OPINION OF THE EUROPEAN GROUP ON ETHICS
IN SCIENCE AND NEW TECHNOLOGIES
TO THE EUROPEAN COMMISSION

No 13 **30 July 1999**

ETHICAL ISSUES OF HEALTHCARE IN THE INFORMATION SOCIETY

Reference : Initiative of the Group
Rapporteur: Prof. Ina Wagner

The European Group on Ethics in Science and New Technologies (EGE),

Having regard to the Treaty on European Community, and in particular its Article 3 relating to a contribution to the attainment of a high level of health protection, its Title XIII and Article 152 on public health and its Title XIV and Article 153 on consumer protection,

Having regard to the Treaty on European Union, and in particular Article 6 of the common provisions concerning the respect for fundamental rights,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to the Directive 92/59/EEC of the Council of 29 June 1992 on general product safety,

Having regard to the Directive 93/42/EEC of the Council of 14 June 1993 concerning medical devices,

Having regard to the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases,

Having regard to Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector,

Having regard to the proposal for a European Parliament and Council Directive on a common framework for electronic signatures (COM(1998) 297 final of 13 May 1998), Having regard to the proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market (COM(1998) 586 of 18 November 1998),

Having regard to Decision No. 99/182/EC of the European Parliament and of the Council of 22 December 1998 concerning the fifth framework programme of the European Community for research, technological development and demonstration activities (1998 to 2002),

Having regard to Decision No. 99/168/EC of the Council of 25 January 1999 adopting a specific programme for research, technological development and demonstration on a user-friendly information society (1998 to 2002),

Having regard to the amended proposal for a Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (COM(1998) 784 final of 14 December 1998),

Having regard to the amended proposal for a European Parliament and Council Decision adopting a Multiannual Community Action Plan on promoting safer use of the Internet (COM(1998) 518 final of 10 September 1998),

Having regard to the Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of Regions on Europe's way to the information society – an Action Plan (COM(1994) 347 final of 19 July 1994),

Having regard to the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on the follow-up to the Green paper on the protection of minors and human dignity in audio-visual and information services including a proposal for a Council Recommendation concerning the protection of minors and human dignity in audio-visual and information services (COM(1997) 570 final of 18 November 1997),

Having regard to the Green paper on public sector information in the information society: a key resource for Europe (COM(1998) 585 of 20 January 1999),

Having regard to the Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data of 28 January 1981,

Having regard to the Council of Europe Recommendation No. R(97)5 on the protection of medical data adopted of 13 February 1997,

Having regard to the Council of Europe Convention on Human Rights and Biomedicine signed on 4 April 1997,

Having regard to the Universal Declaration on the Human Genome and Human Rights adopted at UNESCO level in 1997, and endorsed by the General Assembly of the UN on 9 December 1998, Having regard to the OECD Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data, adopted by the Council on 23 September 1980,

Having regard to the United Nations Guidelines concerning computerised personal data files, adopted by the General Assembly on 14 December 1990,

Having regard to the WHO Regional Office for Europe Declaration on the promotion of patients' rights in Europe of 1994,

Having regard to national regulations and opinions expressed by national ethical bodies within the European Union on the use of personal as well as medical data,

Having regard to the hearing held on 17 March 1999 by the EGE, with experts, representatives of the European Institutions and of interest groups (health, consumers, industry, religions),

Having heard the rapporteurs.

1- WHEREAS

1.1 SCOPE OF THE OPINION

1.1.1 Range of data covered by the present Opinion

- The present Opinion confines itself to the ethical implications of the use of person identifiable personal health data. Person identifiable data includes, as in the terms of the Directive 95/46/EEC, any data which either directly or indirectly identifies an individual by reference to her/his name, identification number or to one or more factors specific to her/his physical, physiological, mental, economic, cultural or social identity.

- Personal health data encompass a wide range of information about an individual, which all touch upon an individual's private life. A health biography could include, not only basic medical data: a history of all medical diagnoses,
diseases and medical interventions,
medications prescribed,
test results, including imaging, etc…,

  but could also include sensitive data: on mental health,
relevant to family history,
behavioral patterns,
sexual life,
social and economic factors, etc …,

  and healthcare administrative data: admissions and discharge data
routine operational data,
insurance and financial transactional data, etc....

Almost all such data can be recorded in digital form and processed electronically and remain sensitive even after the death of an individual.

1.1.2 Range of data uses covered by the present Opinion

- The Opinion covers all aspects of personal health data management: collection, processing, recording, storage, access, uses, management, responsibility, follow up, evaluation, systems and network design, ...
- Personal health data are used not only in the practitioner-patient interaction but also by the numerous spatially distributed third parties. Such third parties may include medical practitioners who are given access to a patient's medical data in the context of shared medical care, administrative bodies charged with the management of healthcare services, as well as other third parties such as insurers, employers, etc....

1.1.3 Issues not considered in the present Opinion

- The present Opinion does not specifically consider the use of non identifiable personal health data.
- The Opinion does not either cover aggregated data concerning the professional activities of healthcare professionals even if these data raise specific ethical questions.

1.2 INFORMATION AND COMMUNICATION TECHNOLOGY TOOLS IN HEALTHCARE

- Medical informatics dates back to the 1960s when computers were first introduced into hospitals to support administrative tasks. Many trials of a wide range of Information and Communication Technology (ICT) tools used in healthcare are currently taking place in Europe, some with the support of European Community funds.

Electronic Health Record (EHR)

- The concept of the electronic health record (EHR) has developed, and now forms a core element of ICT developments in healthcare. An EHR can comprise the medical history of a citizen as well as non-medical information, held in textual and non textual format (image, voice, tactile traces). The electronic recording of data facilitates their transmission and sharing between practitioners and relevant third parties, for clinical, administrative, statistical, research purposes, etc...

Networking and Telemedicine

- Networked systems, in the form of intra-nets, extra-nets and the Internet, can facilitate interdisciplinary co-operation. A hospital intranet system can be used, for example, to send radiological images simultaneously to the treating clinician, so that while the radiologist is working on a diagnosis, the clinician can have an independent view of the images and also converse with the radiologist.

- The EHR opens the possibility of telemedicine in which a practitioner can give a consultation without the physical presence of the patient. The practitioner may, for example, assist the citizen living in a remote area or in transit in an aircraft or at sea.
- In several European countries pilot projects are in operation which connect the practitioner's consultancy with other professionals. Such systems can, for example, allow a practitioner to forward prescriptions directly to the local pharmacy. Thus a pharmacist could perform checks (e.g. for drug incompatibilities, the use of habit-forming drugs) and practitioners could also check if a patient has actually retrieved her/his medication.

Electronic Health Card

- Currently, several European countries are testing the design of an Electronic Health Card, a chip card holding administrative and/or medical data. Such a card may exist either as a practitioner held card, which the practitioner keeps and uses to access the EHR, or as a patient held card, which creates the possibility of a portable health record, through which the patient may give access to her/his complete or partial (for example emergency data) medical record to any practitioner.
- Some European countries are currently testing the design of publicly accessible card reading facilities, through which the citizen holding her/his own health card may have direct or indirect access to her/his medical record.

Decision support technologies

- The development of software and ICT tools for medical specialists allow for the development of decision support systems, which strengthen the diagnostic capacities of individual practitioners. Such technologies can, for example, suggest diagnoses, provide reminders for check ups and preventative measures, or alert practitioners to side-effects.

Medical databases

- The establishment of large medical databases extracted and aggregated from individual clinical and administrative data, can enhance healthcare evaluation, public health surveillance and epidemiology. Such databases may be used, for example, to trace long-term effects of certain drugs, trajectories of particular diseases, outcomes of particular medical interventions, as well as to plot disease incidence.
- Medical databases also provide support for clinical and statistical research activities such as trials, literature searches and in-depth comparisons of research results (meta-analyses).

The Internet

- Citizens, healthcare providers and industry are all making increasing use of the Internet. Citizens are increasingly using the Internet for their own health education and participation in healthcare. They are becoming the consumers of a wide range of health information, goods and services offered on the Internet.

1.3 WIDER SOCIETAL IMPLICATIONS OF ICT IN HEALTHCARE

1.3.1 Changes in the practitioner / patient relationship

- Through the development of the EHR and special software to support the daily administrative work of medical practitioners, computers have become an integral feature of the interactions between practitioners and their patients.
- While formerly most information was collected in personal conversations between doctor and patient, today medical decision making is a spatially distributed process, involving numerous actors, among them nurses, psychotherapists, and various medical specialists. Many of these actors never meet face-to-face to discuss a case but each adds her/his own report which is read, interpreted and integrated by the responsible practitioner.
- In order to allow the shared use of collected data, so that different and spatially distributed healthcare units can retrieve and process such data, it is necessary that the various systems in use can communicate with each other (technical interoperability). Moreover, standardised terminologies used for coding diseases, medical procedures, prescriptions and nursing interventions have been developed (ICD-10, ICNP, READ, Snomed, ...).

1.3.2 Security and reliability in ICT systems

- Since it is difficult to construct absolutely reliable computer systems due to their enormous complexity of the systems.
- Many tools and standards have been developed to ensure that ICT applications in healthcare do not compromise information security, i.e. not only the confidentiality of the data, but also its availability and integrity, requiring that data are accurate and complete, and available where and when required. Security tools may be graded to be commensurate with the security sought.

1.3.3 The citizen and standardisation

- The design of ICT systems and networks influences which personal health data are collected, stored and maintained and who should or could have access to them via the Internet or via inter- or intra-hospital networks or who should have acces to the patient data card.
- One main effect of ICT development is the globalisation of standards and procedures, which may be used, for example, in the determination of protocols for treatment. Standards and protocols can serve as tools for good practice and can form an important part of quality assurance. However the collection of standardised data and the use of such protocols require that the practitioner/patient interaction is structured according to a pre-set format.
- Standards are not neutral. They embody choices (ethical, social, economical, political, epistemological, …) of their creators and will necessarily favour particular views of patients or diseases while excluding others.

1.3.4 The Citizen as a stakeholder

- ICTs are used to improve the citizen's access to health information, to provide the citizen with tools that could enhance her/his choices (such as Internet-based information on healthcare services and providers) and increase her/his demand for healthcare.
- ICTs also support patient centered self-help groups to play a more active role vis-à-vis healthcare institutions and professionals.
- ICTs reinforce the notion of the citizen as a stakeholder in her/his own health, who seeks greater participation in her/his healthcare and therefore greater access to her/his own health information.

1.3.5 Secondary uses of personal health data

- While medical data are used for the care of the patient, personal health data are also used for a wide range of secondary purposes, which include in particular health administration, cost containment, reimbursements, health policy, quality of care auditing, epidemiological and other studies.
- ICT can be a fundamental tool to improve efficiency at both clinical and managerial level, by allowing greater visibility of work and avoiding duplication.
- ICT can be a powerful tool for quality assurance activities and programmes, which may be used to control performance and practice of healthcare professionals.
- Personal health may be used to construct profiles of patient as a basis of health policy decision-making.
- Personal health data are widely used for the control and containment of costs and the allocation of health resources.
- The Icelandic legislation, granting access to a sole pharmaceutical company to the anonymised health data of the population of Iceland for research and development purposes, underlines the economic value of personal health data.

1.3.6 Citizen and ownership of personal health data

- Personal data must be considered in the framework of the rights of personality, even if in some cases they can be subject transactions. However, since personal data continue to reflect the data subject's identity, they cannot be treated as entirely separate from her/him. Thus, some countries regard sensitive personal health data as inalienable in order to protect the dignity of the individual .

1.4 LEGAL ASPECTS

- The general principles of the *European Convention for the protection of Human Rights and Fundamental Freedoms* of 1950, (in particular the respect for private life), which constitute principles of Community law, provide the legal background for the development of specific legislation to protect the interest of the citizen when ICT is used in healthcare.
- The Council of Europe‘s Convention 108 for the protection of individuals with regard to automatic processing of personal data has placed the citizen in a significantly improved position with regard to personal health data.

- With the Directive 95/46/EC, the European Union has now adopted its first comprehensive legisation with regard to fundamental rights and freedoms and in particular the right to privacy. Although Article 8 includes health and sex life data, no specific binding legislation on personal health data and ICT exists.
- Furthermore the diverse nature of healthcare management in the European states has given rise to a particularly disparate array of legislation relevant to ICT and healthcare across Europe.
- Legal standards for the protection of the citizen in healthcare differ from country to country, since they reflect the diversity in long-standing cultural traditions, of medical secrecy, ownership of medical data, patient autonomy, professional liability, etc.

1.5 ETHICAL ASPECTS

1.5.1 Public concerns

While the trends and developments of ICT in healthcare have given rise to many positive developments as described earlier, public concerns about the use of ICT in healthcare have been expressed

- The pervasiveness of a technology which many people do not understand.
- The lack of transparency of the work of healthcare professionals and its effects on the doctor/patient relationship.
- The difficulty of respecting privacy and confidentiality when third parties may have a strong interest in getting access to electronically recorded and stored personal health data.
- The difficulty in ensuring the security of shared personal health data.
- The lack of adequate infrastructure in certain regions and the absence of computer literacy in certain sections of the population which may reinforce existing inequalities.

1.5.2 Value conflicts

- These public concerns about the use of ICT in healthcare echo many well established value conflicts in the provision of healthcare, such as:

Effectiveness versus confidentiality

- The need to know and share patient personal health data, in order to provide good quality of care, creates a situation of shared secrecy which may compromise confidentiality.

Privacy versus the collective good

- Privacy may be traded for certain collective goods (research, administration, planning, prevention...) that benefit the community or population at large.

Quality assurance versus professional autonomy

- Some professionals fear that quality assurance standards (protocols, clinical guidelines, clinical pathways, ...) may restrict or diminish professional autonomy.

Efficiency versus beneficence

- While beneficence indicates giving the best possible care for every patient, this may be very expensive and not feasible. In the context of limited resources, to give a patient expensive care could deprive another patient of much needed basic treatment, a second best treatment may be the most appropriate.

1.5.3 Ethical principles

- In addition to the legal regulations, certain ethical principles may be used to address these value conflicts, namely:

  - Human dignity,

  serving as a basis for requirements of privacy, confidentiality and medical secrecy;

  - Autonomy,

  serving as a basis for requirements of self-determination and participation;

  - Justice,

  serving as a basis for requirements of equitable distribution of limited resources;

  - Beneficence and non-maleficence,

  serving as a basis for the attempts to weigh anticipated benefits against foreseeable risks;

  - Solidarity,

  serving as a basis of the right for everyone to the protection of healthcare, with a special concern for vulnerable groups in society.

* * * * * * * *

2- THE GROUP SUBMITS THE FOLLOWING OPINION

- Personal health data necessarily touch upon the identity and private life of the individual and are thus extremely sensitive.
- ICT creates the potential for the free circulation of personal health data, across local, national and professional borders, giving such data an enhanced European dimension.
- The principles of the European Convention of Human Rights, the rules of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and especially the European Directive 95/46/EC, for the protection of personal data, are an essential source for addressing the ethical questions of healthcare in the Information Society.

2.1 Status of personal health data

- Personal health data form part of the personality of the individual, and must not be treated as mere objects of commercial transaction.

2.2 Confidentiality / privacy

- The Human Right to respect for private life requires that confidentiality of personal health data is guaranteed at all times. It also implies that, in principle, the informed consent of the individual is required for the collection and release of such data.

- Collection of, and access to, personal health data is limited to treating medical practitioners and to those third parties (non-treating medical practitioners, healthcare and social security personnel, administrators, ...) who can demonstrate a legitimate use.
- All legitimate users of personal health data have a duty of confidentiality equivalent to the professional duty of medical secrecy. Exceptions to this duty must be limited and provided for by legal rule.
- Medical secrecy is central to the trustworthiness of the healthcare system, not only in the private interest of the person. Trust is a fundamental ethical value in itself.
- The respect for the confidentiality of health data continues after the death of the person.

2.3 Self-determination

- Health data should be collected directly from the citizen wherever possible.
- Self-determination includes citizens' right to know and to determine which personal health data are collected and recorded, to know who uses them for what purposes, and to correct data if necessary.
- The citizen has the right to oppose, the use of her:his data for secondary purposes not provided for by law.
- The use of personal health data for the purposes from which society as a whole benefits must be justified in the context of the above rights.

2.4 Accountability

- The networking of health institutions fosters new kinds of dependencies and responsibilities. This has to be reflected in new kinds of accountability.
- For all parties using health data an equivalent to the accountability of health professionals should be established.
- When health managers use healthl data for the purposes of health services planning and management, they should be accountable for such data uses.

2.5 Principle of legitimate purpose

- The collection and processing of personal health data should be guided by the principle of a strict relationship between this collection and handling and the legitimate purpose to which those data are used
- Third parties who do not form part of the public health system may require access to medical information for their professional purposes, such as insurers and employers. Such third parties must in no case have direct access to personal health data.

2.6 Security

- The security of ICT in healthcare is an ethical imperative to ensure the respect for human rights and freedoms of the individual, in particular the confidentiality of data and the reliability of ICT systems used in medical care.
- The respect for security requires the use of encryption technology where appropriate, the use of closed networks for the transfer of personal health data and organisational measures to support security.
- Given the importance of the security of personal health data, European security standards should be observed wherever an electronic transfer of person identifiable data occurs.
- Since medicine is a safety ethical environment, ICT systems must be rigoroulsy monitored.

2.7 New ICT technologies

Internet

- The notion of accountability has to be extended to the providers of health information on the Internet.
- Where transactions related to healthcare goods and services (ordering drugs, looking at drug information) are made by Internet, data related to such transactions should be regarded as personal health data.
- Data related to the consultation of health information on the Internet must not be transfered to third parties or used for constructing personal profiles.

Health cards

- All projects and activities concerning the design and use of health cards have to observe the citizens' rights to self-determination and participation.
- No personal health data may be included on the card without the holder's prior consent.
- The card holder must be able to readily restrict access to some or all personal health data held on the card.

2.8 Participation

- The right to participate in the medical decision-making process is a key part of the notion of the citizen as a stakeholder.
- The citizen must have access to his/her electronic health record.
- Procedures (e.g. consensus conferences, participatory systems design, ...) have to be developed to encourage and support the participation of citizens' collectives and users in the design of systems.

2.9 Transparency

- Standardisation is inherent in ICT, increasingly in the healthcare sector where classification and coding (clinical protocols, diagnostic related code, checklists,...) are in widespread use.
- As these standards are not neutral, but embody value-related choices, they must be transparent and may be subject to evaluation by independent bodies (for example ethical committees, patients' organisations, professional associations).

2.10 Evaluation

- Qualitative and quantitative evaluation studies with a focus on core effects and implications of ICT systems, should be undertaken at a European level.

2.11 Education and training

- In order to make the right of self-determination effective, healthcare professionals should inform patients of their rights without a direct request for such information.
- Programmes of information, education and training should be promoted at the European level to provide citizens, health professionals and systems designers with guidance on the ethical implications of ICT in healthcare and information about the potential, the limitations and the appropriateness of the use of ICT systems.

2.12 Actions to be undertaken

- A Directive on medical data protection is desirable within the framework of the current Data Protection Directive to address the particular issues arising from the use of health data in Information Society.
- A European Patient's Charter covering the above aspects, possibly by means of a Recommendation, should be adopted.