



eHealth and Patient Safety

A Position Paper

Prepared by the Patients' and Citizens Task Force, EHTEL

Page intentionally left blank for recto/verso printing

eHealth and Patient Safety

A Position Paper

Prepared by the Patients' and Citizens Task Force
of the
European Health Telematics Association (EHTEL)

Contributors to this paper were:

Angelica Frithiof
Rod Mitchell, IAPO
Nicola Bedlington, European Patients Forum
Harm Jan Roelants
Jean Luc Bernard, Le CISS
Johan Hjertqvist
David Garwood

Preface

In ideal world, the patient would be in total control of the healthcare that he or she receives and take decisions regarding the way in which they are treated. In reality they can only do this with the support of professionals and with the provision of accurate and timely information. Given that we do not live in a perfect world and that professional time is both expensive and limited, patients increasingly rely on peer support groups to advise them.

It is against this background that EHTEL's Patient and Citizens Task Force was established. It is a unique group within the European eHealth community consisting of individuals who are patients in their own right or who represent patient groups but who are also highly qualified from a strategic, technical and managerial perspective within health and medical informatics. At the highest level, it has two main aims: to influence other stakeholders in the ICT and healthcare areas and to empower other patient groups.

Currently, most discussion about the development of eHealth systems happens between the developers and national institutions while there is very little interaction between those organisations and the patient. A key role for the Group is therefore to provide a forum to canvass patient opinion and to communicate these views to the stakeholders described above.

Roles for the Group

The Task Force has two audiences for its work: the key stakeholders in the eHealth/ICT community such as developers and national institutions and, separately, patient organisations. In broad terms, the Task Force has a number of roles to perform in relation to each of these audiences as described below:

A vital activity for the Task Force is in ensuring that stakeholders such as politicians, national health authorities, professional medical and nursing groups and also system developers are made aware of the patient position in relation to eHealth. There is a common feeling that, "we're all patients anyway so we understand the patient view". This is a typical reaction from most national stakeholders and the fact that it is promoted demonstrates a clear misunderstanding of what a patient is and what his/or her view on a particular issue is likely to be. It is commonly used to circumvent the patient view.

Firstly, we are **not** all patients. The vast majority of people are fit and well and go through life as healthy **citizens** who occasionally fall ill and, temporarily, become patients. Others may suffer from chronic diseases or conditions that do place them in the position of being both citizens and patients throughout their lives. Views and opinions offered on the delivery of healthcare by healthy citizens will be very different from those offered by the same individuals when they are undergoing treatment.

It is important therefore that constant and ongoing patient orientated issues are available to policy makers and others in order to ensure that important decisions encompass the needs and requirements of the patient. For eHealth to succeed, acceptance by patients – both short and long term – is vitally important.

Thus the Task force seeks to interact with the national stakeholders across the European Union either directly or by encouraging the involvement of patient organisations in the decision making process. It can do this in two ways: by providing consultancy services to stakeholder groups and by producing position papers that address the many different aspects of eHealth development.

To some degree the issues raised in this paper can be viewed as a “wish list”. However, we view them as an important starting point in the identification of matters that require further investigation and development. They now need to be moved forward either as formal programmes of work or through political lobbying. It is important to note that the views in this paper are not “set in stone” and will be revisited over time to ensure that they accurately reflect changes in the delivery of healthcare and the management of related information.

It is in this context that the following position paper has been prepared.

A Summary of Our Position

Our position in relation to patient safety and eHealth information systems can be summarised as follows:

- We endorse the general principles of the Luxembourg Declaration on Patient Safety although we believe that it does not refer to information systems in sufficient detail.
- All commercially marketed eHealth information systems should be subjected to rigorous and independent safety testing before being deployed for the management of patient care. This activity should be driven by the European Commission.
- All staff operating eHealth information systems should be properly trained in their use.
- We endorse the development of hardware, software and data standards as applied to healthcare information and believe that work should be undertaken by the European Commission to promote consistency across the Union.
- All organisation involved with healthcare information systems should implement incident reporting procedures in line with international standards. Further technology should be exploited to allow patients to contribute to these schemes and to receive appropriate training in their use.
- All eHealth information systems should have properly implemented and managed audit trails
- National health technical infrastructures should be exploited to promote warnings for patients and professionals alike.
- Marking and other schemes should be developed to indicate good quality information sites on the Internet and World Wide Web
- National health technical infrastructures should be exploited to help in the identification of *bona fide* healthcare professionals

Introduction

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 that 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.

Information systems now pervade the healthcare system and these are being developed at a local, national and international (European) levels. Regardless of where these systems are developed, three key issues remain unaffected: patients have the same problems, the demands on the healthcare system continue to increase and the principles against which information is managed increase in complexity.

In view of the extent to which information systems are used in the field of healthcare (and, indeed, everywhere else) they have become accepted as a normal part of the consultation, treatment and associated processes. This familiarity has brought with it an implicit trust in the operation of the systems ie the information they provide is taken to be accurate.

However, there is significant potential for these systems to contribute to patient harm either because they lack integrity (are not operating correctly) are not operated correctly or are not available at critical times. In this paper we set out our position in relation to information systems and patient safety.

The Luxembourg Declaration – Patient Safety – Making it Happen!

During the course of our discussions, we have had due regard to the Luxembourg Declaration on Patient Safety¹. We have referenced it throughout this document as we are generally supportive of its provisions although in some areas we do not believe that it covers adequately eHealth information systems as a specific issue. We are particularly concerned that the testing of information systems does not match the stringent requirements for medical equipment and see this as a significant omission.

Ensuring the Security of eHealth Information Systems

Information systems security is most often taken to refer to the confidentiality of the personal medical record and the measures taken to protect it. In this regard we have set out our position in relation to the electronic health record in a separate position paper². In fact, the accepted definition of security in this context is much wider and includes:

- Integrity: Ensuring that systems are operating correctly and to specification or, more generally operating in the way we expect them to operate
- Availability: The systems are available when and where they are required

Both of the above elements have a significant part to play in the efforts to promote and deliver patient safety.

eHealth information systems are utilised in nearly all aspects of healthcare. Their application includes the maintenance of the electronic health record, management of patient flow and monitoring of vital signs. Any malfunction or programming error that corrupts the information they are processing about a patient can have serious consequences for the individual.

For example, it is possible to envisage an IT application that may process the results of pathology tests. Any malfunction leading to corruption of data could result in either a false positive or false negative result. A false positive is bad enough as it could result in unnecessary treatment (leading, in some cases to lasting damage) and undue worry for the patient. A false negative, however, could lead to the patient not receiving treatment for a possibly serious condition or, at least, having that treatment delayed.

In terms of information not being available as a result of a system or network failure, the possibility exists for incorrect treatment to be given or for the patient to be prescribed drugs to which they have an allergy. This could be the result if the responsible clinician was not able to pick up the relevant markers from the electronic record. In making this point we recognise that basic medical procedures are designed to minimise this possibility but we also recognise the increasing complexity of information systems and the reliance we now place on them. We also note that the Luxembourg Declaration identifies the potential for medication errors.

An issue for the Task Force is that, unlike medical equipment/devices eHealth information systems are not subjected to rigorous and independent testing. Indeed, it is theoretically possible for anyone to write a suite of programs one week and have it implemented in the clinical environment the next. Our position in this regard is that we believe the European Commission should give active consideration to the introduction of such testing across the Union and to initiate work to determine what the testing standards should be.

Legislating for such testing will not be straightforward as each software upgrade would need to be certified leading to delays in implementation and some commercial losses. In addition, it is fairly common practice for individual clinicians and other people to construct their own personal databases on which they rely on to assist in research, treatment, monitoring and

tracking. However, there are recognised eHealth systems implemented internationally that can be identified and could be included in a program of testing.

With regard to testing of eHealth systems we have noted the provision in the Luxembourg Declaration that recommends to the EU Institutions, “to ensure that EU regulations with regard to medical goods and related services are designed with patient safety in mind”. It is not clear whether this section was intended to cover information systems. We suspect not but believe that the Declaration should have specifically covered this issue.

Education and Training in the Use of eHealth Systems

Information safety and security professionals constantly promote the idea that the largest threats come from people. In healthcare institutions, this translates into the staff that use systems that have a potential to impact on patient safety.

A key measure to minimise the risk of mistakes occurring is to ensure that all such staff (at whatever level) receive appropriate and professional training in the use of those systems. This should include a system of accreditation that includes regular refreshes and reflects the different systems operated by the individual(s) concerned. Our position is that this should become a mandatory condition before anyone is allowed to use the systems.

The Importance of Standards

Increasingly, the care and treatment of patients is shared across a community of clinical staff in the primary, secondary and tertiary sectors. Each group is supported by a variety of eHealth systems to assist in the process. It is therefore important that information about an individual or group of patients can flow seamlessly between these groups and across the patient pathway. In the future, we believe and support the view that such pathways will increase in size and will cross European and wider borders.

Access to accurate and complete information about the patient has a major bearing on their safety and it is important therefore that there should be no technical obstructions in terms of hardware, software or data. In order for this effective information flow and sharing to be achieved it is vital that systems are designed to conform to recognised international standards.

We recognise that an enormous amount of work has already been undertaken in the development of such standards including CEN. Our position is to endorse this work and to encourage national authorities to consider the implications of emerging cross-border flows of patients. In other words we believe that work needs to be undertaken to ensure that the standards adopted in one Member State are also utilised in the others.

Incident Reporting

A key element in promoting patient safety is the establishment of incident reporting systems. This is the process whereby any problems arising from the operation of eHealth information systems is recorded and, more importantly, responded to. Key characteristics of an incident

reporting system have been described by the UK Cabinet Office (Central Sponsor for Information Assurance)³ as:

- The process of responding to an incident, including the process of learning from the event in order to reduce the risk of re-occurrence.
- The process of monitoring internal and external sources of information in order to pre-empt incidents, by learning from events affecting others.
- Ensuring that effective incident detection and reporting mechanisms exist, so that incidents affecting information security do not go unnoticed and unmanaged.

Our position as patient representatives is that all organisations operating information systems that could impact upon the safety of the patient should establish appropriate incident reporting procedures. We further believe that these should be developed against the formal standards established by ISO/IEC 17799 (Code of Practice for Information Security Management), and ISO/IEC TR 18044 (Information Technology. Security Techniques. Information Security Incident Management).

Patients have a role to play in contributing to the reporting of incidents (providing that they are appropriately trained) as they are often affected by them. We believe that opportunities exist to exploit IT infrastructures, including the Internet, in order to report problems. It is important that incident reporting is operated on a “no blame” basis as we feel that this will encourage more openness – and thus encourage more citizens to participate - in the reporting process.

Audit Trails

Closely tied to (and supporting) the issue of incident reporting is to ensure that all information systems have suitable audit trails in order to identify who has been interacting with them and for what purpose. Such audit trails should be regularly monitored and include logs to demonstrate that action has been taken to correct any problems.

From a patient’s perspective, such facilities provides them with confidence that, in the event of problems arising in terms of misdiagnosis or misprescribing, that the individual responsible can be held to account. It further ensures that records cannot be amended to misrepresent a particular incident.

Alert Broadcasts

The development of national technical infrastructures brings many opportunities to transform the way in which information is disseminated to health professionals and, indeed, the public. In recent times, there have been examples of health scares such as avian ‘flu that have left members of the public concerned about whether they should be taking any action and what that action should be. We believe that there is an opportunity to include patient support organisations in any alert broadcasting as they can have an important role in disseminating information and advising/supporting their members.

Additionally, there is clinical information, notably about problems with specific drugs and appliances that health care professionals need to have fast and accurate access to. Our position is that we believe national health technical infrastructures should be fully exploited to provide support to both patients and professionals alike.

Quality of Information on the Internet and the World Wide Web

Either through necessity or through a basic desire on the part of patients to better understand and contribute to their own treatment, the Internet has become a valuable resource. The Net has brought a wealth of information to the patient's own home and provides a welcome facility to research aspects of medication and alternative management strategies. Indeed, the patient can often have more time to spend on this issue than a pressured and time-limited professional.

Increased availability of information provides the patient with empowerment and more control. It is also leading to the increased sharing of information within patient support groups and the development of coping strategies supported by other patients. As the Luxembourg Declaration acknowledges, "informed patients are well positioned to safeguard their own health"

Thus the concept of the "informed patient" is one that needs to infiltrate the existing consultation and treatment regime. The views of the patient need to be listened to and respected although it is recognised that this will have an effect on the time available for the consultation process.

It is also a fact that some patients seek to obtain their own medication from the growing number of "pharmacies" now appearing on the Internet. The Task Force does not endorse this practice recognising the serious dangers and potential harm that could arise from self-medication. Its position is, however, that if patients are seeking to follow this course of action, then research is required to understand why they choose to do so.

Whilst increased involvement of the patient in the management of their condition is to be welcomed, it is recognised that they are not medically qualified practitioners. Thus the potential for misinterpretation and, in the case of self medication and some alternative therapies, personal harm is obviously present. However, self management and treatment is likely to increase. Thus, in the future, work needs to be undertaken to provide advice and guidance to patients about options, sources of information and the potential constraints and dangers of self-managed regimes. In turn, further research and work is required in developing quality control for information sources, particularly on the Internet, and, if necessary, in the supply of medicines. In this regard, the Task Force recognises the work of the European Commission in relation to improving and marking the quality of web sites providing health related information.

Health Professional Identification

It is vitally important that patients can have confidence that they are being treated by appropriately qualified professional staff. The responsibility for ensuring this rests with national authorities who work with professional organisations in terms of establishing the required qualifications and registration processes. With the expansion of the European Union and the increased movement of professional staff across the globe, this process of management has become more complex.

As with other areas mentioned earlier, we believe that the technical infrastructures being developed for eHealth including widespread networking could be exploited to support the process of identifying *bona fide* healthcare professionals. We would also wish to see such “electronic registers” being available to patients in order to increase their confidence regarding treatment and consultation.

Conclusion

As a Group we believe that eHealth has an important role to play in improving and enhancing patient safety. Potential areas requiring more investigation with specific reference to this aspect of eHealth include:

- Reducing the potential for medication errors, including sophisticated contra-indication software
- Assisting in the detection of counterfeit drugs
- Addressing cross border issues surrounding access to the patient's electronic health record regardless of geographical location
- Increasing potential for communication between health professionals and partner organisations involved in episodes of care
- Assisting in the identification of *bona fide* health professionals
- Enhanced monitoring of patients in the home environment
- Reducing the potential for transcription errors through the electronic transfer of information
- Encouraging more open communication between patient and clinician through electronic facilities
- Increased communication of consent for matters such as organ donation
- Increased potential for education and training for both patients and professional staff. This might include more information regarding preventative health

References

1. Patient Safety – Making it Happen, European Commission, Luxembourg, 5 April 2005
2. The Electronic Health Record, EHTEL Patient and Citizens Task Force, July 2006
3. http://www.cabinetoffice.gov.uk/csia/ia_governance/incident.asp (accessed 7 July 2006)

EHTEL

EUROPEAN HEALTH TELEMATICS ASSOCIATION

EHTEL Association,

M.E.P.S.
50, rue d'Arlon B-1000
Brussels
Belgium
Tel: +32 (0)2 230 96 50
Fax: +32 (0)2 230 77 73
info@ethel.org
www.ethel.org

