

A Framework for Dealing with Legal and Clinical Risks Arising from the Use of m-Health Systems

*Homer Papadopoulos, Dimitra Pappa, Lefteris Gortzis**

Division of Applied Technologies, National Center for Scientific Research “Demokritos”, Agia Paraskevi, Athens, and * Medical Physics Laboratory, Department of Medical School, University of Patras, Greece.

ABSTRACT

Objectives: The shift of telemedicine from desktop platforms to wireless and mobile technologies is likely to have a significant impact on healthcare in the future. Safety is a fundamental factor that must be taken into account during the design and use of mobile healthcare systems. In this paper we propose a framework for dealing with the risks associated with mobile health (m-health).

Methods: Information was gathered from a variety of sources including three research projects we have participated in, surveys with relevant stakeholders and a literature survey. The information was used to formulate a framework to address the clinical and legal risks that can arise from the application of mobile healthcare services. Key factors taken into consideration when formulating the framework were the behaviour of healthcare practitioners in a mobile setting, the management of supporting medical information and data and the effect of the operating environment (context).

Results: Our proposed framework encompasses three levels that correlate with each other. Level 1 deals with human issues, level 2 with the delivery of healthcare in a mobile environment and level 3 with issues related to the technology failing or performing unreliably. Key factors related to each of these levels are discussed in detail.

Conclusions: A guideline has been proposed for classifying the practical issues related to the legal and clinical risk management issues of mobile health systems. The framework takes into consideration the responsibilities of all stakeholders (patients, clinicians, healthcare organisations, etc) and the inter-relationship between risks. It also recognises the need for flexibility when addressing the legal and clinical risks arising from the provision of mobile healthcare services.

INTRODUCTION

The development of portable and wireless technologies that enable mobile healthcare is perceived to have considerable benefits in the future for both patients and healthcare professionals. Much of the previous research has focused on using mobile technology in a fixed environment e.g. a patient’s home^{1,2}, with the proposal of

Correspondence and reprint requests: Homer Papadopoulos, MBA, PhD, Division of Applied Technologies, National Center for Scientific Research “Demokritos”, Agia Paraskevi 153-10, Athens, Greece. E-mail: homerpap@dat.demokritos.gr.

frameworks to evaluate different aspects of Health Informatics and Information Systems within an organisational environment³⁻⁵. Very little of the research or the literature considers the interaction of people and technology in public areas.

Bringing healthcare technologies beyond the desktop to the public world, in everyday settings, has created an ever-increasing interest in how healthcare professionals and patients interact with the physical environment, and the relationship of the physical environment to technology⁶. Work to improve understanding of the role of computers in co-operative work and enhancing mobility has emphasised the importance of understanding the connections between places, the role of space and time and the use of technology. Mobile telecommunication technologies have presented themselves as a powerful tool to break the barriers of time and space⁷. The benefits of these technologies can be illustrated in a number of different scenarios. For example patient information can be obtained wirelessly by healthcare professionals from anywhere⁷, or handheld devices can be used by patients at home to improve the management of their diabetes through more effective monitoring⁸.

Increasing adoption of technology to support mobile healthcare systems inevitably creates safety issues. Consideration must be given to the likelihood and risks associated with possible failure of the technology and also the level of services expected to provide a safe and reliable level of care. In particular with users (both physicians and patients), free to roam and to utilise a variety of different devices, issues arise due to the inherent risks and limitations of the mobile environment and the need for healthcare practitioners to adopt it as part of their working practice⁷. Consequently if mobile health (m-health) is to have a significant impact on healthcare delivery⁹, it is fundamentally important to develop a framework dealing with how inherent risks should be addressed and managed.

Any framework should embrace a concrete set of procedures, backed by appropriate policy measures, so as to guarantee that all risks associated with an action recommended by an autonomous m-health system are controlled and that the health and safety of patients are not compromised¹⁰. This framework should classify new stakeholders' responsibilities supporting in parallel the need for an "official" standard with clear rules regarding operational procedures and negligence, fraud, abuse etc.

This paper explores the legal and clinical risks associated with the use of mobile systems to support healthcare, focusing on consideration of the limitations and inherent risks of information and communication infrastructures¹¹⁻¹³. The proposed framework is based on a variety of information sources and aims to provide guidance on how legal and clinical risk should be addressed and managed when medical services are delivered using mobile technology.

METHODS

For our proposed framework we collected data from different sources and applied a variety of research methods. Data sources included information derived from

three research and development projects we participated in¹⁴⁻¹⁶, surveys with relevant stakeholders, and a literature review targeting both technological and medical application issues. This combined approach revealed areas of potential interest in m-health that have not been covered in detail by previous or ongoing studies, e.g. the effect of operational context on healthcare delivery.

The projects provided us with valuable insight on user acceptance, problems with and trust in m-health systems. The semi-structured interviews with key stakeholders (n = 30), incorporated evaluation of the services offered, positive and negative experiences of usage and suggestions for improving m-health services.

RESULTS

Our proposed framework encompasses three levels that correlate with each other (Figure 1). The issues of risk can be broadly segregated into human issues and technological issues, although in reality they are very closely linked.

Level 1 is the fundamental level and deals with risks related to human issues, i.e. external factors that affect the way mobile-services are used.

Level 2 deals with the issues associated with using mobile technology to support healthcare.

Level 3 deals with the risks of the technology failing or not performing reliably.

Some of these risks can be managed by complementary services providing elements of care that remote services are unable to provide, e.g. domiciliary visits to assist with bathing. Technology can help to manage other risks, for instance by

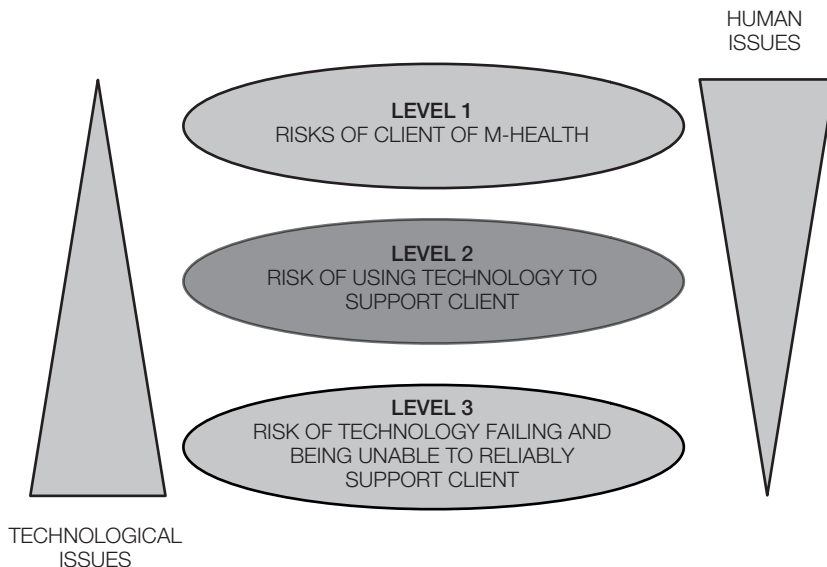


Figure 1. Risks in m-health

including elements of m-health which can both increase the user's confidence and can ensure that problems are automatically identified, allowing for intervention by a remote physician before a major problem occurs. However, m-health itself increases the range of safety issues which must be considered if a client who does require a particular level of care is supported anywhere through the use of mobile technologies (Level 2 in figure 1). More often than not, the technology implemented within a mobile system acts to reduce the risk associated with a particular identified hazard. Consequently, the failure of any device or sub-system associated with the management of risk will have an impact on the ability of the mobile system as a whole to successfully control that risk and therefore its associated hazard (level 3).

DISCUSSION

The proposed model was explored in interviews with eight experienced doctors (including the head of the department) of the Telemedicine unit of Sotiria Hospital in Athens. The interviews were designed to assess their attitude to healthcare delivery in "mobile" environments, and to highlight any intrinsic risk management issues they perceived, taking into account issues in the proposed three level model. Some of these important issues will now be elaborated on.

Risks for Clients of m-Health

An important feature of m-health is that any place can potentially become a remote point of care. This can range from a medical building, e.g. a GP surgery, to an isolated area, such as a forest or mountain. This context is an important variable that must be taken into account when examining the quality of a medical service, and medical experts must take into consideration the context within which medical services are to be delivered. These include:

- The physical environment
- Convenience and accessibility of supporting services
- Appropriateness and timeliness of the whole episode of care

When providing medical care remotely or on the move, risks may emerge due to the fact that care is taking place outside the controlled and protected environment of a medical institution, e.g. a hospital. This requires special provisions to manage environmental risks associated with the absence of medical supervision and the typical care provided in a medical establishment.

Risks of Using Technology to Support Clients

A qualified, practising healthcare professional must possess the necessary knowledge and skills to perform specific medical tasks. The professional responsibility of an individual medical practitioner is critical. By law health professionals are required to exercise the care and skill of a reasonable professional and achieve a "standard of

care". This standard of care is not that of the "best" or most experienced specialist, but of a reasonable specialist. Failing to deliver care to an adequate standard can be considered as negligence. The provision of m-health introduces new risks associated with the inherent complexity of mobile telemedicine services. In the case of technology-assisted care provision, in addition to possessing the necessary medical qualifications, professionals must also have a certain degree of knowledge and skill to enable them to use the technology safely and effectively, e.g. the ability to operate portable medical devices and to use communication devices to transmit or receive information. Although it is generally agreed that all healthcare workers need to be trained in the use of modern healthcare technologies and be aware of the technical limitations that such systems place upon their work, setting a qualification standard for ICT (Information and Communication Technology)-knowledgeable healthcare professionals is a major hurdle. Nevertheless, whenever healthcare professionals make a clinical judgment using mobile systems, they must be satisfied that they have sufficient information to form a judgment and that the information itself is of adequate quality and reliability. If they fail to do this, errors and patient harm may occur.

The impact of m-health is also likely to strongly affect the way doctors and patients interact and lead to the development of 'expert patients', e.g. patients who initiate medication based on remote consultation. In this respect clients of m-health services play a more active role in clinical procedures. They must consequently be properly trained to safely use m-health appliances and understand related technology issues.

Risks of Technology Failing or Being Unable to Reliably Support the Client

The flawless operation of the underlying technical infrastructure is critical to the success of m-health. Quality end-to-end communication and the effective management of information emerge as important challenges.

When medical practitioners and patients are able to roam freely and to utilise different access devices, in terms of both display and processing capabilities and communication characteristics, new problems arise. These include the delivery of information from a variety of sources and in a multitude of formats (ranging from plain messages to multimedia content) in a secure and reliable way. For a successful m-health service, handling of supporting information from monitoring devices, healthcare databases, wireless communication networks and access devices, is essential.

Expert knowledge is also usually required to complement medical information and clinical data. Behavioural/tacit knowledge assets often represent a critical element for medical practice, which can only be mobilised by promoting connectivity among people to facilitate the exchange of individual knowledge and/or experiences. For example, mobile healthcare practitioners, apart from accessing information, often rely on communication with their peers (e.g. to get a second opinion) or with

field experts (e.g. to seek expert advice and guidance) for making medical decisions. Similarly the communication between doctors and patients is increasingly mediated by communication technologies.

The most crucial aspects of the risk of technology failure are:

Communication Networks

The variety and complexity of m-health application scenarios calls for the combined use of wireless technologies (both short- and long-range), wired communication backbones and the Internet in a seamless, secure and reliable way. The employed wireless technologies include Bluetooth, wLAN (wireless local area network), WiFi (wireless fidelity), GSM/GPRS (Global System for Mobile Communication/General Packet Radio Service), UMTS (Universal Mobile Telecommunication System) and satellite communications. Difficulty in achieving operational compatibility between telecommunication networks, terminals and devices continues to be a challenge for m-health applications.

Although high-speed digital communication infrastructures are becoming more widespread, it is often the case that the regions that would benefit the most from electronically delivered healthcare are mostly underserved in terms of telecommunication capabilities. High speed communication networks are still far from being a reality in many remote rural areas in Europe. This limits the options for telemedicine since services can only function well if specific communication criteria are met. Many telehealth applications rely on high-speed broadband IP (internet protocol) networks to deliver high quality, timely and converged voice, video, and data. In many cases ensuring end-to-end quality of service remains an unresolved issue.

Access Devices

M-health employs a multitude of access devices, both wired and wireless, such as portable PCs, cellular phones, Personal Digital Assistants (PDAs), etc. Each one of these appliances has its own limitations in terms of screen size, processor power, memory, and bandwidth and battery life. The service capabilities of the device are determined by these characteristics. Clinicians should be particularly aware of the limitations of the access devices employed, the amount of information they can provide and how well they can display it. One important aspect to this are the limitations of screen sizes particularly for digital images. These are an essential component in many telemedicine applications, e.g. teleradiology, teledermatology and telepathology. The technologies currently available provide excellent pixel density and resolution with a high rate of diagnostic agreement demonstrated between digital and real images. However clinical risk exists of a wrong or missed diagnosis being made on the basis of a digital image which lacks sufficient detail or because an image is altered or corrupted due to technical reasons. Clinicians involved in making a diagnosis or a decision based on a transmitted image, should be aware of this underlying risk¹⁷. This risk may be diminished by medical equipment manufactures adopting and adhering to standards such

as DICOM (Digital Imaging and Communication in Medicine) for transmitting images.

Monitoring Devices

Much effort is being devoted to the development of portable and networked devices for the measurement and monitoring of patient vital-signs. With the help of pervasive and wearable technologies, critical health parameters for acutely ill patients can be measured, stored and transmitted to a database. These processes can also be performed for patients with chronic illnesses on a daily or frequent basis. Wireless Body Area Networks (WBAN) represent an important step in the evolution of monitoring devices. They consist of lightweight and small size sensor platforms that allow for the continuous monitoring of multiple parameters in ambulatory settings.

Unification of Information Sources

Ideally, the entire medical profile of a patient (medical history, current medications, results of laboratory tests, etc.) should be retrievable at the point-of-care at the touch of a button. In practice, an individual patient's data is not held centrally, and is distributed through different organisations which are diverse and heterogeneous in terms of their content and database implementations. This makes access to and retrieval of data from repositories a major problem. Consequently one of the major challenges for mobile health applications is the integration and exploitation of heterogeneous information databases in a seamless way, so as to enable the storage, updating, search and retrieval of all relevant patient information.

The effective employment and exploitation of structured information requires cross mapping and standardisation of the different coding schemes and medical terminologies used in the healthcare sector. Semantic representations can help the process of converting data into different formats, thus helping the understanding and effective analysis of this information.

In many cases, access to medical information or the exchange of data among healthcare providers is hindered due to the non-interoperability of the different information systems in place. Overcoming this barrier requires the adoption of common standards or the development of communication interfaces. A particularly important factor is the creation of standardised Electronic Health Records (EHRs). These will enable the recording of patient data in a commonly agreed format, and thus enable easy communication of patient information between service providers and/or applications.

Table 1. summarises critical issues related to the above mentioned factors, which represent potential sources of risk for the provision of mobile care.

Table 1. *Risks Associated with the Provision of Supporting Information in m-Health Environments*

Factor	Description	Critical Issues
Monitoring devices	On location measurement and monitoring of vital signs of the patient (portable devices, pervasive and wearable technologies)	<ul style="list-style-type: none"> – Reliability of measurement – Product liability – Configuration: setting levels of alert
Information sources	<ul style="list-style-type: none"> – Patient related information: medical profile, results of clinical examination etc. (medical records) – Medical literature – Pharmaceutical information etc. 	<p>Storage, updating, search and retrieval of useful information is hindered by the lack of unification of information sources:</p> <ul style="list-style-type: none"> – Multiple and geographically dispersed repositories – Heterogeneous data (in terms of format, coding scheme, etc.) – Non-interoperable information systems
Communication networks and access devices	<p>Enabling access to information and remote collaboration among healthcare practitioners.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> – Seamless integration of underlying communication infrastructures. – End-to-end secure and reliable communication 	<p>Service capabilities conditioned by:</p> <ul style="list-style-type: none"> – The existence of underserved regions in terms of telecommunication capabilities – The inherent differences of communication technologies (transmission rates, on-demand linkage or permanent connection etc.) – The limitations of the access devices (screen size, processor power, memory and bandwidth, battery life, etc.)

Security and Confidentiality

Healthcare deals with sensitive issues and protection of individual patients’ data is mandatory. Harm may result from unauthorised access or interception of a patient’s medical information and in some cases this may be comparable to harm caused by an erroneous medical decision. It is consequently of paramount importance that the security and confidentiality of medical information is preserved during the entire life-cycle of healthcare, regardless of the communication environment. Given the heterogeneous nature of the communication technologies employed to support m-health (whether individually or in combination), maintaining a high level of security is still a challenge for modern ICT. Critical security hazards include:

- Physical security and computer systems security, for example what happens if a computer storing patient data is lost or stolen.
- Network security issues concerning the safety of data transmitted through satellites, wireless networks, etc.

It is evident that quality considerations should be at the centre of all activities that relate to the planning of telemedicine health systems, both mobile and fixed,

in order to ensure a high level of patient care. Regardless of the means and/or the channels employed for healthcare provision, established standards of care must be attained at all times. Patients have the right to quality healthcare, whether this is delivered face-to-face or by means of modern ICT technologies. Using m-health systems need not necessarily expose patients in remote areas, such as onboard a ship or airplane, to greater risk than occurs with an ordinary face-to-face consultation. Service quality is the responsibility of both healthcare professionals and administrators of healthcare organisations. Healthcare professionals are responsible for their professional practice, whilst management is accountable for the safety and quality of services offered by the organisation.

Due to the complexity of the operating environment, a strong risk management and quality assurance system is required. These should ensure that there are:

- Concrete **lines of action** and **response procedures** for the provision of care over networked environments
- Clear lines of **responsibility** and **accountability** for the overall quality of clinical care
- Comprehensive programs of **quality improvement** activities
- Clear policies aimed at **monitoring performance**
- Clear procedures for **identifying** and **managing risks**, to which the patients may be exposed
- Procedures for all professional groups to identify and **remedy poor performance**
- Accurate and sufficiently detailed **clinical records** of all m-health activities, both to document care delivered and mitigate against potential lawsuits

The most important factors that should be taken into consideration, when aiming for quality healthcare delivery at remote locations or on the move, are the following:

Quality Assurance

This comprises the healthcare personnel's ability to provide telemedicine services (level 2) and the capability of the medical and telecommunication systems to provide critical medical data (level 3).

Modern healthcare services constitute integrated processes that span functions and clinical specialisations and also involve different health services providers. Central to the process of ensuring quality is to define and guide the implementation of a quality policy with clear objectives and real action procedures. To this end, it is necessary to:

- Prepare working instructions and clinical guidelines to assist healthcare practitioners in their decision making process for the care services to be provided. These should take into account both specific health issues and specific clinical circumstances.

- Prepare working instructions for and provide training to consumers of health-care services if a particular service requires their active involvement in the process.
- Ensure that any available and relevant clinical standards and recommendations for telemedicine are implemented in mobile-health systems.
- Ensure that all medical staff involved in the provision of m-health services are properly trained and participate in quality assurance and risk management initiatives.
- Ensure that appropriate organisational and technical measures are put in place to protect patient information against improper or unauthorised disclosure.
- Ensure that accurate and sufficiently detailed clinical records are kept of every service provided.
- Ensure that medical practice is taking place within an environment that is safe and meets the standards for healthcare provision.

Responsibility and Accountability

This is an issue of particular interest to healthcare personnel (level 2) that use the technology to support the client. Concrete programmes of care should be in place, encompassing all healthcare activities to be performed for patients by healthcare providers¹⁸. Clear roles and responsibilities should be defined for each member of staff involved in healthcare processes. Medical practitioners providing m-health services should act within the limits of their expertise and should not attempt to provide advice if they are not in a position to form a sound clinical judgment due to technological or other reasons. To complement this, recording and documentation should provide a traceable history of the services provided, the times, dates and persons that provided advice, treatment, medication or other services and the outcomes of these services. Healthcare records should serve as:

- Evidence that services were provided in accordance with defined guidelines
- A source of information when dealing with any adverse incident or patient complaint arising from use of m-health services

Risk Management

Risk management provisions are required for all three levels of the proposed model. Risk management is critical to any health service and is best achieved through an integrated process approach. This is of particular importance in the case of m-health, due to its inherent complexity and the fact that it is the result of multidisciplinary collaboration. Effective risk management should identify the risks to which the patient is exposed and put in place procedures to regularly monitor, assess and minimise or remove those risks. The ability of the ICT infrastructure (computer software, monitoring and communication appliances, etc.) to satisfy the intended application needs to be confirmed. Patient specific risk assessment should be performed to identify possible adverse events or reactions that may arise as a result of patients

performing a procedure, using equipment, administering drugs, etc. and planning should be customised to ensure that steps are taken to mitigate specific risks.

Performance Monitoring and Poor Performance Remediation

Identifying and remedying poor performance should be achieved through regular audits and the provision for submission of feedback from all parties (level 1 and 2) within the m-health service. Continual performance improvement is a fundamental requirement for all healthcare organisations. To some extent this can be achieved by remaining up to date and implementing new technology as it becomes available. However considerable quality improvements can also result from acting on knowledge gained from past experience, and particularly from adverse events. To this end, once m-health services are established, processes should be put in place to:

- Identify all adverse events that occur.
- Create a scheme for the reporting and investigation of adverse events.
- Establish a procedure for making complaints which is easily accessible to patients who have been treated using the mobile-health system and/or their representatives. This procedure must also be fair to the medical practitioners providing care through the system.
- Identify and remedy poor performance by medical practitioners at an early stage.

Putting in place procedures and information systems for collecting feedback, provides a sound basis for corrective actions and serves the concept of continual improvement. Reporting of incidents requires a non-judgemental and non-punitive attitude towards medical staff if their co-operation is to be achieved¹⁹⁻²⁰.

Security and Confidentiality

One particularly important issue that permeates all m-health services is security and confidentiality. The complex, sensitive and critical nature of healthcare introduces serious security considerations. Mechanisms, policies and procedures are necessary to protect data confidentiality and integrity in each and every step of the information management process: storage and updating, search and retrieval, data transmission, etc. Access rights to patient records and other private information should be strictly regulated and different healthcare professionals (general practitioners, specialists, care team, pharmacy) should have controlled access to this information and safe transmission of personal data should be ensured²¹. Provisions must be made for guaranteeing security of electronically transmitted information including protection of the data exchanged over the network and authentication of remote users. In addition, any use that may be made of any electronic medical record or any other personally identifiable health information about individuals should have the fully informed consent of patients, who should also have the right to know if such information exists and to review it. Since the doctor-patient relationship is bound by trust, any concerns about patient consent, security, confidentiality and ethics must

be taken into account when documenting m-health services, e.g. when making recordings of teleconsultations.

Finally when considering the design of an m-health system, important safety issues that should be considered include:

- The safety of the client
- The safety of the physicians, both formal and informal
- The safety of the premises
- The safety of the immediate community
- The safety and reliability of the equipment

In our framework, risks that are inherent to m-health applications have been categorised into three levels. In our opinion this is not a strict framework, since there are considerable overlaps between categories and often for a specific application scenario, risks that permeate all three levels are present. Consequently defining clear boundaries is a difficult task. Within this framework, the need for flexibility in the provision of m-health services to individual patients, conflicts with the requirements for stability and concrete action procedures for quality assurance. A clinician's individual perception of risks is an important factor when implementing quality management procedures. Healthcare professionals need flexibility to exercise their judgment and deviate from standard care whenever they consider this to be to the benefit of the patient.

In the light of the above, the successful management of hazards to clinical performance calls for a flexible quality model, one that is based on a holistic approach to the investigation of potential risks and whose impact is best achieved through an integrated process approach.

CONCLUSION

We have proposed a practical framework for dealing with the legal and risk management issues associated with the provision of mobile healthcare services. The planning of any m-health service should take into account issues such as quality assurance, responsibility and accountability, risk management, performance monitoring, and security and confidentiality. It must however be appreciated that although most quality management approaches are based on stable, rigid actions and procedures, the provision of healthcare services necessitates flexibility. Consequently, the quality model should be flexible and based on a holistic consideration of potential risks.

Further research is required into quality management activities as well as risk assessment for mobile healthcare services. In addition further research is also needed to address the link between the quality of medical services and the context in which healthcare takes place.

ACKNOWLEDGMENT

The authors wish to thank the participants of the European Research and Development projects MEDASHIP, EMISPHER and GALENOS, as the work performed in these projects provided valuable insight into some of the issues addressed in this paper.

REFERENCES

- 1 Davis FD. Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly* 1989; **13**: 319–40.
- 2 Venkatesh V, Davis FD. A Model of the antecedents of perceived ease of use: development and test. *Decision Sciences* 1996; **27**: 451–81.
- 3 Kaplan B. Organizational evaluation of medical information resources. In: *Evaluation Methods in Medical Informatics*, Friedman CP, Wyatt, JC, eds., New York: Springer-Verlag, 1997, pp. 255–80.
- 4 Grant A, Plante I, Leblanc F. The TEAM methodology for the evaluation of information systems in biomedicine. *Computers in Biology and Medicine* 2002; **32**: 195–207.
- 5 Shaw NT. 'CHEATS': a generic information communication technology (ICT) evaluation framework. *Computers in Biology and Medicine* 2002; **32**: 209–20.
- 6 Moran TP. Context-aware computing. *Human Computer Interaction* 2001; **16**: 87–96.
- 7 Tachakra S, Wang XH, Istepanian RSH, Song YH. Mobile e-health: the unwired evolution of telemedicine. *Telemedicine Journal and e-Health*, 2003; **9**: 247–57.
- 8 Istepanian RSH, Jovanov E, Zhang YT. Beyond seamless mobility and global wireless health-care connectivity. *Information Technology in Biomedicine*, IEEE, 2004; **8**: 405–14.
- 9 Ganz A, Istepanian RSH, Tonguz OK. Advanced mobile technologies for health care applications. *Journal of Mobile Multimedia* 2006; **1**: 271–72.
- 10 Skulimowski AM. The challenges to the medical decision making system posed by mHealth, *IPTS Report*, Issue 81, February 2004
- 11 Tafazolli R, Saarnio J. eMobility – mobile and wireless communications technology platform - *Strategic Research Agenda*, Version 4, 2005. http://www.emobility.eu.org/documents/SRA4_051123_Final.pdf.
- 12 Proposal concerning the seventh framework programme of the European Community for research, technological development and demonstration activities (2007 to 2013). http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0119en01.pdf.
- 13 Braun A, Boden M, Zappacosta M. Healthcare technologies roadmapping: the effective delivery of healthcare in the context of an ageing society (HCTRM). *JRC/IPTS-ESTO Study*, European Commission, Health and Consumer Protection Directorate-General, August 2003.
- 14 MEDASHIP – MEDICAL ASSISTANCE FOR SHIPS, e-Ten Contract no. C27271.
- 15 EMISPHER – Euro-Mediterranean Internet-Satellite Platform for Health, medical Education and Research, Project Number: EUMEDIS 110 Project.
- 16 GALENOS - Generic Advanced Low-cost trans-European Network Over Satellite, Contract Number: TEN 45592 (FS).
- 17 Wilson A, Mann F, Murphy W, et al. Diagnostic efficacy of digitized images versus plain films: a study of the joints of the fingers, *Am. J. Radiol.* 1992; **158**: 437–41.
- 18 EUROPEAN COMMITTEE FOR STANDARDIZATION, prCEN/TS 15224:2005 Health services - Quality management systems - Guide for the use of EN ISO 9001:2000, FINAL DRAFT

- 19 Elnitsky C, Nichols B, Palmer K. Are hospital incidents being reported? *J Nurs Admin* 1997; **27**: 40–46.
- 20 Mant J, Gatherer A. Managing clinical risk. *BMJ* 1994; **308**: 1522–23.
- 21 General Medical Council. *Confidentiality – Guidance from the General Medical Council*. London: GMC, 1995.

