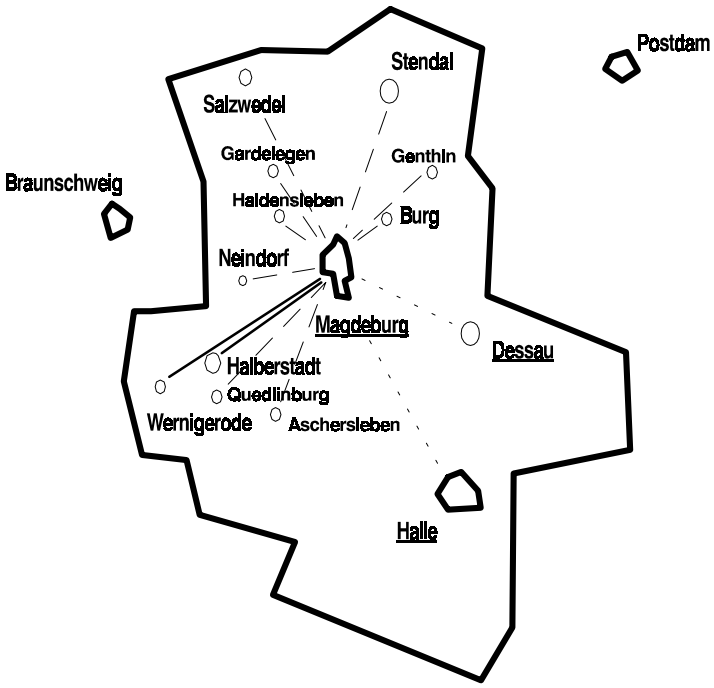

Figure 5: The catchment area of the Magdeburg/Saxony-Anhalt Cancer Register

An optimal effect of the documentation and information system is only achievable with an online connection of all participants. This means, that the system has to be integrated into the oncological care like a realtime system. Currently about one fourth of the partners are working online with the GTDS. At the end of next year all partners will cooperate online with our register.

The regional cancer register contains the patient-related general tumor medical records for all institutions and/or persons, which are integrated in the register and are included into the labour-shared care of cancer patients. As pronounced, the cancer documentation is realized on the basis of the voluntary, written consent of the informed patient with respect to the cooperative tumor documentation. Restraints of the documentation, desired by the patient, e.g. the exclusion of individual persons or institutions from the communication combine, can be realized. However, that must remain the exception, because otherwise the objective of the project would be put in question. Since the general cancer record is a collection of personal, highly sensitive data, particular measures guaranteeing data protection and data security had to be realized. These data security measures concern

- measures in the local networks of the respective user departments, e.g.
  - the design of a communication network structure with attention to legal and managerial (structural, organizational) significance,
  - the implementation of all server equipments as security areas (DB server; application server; communication server, like router, HL7 server etc.; transaction monitors, authority server etc.),
  - security mechanisms of the LAN, like access nodes, address lists, special gateways for external communication (modem, fax, BTX) as well as KAPI (or better S-KAPI) protocols for ISDN communication (see for details [16]),
- measures for the communication by the public telephone system
  - analogous lines, ISDN,

and/or

- other communication media of third parties

– e.g. the scheduled Magdeburg Metropolitan Area Network (MAN), the German scientific information network (WIN) of the DFN union as an example of a Wide Area Network (WAN)).

On one hand, the guarantee of data security includes organizational measures. Among others, the following points are relevant:

- the restraint of the user domains and authorized users to the necessary extension,
- the definition of user groups and the respective rights (functional and data access rights) of these groups,
- a four level identification and authentication system and an extended audit.

Apart from that, organizational and technical measures were realized, such as the exclusive use of the cancer register server for the tumor documentation application as well as the separation of the production mode system from the test & development & training system. Through such measures, the unauthorized access to the application by persons authorized to system access can be prevented. In the same context, the control of the functional and the access rights was realized by the network architecture (communication units and routers). Additionally, an extended password-related access control should be at least realized.

In the first phase of the implementation and the productive work of the regional cancer register, no secure hardware-based identification and authentication including the corresponding right management of individual users was available apart from the three-stage password mechanism and the log-file system. Therefore, an architecture of distributed, closed and secure external subsystems was realized first. The identification and authentication of area and/or client (system) and consequently the access control was realized for the external users connected by analogous lines and modems on the basis of MACS (Modem Access Control System, FAST company). For external users, connected by ISDN, we have installed the Kryptogard LAN L3 equipment (Kryptocom company). This system realizes a secure LAN-to-LAN communication, including firewall functionalities. The information encoding is performed by the application of Triple-DES session keys. These keys are exchanged with RSA encryption, on this way ensuring both the identification and authentication of the coupled domain and the integrity check of communication. Meanwhile also the secure installation of single PC by ISDN Kryptogard PC (Kryptocom company) could be implemented. Figure 6 presents the successful temporary solution in the topicality of May 1996.

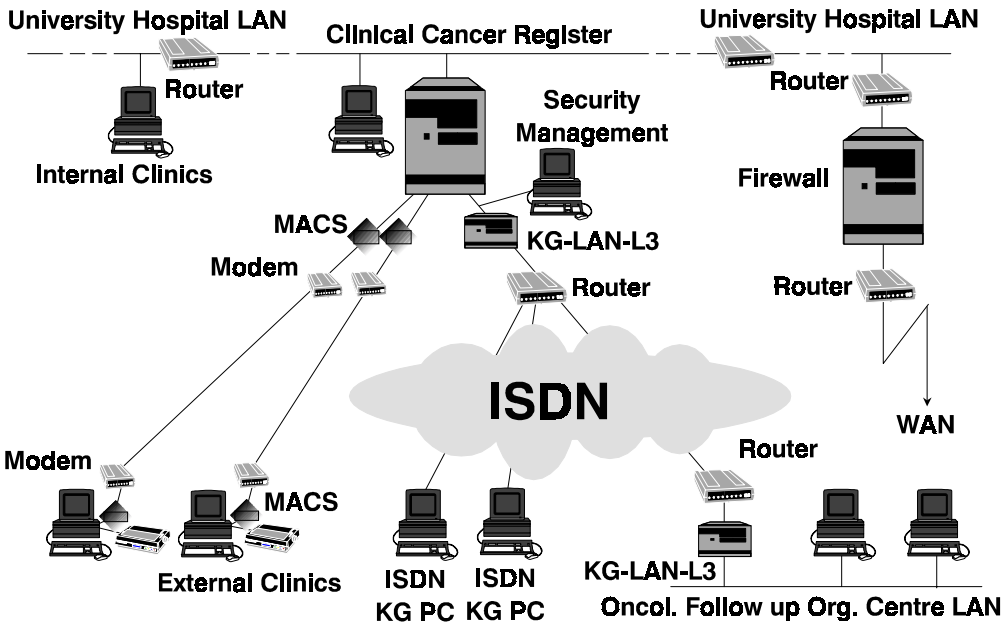

Figure 6: Productive security solution in the regional distributed cancer register

In this context, two development activities should be remembered

- the identification and authentication on the basis of Trusted Third Party services and health professional cards within both the TRUSTHEALTH and the cited German model project,
- a detailed right management (security management of the specific application-related functional and data access rights) in the DHE-framework (Distributed Healthcare Environment) of the HANSA project.

The functional and data access rights result on the one hand from the structural and organizational conditions (classification of users, user hierarchy), and on the other hand from the actual care process (doctor in charge of the case, the confidential doctor-patient relationship, temporary diagnostic and/or therapeutic team). The structural determined right management can be described by Mandatory Access Models (extended matrix of access rights). The patient-related right management has to be described by Discretionary Access Models. In order to master the system, groups and rules for users and rights respectively are defined, which are to be examined for the concrete case. The modelling of the security management based on a defined security policy [7] is discussed [17]. If available, the transfer and the storage of data should be implemented in a cryptographically encoded form. Figure 7 represents the general scheme of security systems, while figure 8 demonstrates security services in multi-stage client-server architectures.

[7] These activities run in the ISHTAR project (Implementation of Secure Healthcare Telematics Applications in Europe; coordinator: *Barry Barber*, Birmingham) as a part of the fourth framework "Telematics Applications Programme", sponsored by the European Commission under use of the results of the SEISMED project of the third EC framework "Advanced Informatics in Medicine (AIM)".

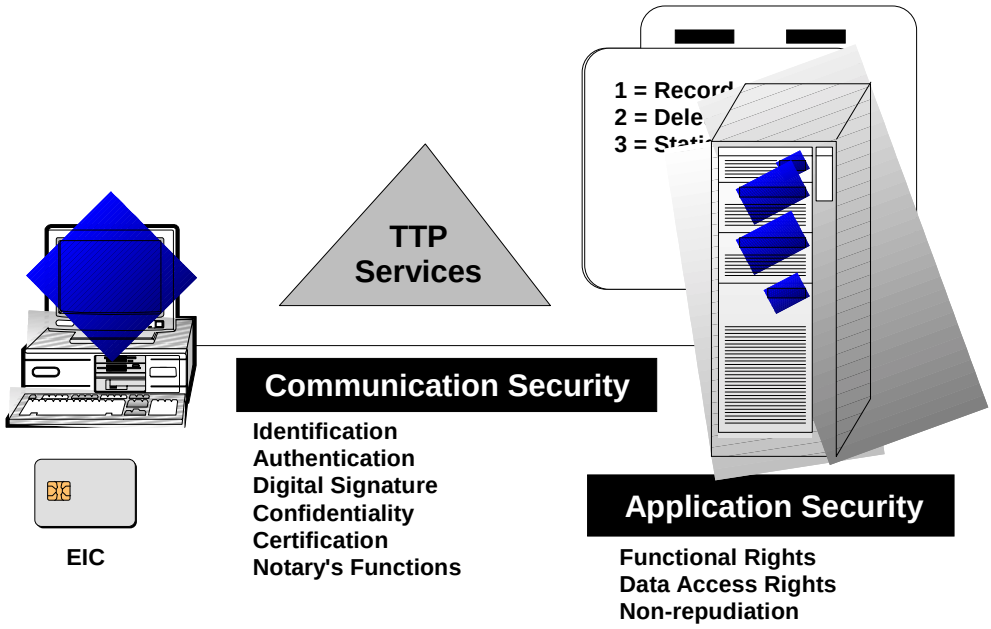

Figure 7: General scheme of security systems

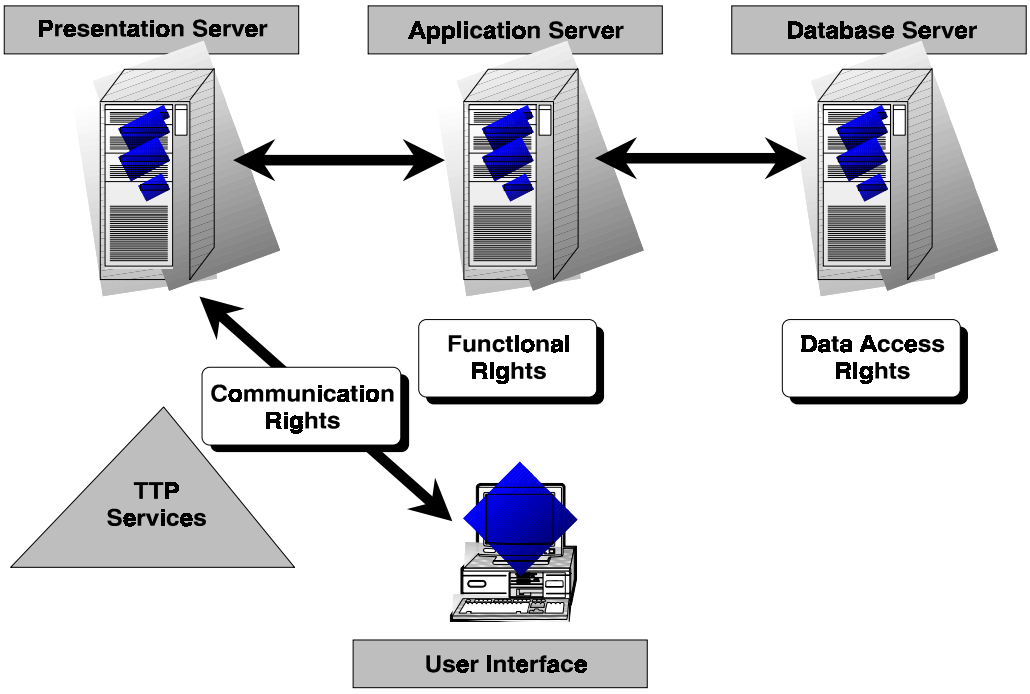

Figure 8: Security services in multi-stage client-server architectures

The success of security measures depends on the security awareness of all related persons, which requires extended education and training.
For the pilot project of the regional Clinical Cancer Register Magdeburg/Saxony-Anhalt the complete furnishing of all partners with HPC and card readers is planned for 1997. That means the installation of about 300 HPC and 200 card readers. As in the pilot's first phase,

the card reader will correspond to the „Multifunktionales Kartenterminal“-Standard (MKT, multi-functional card terminal) [1]. Currently, this standard for a T=1 card reader is discussed in the CEN TC 251.
To standardize the development and implementation activities as well as to improve the quality of work, the use of modern tools, like

- tools for object-oriented system analysis, design and implementation (e.g. SOM, SERM) [28],
- tools for security analysis (SIDERO) [22],
- the SEISMED guidelines with the comprehensive expert’s experience and knowledge [9, 13, 14],
- and own modelling and development tools for secure systems

is an essential basis.
The relationship between chipcard-based information systems and network-based information systems is discussed in e.g. [19, 25].

13. Some Concluding Remarks

- Medical care, care providers' outcome and personal data security are not contradictionally but conditionally.
- Legal conditions, issues, involved persons, requirements and goals as well as need of protection are especially important for planning and performing of health data communication.
- The merge of legal, managerial, and medical competence of the different healthcare-related institutions like governmental organizations, insurance companies and healthcare providers has to be avoided.
- Medical progress should not be supressed by restrictions in the use of new technologies, but this must be accompanied by suitable measures.
- Medical data should be anonymized whenever possible, using also especial algorithms like pseudonyms.
- The responsibility for patient-related medical data is located to the patient-doctor-relationship as the kernel of healthcare.
- The guarantee of patient's human right for informational self-determination requires a higher level of awareness and education to be able for realization that right.

The general higher threats for persons have to be compensated by legal, organizational, and technical measures in data security to realize ethic principles, professional’s responsibility and the protection of the human rights within a democratic and liberal society.

14. Acknowledgement

The author is obliged to the European Commission, DG XIII, to the SEISMED Consortium and to the other EU projects for the support of the activities as well as to the Ministry of Education and Sciences of the Federal State of Saxony-Anhalt for funding.

15. References

[1] Arbeitsgemeinschaft „Karten im Gesundheitswesen“, GMD - Forschungszentrum Informationstechnik GmbH: Multifunktionale KartenTerminals (MKT) für das Gesundheitswesen und andere Anwendungsgebiete. Spezifikation Version 0.9, August 1995.

[2] Arbeitskreis „Health Professional Card“ der Arbeitsgemeinschaft „Karten im Gesundheitswesen“: Deutscher Modellversuch „Health Professional Card (HPC)“, Göttingen, 13.3.1996.

[3] Bundesministerium für Gesundheit: Anforderungen für Modellvorhaben zur Verbesserung der regionalen onkologischen Zusammenarbeit. Bonn, 13.6.1991.

[4] Bundesministerium für Gesundheit: Grundsätze für den Aufbau und Betrieb Klinischer Krebsregister in Behandlungsschwerpunkten zur flächendeckenden regionalen onkologischen Versorgung. Bonn, 17.6.1991.

[5] Council of Europe: EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Strassbourg 1995.

[6] Gesetz zur Sicherung und vorläufigen Fortführung der Datensammlung des „Nationalen Krebsregisters“ der ehemaligen Deutschen Demokratischen Republik (Krebsregistersicherungsgesetz) vom 29.12.1992, BGBl I, 2335.

[7] Gesetz über Krebsregister (Krebsregistergesetz, -KRG) vom 4.11.1994, BGBl I, 3351.

[8] Institut für Medizinische Statistik und Datenverarbeitung Berlin (Hrsg.): Das Gesundheitswesen der Deutschen Demokratischen Republik 1989. 24. Jahrgang, Berlin 1989.

[9] SEISMED Consortium: European Health Data Security Guidelines. IT and Security Personnel. Birmingham 1995.

[10] TRUSTHEALTH1 Consortium - German Group: German Recommendations to the TTP Functional Specification (Draft). Göttingen 1996.

[11] H.-J. Appelrath, J. Michaelis, I. Schmidtmann, W. Thoben: Empfehlung an die Bundesländer zur technischen Umsetzung der Verfahrensweise gemäß Gesetz über Krebsregister (KRG). Technischer Bericht, Tumorzentrum Rheinland-Pfalz, Mainz 1995.

[12] A.R. Bakker: Security in Medical Information Systems. In: J.H. van Bemmel and A.T. McCray (Edrs.): Yearbook of Medical Informatics, pp 52-60. Schattauer, Stuttgart 1993.

[13] B. Barber, J. Davey: The Use of the CCTA Risk Analysis and Management Methodology [CRAMM] in Health Information Systems. In: K.C. Lun, P. Degoulet, T.E. Piemme, O. Rienhoff (Edrs.): MEDINFO 92, pp. 1589-1593. North Holland, Amsterdam 1992.

[14] B. Barber, G. Bleumer, J. Davey, K. Louwerse: How to Achieve Secure Environments for Information Systems in Medicine. In: R.A. Greenes, H.E. Peterson, D.J. Protti (Edrs.): MEDINFO 96, pp. 635-639. North Holland, Amsterdam 1996.

[15] B. Blobel: Datensicherheitsprobleme und -lösungen in offenen medizinischen Informationssystemen. In: B. Blobel (Hrsg.): Datenschutz in medizinischen Informationssystemen, S. 123-138. Verlag Vieweg, Braunschweig - Wiesbaden 1995.

[16] B. Blobel: Open Information Systems and Data Security in Medicine. In: B. Barber, A. Treacher and K. Louwerse (Edrs.): Towards Security in Medical Telematics, pp 168-182. IOS Press, Amsterdam - Oxford - Tokyo - Washington/DC 1996.

[17] B. Blobel: Modelling for Design and Implementation of Secure Health Information Systems. In: A. R. Bakker et al. (Edrs.): Communicating Health Information in an Insecure World. Conference Preprint,

pp 149-156. Data Protection and Security Working Conference, Helsinki 30 September - 3 October 1995.

[18] B. Blobel: Konzeption für Telematikanwendungen im Gesundheitswesen sowie für ältere und behinderte Menschen. Zuarbeit zum Entwurf des Durchführungskonzeptes für eine Telematik-Initiative Sachsen-Anhalt. Magdeburg, 19. Februar 1996.

[19] B. Blobel: A Regional, Secure Cancer Documentation System for an Optimal "Shared Care" in Oncology. Presentation at the MIE ‘96, Copenhagen, August 1996.

[20] K.-H. Ellsässer, C. O. Köhler: Shared Care: Konzept einer verteilten Pflege - Kurz- und langfristige Perspektiven in Europa. Informatik, Biometrie und Epidemiologie in Medizin und Biologie 24 (1993) H.4, S. 188-198.

[21] F.M. Ferrara: The EDITH Approach: The Management Of Authorization And Security In Healthcare Information Systems. In: B. Barber, A Treacher and K. Louwerse (Edrs.): Toward Security in Medical Telematics - Legal and Technical Aspects, pp 200-213. IOS Press, Amsterdam - Oxford - Tokyo - Washington/DC 1996.

[22] E. Flikkenschild, P.v.d. Sluijs, E. Buis, J. Verhage: SIDERO: a relational Database Application for Security Practitioners, supporting the implementation of SEISMED guidelines in Health Care Institutions. AIM SEISMED Deliverable. Leiden 1996.

[23] E.-H.W. Kluge: Health Information, Privacy, Confidentiality and Ethics. B. Barber, A.R. Bakker, S. Bengtson (Edrs.): Caring for Health Information Safety, Security and Secrecy, pp. . Elsevier, Amsterdam 1994.

[24] E.-H.W. Kluge: Health information, the fair information principles and ethics. In: J.H. van Bemmel and A.T. McCray (Edrs.): Yearbook of Medical Informatics, pp 255-264. Schattauer, Stuttgart 1995.

[25] C.O. Köhler, W. Schuster: Informationelle Selbstbestimmung des Patienten durch die Patientenkarte. In: B. Blobel (Hrsg.): Datenschutz in medizinischen Informationssystemen, S. 93-122. Verlag Vieweg, Braunschweig - Wiesbaden 1995.

[26] A. Krtschil, I. Schmidtmann, J. Schüz, J. Michaelis: Bericht über die Pilotstudie zum Krebsregister Rheinland-Pfalz. Technischer Bericht, Tumorzentrum Rheinland-Pfalz, Mainz 1994.

[27] W.H. Mehnert, M. Smans, C.S. Muir, M. Möhner, D. Schön: Atlas der Krebsinzidenz in der ehemaligen Deutschen Demokratischen Republik. Atlas of Cancer Incidence in the Former German Democratic Republic 1978-1982. IARC Scientific Publications No. 106 / BGA Schrift 4/92. International Agency for Research on Cancer, Lyon; Zentralinstitut für Krebsforschung, Berlin; Institut für Sozialmedizin und Epidemiologie des Bundesgesundheitsamtes, Berlin. MMV Medizin Verlag, München 1992. Oxford University Press 1992.

[28] G. Müller-Ettrich (Hrsg.): Fachliche Modellierung von Informationssystemen. Addison-Wesley, Bonn1993.

[29] C.P. Weagemann: Strategy for Information and Image Management in the 1990s. Optical Disk Institute, Boston, Massachusetts 1992.