PROEHTEL

Contract n° IST-1999-29029

Deliverable D 15/A4.3

A Patients' Charter
Position Paper

Authors:
EHTEL Actor Working Group
"Patients, Citizens, Consumers Associations" (A4):

Angelica Frithiof, Sweden
David Garwood, UK
Ekkehard Bahlo, Germany
Harm Jan Roelants, The Netherlands
Jean-Luc Bernard, France

December 2002
edited for form June 2003
(Version Final)

Table of Contents

Preamble **5**

The Patients' Charter for eHealth Information Systems **6**

The right to appropriate information 6

The right to expect eHealth information systems to function and operate correctly 6

The right to have information stored, processed and managed to the highest possible standards 7

The right to access information 7

The right to privacy and confidentiality 7

The patient is to be considered the master of his or her medical records 8

The right to be protected from unsafe and poor quality products and services ordered via the Internet 8

The right to complain 9

The right to receive compensation 9

Annex – Glossary of Terms **10**

Preamble

The emerging world of eHealth can be defined as the application of information, communication and video technologies to the delivery of timely, professional and safe healthcare. Systems now exist which hold increasingly detailed levels of clinical information, remotely monitor vital signs, enable remote diagnosis and treatment and more recently have facilitated surgery by professionals located thousands of miles away from the patient.

While supporting professionals in the delivery of healthcare, EHealth information systems also have the potential to empower the patient. However, to the extent that contractual relations which can be influenced by the patient replace state supervision and responsibility, new requirements for the protection of the individual's rights emerge.

The rights established under this charter take particular account of the increasing use of information technology in health care Thus, it seeks to amend general patients' rights bills or charters as enacted in a number of Member States as well as future members of the European Union. The rights shall be deemed to apply to every patient treated in a hospital, outpatient facility, ambulance, doctor's office, nursing home or any other institution where health care services are provided.

In the paragraphs set out below the individual patient rights are set out. Each of these has a number of supporting requirements associated with them which enable each right to be satisfied.

The Patients' Charter for eHealth Information Systems

The right to appropriate information

- Information about patients should be held in a form that is understandable to all users including the patient. Where this is not possible for accepted clinical or technical reasons, the facility should exist for patients to have entries in their files translated and explained to them.

- Electronic filing provides much more comprehensive information on health and treatment. Accordingly, appropriate time and assistance has to be given to the patient in order to support his or her understanding of diagnosis and proposed treatment also to help in deciding on the options to be followed.

- In order to do this, information should be complete and accurate and not selective so as to promote a commercial organisation's products or a public sector initiative.

- It must be possible to identify the source of the information stored or processed by an EHealth system, particularly where such information is published on the Internet. To this end, this charter supports the EC Guidelines for Quality Criteria for Health Related Websites.

- In support of the above information on health, prevention of diseases and care must be certified in order to protect citizens from inappropriate or false information

- Costs of commercial products and information services to be transparent and in a reasonable relation to the value offered.

The right to expect eHealth information systems to function and operate correctly

- All EHealth systems should be expected to operate safely and reliably in order not to introduce unacceptable levels of risk or harm. For this purpose, safety and reliability can be taken to mean that systems process and store data accurately and be expected to function with minimum amount of downtime.

- In order to achieve the required levels of safety, EHealth systems should be subjected to formal testing to standards similar to those applied to medical equipment before being installed in an operational environment.

- The design, development and maintenance of EHealth systems should be subject to constant and continuing quality control procedures

- EHealth systems should be the subject of constant auditing and monitoring

- All users of EHealth systems should be thoroughly and formally trained in their operation.

- Adequate fallback procedures should be in place in the event of a system failure.

The right to have information stored, processed and managed to the highest possible standards

- Information processed by EHealth systems must be of the highest possible quality regarding comprehensiveness and accuracy according to accepted international standards.

- Information must fit the purpose for which it is to be used.

- EHealth information systems must operate within national laws governing data protection and/or in accordance with EC Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- EHealth information systems must operate within accepted internal standards for data security i.e. ISO I7799.

The right to access information

- EHealth systems should be operated in a supportive and respectful manner. Such considerations might include the provision of information about all treatments available for a particular condition, where they are available, success rates and waiting times

The right to privacy and confidentiality

- As a private individual the patient has the right to control how his or her information is processed or shared.

- Personal information should only be shared or processed (even between healthcare professionals) with the explicit consent of the patient

- EHealth operations must take place within a well defined and agreed framework which places a duty of confidentiality on all those handling personal data. The duty of confidentiality is taken to be in place at all times and to support the patient's right to privacy.

The patient is to be considered the master of his or her medical records

- The processing and transmission of data has to be based on explicit consent of the patients. This is a centrally important and critical issue within the EHealth environment.

- The patient must have the right to validate information held about him or her and to have it corrected where it can be shown to be inaccurate

- It must be possible to identify the source of the information stored or processed by an EHealth system in order to validate the quality, reliability of information according to established international transparency criteria.

- All patients have the right to know what information is held about them, where it is held and who is responsible for it.

- All information held about an individual must be accessible by that patient at any point of contact with the healthcare system

- Where necessary, a data tracking infrastructure must be in place to ensure that information stored about a patient can be identified, located and accessed by that individual

- Where information is held in a coded form or is couched in medical or technical terms, a facility should exist to translate it and make it understandable for the patient.

- Facilities should exist to alert patients when information about them is to be destroyed and to provide them with the right to conserve that information if they so wish.

- The patient must have the right to have information deleted from his record when it can be shown that the information held is either inaccurate or false [which may be in conflict with existing national guidelines governing the conduct of medical professionals]

The right to be protected from unsafe and poor quality products and services ordered via the Internet

- Drugs and other medical products, together with accompanying information (e.g. package leaflets), must be provided at guaranteed quality levels

- The origin and source of products must be transparent in order for appropriate liability to be recognised in the case of poor quality, inadequate or false information leading to patient harm

- The distribution of drugs and other medical products across the Internet must be in accordance with respective country laws.

The right to complain

- National authorities responsible for healthcare and professional regulatory bodies must put in place procedures to enable patients to complain about the safety and quality of EHealth systems.

- Such procedures should make it clear who is responsible for administering them, where they are located and how the patient can initiate a complaint

- National authorities should establish a post of Ombudsman within their respective countries to assist patients in understanding complex IT issues and to serve as an Institution where complaints can be made and followed up.

The right to receive compensation

- EHealth systems have created new opportunities for patients to be physically harmed or otherwise damaged. These new features need to be recognised in and law governing legal liability and the level of damages available. This is particularly important in the field of genetics where a new dimension of data protection requirements is an example for the need of effective and appropriate liability and damage compensation systems in place.

Annex – Glossary of Terms

Access: Right, opportunity, or means of finding, using, or retrieving information.

Accuracy: Attributes of software that bears on the provision of right or agreed results or effects.

Audit: An official and methodical examination and verification.

Confidentiality: The characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner.

Integrity: The property that data has not been modified by an unauthorised entity and is fit for the purpose for which is to be used.

Privacy: The individual rights of a person to protect her or his personal life from the outside world, including the right to be left alone and to decide herself or himself how, what, and to what degree another may dispose of her or his data.

Reliability: The reproducibility of a measure. A measure is reliable if it yields similar results each time it is used on similar samples, or if its components yield similar results for the same or similar samples.
(compare *validity*).
Set of attributes that bear on the capability of software to maintain a level of performance under stated conditions for a stated period of time.

Safety: Freedom from unacceptable risk or harm.

Security: The combination of availability, confidentiality and integrity. It can be defined as the preservation of the availability, access to, confidentiality and integrity of information.

Validity: Used to describe a measurement that reflects what is intended to be measured.