Medical Requirements for Data Protection

Klaus Pommerening[a]

[a]Institut für Medizinische Statistik und Dokumentation,
Johannes-Gutenberg-Universität, D-55101 Mainz, Germany

Medical data are among the most sensitive data of a person. They should be effectively protected. But there are more problems, political and technical, than successful solutions. There is a need for political and public discussion to reach a consensus on conflicting goals; a number of legal issues still need to be resolved. On the other hand there are promising and ready-to-use technical concepts that wait for application. Medical informaticians should make proposals for concrete measures and implement them.

Keyword Codes: K.4.1; K.4.2; K.6.5
Keywords: Public Policy Issues; Social Issues; Security and Protection

1. Data protection in health care

There is a worldwide accord, at least since the Hippocratic oath, that the special relationship between a patient and his physician is subject to confidentiality. Constitutional rights protect the professional discretion in the health sector and the informational self-determination – if these rights don't exist in certain countries they should be put into force right away. The confidentiality of medical data is an essential demand for each kind of data processing and information handling in medicine. New information and communication technologies improve the quality and effiency of health care. But they create new problems. "Data protection, confidentiality and computer security are basic requirements for the appropriate introduction and use of information and communication technologies in health care."[1, p. 1]. Two basic requirements for handling medical data are *safety for the patient* and *protection of medical data.* The first requirement means that automation of diagnostic and therapeutic procedures should do no harm to the patient; this relates to trustworthiness and reliability of systems and to software quality control. The second requirement is the subject of this talk.

The problems with data protection are of a political, legal, administrative, or technical nature. The basic political and legal problem is to control the balance between conflicting goals, e.g. privacy of medical data versus efficiency of health care. The basic administrative problems are the definition of responsibilities, procedures and access rights, and the appropriate allocation of human and economic resources. The basic technical challenge is the openness of modern data processing and communication systems. This means, besides several useful aspects, that whatever data these systems process, they don't protect them in any way. They store data on disks and transfer them via nets where the data are exposed to inspection and forgery. In the past "the relative chaos of the . . . paper system

actually afforded some protection because it wasn't that easy to get to the data." (Elaine O. Patrikas in [2].) The introduction of modern open information and communication systems into health care more and more exposes the most sensitive data of a person. The enthusiasm for computers wipes away all scruples. The processing of medical data hardly ever conforms to the data protection laws – at least in the countries where such laws exist. Lots of people complain about the situation and postulate the need of better measures – since decades. There is virtually no paper on medical data processing that doesn't mention the need of data protection. But with new technologies the situation becomes even worse, as they change the way medical data have to be protected.

The following sections identify some of the main problem domains.

2. The electronic patient record

The first and most important use of a computer in a clinic or a physicians practice is the management of the patient data. The electronic patient record (or computer-based patient record – CPR [3]) serves several purposes: billing the patient, legal documentation, quality control, scientific research. The doctor has to archive the data for several years and has to transmit some of the data to a health insurance company for billing. Technical means should ensure that the patient record is disclosed only to authorized persons or institutions, according to the 'need to know' principle, and that the integrity of the data is protected.

3. Electronic documents

How can we trust electronic documents? Medical documents should serve as evidence or proof in controversies or in a case. How valid and authentic is the communication between health care institutions? How can the pharmacist, with peaceful conscience, accept a prescription that was electronically transmitted? There is a clear need for electronic signature and authentication procedures in medicine. There is a need to create a certification infrastructure for public signature keys (certification authorities, notary service). The legislative authorities should make legal rules as soon as possible.

4. The medical work station

Within a few years every doctor will have his work station on his desk, and all the information he needs at his fingertips. He'll be connected to a world wide net of medical information and knowledge. He'll have access to literature and knowledge bases and to all kinds of patient independent information in international nets. And he'll have immediate acces to all the multimedia patients records in his local system. He'll communicate with colleagues and receive laboratory reports by electronic mail.

But what about security? An essential ingredient is cyptography. Never store patient data in plain text. Never transmit patient data in plain text or without proper authentication procedures. We need security systems for personal computers which use strong encryption and are certified by an ITSEC authority. We need cryptographic device drivers and cryptographic protocols for several layers of the OSI communication model. We need cryptographic chipcards as security tokens, for access control, encryption, and

digital signature.

5. Telemedicine

The growing of wide area networks will have profound affects on health care. Networks will connect primary-care physicians, hospitals, laboratories, and pharmacies. Many tasks will be achieved faster and cheaper than today. The possibilities include administrative information systems and unified electronic claims, world- (or nation-) wide access to the individual medical history for the patient himself, for the general practitioner, for the hospital, for public health professionals, for research teams [3], remote expert consultation (e. g. teleradiology), surgical telepresence, remote interaction between patient and health professional, personal health information systems for everybody. There are some quite optimistic expectations on the benefits of the future data superhighway, combined with the warning: "Without the ability to ensure the privacy and confidentiality of electronic health and medical information the full potential of health information systems will not be realized."[4].

6. The patient card

The age of smart cards in medicine is beginning. In the first turn, at least in Germany, the card contains nothing more than the identifying data of the patient and his insurance. In a next step it could contain risk data such as allergies, incompatibilities, certificates of vaccinations, willingness to donate organs, documentation of X-ray treatment. Prototypes of such cards exist already. In the future the patient card could hold treatment data and finally the complete disease history. In this way each patient could carry a lifelong patient record in his pocket.

There are some obvious benefits of patient cards but also some obvious or hidden problems and dangers. What about access rights? What about access control? The most perfect security provisions on the card don't protect it if the PIN or password becomes compromised. What about an emergency if only the patient can activate the card and is unable to act? What in an embarrassing situation – imagine an employer who wants to see my medical data before he hires me? (Even if this is illegal - I just want the job.) How reliable are the storage media? Is there a backup? Where? Who's responsible? Shall we be emancipated citizens who have complete control over our personal data? Or shall we be externally managed, helpless, dependent beings whose data are open for processing at will by authorities? The patient card offers both possibilities.

In any case, from the view point of data protection, the patient card seems preferable to the universal online patient record. The patient should be the owner of his patient card and of all the data on it. He must have the possibility to read the entire contents on a device of his own, say on his PC at home. Entries by a doctor should be electronically signed. In case of an emergency access all activities must be closely monitored and undergo special audit. This has to be controlled by cryptographic protocols. The storage of more then the most basic information on patient cards should only be allowed on a voluntary base. The patient should have the possibility to give access to only a part of the data without revealing that there's more. Maybe the patient should have the right to delete entries, or to change them. There is a need for thorough public discussion of these

matters.

7. Hospital information systems

A Hospital information system (HIS) is a complex web of diverse, often heterogeneous systems. The data must be timely accessible at specific locations. The patient records are written in various pieces by many contributors, and offer a large variety of diverse views. The providers and administrators are happy when the communication in such a system works in some way, and refrain from introducing additional complexity in form of data protection measures.

There should be a uniform concept for the entire hospital comprising the definition of responsibilities, procedures, and access rights. This is a difficult task, all the more as in a distributed data base it's not obvious where the data are located and which system administrator is responsible. This overall concept has to be implemented in each part of the system and guarded by state of the art security techniques. Each hospital, maybe each department, should have a security administrator. Hospital networks should be disconnected from wide area networks – either physically or logically; at least there should be a firewall.

8. The structure of the health care system

Patient data move between health care institutions virtually without barriers. Data protection is trapped in the triangle between patient, doctor, health insurance. The optimal care becomes more and more expensive. Cost efficiency necessitates greater transparency of the medical processes. The new german 'Gesundheitsstrukturgesetz' (GSG, health system structure law) for example tries to break the upward spiral of medical care costs. It requires the detailed registry of accomplishments and the standardized and detailed documentation of diagnoses and therapeutic procedures for management purposes using classification codes such as ICD and ICPM. The distinction between administrative and medical data disappears. Data must be transmitted in machine readable and patient related form.

This law is an almost universal enabling act for data processing and transfer, and completely disregards the confidentiality between patient and doctor. The constitutional right of privacy is violated – we have conflicting laws. This is a political problem and needs a political solution. Optimizing health care should work otherwise, without disclosing such a huge amount of detailed medical data. "The need for information must not lead to the protection of the human personality being neglected." [1, 3.1.1]

9. Epidemiologic registries

Epidemiology is the study of diseases with regard to an entire population. The results of epidemiologic research typically aren't of benefit to the present patients but only to future generations. But the present patients are asked to 'donate' their data. As long as this is voluntary, based on informed consent, nobody objects. But epidemiologic research makes sense only if there is no bias in the data. For this reason epidemiologists require an obligation or a right to register the data to catch almost all cases.

Epidemiologic registries are comprehensive data collections. They offer the possibility of gathering concentrated information about each citizen by matching with other data collections – if there are no special countermeasures. Anonymizing the data as far as possible is mandatory – but that is not enough. Epidemiologic data cannot be completely anonymous as long as they shall contain any useful information (e. g. place of residence, profession) [5, pp. 156–170]. On the other hand recognizing multiple registration and advoiding homonyms and synonyms in the registry are only possible if the identifying data are present – else the data will be of poor quality and therefore worthless. Moreover in many research projects researchers need the identity of the patients to acquire more data for concrete studies.

For epidemiologic registries we see the classical conflict between common welfare and individual rights. This conflict must be solved by the politicians on the base of a thorough public discussion. Some recommendations:

- Doctors can be given the right or obligation to report cases without consent of the patient, but only if the registry stores the data anonymously,
- legal rules for professional discretion of researchers,
- obligation to register epidemiologic research projects, data access only for research projects approved by a review board,
- legal protection against confiscation of epidemiologic data by authorities,
- administrative and technical data protection measures as strong as possible,
- anonymization of data as far as possible, e.g. aggregation (for statistics), encryption (for storage).

The obligation to register epimiologic research projects must not lead to suppression of unwanted approaches.

For the cancer registry in Rheinland-Pfalz (Rhineland-Palatinate) we proposed the following model: Doctors have the right to report cases. There is a special trustee instance that obtains the data and encrypts the identifying part by an asymmetric cipher. The registry stores the encrypted identity data and the plain medical data. Records are linked via the encrypted identity data. The decrypting key is given to a review board. Deanonymizing of identity data is permitted only under strict injunctions. In case of a concrete research project the inevitable contact with the individual patient has to be done via the trustee and the physician of that person.

10. Standards

Standards for medical data formats should make provision for data protection, in particular for electronic signature and, if this makes sense, for encryption. For example the Arden Syntax for Medical Logic Modules (MLMs), an interchange format for knowledge elements, has fields for author, specialist (who approved the module), validation, but none for a signature. Whether HL-7 should comprise encryption can be debated; maybe encryption should reside on a lower OSI layer. But an electronic signature should be also in HL-7.

11. The motivation of users

The realisation of data protection in the medical domain is in a lamentable state ("alarming" in [1, p. 1]). A possible reason is that the doctors are insensitive or indifferent for data protection matters – there are only few known occurences of data protection violations in the medical sector. Moreover they worry about additional stress, fear barriers for their work flow, and believe that data protection and data security cost a lot of money and time – and don't pay. We should make clear to them, that modern security techniques need not be terribly complicated. Data protection and security should be granted as far as possible by the systems we build, and should involve as little effort by the users as possible. The ideal security token seems to be the smart card with cryptographic features. It makes the access easy for the legitimate user and, if coupled with electronic signature, motivates him to take security seriously. All other security procedures should be hidden from the user, at least as long as he behaves legally. One more example: A logout/login sequence is inappropriate for a change of access rights in a time critical situation. We need 'on line' user authentication without leaving the running application.

12. The motivation of developers

Manufacturers and developers of systems don't see data protection and security as a positive feature that can be attractively presented; negative concepts are awkward in advertisements. There is a big market for cheap hardware and fancy software like graphic user interfaces. There is only a small market for security features, they are expensive and give no spectacular additional functionality. We need clear security standards for the medical domains that developers can rely on. In this respect the US export regulations for cryptographic products have done a lot of harm. The bad guys all over the world have all the cryptography they need. But the mass market for information systems in health care offers almost nothing.

13. Needed actions

There is an urgent need to act! The situation is bad, and it's getting even worse if we don't shift the switches now. As far as legal and political aspects are concerned we as computer scientists or medical informaticians can only warn and elucidate the consequences of short-sighted laws. For example we can demand international efforts by the politicians to coordinate the national approaches to data protection. The experiences in the European Community with these matters make me rather sceptical about the probability of success. We can demand that the politicians not only make the right declarations but also the right laws :-). We need clear and consistent legal rules that protect the confidentiality of medical data.

Then there are the organizational aspects. How can we make the owners and users of medical information systems more aware of data protection issues? How can we achieve the implementation of the necessary administrative measures? We need clear security concepts.

Finally there are the technical aspects. The contribution of computer science for preventing the erosion of constituional rights is the creation and propagation of the state of

the art techniques, and the design and construction of secure systems. A typical example is the use of strong cryptography in communication protocols or data storage. We need the best affordable security features that don't frighten or overcharge the users. The wheel is invented – one could try to optimize it, but it's more important to attach it to the car. That is, we have the necessary security tools – let's implement them to enhance data protection and security. There is no excuse not to use them. An essential step is to create a cryptographic infrastructure for medicine: standardized encryption procedures, electronic signatures, certificate authorities, smart cards, cryptographic protocols for communication. Examples for this are in [6] or [7]. Cryptography is the basic technology for achieving data security in open systems. As medicine becomes more and more open, we can ensure data confidentiality only by cryptographic means. Encryption should be a low level system feature. Access control and electronic signature should be embedded in the application programs. Let's begin with a small but useful step: Let's use PGP for email communication.

There are already some concrete efforts towards security and privacy of health information. Let me mention the IMIA (International Medical Informatics Association) Working group 4 on 'Dataprotection in Health Information Systems' and the corresponding EFMI (European Federation for Medical Informatics) working group 2. The AIM (Advanced Informatics in Medicine) program has funded a project SEISMED (Secure Enviroment for Information Systems in Medicine, cf. [8]). There is a related CEN project 'Security for Health Care Information Systems'. On the national level the german GMDS (Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie) also has a project group on data protection in HIS. There are also efforts to establish security in special systems [9].

14. Political issues

Data protection is only as strong as the political environment allows. Imagine an Orwellian state and think of the possibilities that information and communication technologies offer today. Imagine a totalitarian regime like the Nazis with such an amount of technological power. Should we therefore boycott any form of data storage and processing? Certainly not – they would have other (more primitive) means to enslave us.

There are conflicting goals, such as between patients, health providers, cost providers, research and data confidentiality, use of strong cryptography and battle against the organized crime. Should encryption therefore be banned? No – we need it to protect our data.

We have to discuss these matters publicly and try to reach a consensus, at least nationally, as far as possible internationally. We should identify inadequacies in current legislation and make proposals how to repair them.

REFERENCES

1. The Commission of the European Communities DG XIII/F AIM. *Data Protection and Confidentiality in Health Informatics, AIM Working Conference, Brussels, 19–21 March 1990*, Amsterdam, Washington DC, Tokio, 1991. IOS Press.
2. Michael Pluscauskas. Security of health information debate. Internet forum healthnet@calvin.dgbt.doc.ca, Jan 18, 1994.

3. M. F. Collen and M. J. Ball. Technologies for computer-based patient records. In K. C. Lun, Patrice Degoulet, Thomas E. Piemme, and Otto Rienhoff, editors, *MEDINFO 92*, pages 686–690, Amsterdam, 1992. Elsevier Science Publishers B. V.
4. Michael D. McDonald. Statement before the Subcommittee on Telecommunications and Finance of the House Energy and Commerce Committee. Internet forum health-net@calvin.dgbt.doc.ca, Feb 4, 1994.
5. Peter Paul Spies, editor. *Datenschutz und Datensicherung im Wandel der Informationstechnologien – 1. GI-Fachtagung, München, Oktober 1985*, Informatik-Fachberichte 113, Berlin, 1985. Springer-Verlag.
6. Bruce Schneier. *Applied Cryptography*. John Wiley, New York, 1994.
7. Klaus Pommerening. *Datenschutz und Datensicherheit*. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991.
8. A. R. Bakker. Security in medical information systems. In Jan H. van Bemmel and Alexa T. McCray, editors, *Yearbook of Medical Informatics*, pages 52–60, Stuttgart, 1993. Schattauer.
9. Michael Hortmann. Interim technical recommendations for data protection in CC computer systems: Guidelines for the use of security functions. Deliverable 3, AIM project TANIT, Workpackage PROTEC, 1992.
10. Richard S. Dick and Elaine B. Steen, editors. *The Computer-Based Patient Record: An Essential Technology For Health Care*, Washington, DC, 1991. Institute of Medicine, National Academy of Science, National Academy Press.
11. Molla S. Donaldson and Kathleen N. Lohr, editors. *Health Data in the Information Age: Use, Disclosure and Privacy*, Washington, DC, 1994. Institute of Medicine, National Academy of Science, National Academy Press.