IT FOR HEALTH CARE IN GLOBAL PERSPECTIVE

- Problems and Pitfalls of Telemedicine

Bernd R. Hornung

Creativity and scientific work which is to lead to new findings and results requires quite specific pre-conditions. These have been investigated both in psychological research on creativity and in philosophy and methodology of science. However, they are intrinsically systemic.

One such condition is specified by Ashby's Law of Requisite Variety [1] as a sine qua non for innovative problem-solving. Another one, based on the existence of such variety, is selection and stabilization as elaborated in the theory of evolution [2] and considered an essential element in science since long. In science it takes the form of progress by peer review and peer critique, whereby a too strict adherence to the peer-principle often risks to lead to petrification of in-groups [3]. A third one finally, professed in sociology most explicitly by Luhmann, but also known from work in ecology and biology, is the role of boundaries and, at least relative, closure [4]. Finally, innovation and creativity cannot really be industrially "produced" and planned, although contemporary organized research tries to work along such lines, with a lot of money, a lot of bureaucracy, and often limited success. What can be done is only to provide a favorable environment and to supply the necessary variety and random events fostering creativity and innovation.

The workshop at Norberg turned out to possess nearly all of these characteristics. Requisite variety was not limited to a variety of disciplinary backgrounds, ranging from ethnology, psychology, and sociology to informatics and mathematics. There was also variety in terms of age and career, which ranged from the student to the senior scientist and university professor. Time for review and discussion was available both within the formal sessions, group work, and round-tables, and during the informal meetings in an enjoyable atmosphere at breakfast, lunch, and dinner.

This was enhanced by the “closure” of the conference site, the group being alone at the Karrgruvan Conference Center in the beautiful Swedish forests, as well as by the size of the group which still permitted everybody to know everybody within the two days of the workshop and to establish one single “system of communication” in which all participants took part.

The group work and round-table at the end of the second day, however, also showed the limits of attention and concentration and of the work that can be achieved within two short days. The panorama and the issue had become clear by then, but not enough time remained to sort, to structure, to digest, and to refine in order to arrive at the kind of results which were hoped for. In this sense the present revised paper, at least in its first three chapters, is a result of the workshop rather than the original input.

IT, Users, and Society

With regard to the title of the workshop, ”IT Users and Producers in an Evolving Sociocultural Context”, the present paper will focus on the users and the evolving sociocultural context, which in particular includes the legal context. Before discussing a particular subset of IT, which is to be used in the particular context of the health care system and especially telemedicine, some reflections appear to be necessary about the all-embracing categories of the theme of the workshop. How can ”IT users” and the ”sociocultural context” which in the following will be called ”society” [5], be made manageable? Although discussions circled for quite some time around ”THE” user, already one of the first contributions by Britt Ostlund [6] showed very clearly and convincingly that even a group like the elderly cannot be considered a uniform group of users. This argument can easily be extended to another group investigated at the workshop, the young people. Who is ”young” and behaving correspondingly often depends much more on lifestyle and professional status than on age. The sixteen year old working in a traditional job at a car repair shop may be ”old” already, while a nearly thirty year old doctoral student may still be very ”young”.

Who then is the “user”? A look at IT itself and at society as a social system may help to clarify this issue. Of course we talk, for example, about a computer and its user. The computer consists of hardware and different kinds of software like operating system and applications. All of them are linked to the user by a user interface, consisting itself of hardware and software components, e.g. mouse, keyboard, and graphical user interface presenting information on the screen. Ideally, hardware and operating system should be “transparent”, i.e. the user should not be obliged to care about it. All of this should be mediated by the user interface just like the applications. This means that it should be

possible to talk about “THE” user at the level of the user interface, which in fact concerns everybody using the same IT device in more or less the same manner. But even here uniformity has to be questioned as soon as we talk about different cultural contexts where symbols, icons, and even colors may have different meanings. Taking into account applications, however, we might suspect that each user does not only use different sets of applications but also uses them in different ways from other users and for different purposes.

This is where society comes in and where the question arises, whether producers have solutions for which they are searching problems in order to sell, or whether users have problems for which they seek solutions. Marketing [7] takes the latter approach and investigates the needs and problems of potential clients in order to be able to offer them appropriate solutions. A particular difficulty of IT in this respect is the knowledge gap between user and producers. This frequently prevents the producer from recognizing the real problems of the user and the user to recognize the real value and potential of an IT solution to resolve his problems. Without knowing how IT works and what it can do, a user cannot assess and appreciate how IT could help indeed. Only a close communication and cooperation between producers and users, already in the phase of prototype development, along with serious market research promises to be able to reduce this gap.

Neither with the fiction of THE uniform user nor with the realism of all users of the world being individually different user research and market research can get very far. Rather an appropriate reduction of complexity and an appropriate avoidance of oversimplification has to be found somewhere in between these two extremes. Social systems theory, in particular its problem-functionalist variant as originally proposed by Luhmann [8], can provide a tool for this. Society, in itself a mechanism [9] contributing to resolve the problem of human existence and survival, is composed of a combination of functional and segmentary subsystems at different levels. All of these entail their own specific subsequent problems and respective solutions. Depending on the particular society to be investigated, e.g. Sweden or Germany, but also depending on the degree to which an encompassing and systematic approach is aspired and to which empirical and practically relevant results are required, an appropriate level of abstraction and aggregation for conceptualizing the issue has to be chosen. Such an approach has been developed for the evaluation and technology assessment of IT systems, in particular smart card systems in the health care sector, in the framework of the EUROCARDS Concerted Action for Extending the Use of Patient Data Cards of the European Union [10]. With regard to the present issue such a procedure should permit in a first step to identify a range of relevant social, i.e. national, regional, local or also sector-specific, group-specific, or organization-specific problems. In a second step it should permit to assess whether IT is likely to be able to provide good solutions or not.

Users in Health Care and Telemedicine

The multidimensional evaluation structure for IT systems, as proposed in the EU study mentioned, distinguishes three dimensions: levels, aspects, and goals [11]. The present contribution positions itself primarily at the organizational and international levels. In the dimension of aspects it focusses on IT use in health care and its sociocultural environment. In •terms of goals it is dealing mainly with informational needs and the corresponding safety and security needs including data protection.

Data protection refers to the rights of persons, while data security refers to the security of the data and data processing systems themselves. Both are closely interrelated, but nevertheless need to be clearly distinguished. Data protection concerns only person-related data while data security concerns all kinds of data. The concept of data security, however, is usually limited to data in IT systems, while data protection includes the entire paper sector of conventional bureaucracy and paper archives.

The health care system is a functional subsystem of society in which organizations like hospitals and doctor's offices provide health care to the population. Providing health care is an information intensive process, both in terms of the information required about the particular patient and in terms of the medical knowledge and expertise required by the physician or other medical personnel. Furthermore, the contemporary medical system is characterized by a high degree of specialization and use of highly sophisticated medical technology. This requires teamwork and close communication between the many actors involved in the process.

In this situation IT, or more precisely medical informatics, can provide extremely valuable support to virtually any aspect of the medical, administrative or also educational process in the health care system as is easily shown by a look at the tables of contents of the proceedings of the world congresses on medical informatics organized by the International Medical Informatics Association (IMIA) [12] or also of the European Congresses of Medical Informatics organized by EFMI, the European Federation of Medical Informatics [13].

In such a context telemedicine is a technological procedure by which scarce medical expertise can be make available independently of time and space. This also internationally, in which case the sociocultural and legal context as well as the implementation of an appropriate technological infrastructure constitute quite exigent challenges and pose particularly difficult problems.

Although patients could be direct users of telemedicine, which will be defined more precisely below, as a matter of fact and for a number of reasons to be discussed in the following normally the users of telemedicine are different kinds of health care professionals who work in an organizational context which may be a hospital, a doctor's office or also a small health post.

The Concept of Telemedicine

Telemedicine can be defined in different ways and is sometimes even used synonymously with the rather vague notion of telematics. In the present context a narrow and strict definition appears to be useful, as this allows to delimit rather clearly the challenges and problems in the field of security and data protection which are crucial for success and failure of telemedicine.

As the word says already, one part is medicine referring to the treatment of patients. This includes the classical steps of diagnosis, therapy, monitoring, and rehabilitation. From this it follows that telemedicine as a kind of patient treatment at distance has to do with person-related data. Hence telemedicine systems have to comply with data protection regulations and need to be high security systems. Apart from this they have to comply with medical law and related laws concerning the health care sector. In some cases this body of legal regulations has special provisions to be observed in case of patient treatment at distance.

The other part of the word telemedicine refers to telecommunications or more broadly to information technology (IT) as a means and medium for patient treatment at distance. This implies that also IT regulations are essential for the development, implementation, and use of telemedicine systems. Moreover, such systems require an appropriate technical infrastructure connecting the health care organizations which are cooperating. If necessary this has to be across national boundaries and worldwide from continent to contintent.

With this definition focussing on patient treatment, distance teaching and the collection or transfer of professional knowledge independently from the case of a particular patient do not fall under telemedicine. Methodologically this is correct, because in these cases data protection is not relevant as no person-related data needs to be processed and communicated. Medical resp. health care legislation is relevant at most partially, because patients are not involved. Also excluded are administrative or management applications, which may or may not be person-related, but which at any rate are not different from corresponding applications in any other business sector. For these reasons the narrow definition oftelemedicine as proposed here promises to be more useful than a broad definition in order to work out the specificities of this kind of IT use and its consequences for the users.

In spite of this narrow definition telemedicine is neither a technically homogeneous field nor homogeneous with regard to the different types of applications which are possible. Levels of technical complexity range from simple use of telephone systems permitting synchronous voice communication between health professionals at distance, the use of e-mail as an asynchronous means of exchanging texts, and file transfer permitting the exchange of medical images to much more complex levels of teleconferencing and interactive pointing systems, e.g. to discuss radiological images, and to a fully interactive

mode of remote procedure control (RPC), which at the high end of complexity even permits distant surgery.

The use of telephone systems for telemedicine by means of voice communication is undoubtedly the oldest one. It has been used to take care of sick persons aboard ships but it has been in use also in countries like Greece with its widespread islands, where otherwise a good coverage with medical expertise is difficult [14]. The following discussion, however, will focus on digital, computer-supported systems. Voice communication by analogous telephone is easy and does not imply many problems, at least as long as voice communication cannot be stored in the system. At the very moment that voice communication goes digital, e.g. using voice mail boxes, the legal and sociocultural implications and problems become very much the same like those of e-mail.

Empty Promises of Producers

In the health care sector, just like anywhere else in the professional or private sphere, IT users are caught with empty promises. This often works because the respective users or potential users do not have sufficient expertise in order to be able to realistically assess the systems they are supposed to buy. There are several major empty promises of this type.

Interfaces are Intuitively Understandable

There are at least three reasons why this cannot be true. For one thing, the symbols and icons being used are by no means all clear to the novice. Moreover, as has been mentioned already, many symbols tend to be culture specific. Also there is a priori no “intuitive” reason why certain effects should result from a mouseclick, other ones from a doubleclick and still other ones from clicking the right or, if available, the middle button of a mouse. A second reason is that even if the symbol is clear, a certain understanding of the underlying technical processes is indispensable in order to guess that clicking on something which looks like a black line in a rectangular field in fact activates the diskette drive A: and permits to read files from there etc. Finally, symbols and functions keep multiplying. Even for an experienced user it is often a matter of spending a long time simply to find out where the well-known function required at this moment is hidden.

It is not doubt that graphical interfaces of the windows type facilitate the use of computers. However, rather than on “intuitive understanding” this is based on the degree of de facto standardization achieved meanwhile, last not least by the global spread of Microsoft products. This permits to utilize the results of previous experience (and hours of vain trials and errors) to some extent also with new systems. Standardization and past trial

and error indeed often facilitate familiarization with new systems or up-grades, again on a basis of trial and error.

Systems are Self-explanatory

This assertion is evidently linked to the previous one, which has already been refuted. Without any doubt, systems can be made userfriendly, although many are not. But this does not mean that the user does not need a basic understanding both of the technical processes going on and of the work which should be done by means of the computer system, i.e. the applications. The latter also implies the seemingly trivial practical knowledge of what key to hit in order to finish a program.

In former times many applications were not documented at all or there were more or less voluminous manuals. Only in rare cases such manuals were produced in a didactical and userfriendly way. Nowadays software providers prefer online-help and CD-ROMs which are much more practical and economical for them. Whether this solution is more practical for the users is highly questionable. Online-help seems rarely better than previous paper manuals. It tends to provide either evident answers one does not need or tends to be silent about the problems the user wants in fact to resolve (“Severe software error - in case of repetition contact the producer” - of course this error appears again once in a while!).

The only way to avoid a tremendous waste of time due to such trial and error by non-expert users is to provide an appropriate training, in a large organization like a university hospital this should be ideally in-house [15], in combination with a really available hotline service for more complicated problems. In this case, however, the real costs of computer use caused by working time spent on making inefficient systems go becomes much more visible.

We provide SOLUTIONS

The image of the turn-key system which resolves all your business problems once it is installed (nearly by itself), is well-cultivated by the software industry. And yet, even standard software coming installed on a computer is rarely an immediate solution. It has to be hooked up to the local network or the Internet, the personal or organizational formats, letterheads etc. have to be customized, etc., etc. In case of large systems the implementation tends to create many more and much more serious problems. The needs for user (and operator) training have been mentioned already. Larger software systems have to be integrated into the available or also newly purchased hardware environment, network, and software environment. At all of these levels problems of compatibility, interfaces, and

interoperability have to be resolved.

Furthermore, the workflow and workprocess of the respective organization has to be changed and adapted to the new possibilities offered by a new IT system. In its turn, the system itself has usually to be developed further and to be adapted to the specific requirements of each particular organization in a more or less prolonged phase of routine testing during real use and operation of the system. This entire process of adaptation is complicated by the fact that in detail no organization, no hospital is precisely like any other one and that often the companies producing the “solutions” are very far away from the real life and the everyday problems they promise to solve.

This means that the implementation of an “IT solution” implies, at least during a first phase, a new and not negligeable set of IT and organizational problems. It implies a major challenge to the respective organization or also invidual, like a single physician in his office or a doctoral student deciding to use from now on the new “IT solution”. Only during a second phase, if technical and organizational integration have been successful, real and often very massive profit in terms of savings of time, savings of money or substantially increased efficiency and effectiveness can be expected.

Traps for the Users

Apart from falling victim to empty promises of the IT industry, at least four more traps are awaiting the private or professional innocent who is supposed to invest into IT systems.

The Gadget Trap

This trap is closely related to the issue discussed previously, i.e. IT solutions looking for problems. Producers, not knowing what are the real needs of potential customers, try to convince them by means of 500 melodies which can be downloaded into a mobile phone instead of the usual standard sound indicating a call is arriving, by making video recorders or cameras so multifunctional, that the original function nearly gets unusable, or by adding another 90 functions to a new software system of which the secretary who uses it to write five-line letters has only used 20 percent before and will never use the 90 new ones. The effect of such innovation will be, however, that the old harddisk gets too small, the processor too slow, and the new kind of icons will require a more advanced high resolution screen. The job to be done with this fabulous new system, however, will remain the same [16]. Even in the case of real expert users the next more powerful up-date or version may already be waiting for installation, before it was possible to explore and to put into practical use all the new advantages of the last version.

The only way out of this trap is sufficient own expertise. Such expertise is required at the professional level to know what one really needs and how the work and business process can be re-organized and improved effectively by means of IT. It is also required at the technical level to be able to assess realistically what technical solutions are required and what the proposals of the producers really mean and offer. Talking about users of telemedicine, it is evident that such conditions can be met only by rather large health care organizations which are capable of maintaining themselves a sufficient staff of competent IT experts working closely together with the medical and administrative personnel who is to use a system. In Germany, e.g., most university hospitals have an institute of medical informatics which can take over such a role.

The Resource Trap

IT permits to rationalize and economize very substantially if used properly. This, however, must not lead to the delusion that no substantial initial investments are necessary for hardware and software as well as for training, as has been argued above already. Furthermore, any organization which makes itself dependent on IT, and this happens very, very rapidly, cannot afford to go without an adequate maintenance scheme. This is especially important in a hospital where the life of patients may depend on the 24h availability of an IT system. Maintenance schemes, licences to be paid, hardware and software up-grades easily sum up to very substantial amounts of money. Moreover, sufficient well-trained personnel is necessary for the operation and the user and system administration. If a system cannot be handled properly for lack of personnel, it will not unfold its full potential for the business process and resulting lack of user acceptence may even lead to a loss of the initial investment in hardware, software, and training. Running an IT system is a wonderful solution to many problems, but it is not for free.

The Security Trap

Another trap, from which to escape is also not for free, often becomes evident only after the event. For a private person it may be nasty if the contents of the harddisk was eaten up by a virus or if an intelligent e-mail system has helped to spread all address lists, along with that virus, worldwide without the poor user even knowing it. For a business organization, however, it may be a tragedy if strategic plans, internal budgets or bids being prepared are simply copied over the network by a competitor without leaving a trace.

In still other cases, where person-related data are processed like in hospitals, insecure IT systems mean also violation of laws which may be sanctioned by fines, by shutting down

the system, and usually bad publicity which may cause even more damage to the organization than the direct sanctions.

At the practical level data security, or rather IT security, and data protection as required by law are so closely intertwined that neither the private user nor the business organization which happens not to process person-related data can do without appropriate security. This simply out of the very own interest of not suffering damage and possibly loosing a lot of money.

IT security and close adherence to data protection and IT laws is nevertheless not common everywhere. Reasons for this seem to be that::

- neither users nor producers are sufficiently informed about legal requirements, risks and dangers, and the possible technical solutions;

- IT security is complicated and requires a high level of technical, organizational, and legal competence;

- IT security is expensive to implement for the producer;

- IT security is expensive to implement for the user in terms of equipment, training, labour, time, and money;

- IT security remains invisible as long as it works and insecurity remains invisible as long as nothing happens.

The Complexity Trap

The previous considerations about the security trap already indicated the problem of complexity. It starts with the megabyte and gigabyte of software to be found on a single PC which cannot be really checked and controlled for errors anymore, much less the combinatorial and unforeseeable interplay of a multitude of different programs. In a large organization like a hospital this complexity is exponentially increased by the need to integrate numerous hardware platforms with different operating systems into networks in which several thousand users may cooperate routinely. How such a system will perform cannot be predicted anymore. It can only be tested and because of the combinatorial possibilities it can be tested only very incompletely.

To manage something like this successfully requires, again, the availability of a sufficient staff with sufficient expertise. Moreover, it is not possible without a close cooperation with the producer of such a system and even among several producers themselves. A large hospital like a university hospital is unlikely to have just one system, as different

specialties usually have departmental systems from different producers. These have to be integrated into an overall hospital network and they have to be interoperable with central systems as well as other departmental systems.

To what extent this may work or not work can hardly be judged in advance. It has to be tested in routine tests involving the users and accompanying the further development of the respective systems.

The Global Evolution of the IT Environment

A hospital implementing a Hospital Information System (HIS) is a potential victim of such traps and empty promises. Expanding medical services and supporting IT systems beyond the boundaries of the hospital by means oftelemedicine, however, implies confrontation with still more complexity, both at the level of IT infrastructure and the level of the sociocultural environment.

The scene has been set for present day IT systems and their use, and in particular for exigent and sophisticated applications like telemedicine, by several global lines of development. These are to be found in hardware, networks, transmission technology, international standardization, but also in cryptology.

Hardware

The development of hardware, including storage technologies, involves two complementary directions, which are both highly relevant for telemedicine. These are miniaturization and increase of capacity.

The increase of capacity has led to “main frame” computers with tremendous storage and processing capacities, so that neither speed nor storage is a technical problem anymore [17]. It is simply a question of money to be invested. This is an essential pre-condition for the operation of worldwide networks storing and moving around apparently unlimited quantities of information, last not least voluminous image data. The latter is a main concern of telemedicine for which the sharing of medical image data is of major importance.

However, miniaturization has also led to smaller computers, notebooks, palm tops, and “Personal Assistants”, which permit the user to dispose of computing capacity as well as a certain amount of storage capacity not only at the workplace, but to carry it along anywhere. Even more, in combination with network technology such devices have become portable access to worldwide digital resources from a multitude of potential docking stations.

A further crucial step has been the development of chipcards, in particular the so-called smart cards. The latter do not only contain a memory chip but also a processor. With this they can be used as tiny computers. If equipped with crypto-chips they can serve as portable and secure devices for cryptography. They are secure because secret keys can be stored and used inside without possibility of external access to such a secret. In this way smart cards (or rather crypto-cards) can serve as personal, portable, and secure electronic access and encryption devices. This becomes of particular relevance if networks are used to connect all the different kinds of computers which have evolved until now.

Networks

Also networks have expanded, so to speak, in two directions. On the one side the so-called Wide Area Networks (WANs) have grown and grown together to form a worldwide net, a large part of which is known as “Internet”. However, networks have also expanded towards the “inside”. In most large organizations the workplace computers are somehow connected to a Local Area Network (LAN), which usually is, in some way or another, connected in turn with larger, sometimes also worldwide, corporate networks, inter-corporate business networks or the Internet itself. Moreover, this is not only true for workplace computers, but households and private citizens are also equiped with PCs, Notebooks, etc. which are more often than not connected or connectable to the Internet.

ISDN

Connecting a large number of computers and moving around large amounts of data requires both sufficient computing capacity, which has been discussed under the heading of hardware, and adequate transmission channels. The latter can be provided meanwhile by a combination of several technologies including fiberoptic and satellite technology. Nevertheless, it is highly uneconomical to use separate worldwide networks for different services. In this respect the development of ISDN (Integrated Services Digital Network) has been a tremendous move ahead and an important condition for the development and expansion of cyberspace and information society. ISDN means that data from different media are digitalized and hence can be transported by the same (digital) networks and processed by the same digital machines, usually computers. Multimedia services signify the combination of voice (telephone and radio) with images (TV and movies) and the traditional computer data. Only with ISDN it has become possible to enter information from different media into the same information network and for the user to get everything from the same source if desired, i.e. from his multimedia computer.

Standardization

ISDN as a means of data transmission, however, is not enough to make all the different computers, operating systems, and applications “talk” to each other and “understand” each other. This requires in addition either a same language or at least adequate possibilities of translation.

For this, two sources have developed. On the one hand, official international standardization agencies like ISO (International Standardization Organization) at the worldwide level or CEN (Comite Europeen de Normalisation) at the European level have made considerable progress, developing e.g. the European Article Numbering code (EAN) [18], which is nowadays in use as a bar code even in small supermarkets, or also the EDI format (Electronic Data Interchange). EDI can be used for a considerable number of purposes in electronic business and health care, where it is called EMEDI [19].

On the other hand, a number of initiatives has been taken also by groups of users and/or producers, resulting e.g. in quasi-standards based on technical considerations and a more of less broad agreement. Such a quasi standard for network communications which has turned out to be extremely important is TCP/IP, the standard Internet protocol [20]. Another one is PCMCIA [21] for card sockets in computers and other electronic devices. Still another type of “standard” simply results from the market power of individual producers like Microsoft.

Cryptology

If standards of different kinds permit computers all over the world to “talk” to each other and users to communicate with each other, several question remain like: To whom am I talking? Is the message I receive really from that person? Did that person indeed receive my own message? Did these messages arrive unchanged? Can all the world read or listen to what we have to tell each other?

All of a sudden cryptology, which was of interest mainly to secret services or the military a few decades ago, becomes a concern of the normal citizen. It has been mentioned already that inside a smart card secret cryptographic keys can be carried around without risk of disclosure. Smart cards as powerful tools for cryptography, however, could not unfold their real potential without a crucial development in cryptology itself, the development of so-called asymmetric algorithms. Traditional symmetric algorithms required both parties in a communication to have the same keys, for encryption and for decryption. The big problem in this is key exchange, as both keys have to be kept absolutely secret. Asymmetric algorithms, on the contrary, work with different keys for encryption and decryption. This permits to publish one of the keys, e.g. the one for encryption, like in a telephone book. This is why the use of asymmetric algorithms is also called “Public Key Cryptography”. In

this case anybody can encrypt a message with the published key, but only the correct receiver can decrypt it with his private, secret key and read it. If the procedure is reversed, we obtain the electronic signature. In this case only the sender can encrypt his signature, but anybody can decrypt it by use of the published key, thus checking the true origin of the signature.

Public key cryptography in combination with smart cards as carriers of secret keys and appropriate cryptographic algorithms makes encryption and electronic signatures a practical tool for any citizen. A signature card, or also a so-called Health Professional Card like a physician's or pharmacist's ID-card, can be carried around like a ballpoint pen both for signing electronic documents and for identification.

Nonetheless, these technical developments are necessary but not yet sufficient conditions for the worldwide use and applicability of such devices. The technical infrastructure has to be complemented by a legal and organizational infrastructure.

Global Structure and Dynamics of Legislation

With regard to a legal infrastructure, important developments in legislation on data protection and security have taken place over the past decades. Although the Charter of Human Rights of the United Nations was passed well before the age of computers and information society, a general worlwide legal basis for data protection and data security can be found in the human right for privacy [22].

In classical juridical fashion this can be and has been concretized in regional legislation, e.g. the European Directive on Data Protection, and national legislation. In Germany, e.g., the Federal Data Protection Law was in fact much earlier than the European Directive providing a model for the latter.

In a federal state like Germany the legal hierarchy, paralleled by corresponding institutions for data protection, goes farther down to the State level, where e.g. in the case of Marburg University Hospital the Hessian Data Protection Law is applicable. The Hessian State Data Protection Commissioner is the supervising authority in this case.

The Hessian State law, which is adapted to the European Directive, requires organizations like hospitals to have their own internal Hospital Data Protection Officer, responsible for the implementation of the relevant legal regulations, their observation by staff and management, and the protection of the rights of those concerned [23]. In case of a University Hospital these are the patients, the staff, and the students.

As legal regulations are often not directly applicable to the concrete conditions in an organization, Marburg University Hospital, e.g., has developed its own internal Data Protection and Security Regulation, based on the pertinent legal regulations [24].

Global Effects

The previous considerations about the overall legal and institutional framework for data protection and data security show that there is indeed a common basis for worldwide action. Yet there is also a lot of diversity in the regional and national implementations.

Several developments seem to produce gradually more coherence in this area and promise to

create the necessary harmonization also at the practical, technical level.

In 1983 the German Constitutional Court ruled “Informational Self-Determination”, which is considered the root of all data protection in Germany, to be a constitutional right.

In 1995 the European Union put into effect the European Directive on Data Protection [25], which is strongly inspired by the then valid German Federal Data Protection Law. The European Directive obliges all member states to implement its provisions in national law by 1997. Although this has still not yet happened in all member countries, the Directive constitutes a basis for practical action and has practical consequences.

In 1996 the Health Insurance Portability and Accountability Act (HIPAA) was passed in the United States, This is not yet a national data protection law comparable to the European Directive. However, for a large part of the US health care sector HIPAA moves data protection and data security much closer to the European conditions.

In Japan data protection legislation has not yet moved very far. However, Japanese IT producers want to be in business worldwide. They make considerable efforts to be involved in relevant standardization and to ensure interoperability of their respective products. This is true, last not least, for the smart card sector and electronic signatures.

In the year 2000, finally, the European Directive on Electronic Signatures became effective in the European Union, thus establishing the full legal equivalence of properly signed electronic documents with traditional paper documents.

Although Europe is evidently taking the lead in legal and institutional development so far, the US and Japan are clearly in the boat. Other IT producers will have to adapt and to follow this lead.

Whoever wants to sell systems or components in Europe will have to comply with European data protection and security regulations. Whoever wants to receive person-related services from Europe, be it in banking or in telemedicine, has to comply with its regulations. Person- related data may be transferred to places outside the EU only if a comparable level of data protection and security is provided there. Furthermore, as has been indicated, efforts are under way to create a worldwide infrastructure for smart cards as electronic signature cards to be used in the long run very much like present-day credit

cards. This not only in the health care sector. Smart cards are already now a tremendous business. A uniform ISO standard exists, and for electronic signatures a European standard exists too. Furthermore, a new encryption standard is about to be implemented, replacing the previous, more or less problematic, encryption algorithms.

All of this provides a realistic perspective for a worldwide security infrastructure in which key roles will be played by smart cards as ID and signature cards and by public key cryptography, both for electronic signatures and for ensuring confidentiality.

Advances in International Cryptography - A Key Area

As has been argued before, computers need to ”understand” each other. This is also true in the case of cryptography. It means that the same algorithms have to be available and are being used by all participants in worldwide secure communications. To be universally available such an algorithm should ideally be public domain, free of charge, and not bound to licence agreements.

Technically an algorithm is good if it is published, as all the security should depend on the keys only, not on the algorithm itself. Publication is a pre-condition for an algorithm to be well-analyzed. This is indispensable to make sure that there are no unexpected problems and loop-holes. Another important aspect is of course processing speed.

The most widespread algorithms used so far have all deficiencies in one respect or another. The Triple DES is free of charge but slow. Also it is of US origin, which nourishes the fear, it might have unknown trapdoors accessible to US authorities. The latter is also true for RSA, which, moreover, was patent protected until the year 2000. Thus the legal conditions of its use across international borders were not very clear for quite a while. Another widespread algorithm, which is fast and of Swiss origin, is IDEA. Yet IDEA is licence-protected for non- private use.

In October 2000, after a lengthy period of selection and testing the National Institute of Standards and Technology (NIST) of the United States selected a new symmetric algorithm as “Advanced Encryption Standard” (AES) for the US [26]. This is the Rijndael algorithm. Being of Belgian origin it does not raise suspicions with regard to access by US authorities. Furthermore it is fast, available free of charge and it requires little storage and memory space. It can be considered a highly secure and efficient tool for encryption. Under these conditions the new AES has much promise for a much wider use and application than in the US only.

A Dozen Problems of Telemedicine

So far the argument has been that a whole series of technical, legal, and organizational developments is currently converging. These developments promise not only to create a worldwide IT infrastructure, but above all a secure infrastructure which is still manageable. It should have become clear also, however, that this convergence implies the coming together of a multitude of different aspects which are not only needed, but which are needed to work together coherently, consistently, and in close interaction.

This seems to be a key problem for telemedicine, which constitutes a highly exigent IT application at a very practical day-to-day level. Although innumerable pilot projects have been sponsored meanwhile, e.g. in the framework of the different EU-programs, daily routine use is not yet very widespread, to say the least. This, of course, is not true for the more traditional non-computer applications being based on simple telephone communications etc.

The diversity of aspects involved leads to at least a dozen of more or less practical problems which still need to be resolved, if high-tech telemedicine is to become a widespread application.

1) No chicken and no egg: An important aspect in Germany, but not only there, is the mutual waiting on each other of health care providers, IT producers, and in a way legislation. IT producers still tend to say the market is not there and legislation is not clear, so we don't develop and offer security technology or systems really meeting the EU data protection requirements. On the other side health care providers cannot really go ahead for lack of adequate technology for routine use, and legislators in some cases still argue that technical development and especially standardization is not yet sufficiently advanced to justify legislative action. However, as has been argued above, legislation seems not really to be the big block to progress but rather at the cutting edge at least in the European Union. Also E-Economy, E-Commerce, and EDI, while technically feasible, do not really seem to be adopted by the market at large.

2) The one-to-many relationship: Security is certainly a critical issue. Like in E-Commerce, security in telemedicine in an open environment ("the market") has to include all potential participants, e.g. all doctor's offices, all patients etc. For a health care provider this is a one-to-many relationship involving potentially very many unknown partners. A security infrastructure for such a situation has been outlined in the present paper. It is considered feasible, however, it is not yet a reality. Reality still is that secure communication complying with data protection requirements is only possible with known

and defined partners who have a corresponding piece of software and/or crypto-technology. For a health care provider such a solution is feasible and economical only with a limited number of partners with whom there is regular and frequent cooperation.

3) Security infrastructure: The framework for a largescale, even worldwide security infrastructure including Trusted Third Parties (TTP) exists, but the infrastructure and TTPs themselves are emerging only gradually and are not yet available for largescale routine use.

4) Technical incompatibilities: In spite of progress in standardization technical incompatibilities still persist. This is no wonder, if we look at the multitude of hardware devices, operating systems, network protocols, application systems, databases, data formats, etc. which have to work together.

5) Technical incompetence of IT producers: The lack of interoperability of the different devices and systems is to a considerable extent due to the IT producers themselves. Be it because IT producers do not want to leave their trodden paths to comply with standards, be it because they they do not see the strategic importance of openness and interoperability for their own products, be it because they are not willing to invest money in necessary modifications of their systems, or be it simply because they implement standards their own way, so that their systems still do not fit with others.

6) Transborder telemedicine: Telemedicine is often seen as a good way to provide services beyond the borders of the own country or, in reverse, to obtain scarce and valuable expertise from abroad. In both cases the question has to be answered: Who pays for the services? After the end of a pilot project financed by some sponsor this question often has to remain open. A particular role in aggravating this problem play the basic differences in health care systems and in their financing schemes (see also *problem*).

7) Wassenaar Agreement on Dual Use Products: Dual use products are products which can be used both for civilian and military purposes. Evidently IT equipment, and in particular crypto-products, belong to this category. International agreements like the Wassenaar Agreement [27] often create difficulties in exporting or importing such products.

8) Use of cryptography - national differences: Along the same lines different national

policies impede a free exchange of IT and crypto-products or even their use in the respective country itself.

9) Legality of distant diagnosis and treatment: Like national peculiarities of IT and crypto-legislation national health legislation can impede telemedicine. In Germany, e.g., both distant diagnosis and distant treatment are illegal.

10) Non-harmonized legal systems: Legal conditions differ considerably among countries far beyond the use of cryptography and the admissibility of distant diagnosis and treatment, two issues of particular relevance to telemedicine. Such other differences concern liabilities of health care providers, liabilities of IT producers and providers, but also issues like publicity in the health care sector, cross-border acceptance of social and health insurance schemes, regulations of e-commerce and the legal status of electronic documents. The latter may remain problematic even at the European level, as the European Directive distinguishes several levels of electronic signatures. Only the most sophisticated one, the ..qualified digital signature", provides, e.g. in Germany, full equivalence to a paper document. [28]

11) Unequeal health care systems: Even among European countries the health care systems themselves differ widely, apart from the purely legal aspects. Large scale high-tech telemedicine, not limited to point-to -point interactions with well-known partners, has to rely on establishing working relationships via electronic means, e.g. health professional cards as ID cards. Professional identity, competence, rights and obligations have to be established and documented this way. And yet it is by no means very clear, e.g., who is a physician in different countries? Who is a nurse? What may a physician do? What are the rights and competences of a nurse? Who qualifies as a specialist in radiology? Many more questions and equivalences of this type not clear. Yet clarity would be required for a large scale crossborder telemedicine and the avoidance of conflicts both with patients and their social and health care insurers.

12) Medical networks - security gaps and unclear liabilities: So-called Medical Networks also suffer from all of these problems, once they are to be established internationally. Nationally, conditions are correspondingly varied. In Germany, e.g., there is a strong political pressure to establish Medical Networks in the hope to improve the quality and cost efficiency of health care. In addition to the problems of telemedicine already outlined, medical networks encounter still other particular difficulties. A general security and

electronic signature infrastructure as well as a nationwide health professional card system being underway but not yet operational. Medical Networks aiming at an n-to-n relationship usually encounter a security gap. Security can be guaranteed, once you are in the network. How to get there is another problem. Moreover, the legal status is not clear. Medical data is highly protected by law, as long as it is kept by the physician treating a patient. A database operated by an IT provider, however, does not enjoy such protection. Access rights to medical data depend on the context of treatment. Only a physician actually treating a patient, which in the normal case implies the patient's consent, is entitled to look at and to process the patient's medical data. Already in a large Hospital Information System (HIS) it is often difficult to establish the context of treatment, once different departments and functional units are involved in a patient's treatment. An adequate solution in a HIS can only be implemented by means of an order- entry-system. Order-entry in a medical network with the corresponding (central) administration of user rights etc. does not seem very realistic. A decentral solution, on the other hand, would require each participant to be both online and well-protected against abuse, misuse, and all the security threats which may come out of a network. This may be possible for large hospitals with adequate IT resources and a sufficient and competent IT staff, it is, however, utterly unrealistic for the doctor's office, which after all is the main target in German aspirations at Medical Networks.

Towards Solutions

Telemedicine, it was argued in this paper, is a challenging, complex, and promising IT application. In a complex and difficult environment it encounters a lot of highly diverse problems, and although several major developments in different fields move towards convergence and seem to bring solutions within reach for a considerable part of the problems analyzed.

Sure, there cannot be simple solutions to complex problems and easy recipes to make telemedicine and other IT applications a rapid success. Nevertheless, it seems to be possible to state at a meta-level a number of principles as valid and useful guidelines. They find their justification to some extent in the material presented in this paper and to some extent in the practical experience of IT development the author has been involved in over the years in European projects [29], in Central Asia [30], and last not least at Marburg University Hospital [31].

Such principles to be observed are:

Keep it simple!

The user wants to get his job done. Provide simple tools and solutions which do not require the technologist's patience and fascination to work. Perfection is not a maximum of functions which will never be used, but the multitude of necessary functions which are performed although the user never realizes.

Be problem-oriented!

Carefully and clearly analyze the problem to be resolved before proposing solutions. Also the user may not really know what is his problem, as long as he has not sufficient information about what technology can do for him. But once the problem is clearly specified, provide a simple solution and resist any temptation to create a general problem solver.

Take a REAL marketing approach!

Marketing is not to develop what a producer thinks to be useful for the clients. Marketing is the empirical study of the clients' real needs and the consequent development of products meeting these needs. In IT more often than not real marketing studies are replaced by wishful or prophetic thinking.

Think in systems!

The multitude of aspects involved in the successful operation and use of IT systems and their intricate, often circular, relationships and feedbacks have become evident in the present paper. Without thinking in systems, something like this is not manageable. Technologists and informaticians naturally tend to think in systems, but often only in technological systems. Successful largescale IT development, implementation, and operation, on the contrary, requires the full range from physics to technology, social systems, cultural systems (including law), and even ethics and philosophy.

Work interdisciplinarily!

Systems thinking can be put to work and transformed into practical use only by interdisciplinary teams. Interdisciplinarity does not mean to put the analysis of the medical doctor into the same folder (or book) as the analysis of the computer scientist. It means that the computer scientist writes his analysis taking into account what the medical doctor has to tell and vice-versa. Only in this way a new quality emerges in the product, something which neither the medical doctor nor the computer scientist can produce in isolation on his

own. Interdisciplinary work of this latter kind, after all, was what made the Norberg workshop an inspiring meeting!

Annotations

1) ASHBY, W. Ross: Einfuhrung in die Kybernetik, Suhrkamp Verlag, Frankfurt/Main 1974.
2) Cf. e.g. WICKEN, Jeffrey S.: Evolution, Thermodynamics, and Information, Extending the Darwinian Program, Oxford University Press, Oxford, New York 1987; DARWIN, Charles: Die Entstehung der Arten, durch naturliche Zuchtwahl, Philipp Reclamjun., Stuttgart 1967.
3) Cf. e.g. KUHN, Thomas S.: Die Struktur wissenschaftlicher Revolutionen, (Orig.: The Structure of Scientific Revolutions), Suhrkamp Verlag, Frankfurt/Main 1973.
4) Cf. e.g. EUHMANN, Niklas: Soziale Systeme, Grundriss einer allgemeinen Theorie, Suhrkamp Verlag, Frankfurt/Main 1987.
5) A detailed analysis of the interrelations and differences between the «social» and the «cultural» was presented elsewhere. HORNUNG, Bernd R.: Sociocultural Evolution, Towards the Merging of Material and Informational Evolution, in: ASSOCIATION INTERNATIONALE DE CYBERNETIQUE (AIC) (ed.): 14th International Congress on Cybernetics, Namur (Belgium), August 21st-25th 1995, Proceedings, pp. 867-872, Association Internationale de Cybernetique, Namur 1995.
6) OSTLUND, Britt: «Why Research about IT Users?» and «Elderly People as IT-Users - An Example of Categorization», Presentations at the Norberg Workshop.
7) Some examples for the classical marketing approach are: KOTLER, Philip; DUBOIS: Marketing Management, 4e edition, Publi-Union, Paris 1977; KOTLER, Philip;: Modeles de decision en marketing, Dunod 1982; LEVITT, Theodore: L' Esprit Marketing, (orig.: The Marketing Mode), Collection INSEAD-Management, Les editions d'organisation, Paris 1972; GREEN, Paul; TULL,B Donald: Research for Marketing Decisions, Prentice Hall, Englewood Cliffs N.J. 1970; BEREKOVEN, Ludwig: Internationales Marketing, Betriebswirtschaftlicher Verlag Th. Gabler, Wiesbaden 1978.
8) LUHMANN, Niklas: Funktion und Kausalitat, in: LUHMANN, Niklas: Soziologische Aufklarung 1, S. 9-30, Westdeutscher Verlag, Opladen 1974; LUHMANN, Niklas: Funktionale Methode und Systemtheorie, in: LUHMANN, Niklas: Soziologische Aufklarung 1, S. 31-53, Westdeutscher Verlag, Opladen, Wiesbaden 1974; a description of the problem-functionalist approach to the modelling of social systems is given in HORNUNG, Bernd R.; ADILOVA, Fatima T.: Conceptual Modelling for Technology Assessment of IT Systems, Smart Cards and Health Information Systems, in: Kybernetes, The International Journal of Systems and Cybernetics, vol. 26, no. 6/7, pp. 787-800, MCB University Press, Bradford UK 1997; a more detailed methodological description is to be found in HORNUNG, Bernd R.: Minimal Conceptual Modelling (MINCOMOD), From Theory of Society to IT-Systems in Hospitals, Paper presented at the 2nd International Conference on Sociocybernetics, Panticosa, Spain, June 25th - July 1st, 2000, to be published in the International Review of Sociology.
9) Here the term «mechanism» is used although social systems are clearly not «mechanic»! The reason is that «mechanism» refers to some real-world phenomenon composed of structures and processes, while the term «system» also refers to knowledge and theory, and after all includes systems of functions and systems of problems, i.e. the other dimensions to be distinguished here.
10) EUROCARDS Concerted Action, Working Group 6 (Convenors: COMEAU, Paul-Andree; HORNUNG, Bernd R.): Evaluation Methodology for Systems Applying Data Cards in Healthcare, Final Deliverable, Version July 1996, Commission of the European Community, DG XIII, Brussels 1996.
11) Ibid. p. 69.
12) E.g. GREENES, Robert A.; PETERSON, Hans E.; PROTTI, Denis J. (eds.): MEDINFO '95, Proceedings of the Eighth World Congress on Medical Informatics, Vancouver, British Columbia, Canada, 23-27 July 1995, 2 vols., IMIA, Healthcare Computing & Communications Canada Inc., Edmonton, Alberta, Canada 1996.
13) E.g. ADEASSNIG, Klaus-Peter; GRABNER, Georg; BENGTSSON, Stellan; HANSEN, Rolf (eds.): Medical Informatics Europe 1991, Proceedings, Vienna, Austria, August 19-22, 1991, Eecture Notes in Medical Informatics, vol. 45, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo 1991.
14) E.g. SOTIRIOU, Dimitrious: Telemedicine in Greece, Presentation at the NATO Advanced Networking Workshop «Telemedicine in Central Asia - Applications in Emergency Medicine», Tshkent, Uzbekistan, April 2-4, 2001.
15) At Marburg University Hospital a specialized teacher is doing training in standard software (text processing, spread sheets etc.) for the hospital personnel (not the students!) on a full time basis. Also in the

context of introducing a new hospital information system (HIS) at Marburg University Hospital an encompassing training program was implemented for the basic training of all medical personnel which would be using this system.
16) A very informative report on this kind of innovation was published on the occasion of the 2001 Hannover Fair CEBIT in DER SPIEGEE: Im digitalen Eabyrinth, Die weltgroBte Hightech-Messe Cebit prasentiert eine neue Generation vielseitiger Mobilgerate: Handys spielen Musik und verwalten Termine, Fotokameras zeichnen Videos auf. In Zukunft solljedes Gerat alles konnen. Doch fur den Benutzer wird die Handhabung immer komplizierter, in: DER SPIEGEL, 12/2001, pp. 116-206,2001.
17) Cf. e.g. STRASS, Hermann: Massenspeicher optimal einsetzen, Festplatten, Streamer, CD-ROM, WORM, Halbleiterspeicher, Franzis Verlag, Poing 1994.
18) EAN - International Article Numbering Association: EAN Applications in the Healthcare Sector, EAN - International Article Numbering Association, Brussels 1995. 19) EMEDI; CCG - Centrale flir Coorganisation GmbH: Elektronischer Datenaustausch im deutschen Gesundheitswesen, (Electronic Data Interchange in the German Health Care System), Ein Leitfaden fur Management, EMEDI, CCG, Paris, Koln, 1996.
20) Cf. e.g. GEASER, Gerhard M.; HEIN, Mathias, VOGE, Johannes: TCP/IP, Protokolle, Projektplanung, Realisierung, Datacom, Pulheim 1990.
21) STRASS, Hermann: PCMCIA optimal nutzen, Technische Grundlagen, Normen, Anwendungsmoglichkeiten, Franzis Verlag, Poing 1994.
22) SIEGHART, Paul: The Eawful Rights of Mankind, An Introduction to the International Eegal Code of Human Rights, Oxford University Press, Oxford, New York 1986.
23) § 5 of the Hessian Data Protection Eaw, DER HESSISCHE MINISTER DES INNERN UND FUR EANDWIRTSCHAFT, FORSTEN UND NATURSCHUTZ, Bokel: Hessisches Datenschutzgesetz (HDSG) in der Fassung vom 7. Januar 1999, Bekanntmachung der Neufassung des Hessischen Datenschutzgesetzes vom 7. Januar 1999, in: Gesetz- und Verordnungsblatt fur das Land Hessen, Teil I, Nr. 4, S. 98-111, 19. Februar 1999.
24) HORNUNG, Bernd et al.: Grundlagen und Organisation des Datenschutzes im Universitätsklinikum Marburg, Richtlinie, Version November 1999, Klinikum der Philipps-Universität, Marburg 1999.
25) EUROPEAN COUNCIL: Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement, European Council, Brussels, published in the Official Journal of the European Community, L281, pp. 3 Iff, becoming effective in October 1995.
26) The following is based on WELSCHENBACH, Michael: Advanced Encryption Standard, Design-Aspekte von Rijndael, in: STRUIF, Brui-io (Hrsg.): 11. GMD - Smart Card Workshop, Darmstadt, BB 6.-7. Februar 2001, Tagungsband, GMD - Gesellschaft fiir Mathematik und Datenverarbeitung mbH, Darmstadt 2001.
27) Cf RIENHOFF, Otto; LASKE, Caroline; VAN EECKE, Patrick; WENZLAFF, Paul; PICCOLO, Ursula: A Legal Framework for Security in European Health Care Telematics, Studies in Health Technology and Informatics, vol. 74, IOS Press, Amsterdam, Oxford, Tokyo, Washington DC 2000.
28) Cf BIESER, Wendelin: Novellierung des Signaturgesetzes und der Signaturverordnung auf der Grundlage der EG-Signaturrichtlinie, in: STRUIF, Bruno (Hrsg.): 11. GMD - Smart Card Workshop, Darmstadt, 6.-7. Februar 2001, Tagungsband, GMD - Gesellschaft fur Mathematik und Datenverarbeitung mbH, Darmstadt 2001
29) A summary of important results is given in PERNICE, Antonio; DOARE, Herve; RIENHOFF, Otto (eds.): Healthcare Card Systems, EUROCARDS Concerted Action, Results and Recommendations, Technology and Informatics, vol. 22, IOS Press, Amsterdam, Oxford, Tokyo, Washington DC 1995.
30) NATO Projects carried out with the generous support of NATO, Scientific and Environmental Affairs Division, Priority Area on Environment, Grant ENVIR.CRG 941 323 for the project «MEPSS - Planning Support for Integrated Development Projects in the Aral Basin»; and project CN.NIG 960 388 «IT Network Support for Integrated Health and Environmental Development in Uzbekistan». A short overview of different projects is given in HORNUNG, Bernd R.; ADILOVA, Fatima T.: Conceptual Modelling for Technology Assessment of IT Systems, Smart Cards and Health Information Systems, op. Cit.
31) Cf. KUHN, Klaus A.; LENZ, Richard; BLASER, Rainer: Building a Hospital Information System, Design Considerations Based on Results from a Europe-wide Vendor Selection Process, in: LORENZI, N.M.: Proceedings ofAMIA Symp., pp. 834-838, 1999; LENZ, Richard; BLASER, Rainer; KUHN, Klaus A.: Hospital Information Systems, Chances and Obstacles on the Way to Integration, in: Stud Health Technol Inform, vol. 68, pp. 25-30, 1999; LENZ, Richard; ELSTNER, Thomas; SIEGELE, Hannes; KUHN, Klaus A.: A Practicable Approach to Process Support in Health Information Systems, in: JMIA, forthcoming, 2001.