The Journal on Information Technology in Healthcare

EDITOR
Clyde Saldanha

EDITORIAL BOARD
Lodewijk Bos (Netherlands)
Jimmy Chan (Hong Kong)
Stephen Chu (New Zealand)
Charles Doarn (USA)
Syed Haque (USA)
Robert Istepanian (UK)
Chien-Tsai Liu (Taiwan)
Valentin Masero (Spain)
Jeannette Murphy (UK)
Dean Sittig (USA)
Roger Tackley (UK)

Volume 2 Issue 5
2004
ISSN 1479-649X

The Journal on Information Technology in Healthcare

Aims and Scope

The Journal on Information Technology in Healthcare aims to improve the quality and safety of patient care, by encouraging and promoting the use of information technology (IT) in healthcare. The journal acts as a medium for the international exchange of knowledge and experience of the benefits of IT in healthcare. It publishes papers that educate healthcare professionals on the use of IT in clinical practice, and particularly papers that provide objective evidence of the benefits of IT in healthcare.

Subscriptions

The Journal on Information Technology in Healthcare is published 6 times a year.
2004 subscription prices (6 issues) are:

	Institutional	Individual
Great Britain	£120	£100
Europe	€200	€180
USA	US$220	US$180
Rest of the world	£135	£115

Payment can be made by cheque or banker's draft. Cheques should be made payable to The Journal on Information Technology in Healthcare. Subscription orders and requests for sample copies should be sent to: JITH, 72 Churston Drive, Morden, Surrey, SM4 4JQ, UK. E-mail: subscriptions@jith.net. Fax : +44 (0)870 130 1572.
Claims for issues not received should be made within 3 months of publication of the issue.

Copyright

© The Journal on Information Technology in Healthcare. All rights reserved.
The Journal on Information Technology in Healthcare is protected by copyright. Apart from fair dealing for the purposes of research, private study, criticism or review, no part of this publication may be reproduced, stored or transmitted in any form or by any means without the prior written permission of the Editor.

Disclaimer

All papers are published in good faith. Authors are responsible for the scientific content and accuracy of their papers. Although every effort is made to ensure accuracy and avoid mistakes, no liability on the part of the Editor, publisher or their agents is accepted for the consequences of any inaccurate or misleading information. The opinions, data and statements that appear in articles published in the journal are those of the authors, and not necessarily those of the Editor or publisher. The Editor and publisher disclaim any responsibility or liability for such material and do not guarantee, warrant or endorse any product or service described in this publication.

Publisher: Health Technology Press, 72 Churston Drive, Morden, Surrey, SM4 4JQ, UK.

Advertising: To advertise in this journal, please contact William D'Sa, 25 Oxford Avenue, London, SW20 8LS, UK.
Tel +44 (0)20 8543 1230. Fax +44 (0)870 130 1572.
E-mail: william.dsa@blueyonder.co.uk

Typeset by Toby Matthews, Oxford, UK.
Printed by Saleh Aldossry, KSA.

The Journal on Information Technology in Healthcare

Volume 2 Issue 5

CONTENTS

© *The Journal on Information Technology in Healthcare* 2004; **2**(5): 313–328

Factors that have Contributed to a Lack of Integration in Health Information System Security

Juanita Fernando

Centre for Health Services Operations Management, Monash University, Australia.

ABSTRACT

The rapid advance of information technology in health settings has accentuated the importance of addressing the shortcomings of current health information system security practices. In recent times, health services have often had difficulty in complying with elements of robust security frameworks. This matter is made worse by the regulatory gap between implementing new and emerging information and communication technology (ICT), and managing the security risk the latter represents. Other problems include poor data quality and fragmentation, budgetary constraints, irreconcilable systems architecture, a history of incompatible data standards, confusing privacy jurisdictions and a lack of access to proven evaluation results. This paper argues that it is of crucial importance that technology innovation in health is accompanied by the development of generalisable operational paradigms for establishing secure hospital information systems (HIS). Examples from Australia are presented, together with a synthesis of the literature about HIS security, as a means of providing a foundation for constructing methodical frameworks for use across the sector. The paper also charts the evolution of Australian health privacy legislation over recent decades. The work concludes by outlining a current effort that explores useful ways of developing tools for health services which incorporate standards and legal frameworks.

INTRODUCTION

Health information systems (HIS) comprise the entire infrastructure, organisation, workforce and components for the collection, processing, storage, transmission, display, dissemination and disposition of information in the healthcare industry[1]. In many clinical and hospitals settings, HIS tend to consist of enormous silos of paper-based or electronic data that are fragmented or of poor quality, exposing systems to risk of infraction[2–4]. Rapid advances in information technology (IT) enablers and mobile devices such as personal digital assistants (PDA), or combination personal computer (PC)/phone devices, has done little to diminish these threats. Indeed, as Heslop *et al.*[5] indicate in their review of wireless communications in acute healthcare,

Correspondence and reprint requests: Juanita Fernando, Centre for Health Services Operations Management, Room 305, Faculty of Medicine, Nursing and Health Sciences, Building 15, Clayton Campus, Monash University, Wellington Road, Clayton, VICTORIA 3800, Australia. E-mail: Juanita.Fernando@med.monash.edu.au.

they have complicated the development of sound HIS security approaches by removing physical boundaries from security planning. Henceforth in this paper, the term HIS security refers to measures designed to limit the vulnerability of systems to breaches of data confidentiality, integrity, repudiation and availability.

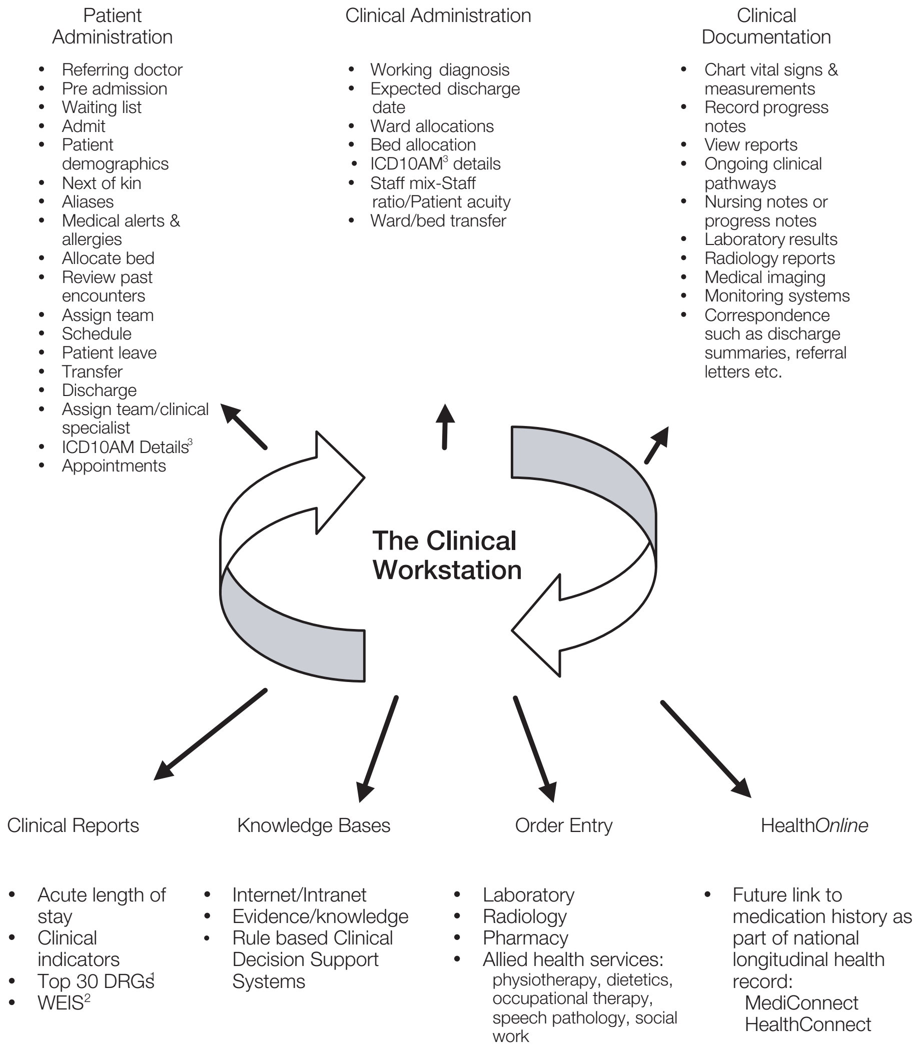
In the context of explaining new and emerging information and communication technologies (ICT) for health, white papers and vendor reports often present the integration of security into HIS as a product feature, rather than as a matter warranting systematic frameworks[6–8]. Lacking access to evaluation reports, health professionals frequently use such documents to justify rollouts of new ICT. Methodically evaluated, the use of IT offers opportunities to support health professionals and improve efficiency and quality of patient care. However, as Ammensworth *et al.*[9] argue, proven evaluations are difficult to find in the HIS literature and this results in problems with guidelines for good practice.

Furthermore, the desire to eradicate risks of compromise to HIS while harnessing the valuable outcomes ICT systems promise is evident throughout security literature. An important axiom that the commentary often avoids, however, is that no HIS can ever be completely secure, regardless of whether all the threats currently envisaged are controlled. A security plan is not a static entity in time; it evolves and changes, as do technologies and potential vulnerabilities. Planning HIS security implementations is about managing this risk and controlling known dangers.

This paper synthesises the literature about HIS security to provide a foundation for establishing generalisable operational paradigms for use across the sector. It also charts the evolution of Australian health privacy legislation over recent decades. The paper identifies the key factors impeding the cultivation of a sound approach to HIS security and concludes by outlining a current effort to develop a health privacy model incorporating standards and statutes for use in the Australian state of Victoria.

THE IMPACT OF NEW AND EMERGING ICT ON HIS CONTROL ISSUES

The healthcare industry is among the most information intensive business sectors in the world. Some theorists estimate that health workers spend between 35% and 60% of their time managing clinical data[10–12]. Every acute care hospital is capable of generating up to five terabytes of data per year, most of which is stored in numerous, widely scattered repositories [13]. Figure 1 models clinical station workflows in Australian hospital settings. While not the focus of this paper, it illustrates the magnitude and complexity of HIS. Using IT to manage the administration of intricate information resources promises significant rewards, such as improved practices and cost savings. However, security concerns about the right mix of technology in complicated health service environments are proving increasingly difficult to meet.



[1]DRG – Diagnosis Related Groups
[2]WEIS – Weighted Inlier Equivalent Separation
[3]ICD10AM – International classification of disease, 10th revision, Australian modification

Figure 1. *The Clinical Station workflow*

The Use of ICT to Manage Information

The capacity for health professionals to share information across disciplines and to acquire accurate information as required is frequently badly organised[14]. Much relevant information is not available to clinicians when they most need it at the point of care. Gathering this information is time-consuming and expensive, causing delays to clinical decision-making and patient care processes. Proponents of wireless systems argue that while electronic health initiatives can improve communication between health professionals and patients, mobile health initiatives provide even more flexible and efficient interactions as the data is always available to clinicians at the point of care, 'untethered' by desk, telephone and computer, or even by specific buildings or locations[15–17].

Given the potential benefits of technological innovation, rollouts of wireless ICT are growing in popularity[18–19]. A recent PDA-based mobile home nursing care trial in Australia was shown to eliminate unnecessary paperwork, improve data accuracy and liberate carers for more direct interaction with patients[17]. Another Australian project demonstrated that the use of patient-held smart cards has the capacity to provide an integrated, accurate, mobile electronic healthcare record (EHR)[20]. The potential for high volume users of hospital-based services to use mobile technology to self-manage chronic conditions more effectively than with paper-based and hard wired systems was evaluated in New South Wales during 2002. Improved efficiency and quality of care outcomes were demonstrated as tangible outcomes of mobile innovation[15].

National EHR database endeavours, such as Health*Online* in Australia, are seen as ways of supporting effective clinical practice by providing patients and health professionals with a portable tool to better manage health information. The EHR embeds patient consent mechanisms for every individual transaction with a service provider; that is, patients can agree that their information be entered into a Health*Online* database while receiving care on one occasion, and can withhold permission for data to be entered in the database on subsequent appointments with the same health service provider[21]. Patients can also decide to withhold all of their data from government EHRs. As the privacy protection of an individual's EHR will be fundamental in attracting viable numbers of participants to Health*Online*, assurances to patients about robust frameworks to keep their information secure are made in documentation supporting Health*Online*.[22] A trust-based relationship with patients provides the cornerstone of Health*Online*, but this presents a dilemma for health authorities since the privacy of records cannot be guaranteed. In the meantime moves to implement the government database nationally are continuing.

The Need for HIS Security Planning

The use of new and emerging technologies in health to manage HIS is becoming a key topic in strategic planning[5,18,23–24]. Successful ICT rollouts depend not only on assessing the functionality of the devices being used, but also on a planning process that incorporates the training needs of personnel and changes to the work environment. Poor implementation can result in failures that may affect security[9,25]. Furthermore, clinicians often raise concerns about patient confidentiality and security of data, as demonstrated by a recent study of doctors' experience with handheld computers in clinical practice[26]. Responses to disquiet about security issues have largely centred on the efficacy of individual products[27] and, as others point out, there is a dearth of proven evaluations that methodically consider the means of establishing an integrated approach to HIS security planning at the care interface[18,28].

Breaches are not confined to new ICT, and occur across a range of technologies. This was highlighted by the US-based Health Privacy Project group in their *Medical Privacy Stories* Web page[29]. Networks and mobile ICT simply increase the magnitude of exposure to risk and add new proportions to the matter of protecting privacy. For example, recently, a well-known Web search engine for Internet users, *Google*, created a link that permitted users to bypass security controls, and get access to the records of 5,500 neurosurgical patients in the US including their personal information as well as details of their therapy[30].

There is no longer any physical perimeter for Internet security systems to protect. Limitations in controlling access, along with data encryption vulnerabilities, problems with interoperability and the fundamental broadcast nature of wireless networks are key concerns in using the technology. In a recent random survey of wireless 'hotspots', a researcher found that 62% of wireless networks in Washington DC did not apply any security protection for data storage, retrieval or transmission. Exposed enterprise networks included hospitals and health services[31].

As this paper shows, timely, sensible and realistic risk management decisions on information system security are lacking in the health area. In Australia, healthcare organisations are becoming rapid adopters of new and emerging ICT. Many hospitals are establishing wireless computer networks in specific building areas and in campus wide implementations. Thus, it is important that the results of technology innovation are accompanied by the development of generalisable operational paradigms for establishing HIS security.

HIS DATA STANDARDS AND CODING SYSTEMS

Obstacles to the development of paradigms for establishing secure HIS include difficulties in establishing interoperable system standards. Frequently, information can neither be shared by two computers on the same network, nor shared between two different applications on the same computer. Attempts to develop engines to provide an interface between applications have proved to be fairly unsatisfactory and the result is poor system performance or inferior data[4]. Groups such as the openEHR Foundation[32] argue that a multiplicity of document formats, poor quality data and fragmentation, along with a range of vendor standards issues, has arisen as a result of the lack of harmonisation between different HIS. What follows is a brief overview of moves to establish international EHR standards to interconnect HIS data, along with a synthesis of the current Australian standards framework and a discussion of the effect of standards gaps on ICT rollouts in health.

International EHR Architectural Standards

Until recently, there were very few cooperative global efforts to develop international clinical and EHR architecture standards defining information models able to integrate clinical applications. In Australia, the ISO/TS 18308 *Health Informatics – Requirements for an Electronic Health Record (EHR) Reference Architecture Standard* that was finalised during 2003, is of particular interest. ISO/TS 18308 specifies the requirements for data and record structures, clinical documentation and communication processes, medico-legal, ethical and EHR systems evolution[4]. ISO/TS 18308 is the result of a merger between Australian open standards developers and a team from University College, London, together with some convergence involving European EHR standards and HL7.

HL7 is an established international standard for messaging between healthcare systems. The Australian government first endorsed HL7 as its nominated healthcare messaging standard in 1997[34]. Version 3 of HL7 is very likely to underpin sections of an Australian EHR architectural standard; it is embedded in the new ISO/TS 18308 standard which may be adopted as the official authorised European standard by 2004 and the international EHR standard by 2005[35].

Australian HIS standards

As part of the Health*Online* project, Australian authorities have a number of key national projects planned in the area of information management, including an agenda to devise national HIS guidelines to incorporate international standards and legal frameworks, such as HL7 and ISO/TS 18308[36]. An earlier standard, the *AS 4400–1995 Personal Privacy Protection in Health Care Information Systems*,[37] was devised specifically for Australian health settings. However, it contravenes Victorian state privacy laws, which has constrained its application[38].

Presently, Australian standards frameworks for health rely on best practice statements and general advisories, such as worksheets combined with exemplars to limit security vulnerabilities. Until strategies to implement a standardised approach are realised, the *HB 174-2003 Information Security Management Implementation Guide for the Health Sector*[39] handbook is being used to guide HIS security. The handbook comprises copies of state and federal government privacy laws and professional codes of conduct. It also interprets the international standard, *ISO/IEC AS/NZ 17799:2001 Information Security Management*,[40] which is based on traditional broad-spectrum threat models.

The Problems of Standards Gaps

Until the adoption of *ISO18308* occurs, health services will continue to provide patient care based on systems that do not provide consistent interoperability. Some experts[41,42] have argued that the need to improve efficiency and quality health outcomes has driven the implementation of various new technologies before health professionals have fully appreciated their security ramifications. In a recent incident, for example, major administrative components in a multi million dollar HIS were unable to interconnect, resulting in the cancellation of surgery in an American hospital because the system could not pay vendors for equipment supplies[33]. Reports of security incidents such as this are becoming more common as the health sector struggles to negotiate the regulatory gap between implementing new and emerging ICT and managing the security risk they present[43–47].

Among the problems impinging on effective negotiation is a lack of adequate tools that meet service providers' needs for protecting patient records. The regulatory gaps between achieving policy doctrines, such as adopting a robust stance in protecting the privacy of patient information, and achieving quality objectives, such as increased efficiency and quality of patient care, not only remain elusive, but are becoming increasingly difficult to achieve as more hospitals use ICT[36,48–50]. Simple questions, which are fundamental to the delivery of health services using ICT, such as "*Can I send a patient referral by email?*" or "*Can I access my patient's diagnostic result electronically?*" remain unresolved. The result is confusion among health professionals about the processes for implementing technological change and inadequate security arrangements across the sector.

FINANCIAL BARRIERS TO EVALUATIONS OF IT

Financial barriers are often cited as a key obstacle to more widespread evaluations of technologies.[19] According to Boston Consulting, over the last twenty years other information intensive sectors, such as finance and insurance, generally outlay 5% to 10% of total budget on IT, while healthcare has spent between 1% and 3%[51]. Currently Australia invests only 2% of health funding on IT while the US spends around 5% on health-related IT initiatives[52]. Nonetheless, there are indications that health sector patterns of investment in IT are set to grow by 2006 due to their potential for increasing patient safety[52–56]. For this potential to be realised, the health sector needs to recognise the worth of evaluations for ICT rollouts, as highlighted in the section below. The section also looks at the costly problem of harmonising legacy electronic and paper-based records with new standards.

Funding for Evaluative Purposes

A recent survey of chief information officers in healthcare indicated inadequate funding as the main barrier to implementing recent IT innovations. Survey participants believed that networked systems significantly improve security in comparison with handwritten records, or stand alone electronic systems[55–56]. However, ICT rollouts can have an adverse affect on operational security and may actually result in harm to patients[43,45]. As Ammenworth *et al.*[9] argue, there is a need for ongoing evaluations of ICT to identify problems. However, evaluation is an expensive process and the contribution of assessment to ICT rollouts is often not valued in terms of returns on investment[57].

The Cost of Interconnecting Data

Even where clinicians are equipped with ICT that have been adequately scrutinised for functionality, the value of the devices is limited without exact patient information. Poor data availability and integrity, that is clinical access to accurate information upon demand, can lead to adverse drug reactions and other patient safety concerns[52]. Interconnecting islands of patient data clearly present significant financial challenges[55]. As the Good Electronic Health Records (GEHR) group[32] have shown, the paper-based and stand-alone computer systems, upon which many services continue to rely have been integrated with care delivery models relevant only to particular sites, thus creating an expensive legacy of fragmented patient records.

Even if technical hindrances, such as the lack of common formats and data quality issues could be overcome, the cost of cleaning, standardising and re-entering patient data by health services across the sector remains prohibitive[33]. The US government has budgeted approximately $US100 million over the next 10 years for converting paper-based health records to electronic records. Researchers estimate that to carry out data conversion may cost each US medical practice between $US15,000 and $US40,000[58].

On the other hand, if relevant legacy data is not integrated into modern systems, costly practical problems such as managing data storage and retrieval using multiple technologies in the future will need to be resolved. Evaluations of financial and legal considerations, such as the cost involved in retooling to the ISO18308 standard, together with security considerations, such as the projected cost of breaches to data, will be paramount in guiding decisions about legacy systems harmonisation as ICT expenditure continues to grow. The use of a valid paradigm for HIS security can offer support for funding decisions associated with technology innovation by identifying potential breaches to patient systems and the impact of operational and financial exposure to events such as network failure and litigation.

HEALTH PRIVACY LEGISLATIVE ENVIRONMENT

Privacy, i.e. the right to be left alone, is recognised globally as a universal value. The use of innovative technologies in the health sector has produced new kinds of information about patients and new ways of collecting it. EHR databases, biometric security services and patient self-management of chronic conditions, are being applied to health business models at an unprecedented rate and so the political and legal mechanisms designed to protect rights to be left alone are rapidly evolving through privacy legislation. IT has the capacity to recognise people from their retinas, voice, DNA or other biometric information. These records are detailed, individualised and computer-processable. Patients understand the implications of new technologies in relation to their information, which has reaffirmed interest in the role of regulation in protecting privacy. However, in Australia, concern about the detail of laws to protect patient privacy has resulted in an overlap of state and federal government privacy jurisdictions, creating complexity and confusion in the health privacy legislative environment.

Patient Views About the Privacy of their Health Information

Recent research commissioned by the Australian Office of the Federal Privacy Commissioner (OFPC) indicates that patients show a clear interest in controlling who handles their health information. In the survey, patients identified health professionals as highly trustworthy. Nevertheless, almost half of the respondents maintained that clinicians should not discuss their details with colleagues without their prior permission, even if disclosure would result in better treatment[59]. These findings have been supported by similar work in the UK and the USA[37,60].

Other work demonstrates that patients are aware of the effects ICT may have on their right to privacy, with more than half the respondents in a UK survey citing concerns about privacy as a barrier to storing health information on the Internet[60–62]. Patient views about controlling their data have helped drive changes to privacy policy formulation and legislation. For example, Iceland's Supreme Court recently upheld a citizen's complaint and ruled that EHR legislation does not comply with the privacy protection afforded by that country's constitution. The Court further ruled that the legislature's obligation to protect privacy can not be replaced by various forms of monitoring entrusted to public agencies and committees[63].

Problems of Overlap in Government Privacy Jurisdictions

In Australia, the State and Federal governments' health privacy laws overlap. This is not dissimilar to the US health privacy legislative environment[64]. During 1988, the Australian government passed the *Privacy Act* to safeguard government information in such areas as social security, health insurance and taxation[65] and in 2000 the *Privacy Amendment (Private Sector) Act* extended the *Privacy Act* to encompass most private sector organisations. The expanded *Act* applies to all health service organisations or businesses storing health information[38]. The problem, however, is that the governments of three states (Australian Capital Territory, New South Wales and Victoria) believed that additional detail was required to protect patient information and so they introduced state-based privacy legislation that contravenes the federal *Act*. A synthesis of changes to Australian health privacy legislation over recent decades is provided in Table 1.

The *Victorian Health Records Act 2001* (VHRA) is a case in point[38]. The *VHRA* is designed to tailor the principles of the *Privacy Act* to the provision of private health services. The protections that the *VHRA* afford are sometimes stronger and sometimes weaker than those in the *Privacy Act*. For example, the *Privacy Act* exempts employee records associated directly with the employee relationship, while the *VHRA* does not. The rules for access to information collected before the legislation came into effect are different for the *Privacy Act* and *VHRA* respectively.

Table 1. *The Evolution of Australian Health Privacy Legislation*

1976	Australian Law Reform Commission (ALRC) directed to report on privacy
1979	ALRC report on *Unfair publication: defamation & privacy* ALRC report on *Privacy & the Census* *Telecommunications (Interception) Act*
1980	OECD *Guidelines on Data Privacy Protection & Transborder Data Flows* released.
1982	*Freedom of Information Act 1982* (*FOI*) *NSW Health Administration Act 1982*
1983	ALRC report on *Privacy* *Archives Act 1983*
1984	Federal government adopts OECD guidelines
1986	*Commonwealth Privacy Bill* proposed but abandoned Australia Card proposed
1987	*Australian Privacy Foundation* established
1988	*Privacy Act* passed regulating most federal public sector agencies Tax File Number introduced *Cash Transactions Report Act* NSW *Privacy and Personal Information Protection Act*
1990	NSW *Mental Health Act*
1991	Review of *Telecommunications (Interception) Act 1979* NSW *Public Health Act*
1992	Amendments re credit reporting made to the *Privacy Act 1988* *National Health and Medical Research Council (NHMRC) Act*
1994	Australian Privacy Charter Council formed
1995	Report on privacy by Commonwealth Parliament House of Representatives Standing Committee on Legal & Constitutional Affairs Breen vs Williams: private patients have no general right of access to their health information
1996	Attorney-General's *Privacy Protection in the Private Sector* discussion paper released NHMRC *Ethical Guidelines on Assisted Reproductive Technology*
1997	Public enquiry on privacy issues conducted by federal Privacy Commissioner Medicare & Pharmaceutical Benefits programs privacy guidelines issued under Section 135A of *National Health Act 1953* *ACT Health Records Act*
1998	*National Principles for Fair Handling of Personal Information* (voluntary code of regulation for private sector) established by the Federal Privacy Commissioner *NSW Health Information Privacy Code of Practice*
1999	Senate Legal & Constitutional References Committee's *Privacy & the Private Sector* report released *National Statement on Ethical Conduct in Research Involving Humans* issued by the (NHMRC)

2000	First reading of Commonwealth *Privacy Amendment (Private Sector)* Bill. Legislation subsequently passed after minor amendments and community criticism
	EU submission to House of Representatives Committee indicates that *Privacy Amendment (Private Sector)* Bill would not meet EU's test of adequacy
	Medical Practioners Board of Victoria v Sifredi: health information pertaining to clinical management of patient before Medical Practioners Board subject to *FOI* requests.
2001	Federal Privacy Commissioner announces research projects on *Privacy & the Community* and on *Privacy, Business & Government*
	Federal Privacy Commissioner releases draft NPP and draft *Health Privacy Guidelines*
	Federal Privacy Commissioner releases consultation paper on *Privacy Issues in the Use of Public Key Infrastructure for Individuals*
	National Health & Medical Research Council releases its draft s.95 and s.95A guidelines
	Federal Privacy Commissioner releases *Health Privacy Guidelines*
	Privacy Amendment (Private Sector) Act comes into effect for large organisations and all private health service providers
	Better Medication Management System (*BMMS*) draft legislation released for comment
2002	*Health Records Act* in Victoria comes into effect
	Privacy Amendment (Private Sector) Act comes into effect for smaller organisations
	Draft *National Health Privacy Code* released for comment
	HealthConnect system testing commences
	Guidelines for the protection of privacy in the conduct of medical research issued by the NHMRC
	NSW Health Records and Information Privacy Act comes into effect
2003	*MediConnect* (known as *BMMS* in development stage) system testing commences
	NHMRC issue publication *When Does Quality Assurance in Health Care Require Independent Critical Review?*
	Draft updated NHMRC *Ethical Guidelines on Assisted Reproductive Technology* released for public comment.

The *Privacy Act* takes a co-regulatory approach to protecting health privacy by recognising professional codes of conduct while the *VHRA* does not[38]. The OFPC frankly acknowledges that there are clear overlaps in jurisdictional intent so that private sector health service providers may believe they are *"simultaneously regulated by two similar, but not entirely consistent, privacy protection schemes"*[66]. Moves to draft nationally consistent legislation are already underway, since compliance with the various laws relating to health information is difficult, if not impossible, for service providers at present.

THE NEED FOR EVALUATION

While the take up of emerging technologies in health settings has proliferated since the 1970s, there has been a notable dearth of methodical research which evaluates the quality of care and efficiency outcomes that the new tools promise. A recent workshop, *New Approaches to the Systematic Evaluation of Health Information Systems* (HIS-EVAL)[9], brought together informatics experts from throughout Europe to look at problems related to the evaluation of HIS. They found that the results and reports from evaluations were often not published, especially if the study failed to find benefits. Proven evaluation methods scarcely existed in the literature and their publication was compromised since documents, such as technical reports, are seldom referenced. Consequently, other health services lack sufficient information to adopt the approach or judge the validity of the conclusions given[9].

In the absence of reliable information to underpin the success of ICT rollouts in health, organisations are forced to negotiate issues ranging from inferior data, conflicting standards, and statutory requirements, at the patient care interface as they occur. Governments are beginning to construct the building blocks of a sound approach to HIS security as part of emerging national EHR systems ventures. In the intervening period, proven HIS evaluations can inform security practice while contributing to the formulation of more generalisable HIS security models.

Current Evaluation Efforts

As strategies are designed to realise the efficiencies and quality of care outcomes that ICT promises, by rolling out wireless-enabled PDA tools at the bedside or using EHRs, the dimensions of potential system breaches have complicated HIS security planning. For initiatives to inspire confidence in health professionals and their clients, it is imperative that work be directed towards developing reliable paradigms for establishing HIS security models that incorporate standards and legal frameworks.

Groups such as HIS-EVAL demonstrate that a basis for HIS evaluation theory and practice is emerging. The mWard group at Monash University is a case in point since it brings together a multidisciplinary group of researchers to evaluate the use of mobile ICT technology in health services[67]. My current research with the mWard group will model health privacy and HIS security standards into an Australian security/privacy matrix stratified by the data drawn from the Clinical Station Workflow model illustrated in Figure 1. The research will evaluate security at various sites according to the matrix and feed the data back into these organisations for their evaluation. It is hoped that the research sites might use the model as a starting point for developing policies to limit threats in HIS security environments and so enhance the quality of care and efficiency outcomes to be gained from using ICT in healthcare. Results from this work will be disseminated as widely as possible to contribute to informatics knowledge about security, and thus play a role in the ongoing work of HIS evaluation theory and practice.

CONCLUSION

The rapid advance of IT in health settings has accentuated the importance of addressing the shortcomings of current HIS security practices. In recent times, health services often have difficulty in complying with the elements of robust security frameworks. This matter is made worse by the regulatory gap between implementing new and emerging ICT, and managing the security risk the latter represents. Other problems include poor data quality and fragmentation, budgetary constraints, irreconcilable systems architecture, a history of incompatible data standards, confusing privacy jurisdictions and a lack of access to proven evaluation results. This paper argues that it is of crucial importance that technology innovation in health is associated with the development of generalisable operational paradigms for establishing secure HIS. Mainly illustrated by examples from Australia, it synthesises the literature about HIS security as a means of providing a foundation for constructing methodical frameworks for use across the sector. The paper also charts the evolution of Australian health privacy legislation over recent decades. The work concludes by outlining a current effort that explores useful ways of developing tools for health services which incorporate standards and legal frameworks.

Ongoing ICT innovations are poised to change the clinician–patient relationship forever and governments are increasingly looking to provide health services, such as national EHR databases, via the Internet. Addressing the factors that contribute to a lack of integration in HIS security is not simply of abstract interest, but of practical and immediate relevance. Clearly, ongoing research is required to evaluate innovative technology implementations and practices to limit threats in HIS security environments and thus enhance the quality of care and efficiency outcomes to be gained from using ICT in healthcare settings.

REFERENCES

1 T1A1, Technical Subcommittee on Performance and Signal Processing (2001) *American National Standard for Telecommunications-Telecom Glossary 2000* (http://www.mk.dmu.ac.uk; directory: /depts/dcis/research/groups; file: /infosys.

2 Chu S. Information retrieval and health/clinical management. *Yearbook of Medical Informatics 2002*, 271–75; www.med.uni-heidelberg.de; directory: /mi/yearbook/2002; file: /chu.pdf.

3 Heard S, Kalra D, Griffiths S, Southgate L. The history and purpose of the medical record. http://www.gehr.org; directory: /introduction; file: /History%20and%20purpose.html.

4 Schloeffel PD. Tutorial; Introduction to openEHR & EHR standards. *Proceedings of Health Informatics Conference 2003 & Royal Australian Conference of General Practitioners 12CC* Darling Harbour, 2003.

5 Heslop L, Howard A, Fernando J, Rothfield A, Wallace L. Review article: wireless communications in the acute health care sector. *Journal of Telemedicine and Telecare* 2003; **9**: 187–93.

6 Stammer L. A show of handhelds: wireless technology is making inroads at the point of care. *Healthcare Informatics* 2001; **18**: 37–38, 40, 42. http://www.healthcare-informatics.com; file: /issues/2001/04_01; directory: /cover.htm.

7 Stolworthy Y. RNs are mobilizing. *Journal of Mobile Informatics* 2003. http://www.pdacortex.com; directory: /RNs_are_Mobilizing.htm.

8 Kitney R. Increasing mobility and improving decision-making with wireless technology British. *Journal of Healthcare Computing and Information Management* 2002; **19**: 31–32.

9 Ammenwerth E, Brender J, Nykanen P, Prokosch H, Rigby M, Talmon J. Visions and strategies to improve evaluation of health information systems: reflections and lessons based on the HIS-EVAL workshop in Innsbruck. 2004; **73**: 479–91.

10 Biscoe G. Computers and nursing in paper presented at From Lamp to Light Pen: Computers in Nursing conference, Adelaide. In Griffin A, MacKay G (eds.), *Nurses Using Computers: Australian Experiences*. Armidale: ACAE Publications, 1989, p. 12.

11 Mackie P. Health computer industry perspective on nursing involvement. In Griffin A, MacKay G (eds.), *Nurses Using Computers: Australian Experiences*. Armidale: ACAE Publications, 1989.

12 Ebell M. Information at the point of care: answering clinical questions. *Journal of American Board of Family Practice* 1999; **12**: 225–35.

13 Crowe BL, McDonald JG. Evaluation of developments on storage and retrieval systems for health information systems. *Proceedings of HIC 99: Health Informatics Conference*. Hobart, 1999, pp. 271–75.

14 Thompson KA, Coates VE, McConnel CJ, Moles K. Documenting diabetes care: the diabetes nurse specialists' perspective. *Journal of Clinical Nursing* 2002; **11**: 763–72.

15 Murray D. Taking care of your health at home. In *The Age*. Melbourne: John Fairfax & Sons Pty., 2003, p. 8.

16 Ayres D. A clinical information systems framework for NSW health at 2nd National Health Online Summit. Brisbane. http://www.health.gov.au; file: /healthonline/docs/summit2, directory: /ayres.pdf.

17 Pen Computer Systems Pty Ltd. Domiciliary nursing: gemino home nursing/mobile computing. Project report for Pen Computer Systems Pty Ltd. Parramatta, 2003, p. 11.

18 Saldanha C. Information technology in healthcare. *The Journal on Information Technology in Healthcare* 2003; **1**: 5–11.

19 Spyglass Consulting. *Healthcare Without Bounds: Trends in Mobile Computing White Paper*. http://www.spyglass-consulting.com; file: /spyglass_whitepaper.html.

20 Department of Health and Ageing (DoHA) Appendix 2. *Health Online*, 2nd edn. http://www.health.gov.au; directory: /healthonline/docs; file: /actplan2b.pdf.

21 HealthConnect. National Health Privacy Code (draft) Consultations. http://www.healthconnect.gov.au; directory: /whats_new; file: /whats_new.html.

22 National e-Health Systems Branch. HealthConnect budget information: privacy, consent and access. http://www.health.gov.au; directory: /healthconnect/building_blocks; file: /privacy.html.

23 National Electronic Health Records Task Force. A health information network for Australia. http://www.health.gov.au; directory: /healthonline; file: /nehrt.htm.

24 Dix A, Rodden T, Davies N, Trevor J, Friday A, Palfreyman K. Exploiting space and location as the design framework for interactive mobile systems. *Communications of the Association of Computing Machinery* 2000; **7**: 285–21.

25 Heeks R, Mundy A, Salazar A. Why health care information systems succeed or fail. http://idpm.man.ac.uk; directory: /publications/wp/igov; file: /igov_wp09.shtml.

26 McAlearney A, Schweikhart S, Medow M. Doctors' experience with handheld computers in clinical practice: qualitative study. *British Medical Journal* 2004; **328**: 1162–70.

27 Kittler A, Wald J, Volk L, *et al.* The role of primary care non-physician staff in e-mail communication with patients *International Journal of Medical Informatics* 2004; **73**: 333–40.

28 Sausser G. Use of PDAs in health care poses risks and rewards. *Healthcare Financial Management* 2002; **56**: 86–88.

29 Health Privacy Project. Health privacy stories. http://www.healthprivacy.org; directory: /usr_doc; file: /privacystories.pdf.

30 PractiSure. Examples of recent healthcare privacy & security breaches. http://www.practisure.com; file: /breaches.html.

31 Taylor G. Wireless LANs are wide open in our nation's capitol. http://www.wificonsulting.com; directory: /Security; file: /SecurityArticle-1.htm.

32 Schloeffel PD, Beale T, Heard S, Rowed DD. Background and overview of the Good Electronic Health Record (GEHR) http://www.gehr.org; directory: /Documents; file: /-BackgroundOverview_of_GEHR.htm.

33 iHealth Beat VA *Hospital Reports Computer System Problems*.

34 HL7. About HL7 (Health Level Seven). http://www.hl7.org; directory: /about; file:/hl7about.htm.

35 Ocean Informatics Pty Ltd. EHR standards. http://www.oceaninformatics.biz; file: /standards.html.

36 National Health Information Standards Advisory Committee (NHISAC). Setting the standards – a national health information standards plan for Australia: an action paper arising. *Health Online: A Health Information Action Plan for Australia*. http://www.health.gov.au; directory: /healthonline/docs; file: /setstand.pdfNational.

37 Australian National Audit Office (ANAO).Internet security for commonwealth govt agencies. *Audit Report No. 13, 2001–2002*. http://www.anao.gov.au/.

38 Smith L. Is it only naughty if you get caught? Complying with new privacy laws. Unpublished Paper, Privacy Management Pty. Ltd., 2002, p. 6.

39 Standards Australia HB 174–2003 handbook: information security management – implementation guide for the health sector. http://www.standards.com.au; directory: /catalogue/.

40 Standards Australia AS/NZS 7799.2:2001 information technology – code of practice for information security management. http://www.standards.com.au; directory: /catalogue/.

41 Fairey M. Security, integrity and confidentiality. *British Journal of Healthcare Computing and Information Management* 2000; 17: 9.

42 Simons M. *NHS* plan poses IT challenge. http://infotrac.galegroup.com; directory: /itw/infomark/294/486/35016350w7; file: /purl=rc1_EAIM_0_A69801878&dyn=14!nxt_3_0_A69801878?sw_aep=monash.

43 Berinato S. All systems down. http://www.cio.com.au; file: /index.php?id=1681249874.

44 de la Garza P. VA takes a closer look at Bay Pines; VA officials will review claims of a malfunctioning computer system and a hostile work atmosphere. http://sptimes.com/; directory: 2004/02/20/Tampabay; file: /VA_takes_a_closer_loo.shtml.

45 Walsh R. Glitch blocks heart patient appointments. http://www.nzherald.co.nz/; file: /storydisplay.cfm?thesection=news&thesubsection=&storyID=3520652&reportID=212578.

46 Colliver V. Software glitch reveals stranger's health history, Kaiser applicant sees woman's information. http://www.sfgate.com; directory: /cgi-bin/article.cgi?file=/chronicle/archive/2004/03; file: /12/BUGND5J3PR1.DTL.

47 Chin T. Come ogle my patients data. http://www.ama-assn.org; directory: /sci-pubs/amnews/pick_03; file: /bisc0324.htm.

48 National Office for the Information Economy (NOIE) Better practice in online service delivery. http://www.noie.gov.au; directory: /projects/egovernment/Better_Practice/BPGuide File: /bp_index.htm.

49 Department of Human Services Compliance tools [online] (viewed 25 September 2003). http://www.dhs.vic.gov.au; directory: /privacy/tools; file: /index.htm#risk.

50 Australian Medical Association (AMA). The AMA's submission on draft health privacy guidelines. http://domino.ama.com.au; directory: /web.nsf/doc/SHED-5FV34P/$file; file: /AMA's%20Submissions%20on%20Draft%20HPG.pdf.

51 Multimedia Victoria. IT network and application security: best practice statements. www.mmv.vic.gov.au/; directory: /b411d8aa37220008ca2569990007eef9$FILE; file: /Security%20Best%20Practice.doc.

52 Woodhead B, Bryan M. Healthcare's data systems in sick state. *The Australian Financial Review* 2003: 31.

53 Alexander B. $323m technology budget boost for Victorian health. http://hnb.dhs.vic.gov.au; directory: /web/pubaff/medrel.nsf/2d2ad2319e3f63aa4a25656a0014ee89; file: /dfc6c7623ddc0099ca256d1e000460e8?OpenDocument.

54 Wilson F. Health Smart: ICT strategy for Victoria. Unpublished paper presented at HISA Vic monthly seminar on 30 July 2003, AMREP auditorium, Alfred Hospital: Prahran.

56 Health Data Management. CIOs stay focused on patient safety. http://healthdatamanagement.com; directory: /html/news; file: /NewsStory.cfm?DID=11363.

57 iHealth Beat Funding tops list of EMR barriers. http://ihealthbeat.org; directory: /members; file: /basecontent.asp?oldcoll=576&contentid=25309&collectionid=552&program=1&contentarea=120021.

58 Przybyla H. US plans more health files online. http://www.theage.com.au; directory: /articles/2004/05/31; file: /1085855477245.html?from=storyrhs.

59 The Office of the Federal Privacy Commissioner. Privacy and business. http://www.privacy.gov.au; directory: /business/research; file: /index.html#1.

60 Princeton Survey Research Associates for the California HealthCare Foundation. Americans worry about the privacy of their computerized medical records. http://www.chcf.org; directory: /press; file: /view.cfm?itemID=12267.

61 Denton IC. Will patients use electronic personal health records? Responses from a real-life experience. *Journal of Healthcare Information Management* 2001; **15**: 251–59.

62 Bomba D, Land T. A Survey of patient attitudes towards the use of computerised medical records and unique identifiers in four Australian GP Practice. *The Journal on Information Technology in Healthcare* 2003; **1**: 31–38.

63 Electronic Privacy Information Center (EPIC) Ragnhildur Guðmundsdóttir vs The State of Iceland No.151/2003 Icelandic Supreme Court. http://www.epic.org; directory: /privacy/genetic; file: /iceland_opinion.pdf.

64 Reed Smith LLP .50 State HIPA. A privacy study. http://www.statehipaastudy.com; file: /home.aspx.

65 Caslon Analytics Privacy Guide. http://www.caslon.com.au; file: /privacyguide2.htm.

66 Crompton M. Speech notes: privacy, technology and the healthcare sector. In *Privacy, Technology and the Healthcare Sector*. Sydney: The Australian Financial Review 4th Annual Health Congress Conference. http://www.privacy.gov.au; directory: news/speeches; file: /sp79notes.html/.

67 Centre for Health Services Operations Management (CHSOM). Monash neurology ward goes wireless. http://www.monash.edu.au; directory: /news/releases; file: /ward54.html.

© *The Journal on Information Technology in Healthcare* 2004; **2**(5): 329–339

Construction of a Diabetes Database and Pilot Evaluation of iKey Controlled GP–Patient Access

David Bomba, John Fulcher, Andrew Dalley*[†]

Centre for Health Service Development, * School of Information Technology and Computer Science, University of Wollongong, and † Illawarra Division of General Practice, Australia.

ABSTRACT

Objective: In Australia, the management of diabetes is a national health priority area. The objectives of this research were twofold. (i) To test the feasibility of building and accessing a centralised chronic disease registry for Type 2 diabetes patients with the aim of improving decision-making by providers at the point of care. (ii) To evaluate the feasibility of using a smart identification system for controlling access to Web-based diabetes patients' records by general practitioners (GPs) and patients.

Design: Developmental process.

Setting: The Illawarra region, New South Wales, Australia.

Methods: The diabetes registry was constructed using an automated dial-up program to transfer data electronically from GPs' computers to a diabetes database held at the Illawarra Division of General Practice (IDGP). Data is converted from text to numerical format and standardised. To evaluate controlled access to this database a field trial was undertaken during 2002. Twenty Type 2 diabetes patients and six GPs enrolled in the regional diabetes programme, were issued with USB iKeys containing unique identifiers. The patient first inserted their iKey in the USB port of the practice computer, and after removing it the doctor inserted their iKey. For as long as the latter was connected to the USB port, access was enabled to that particular patient's complete medical record held on the IDGP central server. Patients were also able to independently gain Web access to their own medical records.

Results: The system was able to successfully pull data from multiple sites and disparate laboratory (pathology) systems to create the diabetes database. At present it contains data from approximately 550 patients cared for by 40 GPs. The feasibility of using iKeys as a secure, portable mechanism for remotely accessing patient medical records held on the database was confirmed by the field trial. Post-trial evaluation of both patients and doctors revealed minimal impact on consultation times, as well as a positive disposition to the use of iKeys. Patients and providers also reported some negative experiences including technical problems and lengthy access times. Due to their ability to view their records, some patients were able to report incorrect entries in their medical records.

Conclusion: The project demonstrated the feasibility of using iKeys as an authentication and authorisation mechanism for controlling access to an individual patient's health record over the Web by both patients and their GPs. A limited evaluation of patient and provider users revealed both benefits and limits for the use of the iKeys in supporting the care of patients with Type 2 diabetes. Despite the small participant sample, the iKey system was seen as an acceptable innovation which could be rolled out to the wider community.

Correspondence and reprint requests: Dr David Bomba, Centre for Health Service Development, University of Wollongong, NSW, Australia. E-mail: bomba@uow.edu.au.

INTRODUCTION

Globally, diabetes affects millions of people and is a significant cause of mortality and morbidity[1,2]. In Australia it is the sixth leading cause of death and contributes to significant illness, disability, poor quality of life and premature mortality[3]. The management of diabetes has consequently been given high health priority.

To improve the management of diabetic patients and their outcomes, information technology is being used in new and innovative ways. This is illustrated by the approach of the Illawarra region in New South Wales which is an area immediately south of Sydney and encompasses the cities of Wollongong, Shellharbour and adjoining townships. In the year 2000, the University of Wollongong and the Illawarra Division of General Practice (IDGP) undertook a research project to develop an information system to improve the management of patients with Type 2 diabetes (non insulin dependent diabetes). In designing the system, the following features were felt to be important:

- The data collected had to be accurate and comparable
- The system for collecting data had to be largely automated
- Patients had to be able to move between providers knowing their information would follow them, rather than resting irretrievably with the GP who had originally recruited them
- Patients would be able to control GP access to their data

To meet these requirements it was decided to use the Medical Director for Windows (MDW) clinical management package used by GPs and to combine it with a Web-based server to enable remote access to the medical records of diabetic patients. To enable secure access to the information it was elected to use a smart identification (Smart_ID) system using universal serial bus (USB) port iKeys (Figure 1). The iKey is technologically similar to a smart card in that it contains a small computer chip for securely storing information, but differs in physical structure and communications interface. It provides a suitable interface to both the Web and

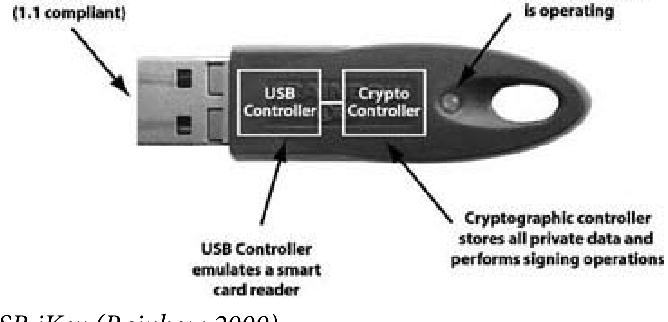

USB Connector
(1.1 compliant)
LED indicates iKey is operating
USB Controller
Crypto Controller
USB Controller emulates a smart card reader
Cryptographic controller stores all private data and performs signing operations

Figure 1. *USB iKey (Rainbow 2000)*

MDW management software program and can also be used to provide authentication and authorisation. A smart token was selected over password access because it was deemed to be easier than having to remember a password.

Patients and GPs were issued with iKeys, and both needed to insert their respective keys into the GP's computer in order to access a patient's medical record. The system was evaluated by a field trial conducted in 2002.

METHODS

The Diabetes Information System is illustrated in Figure 2. It comprises an automated dial-up program that transfers data electronically from the GP's computer to a diabetes database held at the IDGP. The uploading program is set to dial up once per week at a time most convenient to the GP and their practice. The program works by searching for new data entered in MDW on all patients who are listed in the diabetes database. To ensure data on the correct patient is received, the program interrogates MDW, matching the patient's name, date of birth and address with those entered into the database. Once matched, specific new data is extracted and imported to this diabetes database. This data is converted from text to numerical format and standardised to allow for inter-pathology company variability of normal ranges.

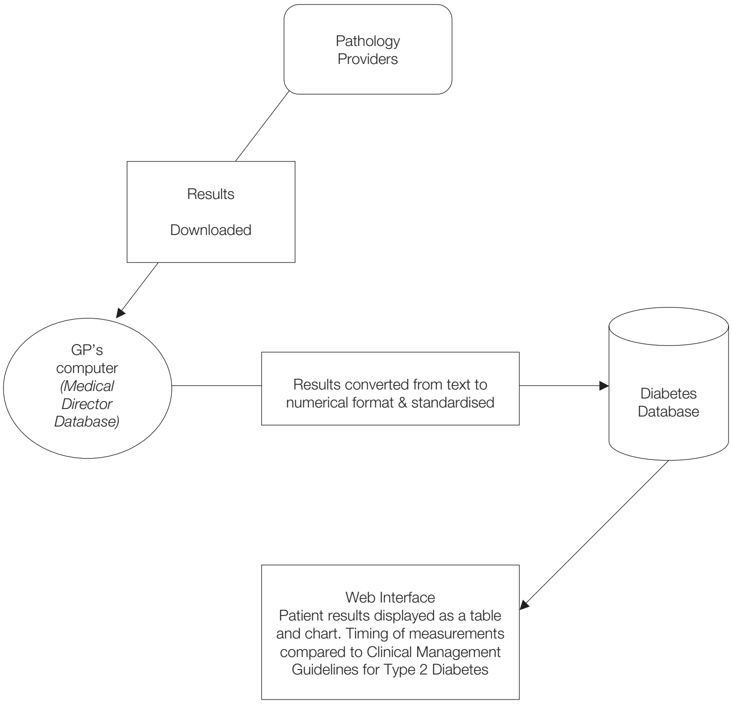

Pathology Providers
Results
Downloaded
GP's computer *(Medical Director Database)*
Results converted from text to numerical format & standardised
Diabetes Database
Web Interface
Patient results displayed as a table and chart. Timing of measurements compared to Clinical Management Guidelines for Type 2 Diabetes

Figure 2. *Diabetes Information System*

A Web interface program was developed to interact with the database and to display patient records and their adherence with the NSW Health Clinical Management Guidelines (CMGs) for Type 2 Diabetes. During the pilot phase the Web interface was only accessible by the GP who recruited the patient to the program.

Data collected by the Diabetes Program included the following test results:

- HbA1c (glycosylated haemoglobin)
- Total cholesterol
- HDL cholesterol
- LDL cholesterol
- Triglycerides

These results are loaded into MDW through an automatic electronic download from the pathology laboratories. Weight, height and blood pressure are also uploaded; however, these results must be manually entered into the diabetes record component of MDW by the GP. All data is extracted directly from MDW.

FIELD TRIAL

To test the feasibility of patients being able to control access to their medical records, patients and doctors enrolled in the Diabetes Program were issued with USB iKeys containing stored unique identifiers. These unique identifiers take the form of 1024-bit random numbers generated by the IDGP. To obtain access to the patient's record, the patient had to insert his/her iKey into the USB port of the doctor's computer and after removing it the doctor had to insert his/her iKey. While the doctor's iKey remained connected to the USB port:

(i) That particular patient's record was opened within the doctor's MDW desktop package.

(ii) A remote connection was made to the patient's record residing on the IDGP central server. This included a subset of that held on MDW from any GP previously visited with uploaded results.

It should be emphasised that no patient data *per se* was stored on these iKeys, only a unique identifier which functioned as a secure access mechanism.

The design and evaluation for the field trial focused on the feasibility of using iKeys among participants in the trial. Key questions addressed were:

(i) Satisfaction of GPs and patients with the iKey system and in particular whether the actual experience of using the system met their expectations.

(ii) Whether the system led to perceived improvements in service provision (information access and impact on the consultation) for the GPs and their patients.

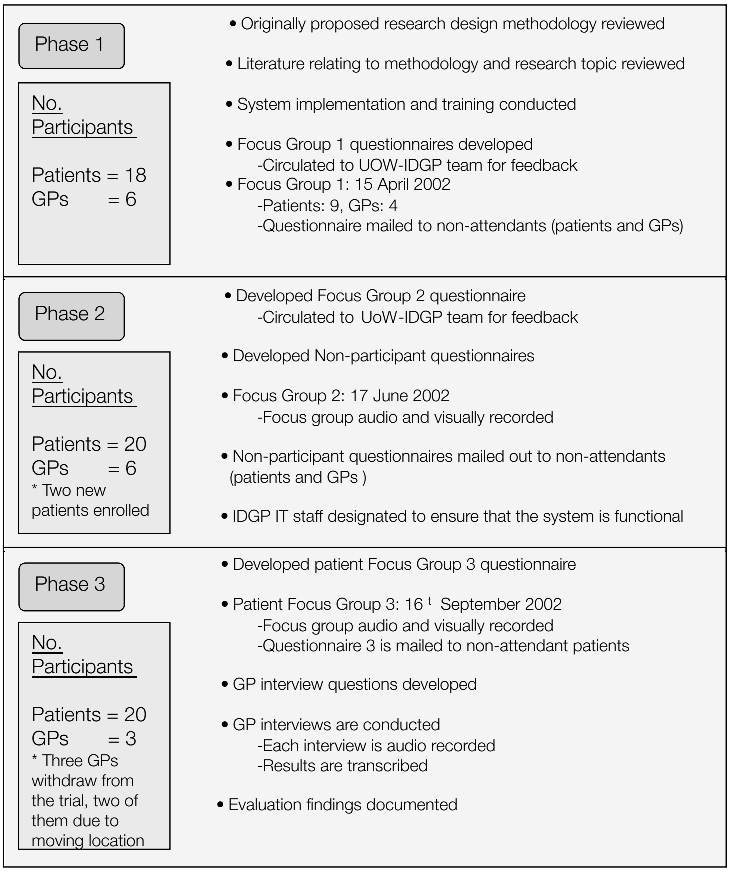
(iii) What factors impeded or assisted the adoption process.

The IDGP nominated forty GPs from their Diabetes Program Trial to participate in the project. These forty GPs and their diabetes patients (about 20–30 per

GP) were offered the opportunity to voluntarily register in the iKey Trial. Both GPs and patients were informed about the features of iKeys and how iKeys could be used to enable safe access to patient information consistent with the requirements of the Australian Privacy Principles as set out by the Office of The Federal Privacy Commissioner[4]. To help with the recruitment and awareness process, GP and patient information days were carried out by various project team members. Mail-outs were also sent to GPs and patients and specific information packs were prepared for them. These contained instructions, consent forms to participate and withdraw, frequently asked questions, and general information outlining all facets of the project. Articles also appeared in the local GP newsletter publicising the project. Figure 3 presents the summarised evaluation timeline and design. The actual registration and evaluation began in April 2002 and continued until the end of October 2002.

Evaluation utilised the following data collection methods (Figure 3):

- Semi-structured questionnaires within focus group settings



Phase 1

No. Participants

Patients = 18
GPs = 6

- Originally proposed research design methodology reviewed
- Literature relating to methodology and research topic reviewed
- System implementation and training conducted
- Focus Group 1 questionnaires developed
  -Circulated to UOW-IDGP team for feedback
- Focus Group 1: 15 April 2002
  -Patients: 9, GPs: 4
  -Questionnaire mailed to non-attendants (patients and GPs)

Phase 2

No. Participants

Patients = 20
GPs = 6
* Two new patients enrolled

- Developed Focus Group 2 questionnaire
  -Circulated to UoW-IDGP team for feedback
- Developed Non-participant questionnaires
- Focus Group 2: 17 June 2002
  -Focus group audio and visually recorded
- Non-participant questionnaires mailed out to non-attendants (patients and GPs)
- IDGP IT staff designated to ensure that the system is functional

Phase 3

No. Participants

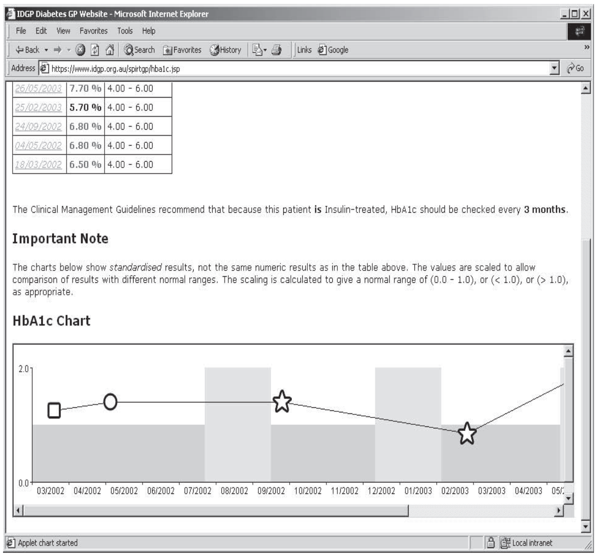
Patients = 20
GPs = 3
* Three GPs withdraw from the trial, two of them due to moving location

- Developed patient Focus Group 3 questionnaire
- Patient Focus Group 3: 16^{t} September 2002
  -Focus group audio and visually recorded
  -Questionnaire 3 is mailed to non-attendant patients
- GP interview questions developed
- GP interviews are conducted
  -Each interview is audio recorded
  -Results are transcribed
- Evaluation findings documented

Figure 3. *iKey evaluation overview*

- One-to-one interviews
- Postal surveys for patients who did not attend the focus groups

The focus groups were guided by a moderator using a semi-structured instrument. The development of the instrument and survey questionnaires (mailed to non-attendants) were circulated amongst the project management committee and modified according to individual suggestions. Instruments were developed for both patient and GP focus groups and contained both open and closed questions. Three patient and two GP focus groups were conducted. These were scheduled at the start, middle and end of the field trial in order to ascertain the views of patients and GPs at different stages of the trial. The focus groups were run separately so that patients did not feel intimidated by having their GP present. The semi-structured questionnaire used within each focus group consisted of questions that reflected the particular stage of the trial. The questions revolved around user expectations of the iKey system, patient identifiers, actual experiences of the system, levels of patient and GP satisfaction, problems or improvements in service provision (information access and impact on the consultation), the Web site, and factors that impede or assist in the system adoption process. Each focus group lasted approximately two hours. Patients who did not attend a focus group had a questionnaire mailed to them. Simple observation and analysis of video taped consultations


IDGP Diabetes GP Website - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Links
Google
Address
https://www.idgp.org.au/spirtgp/hba1c.jsp
Go

26/05/2003	7.70 %	4.00 - 6.00
25/02/2003	**5.70 %**	4.00 - 6.00
24/09/2002	6.80 %	4.00 - 6.00
04/05/2002	6.80 %	4.00 - 6.00
18/03/2002	6.50 %	4.00 - 6.00

The Clinical Management Guidelines recommend that because this patient **is** Insulin-treated, HbA1c should be checked every **3 months**.

Important Note

The charts below show *standardised* results, not the same numeric results as in the table above. The values are scaled to allow comparison of results with different normal ranges. The scaling is calculated to give a normal range of (0.0 - 1.0), or (< 1.0), or (> 1.0), as appropriate.

HbA1c Chart

Legend

□ = Initial test result

○ = Early test result

☆ = Late test result

Figure 4. *Screen shot of the Web-based patient record*

were also undertaken to evaluate system speed, ergonomics and impact on the consultation.

RESULTS

Database

Figure 4 is a screen capture of the Web-based patient record generated after both the GP's and patient's iKeys had been inserted to enable access through the Web interface. The GP–Patient access page gave a text view and a graphical view of results and how they compared with NSW Health CMGs. The text based area shows the date of the result, the actual result and the CMG result range in tabular form. The actual results (located in the second column of the table) are presented in red or black to enable easy identification of results within and outside the standard range. The chart shows the same results in an easy-to-understand image. The vertical axis line depicts the standard range, while the horizontal axis depicts the time period over which the results were recorded. Results on the Web page are normally shown graphically by coloured dots; in this article as symbols (see Figure 4 legend below). The screen capture below is based on HbA1c results. We chose to display HbA1c as this is generally regarded as the best standard for monitoring diabetes control.

Report Generation

Reports on the Web are generated at two levels: individual and population level. At the individual level, sequential results are graphed and fed back to the GP. A similar format is available to the patient but through a different Web page. Individual GPs can also view adherence to the CMG for each patient. If a patient has abnormally

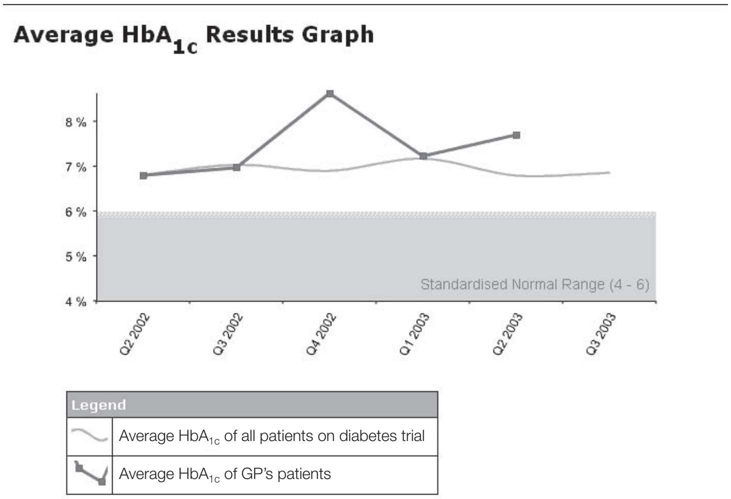


Figure 5. *Example screen shot of report generated*

high results the graph makes it easy to identify this. To access the records a GP can click on the square at the peak of the line and the patients are listed, allowing the records to be viewed, as shown in Figure 5.

Averaged aggregated results are fed back to the patient so they can view the average progress of the entire cohort (approximately 550 patients). Averaged aggregated results are also graphed and compared to the averaged aggregated results of a group of patients treated by a particular GP. This information is presented to the GP quarterly.

Field Trial

A total of six GPs and twenty patients participated in the field trial. Non-participating GPs and diabetes patients were sent questionnaires to establish their reasons for not taking part in the iKey trial. Two-thirds (66%) of GPs stated that they could not spare the time to be trained in using the Smart iKey system and more than half claimed they were already participating in enough IDGP activities. Of non-participating diabetes patients, 33% stated they either did not know or were uncertain about what was involved with the Smart_ID Project (and 25% of those that did were unsure of how to enrol). Most non-participating patients were not confident in using computers (the reverse was true of participating patients). While 80% were reluctant to change the format of their consultations with their GPs, 60% claimed they could access most of their diabetes information without participating in the trial.

Seven patients used their iKey to access records during a consultation with their GP and four patients used their iKeys to access their records independently. Five of these patients experienced technical difficulties, mostly in relation to using iKeys during consultations with their GPs. Patients also commented on the fact that transfer of data to and from the GP's computer seemed very slow. In consultations in which the iKey was used, the video demonstrated more mutual discussion between the patient and the GP.

DISCUSSION

The project has successfully managed to achieve its objective of creating a Web-based patient record for diabetes patients with automated data collection. Creation of such a database will give patients the confidence and freedom to move between different GPs knowing that their records can be accessed by any GP and will seamlessly continue to be updated and maintained. It also enables GPs to readily have access to all relevant patient information and to be able to compare their management and outcomes against national guidelines and with their peers. This should improve patient outcomes.

The project is in keeping with HealthConnect, the current major electronic health record initiative for patient healthcare in Australia. This national programme aims to collect and store individual patient information online, making it accessible to authorised health professionals[5]. It should enable consumers and healthcare providers to make informed decisions in regard to the treatment and management of a patient's health[6]. HealthConnect involves live trial sites that consist of small user groups testing elements of the broader system. The work undertaken over a two-year period will determine both the feasibility and sustainability of HealthConnect as a national network. The trial sites for HealthConnect became operational in late 2002 and are a key mechanism in determining how the network will function in the event of a national rollout[7].

Despite this government initiative, the small number of GP participants in our field trial highlights a fundamental difficulty in recruiting GPs to participate in studies. At present general practice is largely funded by a fee-for-service mechanism. This fails to encourage GPs to adopt a broader research or academically focused view as there is little incentive to do additional work beyond the immediate confines of the consultation. This situation creates a dilemma with respect to implementation of information technology. Proper and effective use of information technology solutions are necessary to improve the efficiency and outcomes of GP care. However, if GPs do not have the time or inclination to evaluate and learn how to use new information technology, they will be unable to reap its benefits.

Nevertheless, the small number of participants in the trial provided valuable insight on experience with the system. In particular, it demonstrated the feasibility of using the system to enable patients to control GP access to their data. Transfer of data to and from the GP's computer was, however, slow and could lead to an increase in consultation times. On average consultations in which the iKey was used took twelve minutes compared to ten minutes in which the iKey was not used. This difference in consultation times could be reduced by the use of broadband connections instead of dial-up modems. However, the possibility that the increase in consultation times could partially be attributed to the more mutual discussion observed in consultations in which the iKey was used, should also be borne in mind.

The patients' views on iKey were favourable. Those who accessed their Web site during the field trial were happy with its contents and a few of them also reported incorrect data that had been entered in their record. The benefits of patients reviewing their medical records has been previously demonstrated. One study found that when they did this approximately one quarter of them provided new health maintenance data and approximately one fifth provided new medication data[8]. Patients consequently regarded the iKey as an empowering technology.

From a practical point of view there is a potential for patients or doctors to misplace or forget their iKey. In this case the GP will not be able to obtain access to the Web-based patient's records. There is also a possibility that patients and doctors may accidentally switch their iKeys. This possibility may be minimised by the use of colour-coded iKeys. Finally, because the patient and GP discuss information that is viewed on the computer screen, the positioning of the patient within the GP's surgery is an important ergonomic consideration.

Overall, the iKeys were viewed as a good mechanism for accessing patient records held at the IDGP. All field trial participants – both GPs and patients – agreed the Smart_ID iKey system had the potential for improving information management in medical practices, and most supported the continued use of such a system in the future. Moreover, almost all expressed a preference for iKeys over smart cards since iKeys could be conveniently placed on a key chain. More generally, most patients also viewed computer/Web-based medical records as being an essential technology for healthcare in the future which is consistent with earlier findings[9,10].

CONCLUSION

The system described here incorporates a generic software interface which is capable of automatically collecting clinical data from MDW on various doctors' computers and uploading this to a patient medical record held on a remote server. A Web interface provided by this server can (a) seamlessly query the patient's database and automatically download new information to MDW at the doctor's surgery; and (b) allow patients access to their own clinical data via the Web.

The use of iKeys for successfully providing patient-controlled access to a centralised electronic health record has been demonstrated. The system promotes patient empowerment through patients being able to visit different GPs and have their records accessed. The system does, however, challenge the traditional notion of a single GP being the sole gatekeeper of patient information.

ACKNOWLEDGMENTS

The Smart_ID System for GPs Project was funded by the Australian Research Council under the Strategic Partnerships with Industry Research and Training Scheme – SPIRT (now referred to as Linkage Grants) – project#C00001904. The permission of the Illawarra Division of General Practice to publish this work is gratefully acknowledged. Thanks are also due to Kellie Kembrey, Liesel Wett, Louisa Raft, Linda Blackmore, Ken Lynch and Peter Feltham of IDGP and to Oliver Jovanovski, Jesse Mitchell, Jarrah Watson, Sherine Antoun and Karolyn Spinks of UoW for their contributions to the project.

REFERENCES

1 UKPDS Group. Effect of intensive blood glucose control with metformin on complications in overweight patients with type 2 diabetes (UKPDS 34). *The Lancet,* 1998; **352**: 854–65.

2 UKPDS Group. Association of glycaemia with microvascular complications of type 2 diabetes (UKPDS 35): prospective observational study. *BMJ*, 2000; **321**: 405–12.

3 Australian Institute of Health and Welfare, *Australia's Health 2002*. Canberra: AIHW, 2002.

4 http://www.privacy.gov.au/act/.

5 http://www.health.gov.au/healthconnect.

6 Davies K. Next to go online: your medical record, *Australian Financial Review*, 16 April; 2002: 16.

7 Commonwealth Department of Health and Aged Care Direction set for HealthConnect. http://www.health.gov.au/healthonline.

8 Kuperman DJ, Sussman A, Schneider LI, Fisiko JM, Bates DW. Towards improving the accuracy of the clinical database: allowing outpatients to review their computerized data. *Proc AMIA Symp* 1998; 220–24.

9 Bomba D, de Silva A. An Australian case study of patient attitudes towards the use of computerised medical records and unique identifiers. *Proc.World Medical Informatics Conference* 2001, London: 1430–4.

10 Bomba D, Land T. A Survey of patient attitudes towards the use of computerised medical records and unique identifiers in four Australian GP practices. *The Journal on Information Technology in Healthcare* 2003; **1**: 31–45.

INVITED COMMENTARY

The business and financial applications of computers in healthcare are undeniably meritorious. In clinical practice their merits in applications such as image processing are also undeniable. However, in other areas of healthcare, and in particular with respect to direct patient care, convincing relevant stakeholders of their merits is more difficult. The reasons for this are multi-factorial but pertinent factors include fear and ignorance of new technology, a perception by healthcare providers that the use of computers will require more of their precious time, and a perception by payers that their use will require more of their limited funds. As a consequence, the historical imperative presented by the miraculous personal computer (PC) over a quarter of a century ago, is yet to be fulfilled in patient care.

To appreciate the concept, merit may be broken down into its elemental parts. Obviously, merit includes an element of *time spent* and an element of *reimbursement obtained*. Merit must also include an element of the *perceived value of the task*. Notably, each element is assigned a subjective merit by a different individual who is a stakeholder in the outcome. For example, while the *time spent* element is mainly under the control of the provider, the *reimbursement granted* element is entirely under the control of the payer and the *perceived value* element is mainly under the control of the patient. While each individual may assign great merit to their respective element, any given task may or may not be performed depending on the relative merits assigned by the other stakeholders. In other words, tasks that are done routinely have elements whose assigned merit satisfies all three stakeholders.

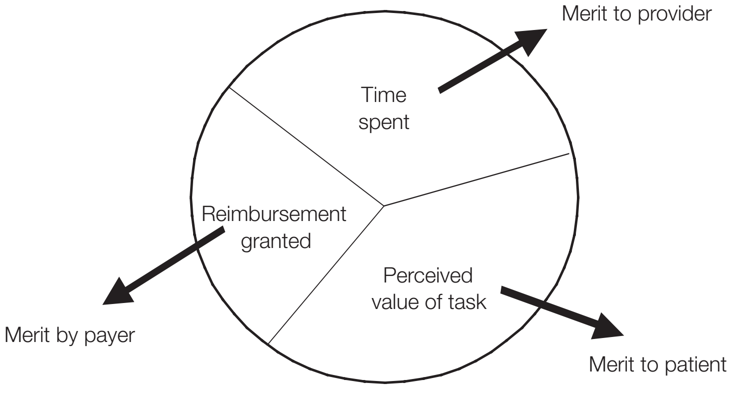


Figure 1. *Typical circle of merit showing sectors containing respectively, elements of time spent, perceived value of task and reimbursement granted*

Each element has a stakeholder, respectively, the provider, the patient and the payer, who subjectively assigns merit as shown by the attached callouts. The circle is not balanced, i.e., the segments are not of equal size.

The question, therefore, arises as to how these three disparate elements may be reconciled in such a way as to predict the overall merit of any initiative, e.g. of a project deploying information technology (IT) in patient care.

One approach is to assume that these three elements can be combined according to the universal tenets of the human psyche, best represented by the simple question, 'What's in it for me?' For any given task to have overall merit, there obviously must be a balance among these three elements. Accordingly, merit may be thought of as a circle with three segments as shown in Figure 1. Unless the segments are equal, one or more of the stakeholders will experience an element of unfairness and the overall merit of the task will be questioned. Such tasks will not be performed routinely until the element of unfairness is removed. This appears to be the definitive working rule when it comes to applications of IT in patient care[1].

By applying the circle of merit it is possible to explore various scenarios. For example, let us assume that a conscientious payer is familiar with the Diabetes Control and Complications Trial[2,3]. As a consequence the payer perceives the possibility of reducing ongoing and future costs by granting a meaningful reimbursement for providers to intensify their care of diabetic patients in order to improve blood glucose control. To achieve this while avoiding the greater costs of manual methods[3], the payer agrees to cover telemedicine services providing formal blood glucose control algorithms and outcomes monitoring to diabetic patients using technology capable of these goals[4]. Given this financial incentive, it is likely that providers will spend the time and effort to offer telemedicine services to their diabetic patients. Patients would participate in the project due to the benefits associated with improved blood glucose control. The payer would, however, probably enter stipulations, e.g. payment would only be made for patients whose clinical outcomes showed merit, and reimbursement would be restricted to additional blood glucose monitoring equipment and test strips required for reporting to the telemedicine resource and for use in the blood glucose control algorithms. These stipulations are in keeping with the 'What's in it for me?' question. It works best when it works both ways. The circle of merit would be balanced.

At this point it should be clear that the payer can influence, if not outrightly control, the overall merit of any clinical task simply by granting or denying reimbursement. This privilege is not granted to any of the other stakeholders. Thus regardless of the merit assigned to any new clinical activity by the provider or the patient, the new task will not become part of routine practice unless the payer, finding similar merit, grants a fair reimbursement.

This paper from an Australian group describes the development and testing of a simple tool for patients to control access to a remote database containing information relevant to their diabetes care. Fields were filled automatically from laboratories and manually by the providers. Access was controlled by the sequential insertion of USB iKeys by the patient and then the provider. The iKeys contained an encrypted password. Preliminary testing of the technical aspects demonstrated the feasibility of such a database and the validity of control of access using these portable key-devices. Notwithstanding the value of such a solution in the management of diabetes, provider enthusiasm was limited, as reflected by the low number of general practitioners (GPs) who participated in the trial. The limited enthusiasm arose due to the extra time needed to learn how to use the system and the GPs feeling that they were already involved in enough activities. There was also an absence of reimbursement to encourage participation. Notwithstanding the merit of the technical solution, the aforementioned circle of merit is not balanced. Until the circle is balanced with payers acknowledging the merit and granting adequate reimbursements, computers in diabetic patient care may well continue to be a solution in search of a problem.

REFERENCES

1 Albisser AM, Harris RI, Albisser JB, Sperlich M. The impact of initiatives in education, self-management training, and computer-assisted self-care on outcomes in diabetes disease management. *Diabetes Technol Ther* 2001; **3**: 571–79.

2 The DCCT Research Group. The effect of intensive treatment of diabetes on the development and progression of long-term complications in insulin-dependent diabetes mellitus. *N Engl J Med* 1993; **329**: 977–86.

3 The DCCT Research Group. Resource utilization and costs of care in the Diabetes Control and Complications Trial. *Diabetes Care* 1995; **18**: 1468–78.

4 Albisser AM, Harris RI, Sakkal S, Parson ID, Chao SC. Diabetes intervention in the information age. *Med Inform (Lond)* 1996; **21**: 297–316.

A Michael Albisser, PhD.
Chronic Disease Management Services,
1400 South Ocean Drive #604,
FL 33019
USA
albisser@nidm.org

© *The Journal on Information Technology in Healthcare* 2004; **2**(5): 343–352

Peer-to-Peer Communication System for Sharing Electronic Medical Records

*Shinji Kobayashi, Takefumi Ueno**, *Kazuhiko Kato*[†], *Yoshiaki Nose*[§], *Mine Harada*

Departments of Medicine and Biosystemic Science, Kyushu University Graduate School of Medical Sciences, [*]Computer Science, University of Tsukuba, [†]Psychiatry, Kurume Medical University and [§]Medical Information Science, Kyushu University Graduate School of Medical Sciences, Japan.

ABSTRACT

Objective: Collaboration among medical specialists is necessary for effective care. Although a number of regional medical collaboration systems have been developed using client/server (C/S) models, the drawback of this system is that collaboration between doctors is limited to within this network. To overcome this barrier to collaboration, we have developed a preliminary peer-to-peer (P2P) medical collaboration system as open source software.

Design: A medical collaboration system using a peer-to-peer (P2P) network model.

Setting: The system can be used for medical collaboration in any country.

Method: We adopted Java as the development language and used JXTA 2.1 as the P2P framework. The software consists of three modules: P2P communication, referral letter editor and message management modules. Messages are sent and received via an encrypted pipe to counter Internet sniffing.

Result: We successfully managed to send medical referral letters using our P2P medical collaboration grid system. The system has been developed using open source code and is considerably cheaper than a client server network.

Conclusion: This system enables seamless collaboration between medical institutes over a wide area, at low cost, using a robust network. Some problems remain to be solved, but this next-generation network has the capacity to enrich medical practice.

INTRODUCTION

Optimal shared patient care requires medical professionals to collaborate through referral letters that summarise a patient's medical history and/or give recent pertinent medical information. This has traditionally been done using paper documents, but there is a global move towards electronic referrals. In practice this can be achieved over a wide area network, using a client/server (C/S) model[1–5]. One of

Correspondence and reprint requests: Dr Shinji Kobayashi, Medicine and Biosystemic Science, Internal Medicine, Medicine and Surgery, Kyushu University Graduate School of Medical Sciences, Fukuoka 812-8582, Japan. E-mail: skoba@intmed1.med.kyushu-u.ac.jp.

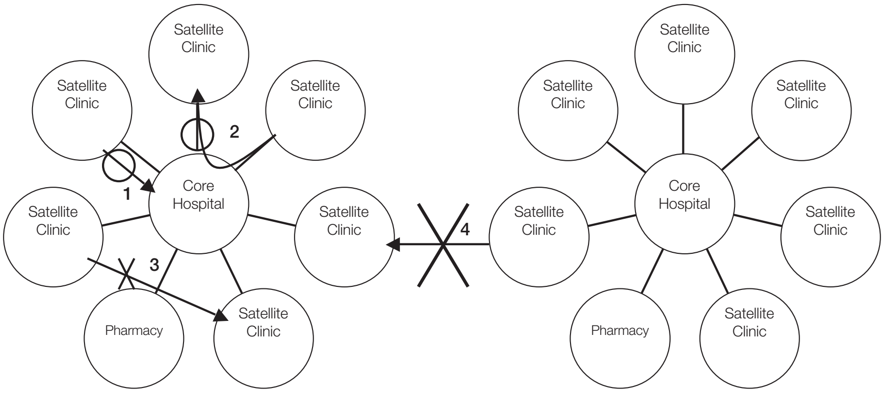


Figure 1. *Typical client/server network model*

In this model, a satellite participant can refer a patient from the satellite to the central hospital (arrow 1) or to another satellite via the central hospital (arrow 2). However, a participant cannot refer a patient to another satellite directly (arrow 3) or to another network (arrow 4).

the drawbacks of this model is that it limits communication and collaboration for electronic medical records (EMRs) and referral letters to within a specified network (Figure 1). A doctor can only make an electronic referral to another doctor if both doctors belong to the same network. In practice, medical professionals frequently refer patients to colleagues who are outside their own computer network. Consequently the C/S model does not adequately meet the needs of real medical

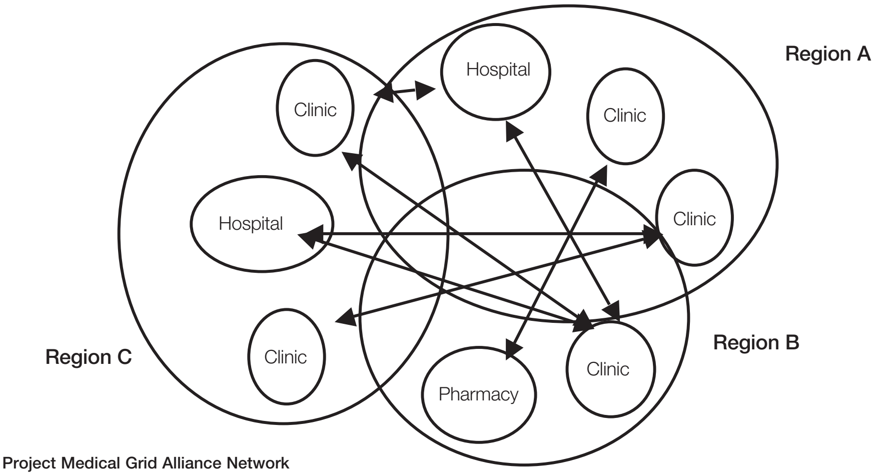


Figure 2. *P2P network model*

In this model, a participant can make seamless referrals to other participants outside the network region.

relationships. In addition it is very expensive to maintain the network in a C/S model. The server contains many electronic patient records and secure administration of this server is expensive.

To overcome this barrier to medical communication, we have attempted to develop a medical-record-sharing system using a peer-to-peer (P2P) network (Figure 2). The perceived advantages of our system are that it will enable all hospitals to be connected seamlessly and will be cheaper to maintain than a C/S model. The system is based on open source software[6], and consequently any medical information system can freely join the network.

METHODS

Java was adopted as the development language and the system was developed using Sun Java 2 Standard Edition Software Development Kit (J2SE SDK) 1.4.2[7]. JXTA 2.1[8] (JXTA technology is a set of open, generalised peer-to-peer protocols that allows any connected device on the network to communicate and collaborate), was used as the P2P framework. Eclipse 2.1.1[9] was used as the integrated development environment (IDE) and Concurrent Versions System (CVS) [10] used to administer the source code.

The system has three modules:

- Medical referral letter editor
- P2P communication
- Message management modules

Medical Referral Letter Editor Module

The patient referral letter implements a graphical user interface (GUI) to edit the message. The information in each message is stored as a Java instance and contains:

- Patient name
- Date of birth
- Sex
- Age
- Chronic illnesses
- Clinical course
- Past medical history
- Family history
- Prescribed medications
- Other notes

After editing the message, the doctor sends it to another doctor using the P2P communication module. Doctors available on the P2P network are listed in a window and can be selected by the user. Sent messages are stored by the message management module.

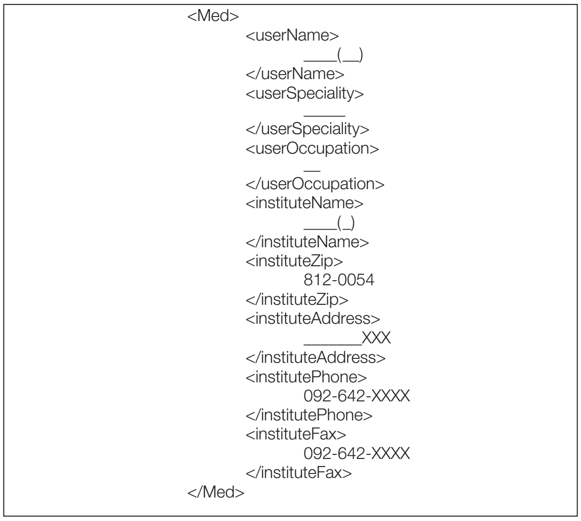
P2P Communication Module

There are three main classes used for managing P2P communications, and sixteen supplementary classes. Further details regarding implementation of this module can be found in the programmer's guide for JXTA[11]. This module offers the following features:

- The ability to create or join a PeerGroup with password authentication.
- The option of extending PeerAdvertisement with the hospital (institute) name, address, doctor's name, doctor's speciality, telephone number and fax number.
- The ability to publish and discover the extended PeerAdvertisement in real time.
- Secure peer-to-peer connection via an encrypted pipe.

The peer discovery algorithm is a distributed hash table model implemented with JXTA. A PeerAdvertisement is generated when initiating a group on a peer, and contains all the necessary parameters, including the participant's medical information in eXtensible Markup **L**anguage (XML) format (Figure 3). PeerAdvertisement propagates within the PeerGroup, which can connect segments within a network cloud, and requires password authentication to join.

The network authentication procedure starts when a user logs into the P2P network using his/her ID and password. Next, each peer searches the PeerGroup for medical communications or creates a PeerGroup with password authentication. Finally, each peer joins a PeerGroup using a common password. Each peer propa-



```
<Med>
        <userName>
                ____(__)
        </userName>
        <userSpeciality>
                _____
        </userSpeciality>
        <userOccupation>
                __
        </userOccupation>
        <instituteName>
                ____(_)
        </instituteName>
        <instituteZip>
                812-0054
        </instituteZip>
        <instituteAddress>
                _______XXX
        </instituteAddress>
        <institutePhone>
                092-642-XXXX
        </institutePhone>
        <instituteFax>
                092-642-XXXX
        </instituteFax>
</Med>
```

Figure 3. *The medical information contained in the extended PeerAdvertisement*

The JXTA PeerAdvertisement uses XML format. We extended this to describe peer information with respect to medical speciality and organisation.

gates its organisation's and doctor's information within this password-protected PeerGroup. A participant can send an electronic referral letter to another doctor, who can join this network using this authentication, on demand. The PeerGroup provides an encrypted pipe for peer-to-peer connections and sends a ciphered message with patient information using the TLS 1.0 protocol[12] to provide security against Internet sniffing.

When a message is received, this module decrypts the message and stores it on a local hard disk using the message management module.

Message Management Module

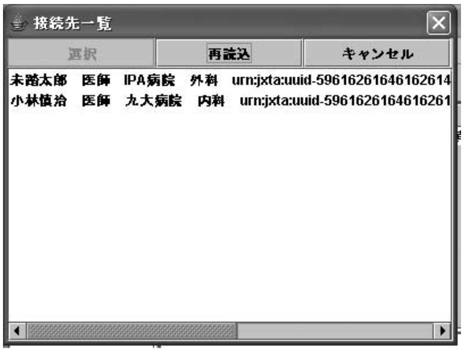
Each electronic medical referral letter is serialised as a Java instance. The serialised instance is saved and loaded on a local disk via a Java stream. This module stores messages that are sent and received via the P2P communication module. The messages are listed in a table and can be viewed as three windows, similar to the layout in MS-OutLook. This module also manages other items in the extended PeerAdvertisement, as already described.

RESULTS

Deployment

It takes about five minutes to configure this system for use after downloading it. As there is no server, a client only needs to configure for his/her network. The configuration needs the P2P setting and user information. The only cost to join this network is that of downloading it.

We have used this P2P network to successfully transfer encrypted electronic medical referral letters between doctors. The system finds peers automatically and



未踏太郎　医師　IPA病院　外科　urn:jxta:uuid-59616261646162614

小林慎治　医師　九大病院　内科　urn:jxta:uuid-5961626164616261

Figure 4. *List of connected peers*

The list shows information on the participants. Any participant can select a medical specialist for collaboration from this list. There are buttons for Select, Reload, and Cancel. Each line conveys information on the medical specialist: his/her name, occupation, organisation name, speciality field, and JXTA unique ID.

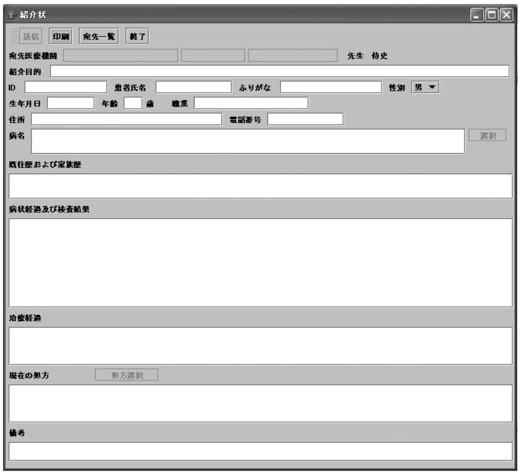
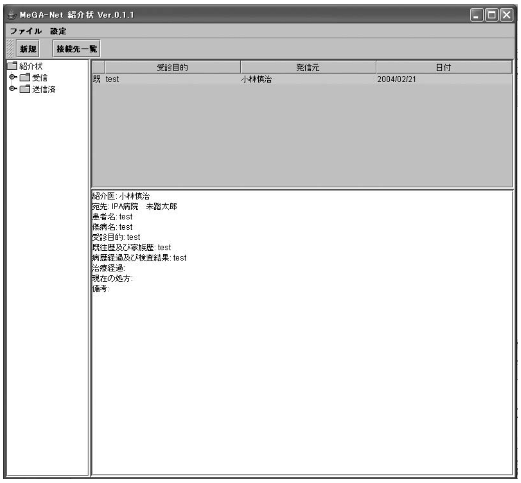


Figure 5. *Editor for the referral letter*

A user can edit a medical referral letter and send it to another user. The four buttons are for Send, Print, List connected peers, and Quit. The first line includes the name and address of the medical organisation and the doctor's name and department. The second line is the field outlining the aim of the introduction. The fields below the third line include patient information (from upper left to lower right): identification, name, pronunciation of the name, sex, birthday, age, occupation, address, phone number, diseases, past and family history, history of present complaint, laboratory data, clinical course, medications taken and notes.



	受診目的	発信元	日付
既	test	小林慎治	2004/02/21

紹介医: 小林慎治
宛先: IPA病院　未踏太郎
患者名: test
傷病名: test
受診目的: test
既往歴及び家族歴: test
病歴経過及び検査結果: test
治療経過:
現在の処方:
備考:

Figure 6 Message management

Messages are saved to two folders: 'Sent' and 'Received', which can be switched by choosing the left panel tree. The list of messages can be viewed by choosing the relevant folder in the left panel and each message can be viewed by choosing the subject in the upper panel: aim of introduction, sender/receiver, and date. The chosen message is viewed in the lower right panel.

information on peers can be viewed in a list window (Figure 4). The list shows the doctor's name, speciality, organisation name and JXTA peer ID. The recipient of the letter can be chosen from this list.

The user can edit a referral letter within a GUI (Figure 5). After editing it, the message is instantly sent to the selected peer. Messages are received automatically and saved on a local hard disk. Messages are saved in two folders: 'Sent' and 'Received'. The list of messages can be viewed by choosing the relevant folder in the left panel, and individual messages can be viewed by choosing the subject in the upper panel (Figure 6).

DISCUSSION

The project has so far demonstrated that it is possible to transfer encrypted electronic medical referral letters between doctors using a P2P network. This overcomes the major problem of interconnecting centres when setting up a healthcare network[13]. Use of the P2P network gives doctors the freedom to choose which medical specialist to collaborate with rather than having this decided for them by the network architecture. Since the system runs on Java VM, it also does not require a specific operating system (OS). Consequently the system has few restrictions, not only in terms of medical use, but also in terms of the computer environment.

Although there are standard messaging protocols in healthcare, e.g. HL-7[14], these protocols do not govern the transmission protocol. We are unable to develop a method of transferring messages to all hospital information systems, because some medical standards are incompatible with an open source license. For example, we cannot include HL-7 protocol specifications in our documents and publish them as open source software. The definition of open source[15], as defined by the Open Source Initiative, consists of ten criteria which are incompatible with HL-7 ownership, even though HL7 is an open standard and in the public domain. This problem has been addressed by others by using an XML data schema for their system instead of medical standards[16]. We, however, chose to use an open source license over medical standards because there are more available resources in the open source field than in the medical standard field.

Table 1. *Cost of the network*

(Estimate based on other medical record network services developed in Japan using national funds.)

Network model	Development	Maintenance (Server)	Maintenance (Participant)
P2P	$60,000	$0	$0
C/S	$2,000,000	>$100,000/year	>$1,000/year

One remarkable advantage of this system is its total cost (Table 1). There is no cost for a network server and since we used open source products, we did not incur significant development costs. There is, in addition, no cost or fee for participants who wish to join this network. This constitutes a major advantage, as compared to other systems. In Santa Barbara County, USA, a P2P-based medical system has been demonstrated to reduce the costs of medical communication[17].

However, there are a number of disadvantages with the system compared to C/S systems. The most critical of these is that the system cannot send a message to an off-line participant. In the C/S system, the server stores messages for off-line participants. To resolve this problem, we are working on a method to enable messages to be sent to off-line participants. The system will queue a message locally until the participant is on-line and can receive the message.

Compared to the C/S model, the P2P network is also a looser combination of information systems. In general, tight information integration is easier to achieve when systems share the same database. If, for example, chronologically ordered data such as laboratory data are needed, the C/S model is superior in integrating this data[4]. Consequently, to optimise performance it may be necessary to develop a tight information combination interface with other systems. However, since our source code is open, others can adapt it to the communication module of their hospital information system. Our licence permits the use of our source code in other proprietary software.

This system is robust against malicious Internet attack because the target is widely distributed and therefore it is impossible for an attacker to jeopardize the entire system. Even if an attacker affects the system of one participant, the other participants can still communicate with each other. The system does scatter peer information, including the organisation's name, doctor's name, address, phone number, and FAX number, but this information is also available in public directories such as Yellow Pages. The system, however, does not scatter patient records; it sends a message only to the relevant medical specialist. To satisfy patient privacy regulations we have devised a security policy in which peers can only send an EMR to an associated doctor when referring a patient. In addition, the documented agreement of the patient is necessary to allow this transfer to take place. Another peer cannot access unrelated EMRs. Under this policy, the risk of information leakage should be minimal because each participant only stores information on his/her own patients.

Although this system encrypts the message for transmission, individual peer credentials are insufficient. We recognised the need for implementing a public key infrastructure (PKI)-based digital signature and authentication mechanism instead of password authentication. However, maintaining the certificate authority (CA) does incur some expense. The Japanese government is planning to implement a government PKI (GPKI) for healthcare, and we anticipate using it, rather than attempting to build our own CA. An alternative solution for authentication is to apply a distributed trust model[18], which is a network of trust, like a Pretty Good Privacy (PGP)[19] key ring. The project JXTA that we have applied to our system attempts, with difficulty, to deal with security issues and the implementation of PKI[3] and we are now designing a new PKI-based security system.

CONCLUSION

We have developed a preliminary P2P collaboration system that can transfer electronic medical information seamlessly. As compared to other systems, our system has fewer restrictions, is inexpensive and can be used to construct a robust network. The system does have a number of problems to overcome, but the use of open source software gives it the potential to evolve to overcome these problems. In our opinion this system has the capability and potential to enrich medical practice.

ACKNOWLEDGEMENT

This project was supported by a grant under the Exploratory Software Project FY2003 (IPA, Japan).

REFERENCES

1 Takeda H, Matsumura Y, Kuwata S *et al.* Architecture for networked electronic patient record systems. *Int J Med Inf* 2000; **60**: 161–67.

2 Bruun-Rasmussen M, Bernstein K, Chronaki C. Collaboration: a new IT-service in the next generation of regional health care networks. *Int J Med Inf* 2003; **70**: 205–14.

3 Altman JE. PKI security for JXTA overlay network. http://www.jxta.org/docs/pki-security-for-jxta.pdf.

4 Hung K, Zhang YT. Implementation of a WAP-based telemedicine system for patient monitoring. *IEEE Trans Inf Technol Biomed* 2003; **7**: 101–7.

5 Lampsas P, Vidalis I, Papanikolaou C, Vagelatos A. Implementation and integration of regional health care data networks in the Hellenic National Health Service. *J Med Internet Res* 2002; **4**: E20.

6 The BSD License. http://www.opensource.org/licenses/bsd-license.php.

7 Java[tm] 2 SDK, Standard Edition Version 1.4.2; at http://java.sun.com/j2se/1.4.2/download.html.

8 JXTA 2.1. At http://download.jxta.org/archive/jxta2.1_bin.zip.

9 Eclipse 2.1.1. At http://www.eclipse.org/downloads/.

10 Price D. CVS. At http://www.cvshome.org/.

11 Project JXTA v2.0. *Java Programmer's Guide*. http://www.jxta.org/docs/JxtaProgGuide_v2.pdf.

12 Dierks T, Allen C. The TLS protocol Version 1.0 in *RFC 2246*. http://www.ietf.org/rfc/rfc2246.txt.

13 Ruotsalainen P. A cross-platform model for secure electronic health record communication. *Int J Med Inf* 2004; **73**: 291–95.

14 Bylaws of Health Level Seven. http://www.hl7.org/about/bylaw.htm.

15 The Open Source Definition. http://www.opensource.org/docs/definition.php.

16 Brelstaff G, Moehrs S, Anedda P, Tuveri M, Zanetti G. Internet patient records: new techniques. *J Med Internet Res* 2001; **3**: E8.

17 Czerwinski AA. Bringing everyone's information closer to the point of care. In: *Annual Healthcare Information and Management Systems Society Conference and Exhibition*. Atlanta, USA, 2002.

18 Chan R, Poblano YW. A distributed Trust model for Peer-to-Peer Networks. http://www.jxta.org/docs/trust.pdf.

19 PGP. http://www.pgp.com/.

INVITED COMMENTARY

World wide, healthcare institutions are moving towards the establishment of electronic medical records as part of a strategy to improve quality, efficiency and cost-effectiveness of care. Ready access to electronic health data is essential to these aims. In addition as part of a global movement towards patient empowerment, there is growing awareness and demand by patients to have access to and control of their health (and wellness) data. For IT professionals in healthcare, this, however, raises the problem as to what architecture to use to cope with the expected future demand for medical exchange whilst at the same time ensuring privacy and confidentiality of patient data.

In Austria, for over a decade, electronic exchange of medical reports has taken place through privately operated mailbox dialup systems. However, the security of standard systems is not adequate to satisfy the requirements for confidentiality and privacy. Today these communication networks have migrated to a new, Internet-based infrastructure using S/MIME (Secure/Multipurpose Internet Mail Extensions) encoded emails and PKI (Public Key Infrastructure) to enable secure communication between healthcare institutions. The ability to find relevant personnel has been aided by the development of LDAP (Lightweight Directory Access Protocol). LDAP servers, such as ClickMail Central Directory, index all the data in their entries, and 'filters' may be used to select just the person or group you want. The Austrian Medical Association has make extensive efforts in recent years to establish an officially certified LDAP directory of all healthcare institutions and professionals in Austria, providing the basis for using PKI for secure communication.

Establishing Web portals was a logical step for larger healthcare institutions to enable them to be more flexible and independent. However, although this may serve their own individual requirements, it does not readily enable the average general practitioner to communicate with the institution. In addition, a Web portal does not really solve the problem of exchanging data between the IT systems of different healthcare institutions.

One possible solution to overcoming these problems is the use of peer-to-peer (or 'GRID') technology. It is consequently pleasing to read the efforts of Kobayashi and colleagues to develop such a network. They have demonstrated the feasibility of using this in practice and elaborated on several of its features, such as Peer-Advertisement, that will enable doctors to find essential information on other doctors quickly and easily. This should advance the process of providing reliable and practicable authentication between communicating parties.

The authors deserve congratulations on their innovative work and I wish them luck in further developing it and establishing it as a communication system for healthcare professionals.

Dr. Raimund Vogl, PhD
Managing Director
HITT – Health Information Technologies Tirol
Templstrasse 32/2
A-6020 Innsbruck
r.vogl@hitt.at

HIT J © *The Journal on Information Technology in Healthcare* 2004; **2**(5): 355–364

Development of an Expert System for Aiding Migraine Diagnosis

Danny Kopec, Gennady Shagas, Jay Selman, Daniel Reinharth*, Suzanne Tamang*

Department of Computer and Information Science, Brooklyn College and * Albert Einstein School of Medicine, Bronx, New York, USA.

ABSTRACT

Objective: To design and develop a prototype expert system to aid physicians in diagnosing migraines and their sub-types.

Design: Developmental process.

Setting: Since the system is Web-based, it is accessible to any physician or healthcare provider anywhere in the world.

Methods: The knowledge acquisition process was facilitated by a physician who served as our domain expert to identify the application's key elements. We have included the essential questions and rules that are necessary for building an expert system for aiding migraine diagnosis and distinguishing migraines from other types of headaches. The application utilises a data collection form, the C Language Integrated Production System (CLIPS), and a program with the appropriate rules, which are written in the CLIPS language. The front end and middle tier is built, and the connection between the HTML (Hypertext Markup Language) front end and the expert system shell CLIPS is established. We also created an XML (Extensible Markup Language) representation of the International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), including the disease category 346 (Migraine), and published it on the Web. The system was tested using data from six patients with a clinical diagnosis of migraine.

Results: For each of the six cases the system indicated that the likelihood of the diagnosis of migraine was greater than 75%, with the probability for fourteen different sub-types ranging from 0% to 97%. The time taken by the system to process the data was related to the number of questions asked and the number of sub-types embedded in the system, but was less than thirty seconds for all cases tested.

Conclusion: We have developed an expert system for aiding physicians in the diagnosis of migraines and their sub-types. Further development and evaluation of the clinical accuracy of the system are necessary before it can be recommended for routine clinical use.

Correspondence and reprint requests: Danny Kopec, Department of Computer and Information Science, Brooklyn College, 2900 Bedford Avenune, Brooklyn, NY 11210, USA. E-mail: kopec@sci.brooklyn.cuny.edu.

INTRODUCTION

Headaches in a variety of forms are one of the most common areas of complaint presenting to physicians. They present a diagnostic challenge as they can be caused by more than 100 diseases[1], and accurate diagnosis of the cause is essential to optimal treatment. With respect to migraines, there are at least twenty different types and specific, individualised treatment is more effective than nonspecific therapies in relieving symptoms, preventing attacks and maintaining patient function[2]. However, migraines are frequently underdiagnosed or misdiagnosed as tension type headaches[3–6]. Consequently many patients do not receive appropriate treatment and continue to suffer attacks with associated disabling symptoms.

The International Headache Society has proposed a classification scheme for headaches including rules to diagnose migraines[7,8]. These, however, appear to be over-simplified and we consequently have developed a Web-enabled application using more sophisticated rules to aid diagnosis of migraines. The rules for the application are represented in the C Language Integrated Production System (CLIPS) expert system shell. CLIPS is a product development and delivery expert system tool which provides a complete environment for the construction of rule and/or object based expert systems[9].

METHODS

The CLIPS expert system shell provides a cohesive tool for handling a wide variety of knowledge with support for three different programming paradigms:

- Rule-based
- Object-oriented
- Procedural

Rule-based programming allows knowledge to be represented as heuristics, or 'rule of thumb', which specify a set of actions to be performed for a given situation. Object-oriented programming allows complex systems to be modeled as modular components, which can be easily reused later. The procedural programming capabilities are similar to capabilities found in languages such as C. CLIPS can be embedded within procedural code, called as a subroutine, and integrated with languages such as C and Java. CLIPS can easily be extended by a user through the use of several well-defined protocols, and it can be implemented in Web-based applications using the Common Gateway Interface (CGI) bin or Java servlets.

The clinical diagnosis of migraine is based on headache characteristics and associated symptoms, particularly nausea and vomiting. Figures A3 and A4 in the Appendix show the form containing the questions identified as relevant to the diagnosis. The program itself can dynamically generate the forms and these are directly filled in on the computer. Paper forms are not required but may be necessary for people without direct access to a computer. If paper forms are used then data entered from the form to a computer will need to be validated and corrected, if necessary.

The International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), classifies migraines into twenty different sub-types[10]. To test our system, research was performed on a subset of questions and types of migraines. We selected only ten of these questions for our research, and created the appropriate program. From the twenty known types of migraines we randomly selected fourteen types. The rules we created are based on existing criteria[6–7]; however, we introduced additional artificial dependencies for the purpose of testing system performance. The certainty of each diagnosis is calculated by three parameters; these parameters are chosen by the program according to certain rules related to the answers given.

Table 1. *Migraine Expert System Questions and Answers for six cases with a clinical diagnosis of migraine*

	Answers for Case					
Question	1	2	3	4	5	6
1 Age (in years)?	0–29	30–49	50–69	70–up	0–29	50–69
2 Gender?	female	male	female	male	male	female
3 Does your headache occur during menstruation, ovulation, menopause or oral contraceptives?	yes	–	–	–	–	–
4 Does your headache BEGIN on right side?	yes	yes	no	yes	no	no
5 How does your headache feel?	dull	aching	throbbing	unknown	aching	dull
6 Does pain interfere significantly with school activity*	yes	no	no	no	no	no
7 Does vomiting accompany the headache?	no	yes	no	yes	yes	no
8 Does nausea accompany the headache?	yes	–	no	–	–	no
9 The number of headaches per month?	0–2	6–9	10–19	0–2	3–5	6–9
10 Can your headache be triggered by certain foods, odors, stress or weather changes?	yes	no	yes	no	no	yes

Note: School would apply to an adolescent or young adult in graduate school.
Here we present only ten questions, but we are currently working on the comprehensive program containing the set of all available questions and rules.

These simplifications are necessary to create a prototype of the expert system for migraines, and to test the rules and performance, and to later extend the system. We also introduced additional complexity into the CLIPS rules to increase the accuracy of migraine diagnosis.

To test our system we entered answers obtained by interviewing six patients, diagnosed with migraines. The data was entered directly using an existing CLIPS interface. The user's dialogue with the CLIPS application is presented in the Appendix.

We also evaluated the execution time of the system with respect to the number of questions asked and the number of migraine types embedded in the system.

RESULTS

The results from the CLIPS system for the six patients with a known diagnosis of migraine are shown in Table 2 below: In all patients the certainty for a diagnosis of migraine is at least 75%, but the sub-diagnoses vary from 0% to 97%. For example, Patient 1 has three possible types of migraine with the certainty of Horton's neuralgia being highest (88%), and for atypical migraine being lowest (40%). Missing values for the other eleven types of migraine indicate that the certainty of such types is negligible. For the six patients evaluated, for the fourteen different types of migraine, the system helps to narrow 84 (14 × 6) possible diagnoses down to 48 (3 + 11 + 8 + 13 + 7 + 4).

The precision of the system may be improved by increasing the number of questions. As shown in Figure 1 this increases the time that the system takes to process the data. This increase in time of a few seconds is, however, of no clinical

Table 2. *Certainty of a specific diagnosis for various cases*

			Certainty for each Case Number (%)					
	ICD-9 Code	Migraine description	1	2	3	4	5	6
1	346.0.1	Migraine preceded by ...	–	40	92	36	–	40
2	346.0.2	Migraine with aura	–	–	–	20	20	–
3	346.1.1	Atypical migraine	40	–	–	20	20	–
4	346.1.2	Sick Headache	–	36	36	59	20	–
5	346.2.1	Cluster headache	64	20	–	36	–	–
6	346.2.2	Histamine cephardia	–	36	36	59	–	40
7	346.2.3	Horton's neuralgia	88	20	20	20	–	80
8	346.2.4.1	Migraine abdominal	–	20	–	36	–	–
9	346.2.4.2	Migraine basilar	–	76	–	76	76	–
10	346.2.4.3	Migraine lower half	–	40	40	68	40	–
11	346.2.4.4	Migraine retinal	–	40	–	68	40	–
12	346.2.5	Neuralgia	–	40	40	20	–	–
13	346.2.8.1	Migraine hemiplegics	–	–	97	–	–	80
14	346.9	Migraine, unspecified	–	40	40	68	40	–

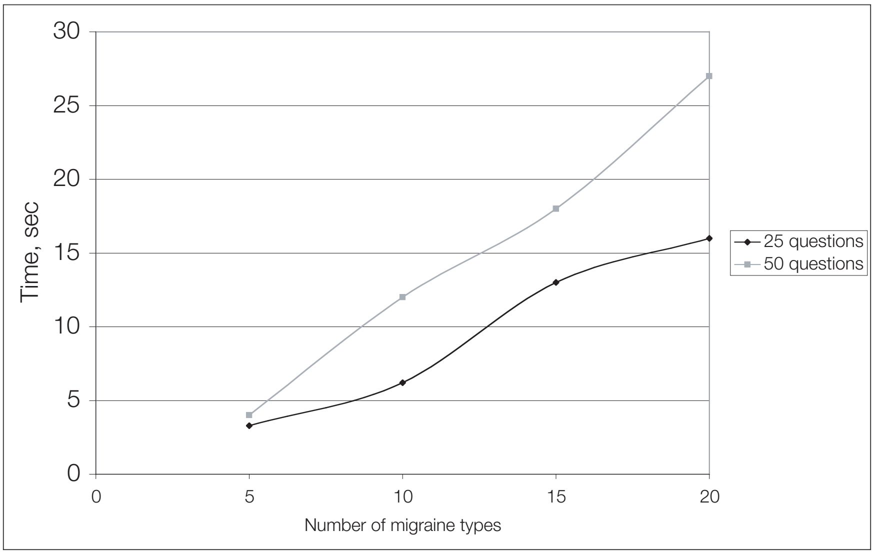


Figure 1. *The execution time for the CLIPS procedure with respect to the number of questions asked and the number of migraine types embedded into the system*

significance. The time to process the data is also affected by the number of migraine types embedded into the expert system. Increasing the number from the 5 most common migraine diagnoses to 20 types increases the execution time from 3 to 17 seconds (see Figure 1). Again this increase in time is of no clinical significance.

DISCUSSION

Recent advances in understanding the pathophysiology of migraine combined with better pharmacotherapy have improved treatment of migraineurs with respect to relieving symptoms, preventing attacks and maintaining functionality. However, for patients to benefit from appropriate therapy, accurate diagnosis of migraines is essential. This is based on the history, but physicians frequently fail to ask all the relevant questions necessary to make the diagnosis. This is demonstrated by a recent study which found that the documented history was inadequate to exclude the diagnosis of migraine in two-thirds of cases in which a diagnosis of non-migraine headaches was made[6]. Data from other studies and surveys have also confirmed that migraines are frequently underdiagnosed or misdiagnosed as tension headaches[2–5].

The system we have developed aids the diagnosis of migraines by ensuring that necessary questions to make the diagnosis are asked. The system was tested using only ten questions but twenty-three essential questions have been identified for helping to distinguish migraines from headaches. More questions should help to improve discrimination. Some of these questions may be omitted depending on answers to previous questions. For example, the question 'Does your headache occur during menstruation, ovulation, menopause or oral contraceptives?' will appear only if the answers to the previous questions 'Age (in years)?' and 'Gender?' are '0–29 or 30–49' and 'Female' respectively .

The system has been developed using the CLIPS expert system shell as this tool provides a complete environment for the construction of rule- and/or object-based expert systems[9]. It can include a number of features including support for modular design and partitioning of a knowledge base, static and dynamic constraint checking of slot values and function arguments, and semantic analysis of rule patterns to determine if inconsistencies could prevent a rule from firing or generating an error.

The application is intended primarily for physicians, but patients could use a modified version. This could be provided as either an online or stand-alone application, but an online approach is better for new data collection and updating rules. The procedure requires about 1 minute to physically enter the answers to the questions (but obviously takes longer to ask or read the questions), and execute the expert system. To provide likely diagnoses takes less than 30 seconds and depending on the patient's symptoms the system can reduce the number of possible types of migraine by almost 50%. We estimate that use of such a system during a typical consultation for headaches will save several minutes of the doctor's and patient's time. It should also reduce the need for unnecessary investigations. Through both these mechanisms it should produce cost-savings. However, this and the system's ability to improve migraine diagnosis including differentiating them from tension headaches remains to be proven.

CONCLUSION

We have created a program, written in the CLIPS language for expert systems, to aid the diagnosis of migraines and to distinguish them from headaches. We have identified essential questions necessary for building an expert system that distinguishes migraines from headaches. The execution time depends on the number of migraine types embedded in the expert system. The time varies from three seconds for the five most common migraine cases to seventeen seconds for the entire set of twenty types of migraine according to the ICD-9-CM classification. We also created an XML representation of the International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), including disease category 346 (Migraines), and published it on the Web. The clinical accuracy of the system and its benefits remain to be established.

ACKNOWLEDGEMENT

We would like to acknowledge Mr. Avi Bindell for carefully proofreading and editing this document.

REFERENCES

1 Deutsche Migräne- und Kopfschmerz-Gesellschaft e.V. / DMKG. *ICD 10 Liste aller klassifizierten Kopfschmerzsyndrome*. Available: http://www.dmkg.de/fortbild/icd.htm.

2 Cady R, Dodick DW. Diagnosis and treatment of migraine. *Mayo Clin Proc* 2002; **77**: 255–61.

3 Lipton RB, Cady RK, Stewart WF, Wilks K, Hall C. Diagnostic lessons from the spectrum study. *Neurology* 2002; **58**(9 Suppl 6): S27–31

4 Lipton RB, Diamond S, Reed M, Diamond ML, Stewart WF. Migraine diagnosis and treatment: results from the American Migraine Study II. *Headache* 2001; **41**: 638–45.

5 Kaniecki RG. Migraine and tension-type headache: an assessment of challenges in diagnosis. *Neurology* 2002; **58**(9 Suppl 6): S15–20.

6 Maizels M. Headache evaluation and treatment by primary care physicians in an emergency department in the era of triptans. *Arch Intern Med* 2001; **161**: 1969–73.

7 Olesen, J. Classification and diagnostic criteria for headache disorders, cranial neuralgia, and facial pain. *Cephalalgia Headache Classification Committee of the International Headache Society* 1988; **8** (suppl 7): 1–96. Available: http://www.i-h-s.org.

8 Troost, T. M.D. *Migraine and other Headaches,* Wake Forest University School of Medicine (2002). Available: http://imigraine.net/migraine/intro.html.

9 GHG Internet Services, *CLIPS, A Tool for Building Expert Systems*. Available:http://www.ghg.net/clips/CLIPS.html [June 2003].

10 International Headache Classification Committee (IHCC*)*. ICD-10 guide for headaches. *Cephalalgia* 1997; **17**(suppl 19): 1–82.

APPENDIX

The research application prototypes were developed on both UNIX and Windows platforms using the following techniques: data mining, online transaction analytical processing

Open source and freeware tools such as Java, MySQL (Structured Query Language) database, Apache Web server, and CLIPS Expert System shell were used in the development process.

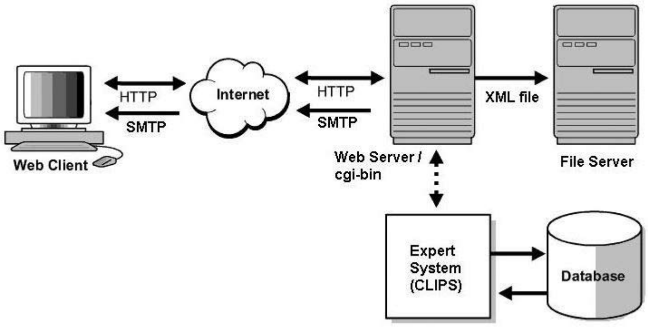
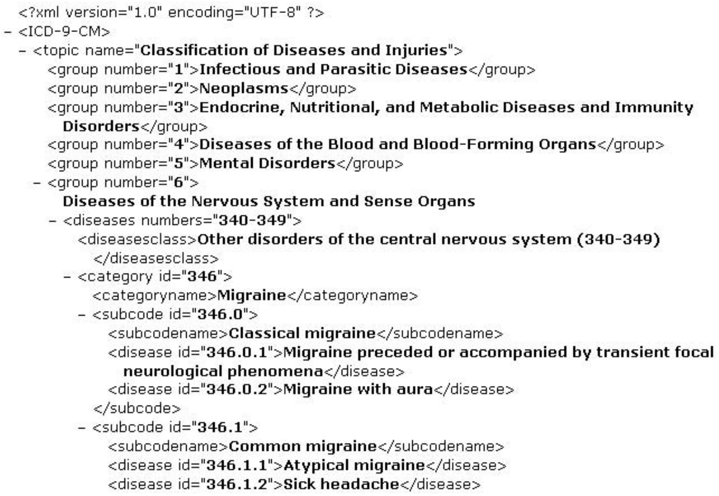


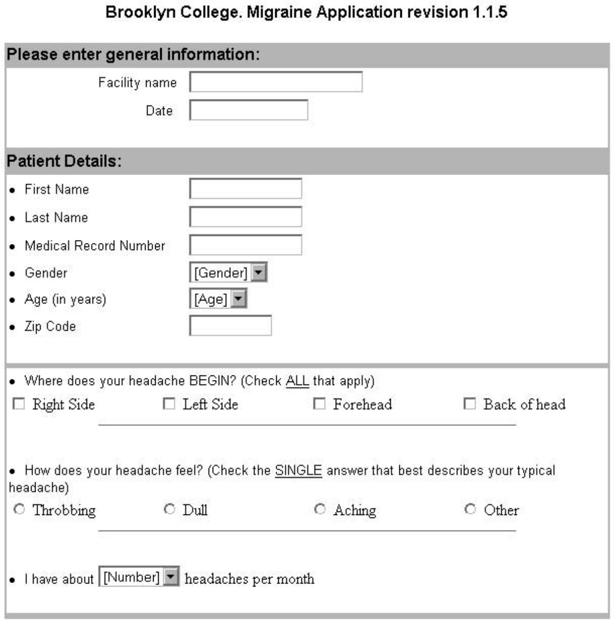
Figure A1. *The Migraine / Headaches Application Schema*

The graphic user interface (GUI) and presentation layer are written in HTML and JavaScript, while the Application and data manipulation layers are written in Common Gateway Interface (CGI) Perl script. In our present implementation, data is collected in the XML format as a file for future analysis and sent by e-mail (Figure A1).



```
  <?xml version="1.0" encoding="UTF-8" ?>
- <ICD-9-CM>
  - <topic name="Classification of Diseases and Injuries">
      <group number="1">Infectious and Parasitic Diseases</group>
      <group number="2">Neoplasms</group>
      <group number="3">Endocrine, Nutritional, and Metabolic Diseases and Immunity
        Disorders</group>
      <group number="4">Diseases of the Blood and Blood-Forming Organs</group>
      <group number="5">Mental Disorders</group>
    - <group number="6">
        Diseases of the Nervous System and Sense Organs
      - <diseases numbers="340-349">
          <diseasesclass>Other disorders of the central nervous system (340-349)
            </diseasesclass>
        - <category id="346">
            <categoryname>Migraine</categoryname>
          - <subcode id="346.0">
              <subcodename>Classical migraine</subcodename>
              <disease id="346.0.1">Migraine preceded or accompanied by transient focal
                neurological phenomena</disease>
              <disease id="346.0.2">Migraine with aura</disease>
            </subcode>
          - <subcode id="346.1">
              <subcodename>Common migraine</subcodename>
              <disease id="346.1.1">Atypical migraine</disease>
              <disease id="346.1.2">Sick headache</disease>
```

Figure A2. *International Classification of Diseases (ICD-9-CM) (Fragment)*



Brooklyn College. Migraine Application revision 1.1.5

Please enter general information:

Facility name ______

Date ______

Patient Details:

- First Name ______
- Last Name ______
- Medical Record Number ______
- Gender [Gender] ▾
- Age (in years) [Age] ▾
- Zip Code ______

- Where does your headache BEGIN? (Check ALL that apply)

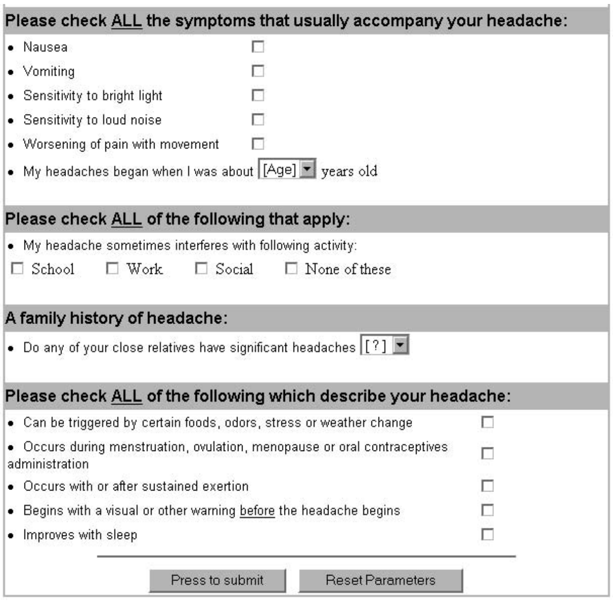
□ Right Side □ Left Side □ Forehead □ Back of head

- How does your headache feel? (Check the SINGLE answer that best describes your typical headache)

○ Throbbing ○ Dull ○ Aching ○ Other

- I have about [Number] ▾ headaches per month

Figure A3. *Migraine Application HTML Form (fragment – upper part)*



Please check ALL the symptoms that usually accompany your headache:

- Nausea □
- Vomiting □
- Sensitivity to bright light □
- Sensitivity to loud noise □
- Worsening of pain with movement □
- My headaches began when I was about [Age] ▾ years old

Please check ALL of the following that apply:

- My headache sometimes interferes with following activity:

□ School □ Work □ Social □ None of these

A family history of headache:

- Do any of your close relatives have significant headaches [?] ▾

Please check ALL of the following which describe your headache:

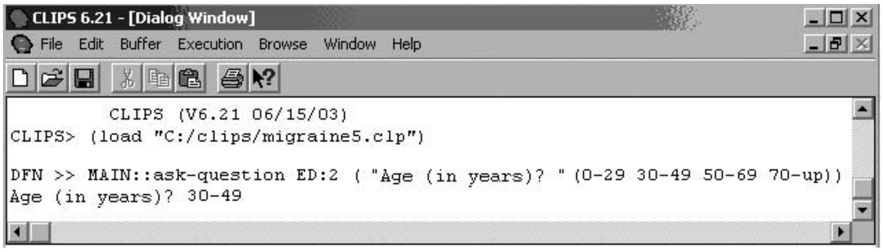
- Can be triggered by certain foods, odors, stress or weather change □
- Occurs during menstruation, ovulation, menopause or oral contraceptives administration □
- Occurs with or after sustained exertion □
- Begins with a visual or other warning before the headache begins □
- Improves with sleep □

Figure A4. *Migraine Application HTML Form (fragment – lower part)*

Note 1. Most of the questions are based on the identification of headache syndromes in accordance with the International Headache Society (HIS) or the World Health Organization's International Classification of Diseases (ICD-10).

Note 2. School would apply to an adolescent or young adult in graduate school.

A Java extraction transformation loading (ETL) procedure was used to transform the source text file into an XML file. It was then utilised to build the XML representation of the original International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM) as shown in Figure A2. The Migraines and Headaches Application Form (Figures A3 and A4) was developed and published on the Web. The Perl script simple-form.cgi takes the input from a form, sends it to a specified email address, appends information to the XML file and returns a confirmation page.



CLIPS 6.21 - [Dialog Window]
File Edit Buffer Execution Browse Window Help

```
         CLIPS (V6.21 06/15/03)
CLIPS> (load "C:/clips/migraine5.clp")

DFN >> MAIN::ask-question ED:2 ( "Age (in years)? " (0-29 30-49 50-69 70-up))
Age (in years)? 30-49
```

Figure A5. *User's dialogue with CLIPS application (fragment)*

The answers from six patients, diagnosed with migraine, were obtained by interviewing. The data was entered directly using an existing CLIPS interface. Patients' potential diagnoses are presented in Table 2.

Patient Case1 – Dialogue with CLIPS system:

CLIPS: "Age (in years)?" (0–29 30–49 50–69 70-up) /* valid answers, see Figure A5 */
Patient: 0–29.

CLIPS: Gender? (Male/Female)
Patient: Female.

CLIPS: Does your headache occur during menstruation, ovulation, menopause or oral contraceptives? (Yes/No)
Patient: Yes.

CLIPS: Does your headache BEGIN on right side? (Yes/No)
Patient: Yes.

CLIPS: How does your headache feel? (throbbing dull aching other unknown)
Patient: Dull.

CLIPS: Does pain interfere significantly with school activity? (Yes/No)
Patient: Yes.

CLIPS: Does vomiting accompany your headache? (Yes/No)
Patient: No.

CLIPS: Does nausea accompany your headache? (Yes/No)
Patient: Yes.

CLIPS: The number of headaches per month? (0–2 3–5 6–9 10–19 20-up)
Patient: 0–2.

CLIPS: Can your headache be triggered by certain foods, odors, stress or weather changes? (Yes/No)
Patient: Yes

HITJ © *The Journal on Information Technology in Healthcare* 2004; **2**(5): 365–373

Mobile Patient Monitoring: The MobiHealth System

Aart Van Halteren, Richard Bults, Katarzyna Wac,
Dimitri Konstantas, Ing Widya, Nicolay Dokovsky,
*George Koprinkov, Val Jones, Rainer Herzog**

University of Twente, The Netherlands and * Ericsson GmbH, Germany.

ABSTRACT

The forthcoming wide availability of high bandwidth public wireless networks will give rise to new mobile healthcare services. To this end, the MobiHealth project has developed and trialed a highly customisable vital signs monitoring system based on a body area network (BAN) and a mobile-health (m-health) service platform utilising next generation public wireless networks. The developed system allows the incorporation of diverse medical sensors via wireless connections, and the live transmission of the measured vital signs over public wireless networks to healthcare providers. Nine trials with different healthcare scenarios and patient groups in four different European countries have been conducted. These have been performed to test the service and the network infrastructure including its suitability for mobile healthcare applications. Preliminarly results have documented the feasibility of using the system, but also demonstrated logistical problems with use of the BANs and the infrastructure for transmitting mobile healthcare data.

INTRODUCTION

The expansion and availability of high (mobile) bandwidth (General Packet Radio Service [GPRS] and Universal Mobile Telecommunications System [UMTS]) combined with the ever-advancing miniaturisation of sensor devices and computers, will give rise to new services and applications that will affect and change the daily life of citizens. An area where these new technological advances will have a major effect is healthcare. In the future, patients will be able to receive medical advice from a distance and be able to send full, detailed and accurate vital signs measurements irrespective of where they are. This data will be of an equivalent standard to that obtained in a medical centre, implementing the concept of 'ubiquitous medical care'.

In keeping with this vision, the MobiHealth project (supported by the Commission of the European Union in the frame of the 5th research Framework

Correspondence and reprint requests: Dimitri Konstantas, University of Twente, EWI/CTIT, PO Box 217, NL-7500 AE Enschede, The Netherlands. E-mail: Dimitri.Konstantas@cui.unige.ch.

under project number IST-2001-36006) has developed an innovative value-added mobile health service platform for patients and health professionals. The service enables remote patient monitoring through the use of advanced wireless communications and integration of sensors to a wireless body area network (BAN). It permits remote management of chronic conditions and detection of health emergencies whilst maximising patient mobility.

THE MOBIHEALTH SYSTEM

The MobiHealth system provides a complete end-to-end m-health platform for ambulant patient monitoring, deployed over UMTS and GPRS networks. The MobiHealth patient/user is equipped with different sensors that constantly monitor vital signals, e.g. blood pressure, heart rate and electrocardiogram (ECG). These are interconnected via a healthcare *body area network* (BAN)[1–4]. In essence this consists of sensors, actuators, communication and processing facilities connected via a wireless network. This is worn on the body and moves around with the person, i.e. the BAN is a roaming unit.

The central point of the healthcare BAN is the *Mobile Base Unit* (MBU). This aggregates the vital sensor measurements and transmits them via UMTS or GPRS to the back-end system. The back-end system can be located within the healthcare provider premises or be part of the wireless services provider. From there the measurements are dispatched to the healthcare provider where they are monitored by medical personnel. At present automated monitoring and patient feedback is not supported by the MobiHealth system.

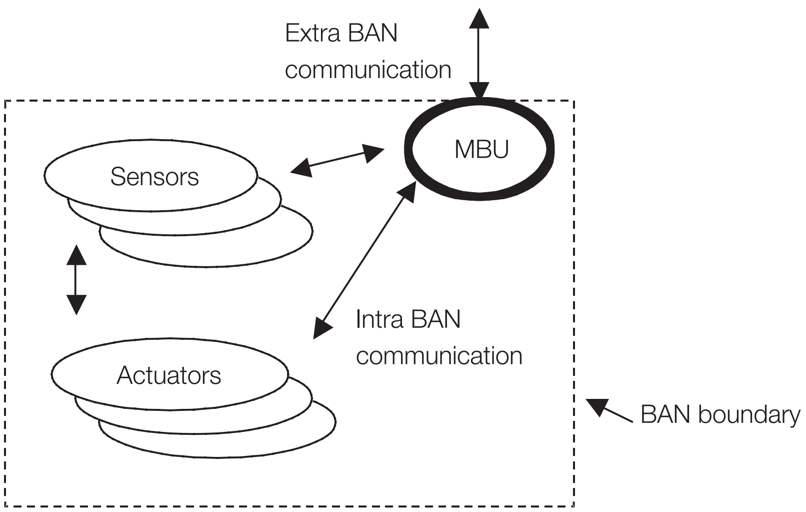


Figure 1. *Healthcare BAN architecture*

Communication between entities within a BAN are referred to as *intra-BAN communication*. *Extra-BAN communication* is performed through the Mobile Base Unit and enables remote monitoring. Intra-BAN communication is based on short range wireless networks like Bluetooth[5] and Zigbee[6], while extra-BAN communication employs GPRS and UMTS. Figure 1 shows the architecture of a healthcare BAN.

The sensors used in the BAN are responsible for the data acquisition process. They monitor and capture a physical phenomenon, such as patient movement, muscle activity or blood flow. This is converted to an electrical signal, which is then amplified, conditioned, digitised and communicated within the BAN.

The Healthcare BAN sensors can be self-supporting and/or front-end supported. Self-supporting sensors have their own power supply and facilities for amplification, conditioning, digitisation and communication. Self-supporting sensors are independent building blocks of a BAN and ensure a highly configurable healthcare BAN. However, each sensor runs to its own internal clock and may have a different sample frequency. Consequently, mechanisms for synchronisation between sensors may be needed. Front-end supported sensors share a common power supply and data acquisition facilities. Consequently, front-end supported sensors typically operate on the same front-end clock and jointly provide multiplexed sensor samples as a single data block. This avoids the need for synchronisation between sensors.

Service Platform Architecture

Collecting and transmitting vital signal measurements is only part of the healthcare service developed in the MobiHealth project. The healthcare BAN is only one part of a service platform that integrates the mobile part (healthcare BAN) and the healthcare agent resident system. Figure 2 shows the overall functional architecture of the MobiHealth service platform. The dotted square boxes indicate the physical location where parts of the service platform are executed. The rounded boxes represent the functional layers of the architecture. The m-health service

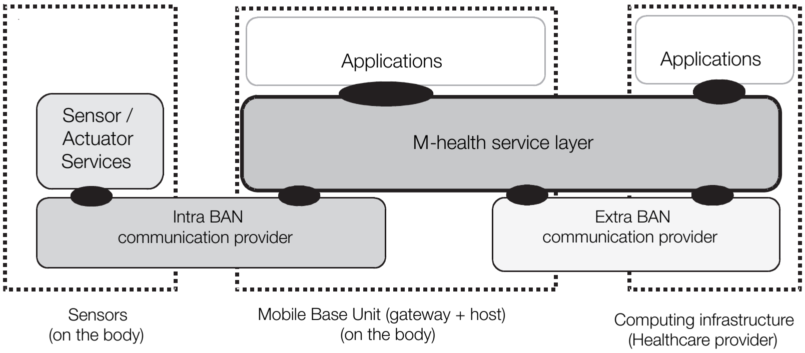

Applications
Applications
Sensor / Actuator Services
M-health service layer
Intra BAN communication provider
Extra BAN communication provider
Sensors (on the body)
Mobile Base Unit (gateway + host) (on the body)
Computing infrastructure (Healthcare provider)

Figure 2. *Service platform functional architecture*

platform consists of sensor and actuator services, intra-BAN and extra-BAN communication providers and an m-health service layer. The intra-BAN and extra-BAN communication providers represent the communication services offered by intra-BAN communication networks (e.g. Bluetooth) and extra-BAN communication networks (e.g. UMTS), respectively. The m-health service layer integrates and adds value to the intra-BAN and extra-BAN communication providers.

Applications that run on top of the service platform can either be deployed on the MBU (for on-site use, e.g. by a visiting nurse) or on the servers or workstations of the healthcare provider, e.g. a call centre or secondary care centre. Applications that use the m-health service layer can range from simple viewer applications that provide a graphical display of the BAN data, to complicated applications that analyse the data.

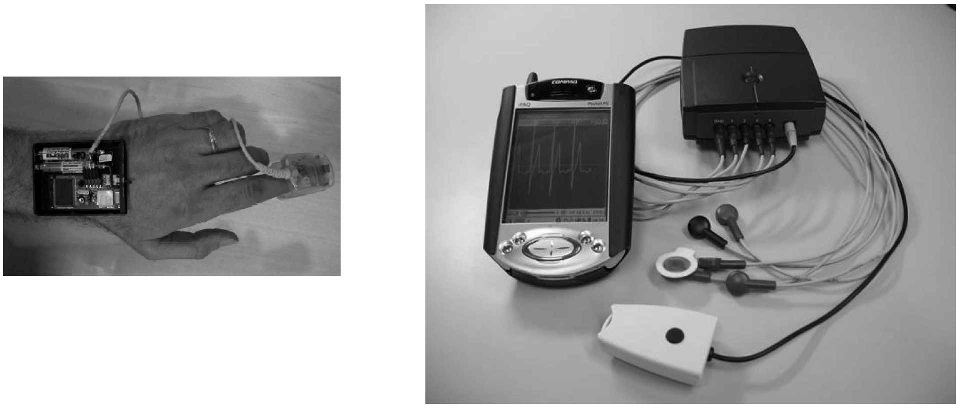


Figure 3. *Self supporting sensor (left) and complete front-end system with ECG and oxygen saturation sensors*

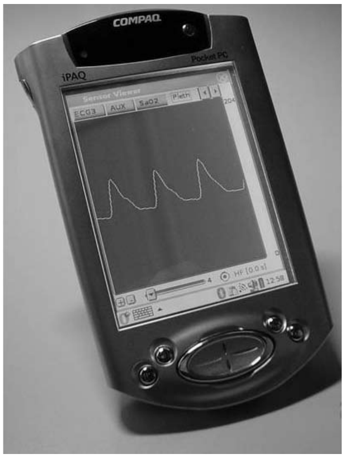


Figure 4. *iPAQ H3870 acts as MBU*

The healthcare BAN has been implemented using both front-end supported and self-supporting sensors. Figure 3 shows the self-supporting EISlab sensor[7] (left) and a TMSI front-end (right) with ECG and oxygen saturation sensors. Both approaches use Bluetooth for intra-BAN communication. The front-end also allows ZigBee as an alternative intra-BAN communication technology. ECG electrodes, a movement sensor, a pulse oximeter and an alarm button are examples of sensing devices that can be attached to the front-end.

The MBU was implemented on an iPAQ H3870. This device has built-in Bluetooth capabilities and can be extended with a GPRS extension jacket. Figure 4 shows a picture of the MBU that also runs a viewer application.

THE MOBIHEALTH TRIALS

The primary question addressed by the MobiHealth project was whether 2.5G and 3G generation communications technologies can support the MobiHealth vision, i.e., enable empowered managed care based on mobile health care systems. To address this question, we organised and conducted nine trials in four European countries. These trials allowed us to identify problems and issues in the development of mobile health services and identify limitations and shortcomings of the existing and forthcoming public network infrastructure. It should be made clear that the primary aim of the project was to evaluate 2.5/3G infrastructures and *not* to clinically validate new medical tools and processes.

The trials were targeted at the areas of acute (trauma) care, chronic and high-risk patient monitoring, and domiciliary care. A range of medical conditions was covered including pregnancy, trauma, cardiology (arrhythmias), rheumatoid arthritis (RA) and respiratory insufficiency (chronic obstructive pulmonary disease). In cases of trauma and other acute situations, the BANs were applied to the patients by medical staff, e.g. nurses or paramedics. In other situations the patients usually applied the BAN themselves.

The trials were selected to represent a range of bandwidth requirements: low (less than 12 Kbps), medium (12–24 Kbps) and high (greater than 24 Kbps), and to include both non-real-time (e.g. routine transmission of tri-weekly ECG) and real-time requirements (e.g. alarms or transmission of vital signs in a critical trauma situation). For each application, the generic MobiHealth BAN is customised by addition of the appropriate sensor set and corresponding application software.

The participating countries and trials were:

1. Germany – Telemonitoring of cardiac arrhythmias.
2. The Netherlands – Integrated homecare for high-risk pregnancies.
3. The Netherlands – Teletrauma.
4. Spain – Support of home-based healthcare services.
5. Spain – Outdoor patient rehabilitation.
6. Sweden – Lighthouse alarm and locator trial.

7. Sweden – Physical activity and impediments to activity for women with RA.
8. Sweden – Monitoring of vital parameters in patients with respiratory insufficiency.
9. Sweden – Home care and remote consultation for recently hospitalised patients in a rural area.

More details on the trials can be found on the project site http://www.mobihealth.org.

Data collected in the trials was aimed at:

- Verifying the state of the UMTS (and GPRS) infrastructure and its suitability for mobile health applications.
- Exploring the added value that the MobiHealth system can bring to different healthcare domains.

RESULTS

Analysis of the project was performed early in 2004 whilst the trial was still in progress. The data presented here pertains to the Twente region in the Netherlands where the UMTS network is provided by Vodafone. It should be noted that the MobiHealth project was the *only* user of the Vodafone UMTS network in the Twente region. Thus we are running under the best-case environment, that is, on an empty network.

The stability of the Vodafone UMTS was demonstrated by tests done with a moving car travelling in the Enschede area. We were able to maintain a connection with a nominal capacity of 64Kbps (up and down link) crossing over cell boundaries and under different speeds. The maximum bandwidth available for a fixed station of 64Kbps uplink and 384Kbps downlink was readily available and stable thoughtout the coverage area (our terminal devices – pre-commercial Nokia 6650 UMTS telephones – do not allow us to obtain higher bandwidths).

A fundamental problem was encountered relating to the use of the UTMS (and GPRS) networks. The public networks were designed for applications where the end-user is a consumer of information, i.e. a typical user will send small amounts of data and receive large amounts of data. The MobiHealth system, however, is based on the reverse model: the end-user is the producer of information and not the consumer. The present network and terminal devices in their present configuration are not designed to support high bandwidth transmission emanating from the end-user. This limits the measurements that the MobiHealth system can send to the healthcare provider.

Problems were also encountered with the HTTP (HyperText Transfer Protocol) for transporting vital signals. To enhance portability and compatability with the operating systems available on portable telephones, the MobiHealth application on the MBU was programmed in Java under the Connected Limited Device Configuration (CLDC) Java Virtual Machine (VM)[8]. However, the current HTTP protocol implementation under the CLDC Java VM does not allow for persistent HTTP connections. That means that whenever the MBU needs to send data it must establish a new TCP/IP (Transmission Control Protocol/Internet Protocol) connection. This, however, impedes performance. A possible solution would be for the mobile telephones to be able to use the Connected Device Configuration[9] platform that allows direct access to the TCP/IP layer.

A second issue related to the use of the HTTP protocol is the fact that every time a request is sent, the communication is blocked until an acknowledgment or reply is received. To overcome this problem we used a technique called *chunking*[10]. This enables multiple requests to be sent without having to wait for a reply. However, not all operators allow the use of chunking for their GPRS network. This eventually might cause standardisation problems for services and applications that transmit continuous real-time data over the GPRS and possibly UMTS.

During the UMTS performance tests (active measurements), we performed tests trying to emulate a high load on the network by running ten simultaneous UMTS transmissions. The tests indicated a performance degradation when high bandwidth from ten UMTS connections are simultaneously transmitted (from the same room, with each UMTS connection running from its own unique terminal). The reason for this failure is, however, not clear at present and is being further investigated.

DISCUSSION

MobiHealth aims to give patients a more active role in the healthcare process while at the same time enabling healthcare payers to manage costs more directly. The healthcare BAN and supporting service platform is an emerging technology that promises to support this aim.

MobiHealth has resulted in an early prototype of a BAN, engineered mainly by integration of existing technologies without focusing on miniaturisation or optimisation of power consumption. The main focus has been on the architecture, design and implementation of an m-health service platform. The result is a first version of a service platform whose architecture is comprised of a set of clearly defined components.

Preliminary trials have shown the feasibility of using the system, but a number of problems have been encountered. Not all of these problems can be overcome with the use of current technologies. Ambulatory monitoring is more successful for some biosignals than others, for example some measurements are severely disrupted by movement artefacts. Some monitoring equipment is still too cumbersome for ambulatory use, because of the nature of the equipment or because of power requirements. In the area of wireless (tele)communication technologies (even with GPRS and UMTS) we still suffer from limited bandwidth for some applications, such as those which require monitoring many simultaneous signals per user.

The available data bandwidth over GPRS (and UMTS) depends also on the strength of the signal at the user location. Although the GPRS and UMTS telephones do indicate the signal strength during operation, this is not the case for the PCMCIA (Personal Computer Memory Card International Association) cards integrated with the iPAQ. PCMCIA cards allow the control of the signal strength using proprietary software, *but only during set up*. During data transmission the signal strength information is not available. However, this information is of major importance for the MobiHealth application, since it will allow us to estimate the available bandwidth and to control the data transmission rate accordingly. Currently, we have a situation where, if we are transmitting at high bandwidth in an area with a strong signal and pass to an area where the signal is weak, we are unable to lower the data transmission rate and consequently lose the connection. We thus believe that the signal rate as well as the encoding schema used during the transmission should be available to the application under a standardised application program interface for all types of GPRS/UMTS terminals, whether these terminals are PCMCIA cards or regular mobile phones.

The use of BANs and wireless communications in personal healthcare systems will also raise important challenges relating to security, integrity and privacy of data during transmission. End-to-end security and quality of service guarantees need to be implemented. Safety of hardware (e.g. electrical safety, emissions, interference) and reliability and correctness of applications must also be a priority in deployment of mobile services. Comfort and convenience of sensors or BANs worn long term for continuous monitoring is important for usability and user acceptance. Timeliness of information availability in the face of unreliable performance of underlying network services is another issue. Provision of seamless services across regional and national boundaries multiplies these difficulties. Powering *always on* devices and continuous transmission will continue to raise technical challenges. Business models for healthcare and accounting and billing models for network services need to evolve if technical innovations are to be exploited fully. Standardisation at all levels is essential for open solutions to prevail. At the same time specialisation, customisation and personalisation are widely considered to be success criteria for innovative services.

Despite all these problems, there is much interest and enthusiasm for the project both from patients and healthcare professionals. We will continue to develop and implement the system and expect that it will be available commercially in several European countries during 2005.

CONCLUSION

The results of the project include an architecture for, and a prototype of, a generic service platform for provision of ubiquitous healthcare services based on body area networks. The MobiHealth System can support not only sensors, but potentially any body-worn device. Consequently the system has potentially many applications in healthcare and will enable a variety of healthcare services to delivered in the community. However, a number of technical problems remain to be resolved before the system can be used in routine practice.

ACKNOWLEDGEMENT

The MobiHealth project was supported by the Commission of the European Union in the frame of the 5th research Framework under project number IST-2001-36006.

REFERENCES

1 Zimmerman TG. Wireless networked devices: a new paradigm for computing and communication. *IBM Systems Journal* 1999; **38**: Page Nos.

2 van Dam KS, Pitchers Initial, Barnard M. 'Body area networks: towards a wearable future. *Proc. WWRF Kick Off Meeting*, Munich, 2001; http://www.wireless-world-research.org/.

3 Jones VM, Bults RGA, Konstantas D, Vierhout PAM. Healthcare PANs: personal area networks for trauma care and home care. *Proceedings Fourth International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Aalborg, Denmark, 2001, http://wpmc01.org/.

4 Schmidt R, *Patients Emit an Aura of Data*. Fraunhofer-Gesellschaft, 2001, www.fraunhofer.de/english/press/md/md2001/md11-2001_t1.html.

5 Bluetooth. http://www.bluetooth.org/.

6 ZigBee Alliance. *IEEE 802.15.4, ZigBee Standard*. http://www.zigbee.org/.

7 Östmark Å, Svensson L, Lindgren P, Delsing J. Mobile medical applications made feasible through use of EIS platforms. *IMTC 2003 – Instrumentation and Measurement Technology Conference*. Vail, USA, 2003.

8 Sun Microsystems. *Connected Limited Device Configuration (CLDC)*. http://java.sun.com/products/cldc/.

9 Sun Microsystems. *Connected Device Configuration (CDC)*. http://java.sun.com/products/cdc/.

10 Sun Microsystems. *HTTP Chunking*. http://developers.sun.com/techtopics/mobility/midp/questions/chunking/.

CALL FOR PAPERS

The journal aims to educate healthcare professionals on the use of IT in healthcare, and to provide them with objective evidence of the benefits of IT in clinical practice. To achieve these aims the journal seeks to publish the following types of papers:

(i) Articles that educate healthcare professionals on the principles and practice of the use of IT in healthcare. Articles should be written in a format that can be understood and appreciated by readers without in-depth knowledge of computers or medical informatics.

(ii) Articles that provide practical advice for selecting and implementing IT solutions into clinical practice and/or optimising use of existing IT systems.

(iii) Papers that provide objective evidence of the benefits of IT in clinical practice.

All articles submitted to the journal undergo peer review. To ensure their international relevance, and that they can be understood and appreciated by an international readership, at least 2 reviewers for each article are not from the same country as the author(s). In addition, for research papers, at least 2 reviewers are clinicians.

If you would like to submit an article or paper to the journal, please see the 'Instructions for Authors'.

ONLINE COMMUNITY

http://www.communityzero.com/JITH

An online community has been created for readers of the journal to enable them to exchange ideas, knowledge and experience. Among its features members can:

Access papers published in the journal
Participate in discussions
Vote in polls
Post notices of meetings

Membership to the community is free. The website can be explored by clicking on the Preview button and following the instructions.

If you have any questions or would like further information about the online community, please e-mail editor@jith.net.

REVIEWERS

The journal is dependent on reviewers to ensure the quality and originality of the papers it publishes. If you would like to act as a reviewer for papers submitted to the journal, please e-mail your details and areas of interest to editor@jith.net.

HITJ The Journal on Information Technology in Healthcare

INSTRUCTIONS FOR AUTHORS

Aims and Scope: *The Journal on Information Technology in Healthcare* aims to improve the quality and safety of patient care, by encouraging and promoting the use of information technology (IT) in healthcare. The journal acts as a medium for the international exchange of knowledge and experience of the benefits of IT in healthcare. It principally publishes papers that objectively demonstrate clinical and cost benefits of IT in healthcare. It also publishes papers that offer practical advice for selecting and implementing IT systems.

Submission of Papers: Papers in keeping with the aims of the journal should be submitted to the Editor. The journal will accept papers submitted by e-mail to editor@jith.net. Manuscripts submitted by post should be typed, with double spacing, on one side of A4. One copy of the typescript and illustrations, together with an exact matching copy on floppy disk or CD-ROM should be sent to:

Clyde Saldanha, Editor, The Journal on Information Technology in Healthcare, 72 Churston Drive, Morden, Surrey, SM4 4JQ, UK.

A copy of the manuscript should be retained as insurance against loss in the mail.

Acknowledgements of Submissions: All submissions will be acknowledged on receipt by e-mail to the corresponding author. Further correspondence will be made as appropriate.

Abstract: Research papers should have a structured abstract with the following headings: Objective, Design, Setting, Methods, Results, Conclusion.

Style and Content of Manuscript: Papers should be set out under the headings: Introduction, Methods, Results and Discussion. They should as far as possible be written in a format that can be understood by readers who do not have in-depth knowledge of computers or medical informatics. Papers should ideally contain sufficient information for interested readers to be able to evaluate the feasibility and cost-effectiveness of implementing a described system into their practice. Studies should abide by high ethical standards, and if appropriate, should have received ethical approval from the local institutional human research committee.

Use British rather than American spelling throughout the manuscript.

References: References should be identified by Arabic superscripts in the text and numbered in the order in which they appear in the paper. They should be listed at the end of the paper in the order that they are first cited in the text. Give the full names and initials of all authors, unless there are more than six, when only the first three should be given, followed by et al. Names should be followed by the title of the article; the title of the journal; the year of publication; the volume number and the first and last page numbers. Journal titles should be given in full or abbreviated according to the style of *Index Medicus*. Titles of books should be followed by the place of publication; the publisher and the year.

Peer Review: All papers submitted to *The Journal on Information Technology in Healthcare* undergo a peer review process. On the basis of the reviewers' responses, papers will be rejected, accepted subject to revision or accepted unconditionally. Rejected manuscripts will not be returned to authors unless expressly requested.

Acceptance of Papers: On acceptance the Editor retains the right to make stylistic changes, decide on the date of publication and shorten material if necessary.

Final versions of all accepted manuscripts must be submitted in electronic format.

Proofs: Authors are sent one copy of the proofs. Corrections should be confined to typographical errors or matters of accuracy. Extensive amendments are not permissible. Authors should return proofs as soon as possible and not later than the date given in the covering letter.

Reprints: These are available if ordered at the time of returning the proofs. Details of charges will be sent with the proofs.

Copyright: All material received by *The Journal on Information Technology in Healthcare* are assumed to be submitted exclusively and not to have been previously published in the English language.

The author(s) bear(s) the responsibility for checking whether material submitted is subject to copyright or ownership rights; for example in the use of diagrams or tables. If a submission is finally published the copyright becomes that of *The Journal on Information Technology in Healthcare*, and permission for any reproduction must be sought from the Editor.

Dual Publication: A paper is accepted for publication on the understanding that it has not been submitted simultaneously to another journal in the English language.

Accuracy and Liability: A contribution is accepted on the strict understanding that its author(s) is (are) responsible for the accuracy of all information contained in the contribution and that references to named people and/or organisations are both accurate and without libelous implications.

Conflict of Interest: If authors have received payment/substantial gifts from companies whose products are featured in the paper, or have a commercial interest in the hardware and/or software used for the study, this must be acknowledged in a statement at the end of the text.

Subscription To

The Journal on Information Technology in Healthcare

□ Please enter my 2004 subscription to The Journal on Information Technology in Healthcare (ISSN 1479-649X), for Volume 2 (6 issues).

SUBSCRIPTION RATES

	Institutional	Individual
Great Britain	£120	£100
Europe	€200	€180
USA	US$220	US$180
Rest of the world	£135	£115

□ I enclose cheque/ banker's draft made payable to The Journal on Information Technology in Healthcare.

□ Please invoice me.

□ I have arranged payment by Bankers Automated Credit Service (BACS) to Barclays Bank, 8 Alexandra House, Wimbledon, London SW19 7LA.
Sort Code 20-96-89
Account Number 00728837
Name of account: The Journal on Information Technology in Healthcare

Name:

Address:

Postcode:

Country:

Tel:

Fax:

E-mail:

PLEASE POST TO:

Subscriptions
The Journal on Information Technology in Healthcare
72 Churston Drive
Morden
Surrey
SM4 4JQ
United Kingdom

E-mail : subscriptions@jith.net
Fax : +44 (0)870 130 1572