Medical Requirements for Data Protection

Klaus Pommerening

Institut für Medizinische Statistik und Dokumentation
der Johannes-Gutenberg-Universität

D-55101 Mainz

Data Protection in Health Care

Confidentiality of medical data –

- professional discretion (Hippocratic oath),
- constitutional rights (informational self-determination).

New information and communication technologies …

- improve quality and efficiency of health care,
- create new challenges for confidentiality.

Data protection, confidentiality and computer security are basic requirements for the appropriate introduction and use of information and communication technologies in health care. [CEC DG XIII]

Two basic security requirements for medical data processing

1. Safety for the Patient:

- Automation of diagnostic and therapeutic procedures must do no harm to the patient.

→ Need for trustworthy and reliable systems.

→ Need for software quality control.

2. Protection of medical data:

→ Political, legal, administrative, and technical problems

The relative chaos of the paper system actually afforded some protection because it wasn't that easy to get to the data.

[Patrikas]

In view of the new electronic media any sloppy handling of medical data can no longer be tolerated.

Basic political/legal problem:

Control the balance between conflicting goals,

e. g. privacy of medical data vs. efficiency of health care.

Basic administrative problems:

Define responsibilities, procedures, and access rights.

Allocate human and economic resources appropriately.

Basic technical challenge:

Cope with the openness of data processing and communication systems.

Data are exposed to inspection and forgery
on storage media and on nets.

The electronic patient record

(Computer-based patient record - CPR)

Management of patient data (in a clinic or a doctor's office):

- billing the patient,
- legal documentation,
- quality control,
- scientific research.

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.

Electronic documents

How can we trust electronic documents?

Medical documents as evidence or proof?

Electronically transmitted prescription authentic?

→ Need for electronic signature and authentication procedures.

→ Need for certification infrastructure.

→ Need for legal rules.

The medical work station

All the information at the doctor’s fingertips.

World wide net of medical information and knowledge.

Access to literature and knowledge bases.

Access to multimedia patient records (local and remote).

Communication with colleagues and experts.

→ Need for security systems for personal computers.

→ Need for cryptographic device drivers.

→ Need for cryptographic chipcards (security tokens).

Medical data on the superhighway?

World- (or nation-) wide access to the individual medical history for

- the patient himself,
- the general practitioner,
- the hospital,
- public health professionals,
- research teams.

Remote expert consultation.

Surgical telepresence.

Remote interaction between patient and doctor.

Personal health information systems for everybody.

Telemedicine

Growing of wide area networks – affects on health care:

- primary care physicians,
- hospitals,
- laboratories,
- pharmacies

are all connected.

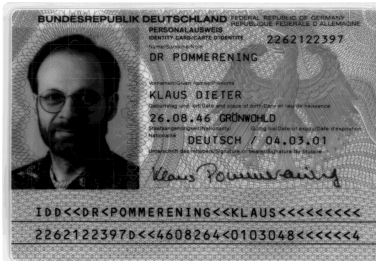
→ Need for strong cryptography.

→ Need for cryptographic protocols for communication.

→ Need for authentication procedures.

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.
[McDonald]

The smart patient card



1. Stage: Identifying data, insurance data

   (as presently in Germany).

2. Stage: Risk data –

   – allergies,
   – incompatibilities,
   – certificates of vaccinations,
   – consent to donate organs,
   – documentation of X-ray treatment.

   (Prototypes exist.)

3. Stage: The complete disease history –

   Each patient carries a lifelong patient record in his pocket?

   Alternative or supplement to the universal online patient record.

The patient card – problems and dangers

Who owns the card and the data?

Who has access to the data?

What about access control?

What if the PIN is stolen?

What if the PIN is forgotten? What in emergency?

What in embarassing situations?

How reliable are the storage media?

Is there a backup? Where? Who's responsible?

Emancipated citizens who have complete control over their personal data?

Or externally managed, helpless, dependent beings whose data are open for processing at will by authorities?

The patient card – requirements

The patient should be the owner of his patient card and of all the data on it.

He should have the opportunity 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.

Emergency access:

- All activities must be closely monitored and undergo special audit.
- Controlled by cryptographic protocols.

The storage of more then the most basic information on patient cards should only be allowed on a voluntary base.

Maybe the patient should have the right to delete entries, or to change them.

Key Feature: *The patient should have the possibility to give access to only a part of the data without revealing that there's more.*

Hospital information systems

Complex web of diverse and often heterogeneous systems.

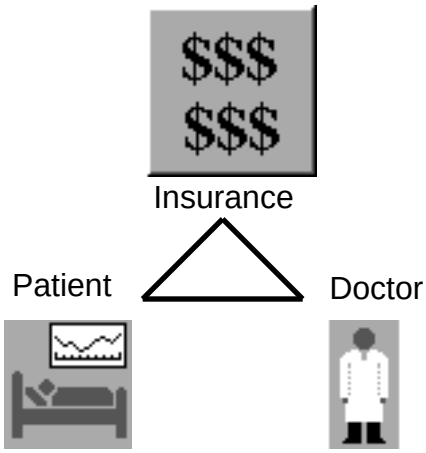
Weak or nonexistent data protection measures.

Providers and administrators refrain from introducing additional complexity (= data protection measures).

Requirements:

- Uniform concept for the entire hospital.
- Security techniques:
  state of the art ,
  easy to implement.
- Security administrators.
- Firewall.
- Reference installations.

The structure of the health care system



Upward spiral of medical care costs.

Cost efficiency necessitates greater transparency of medical processes.

Data must be transmitted to health insurance institutions in machine readable form.

New health care reform laws or proposals conflict with data protection laws.

→ Need for political solution.

Optimizing health care should work without disclosing a huge amount of detailed medical data.

The need for information must not lead to the protection of the human personality being neglected.
[CEC DG XIII]

Epidmiologic registries

Study of diseases with regard to an entire population.

Benefit 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.

Epidemiologic research makes sense only if there is no bias in the data.

Epidemiologists require an obligation or a right to register the data to catch almost all cases.

Comprehensive data collections – matching with other data collections.

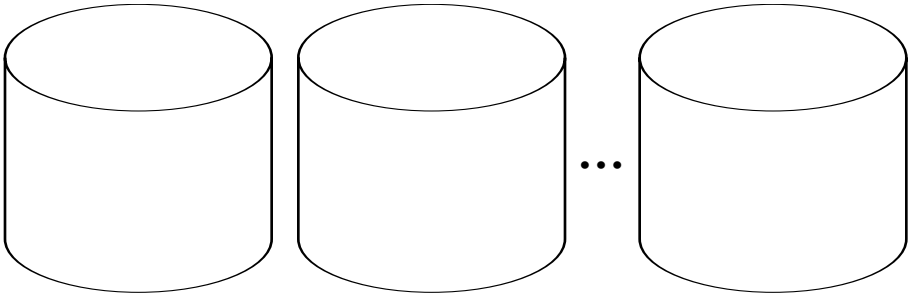
Epidemiologic data cannot be completely anonymous as long as they shall contain any useful information (e. g. place of residence, profession).

Problems: Multiple registration, homonyms, synonyms.

Researchers often need identity data to gather more information.

→ Need for political solution of conflict between common welfare and individual rights on the base of a thorough public discussion.

Health data bases



Population-wide comprehensive collections of personal health data

Promises: Benefits for financial, organizational, quality improvement, and research purposes.

Assumption: The more data you have there more problems you can solve. (?)

But huge data collections suffer from

- poor quality, poor reliability,
- $\Rightarrow$ little use („Datenfriedhof“),
- high potential for misuse.

Epidemiologic registries – recommendations

- Medical 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.

The cancer registry of Rheinland-Pfalz

Doctors have the right to report cases (without consent).

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 kept by a review instance.

Deanonymizing of identity data is permitted only under strict injunctions.

In case of a concrete research project inevitable contact with the individual patient has to be established via the trustee office and the physician of that person.

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 has no field for a signature.

Should HL-7 comprise encryption?

Electronic signature should be in HL-7.

The motivation of users

The realisation of data protection in the medical domain is in an *alarming* state. [CEC DG XIII]

Are medical doctors insensitive for data protection matters?

Additional stress, barriers for work flow?

Data protection and data security too expensive?

Modern security techniques need not be terribly complicated!
(E.g. encryption is just simple arithmetic, no matter whether it's strong or weak.)

Data protection and security should be granted by the systems.

… and should involve as little effort by the users as possible.

Example: 'On line' user authentication without leaving the running application.

Smart card as ideal security token –

– makes the access easy for the legitimate user

– if coupled with electronic signature, motivates him to take security seriously.

The motivation of developers/suppliers

Data protection and security:
not positive features that can be attractively presented;
negative concepts are awkward in advertisements.

Big market for cheap hardware and fancy software like graphic user interfaces.

Small market for security features, they are expensive and give no spectacular additional functionality.

Developers are demotivated by US export regulations for cryptographic products; the mass market for information systems in health care offers almost no security features.

Standards and infrastructure are missing.

→ We need clear security standards for the medical domains that developers can rely on.

Needed actions – legal, political, organizational

What can computer scientists or medical informaticians do?

Legal and political aspects:

- Warn and elucidate the consequences of short-sighted or missing laws.
- Demand international efforts by the politicians to coordinate the national approaches to data protection.
- Demand clear and consistent legal rules that protect the confidentiality of medical data.

Organizational aspects:

- Design clear security concepts.

→ Need for interdisciplinary efforts.

Needed actions – Technical aspects

Contributions of computer science:

- Develop and propagate state of the art techniques.
- Design and construct secure systems.
- Implement existing security tools.

  Example: Use strong cryptography in communication protocols or data storage.

- Create a cryptographic infrastructure for medicine: standardized encryption procedures, electronic signatures, certificate authorities, smart cards, cryptographic protocols for communication.
- 1. step: Use PGP for email communication.

The cryptographic infrastructure is an essential prerequisite for data protection in information and communication systems.

Caveat: Don’t frighten or overcharge the users –

Security measures should be strong but easy to use.
(E.g. single point of authentication.)

Institutional efforts

- IMIA Working group 4
  'Dataprotection in Health Information Systems'
- EFMI working group 2.
- AIM (Advanced Informatics in Medicine) program –
  project SEISMED (Secure Enviroment for Information Systems in Medicine).
- CEN project 'Security for Health Care Information Systems'.
- GMDS (Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie) –
  project group on data protection in HIS.
- Efforts to establish security in special systems.

Résumé

Data protection is only as strong as the political environment allows.

Resolve conflicting goals

- patients vs. health providers vs. cost providers,
- research vs. data confidentiality,
- use of strong cryptography vs. battle against the organized crime,

in favour of data protection and confidentiality.

Identify inadequacies in current legislation and make proposals how to repair them.

Cryptography is the key to data protection in open systems, on the superhighway, and in the medical workstation.

Say YES to telemedicine, if the necessary cryptographic infrastructure and end-to-end encryption is provided.

Just say NO to comprehensive multipurpose data bases of patient data.

The free access to information should stop short of patient data.

More important for health care than collecting more and more data is that the patient has personal confidence in his doctor.

We don't want the medical doctor become a part of an impenetrable, mysterious, inhuman, data collecting, efficient machinery.