MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

Everyone's a winner, baby?

Sue Whetton[a], Jon Hilton[b]

[a] *University Department of Rural Health, Tasmania*

Abstract

Electronic health records have the potential to become the cornerstone of sustainable health services for the future. Before this can occur there are a number of risks that need to be managed. Existing risks relate to finding the balance between privacy and adequate access, and to developing systems that minimise the potential for unauthorised or illegal use of information. Current approaches, at least in Australia, are somewhat chaotic. Nevertheless, it is anticipated that these risks will be managed. Future risks are a cause for concern. As the electronic health record becomes more comprehensive and more accessible, there will be increasing pressure from a range of non-health care organisations for access to the information. The proposed uses for this information may not always be in the interest of the consumer. Health informatics professionals should be aware of this possibility, should contribute to any discussion around potential future use of health information and understand that the systems they help to build may be used in such a way that not everyone will be a winner.

Key words:
privacy, security, electronic record, risks

Introduction: sustainable health services

Health informatics has the potential to support dramatic and widespread changes to the structures and processes of our health care systems. Such changes are increasingly viewed as essential for the sustainability of health services in the future [1, 2]. It is a view shared by health professionals and consumers alike. A 1998 survey of patient satisfaction, sponsored by the Harvard School of Public Health, found that in each of three countries—the USA, Canada and Australia—79 per cent of the population said their system needs either 'fundamental change' or to be 'completely rebuilt'. The same sentiment was expressed by 89 per cent in New Zealand and by 72 per cent in the United Kingdom [3]

There are different ideas about how a fundamentally changed and presumably more sustainable, health care system will look and operate. Berwick [1] envisions a system that offers '24/7/365 access to help that is uncompromising, meeting whatever need exists, whenever and wherever it exists, in whatever form requested.' While this is more than most think possible, or perhaps even desirable, there is consensus that in a sustainable system, information is the key and that the increasing use of technological and other information and communications systems to access this information will fundamentally change the way health care services are structured and accessed. And for many, the electronic health record will be at the heart of these changes. It is the electronic health record that will finally deliver the health informatics promise of more effective and efficient health services, better quality care and long-term positive health outcomes for individuals and the community as a whole.

At the same time, this vision is tempered by the realisation that we need to manage the very real risks inherent in the implementation of an electronic health record. These can be considered as existing risks and potential future risks. Existing risks are widely discussed in the literature and relate to the need to maintain the privacy of the individual consumer while ensuring appropriate access for health professionals involved directly in the provision of health care or seeking access to data for secondary purposes. Existing risks also include those around the potential for unauthorised access and use of data from electronic records. Future risks refer to the potential for a broadening the range of legitimate uses of health data. Griener [4] suggests that we need to be vigilant and not assume that these will always be benign. In other words, although it is widely anticipated that mechanisms will be developed to effectively manage the risks and facilitate the benefits, we should not assume that everyone's a winner (baby).

Managing existing risks

Efforts to manage existing risks focuses on maintaining the privacy of the individual, ensuring appropriate access for authorised health professionals and developing mechanisms to minimise unauthorised access and use of data.

The sensitive nature of much health data and information means that privacy and confidentiality need to be stringently protected. The consequences of breaches of privacy and confidentiality can range from embarrassment arising from disclosure of sensitive information to serious discrimination, including bias by health carers, insurance organisations, and employers. Enquiries suggest that abuse of personal health information is not uncommon, and offenders are often organisations who should know better [5]. However deciding on what information should be kept confidential is not always straightforward. The purpose of

an electronic health record is to ensure that useful and relevant information is available for use by properly authorised people. This raises the question: *what is relevant?* While some (health professionals in particular), might answer 'Why, everything, of course', others will not be so sure. As the NSW Ministerial Advisory Committee observes 'Even seemingly innocuous information can be contentious. The fact that a person was treated in a particular hospital or location, such as a prison or sexual health centre, could indirectly reveal information about the person. Even though summary information such as name of hospital and health provider may not appear to be 'health information' as such, to the extent that it reveals something about a person's health status it may need to be treated with the same sensitivity as other health information [5].

Nor is there a straightforward answer to the question of who might be considered as 'properly authorised.' Everyone seeking access to information may consider themselves properly authorised. Patients may not agree and this gives rise to one more question: *Who decides these things?*

The health care environment comprises many stakeholder groups with different, sometimes conflicting views and priorities. This is demonstrated at the strategic level where the perceived relative importance of privacy and confidentiality varies between different stakeholder groups. A Report on Research Challenges in E-Health Technologies identified patient privacy as a primary issue for both research and the practice of health information management [6]. Yet health executives responding to the Commonwealth Fund International Health Policy Survey [7] viewed privacy concerns as less of an issue than start-up costs, maintenance costs and lack of standards (Table 1).

Table 1- Major barriers to greater use of computer technology

Per cent naming	*Aust*	*Can*	*NZ*	*UK*	*USA*
High start-up costs	84	84	93	69	71
Projected maintenance costs	49	42	32	52	27
Lack of uniform standards	49	35	50	31	44
Privacy concerns	20	26	7	8	17

Commonwealth Fund International Health Policy Survey

This suggests that there will therefore be situations when a balance will need to be struck between the priorities of different stakeholders. Unfortunately all groups are not equally represented in such discussions. More powerful groups are often able to exert more influence than marginal groups and consequently there may be situations where everyone is not a winner. Consider the following perspectives:

- Health Minister, Tony Abbott has put federal health IT bureaucrats on notice saying he expects tangible results within a year – specifically, a functioning electronic health record and accompanying smartcard system – or heads would start to roll [8].
- I am writing to question the need for or value to be gained from a privacy forum. There seem to be many other issues that are more pressing…We feel that most practitioners are very familiar with general privacy requirements… the problem is really only around how privacy is handled in the electronic referral environment [9].
- Sure there'll be breaches in privacy – but we can deal with those as they happen – the main thing is to get an electronic health record out there [10].
- It's very hard to retrofit and put privacy in at the end…we say build it in…Health information is seen as sensitive, so there are extra safeguards that apply to it… potentially there are a lot of bad outcomes if health information isn't appropriately looked after… [11]

Arguably, all stakeholder views should be able to be accommodated. However, if we consider the role and relative influence of the stakeholder groups, the reality is that some stakeholder views prevail, while others are marginalised.

- Governments pass legislation, establish policies and provide many of the resources to enable health care organisations to develop electronic health records, particularly where health care is partially or fully resourced from public funds. This translates into a significant ability to shape the views and activities of organisations and services.
- Senior management within health care organisations also set strategic directions that shape the development of electronic health records. Health care organisations seek to provide high quality, efficient services to the greatest number of consumers at the lowest cost. For private health care organisations, a profit margin may also be part of the equation. Health organisations have finite resources and many demands for these. The views of senior management will set parameters around the nature, scope and priorities of electronic health record projects. A focus on efficiency, technology or quality care will produce different issues and different outcomes.
- Health professionals are concerned with providing high quality care for their patients. They will therefore view the development of electronic records in terms of

relevance to, and effectiveness in furthering this goal. While clinicians support the principle of the right information in the right place at the right time, many are reluctant to give up their role as owner of the medical record and possibly arbiter of 'the right information in the right place'. The traditional status of the clinician in the biomedical model of health care bestows a considerable ability to influence discussion around this issue.

- Health informatics professionals are also able to influence the form and functions of an electronic record, but may temper their views for pragmatic reasons such as government support for their organisations. Alternatively, as a recent survey by the Health Informatics Society of Australia (HISA) suggested, heath informatics professionals may consider privacy issues to be important, but do not necessarily view the non-technical elements as being in their domain (One comment illustrating this point was: *The problem with the privacy debate is that the Australian government has not set up clear privacy legislation*.)
- Consumers are arguably the least influential stakeholder group. Horsfield and Peterson [12] suggest that consumers are not only marginalised, but also mediated – issues identified as of importance to consumers may reflect the concerns of the mediating group. Consumer issues currently tend to focus 'educating them' about the benefits of an electronic health record and the meaning of informed consent. Consumer representation at the strategic level of discussion and decision making is limited. While limited representation is better than none at all it is clear that consumer influence is somewhat less than many other stakeholder groups.

The challenge of obtaining a balance between privacy and security issues, and appropriate access to information by properly authorised individuals becomes more pressing and more complex as the increasing sophistication of electronic health records enables more and more information to be collected, stored and disseminated across departments and organisations. The complex mix of users and technical standards found in the health care environment make privacy, security and appropriate access significant challenges.

Responding to existing risks

The current approach to managing the need for privacy and authorised access includes a combination of legislation and professional self-regulation in the form of codes of ethics, supported by governance arrangements the development and use of electronic health records.

Unfortunately, legislation in Australia at least, is not straightforward. Table 2 shows the multiple jurisdictions each with their own complex legislation.

Table 2 - Privacy Specific Legislation and Administrative Instructions

Jurisdiction	Public Sector	Private Sector
Commonwealth	Privacy Act 1988 (Cth)	Privacy Act 1988 (Cth)
Australian Capital Territory	Health Record (Privacy and Access) Act 1997 (ACT) Privacy Act 1988 (Cth)	Health Record (Privacy and Access) Act 1997 (ACT) Privacy Act 1988 (Cth)
New South Wales	Health Records and Information Privacy Act 2002 (NSW)	Health Records and Information Privacy Act 2002 (NSW) Privacy Act 1988 (Cth)
Northern Territory	Information Act 2002 (NT)	Privacy Act 1988 (Cth)
Queensland	Information Standards 42A(Health)	Privacy Act 1988 (Cth)
South Australia	Code for Fair Information Practice	Privacy Act 1988 (Cth)
Tasmania	Personal Information Protection Act 2004 (Tas)	Privacy Act 1988 (Cth)
Victoria	Health Records Act 2001 (Vic)	Health Records Act 2001 (Vic) Privacy Act 1988 (Cth)
Western Australia	None	Privacy Act 1988 (Cth)

(Source: NEHTA's Approach to Privacy Version 1.0, July 2006)

Most Australian privacy legislation is built around a set of *privacy principles* with the concept of *informed consent* playing a major role in their application. Inherent in the privacy principle is the understanding that the right to privacy can never be absolute. No matter what the jurisdiction or type of information, there will always be situations that require a decision to be made around competing rights: while consumers of health care have a reasonable expectation that they should be able to control access to their information, this right may conflict with health care providers need to access accurate and up to date information, with the public health official's need for information to prevent or manage major public health risks or even with the government official enacting overriding legislation such as the National Security Information (Criminal and Civil Proceedings) Act 2004. This Act, a response to perceived security threats, is a suite of legislation that can lead to individual privacy being overridden by "the common good", while protecting the administration's right to privacy in.

Informed consent therefore clearly should include the understanding that this is so. It should also include the understanding that legislation is always subject to change,

Health informatics professionals should understand the complexities of informed consent and the possible consequences arising from the systems they help to create. Professional codes of ethics are intended to provide guide-

lines to this end. The IMIA Code of Ethics, for example, outlines a number of principles and rules for ethical conduct such as 'HIPs have a duty to ensure, to the best of their ability, that appropriate structures are in place to evaluate the technical, legal and ethical acceptability of the data-collection, storage, retrieval, processing, accessing, communication, and utilization of data in the settings in which they carry out their work or with which they are affiliated' [13].

To facilitate effective privacy-confidentiality-access of electronic health records, legislation and codes of ethics need to be supported by strong governance arrangements. The broader the reach of an electronic health record, the greater the number of individuals seeking access and the greater the amount of information stored in such records, the greater will be the need for strong governance. Current responses to the need for broad-ranging governance structures are many and varied, and generally ad-hoc, This is almost inevitable in a health care environment where the ultimate responsibility for maintaining privacy falls to the health care provider. Practitioners who work for a publicly funded health service will also be accountable to that service, which will be accountable to a funding body or bodies. Private providers may be accountable to insurers, shareholders, medical indemnity organisations. All of these layers of governance will be involved to some extent with the privacy aspects of a shared EHR. It is, however, leading to 'uncoordinated silos… governance by default where mechanisms are introduced one at a time to address a particular need' [14]. This does little to address the potential risks inherent in electronic health records.

These risks relate to processes utilised in the collection, storage and sharing of health information in electronic health records. While they pose a significant challenge, it is not unrealistic to expect that mechanisms will be developed to effectively manage them and thus deliver the promise of more effective and efficient health services, better quality care and long-term positive health outcomes for individuals and the community as a whole. Everyone will be a winner.

The same may not be true of future risks which relate to potential new uses of information contained in an electronic health record

Future risks

The majority of discussions around privacy, confidentiality and access to information focus on minimising the risk of unauthorised and illegal use of information contained within the electronic health record. These discussions are underpinned by the assumption that those determining appropriate and legal use will get it right, while at the same time begging the question of whether what can legally be done with information is always in the interests of the individual.

There is some concern, however, that this may not always be the case. As the electronic health record becomes more comprehensive and more accessible, it is suggested that there will be increasing pressure from a range of non-health care organisations for access to the information and that the proposed uses may not always be in the interest of the consumer [4, 6, 15]. Indeed, there have been incidents already that suggest this may be so. The West Australian police recently used Guthrie test samples to match DNA samples taken from a crime scene [16]. This may well appear to be a legitimate use of such material – we all want to see criminals apprehended. However, would this still be acceptable if content from medical records were provided to insurance companies or employers? The New South Wales Ministerial Advisory Committee on Privacy and Health Information [5] flagged this possibility when it suggested that 'there may be increasing pressure and demands placed on the information by non-health care bodies (for example insurers, employers, law enforcement agencies and some government agencies)'.

A recent report published in the United States included homeland security in a list of potential uses for an electronic health record [4], while comments on the proposed Australian Department of Human Services Access Card noted that 'the government had played a clever game of avoiding engagement on privacy issues' [17] and 'the more details that are settled, the more certain is the loss of control over our personal information' [18].

It can be concluded that health data that we are happy to share now may become a liability in the future.

While we are not advocating cessation of work on the electronic health record, these future risks are a cause for concern. Clearly, there is a need for a wider, fully informed public debate, one in which we, the health informatics community, have a responsibility to speculate, debate and engage both our own members and the wider community.

A requirement is an open and public discussion about the legitimate uses of health information. Many of the proposed secondary uses have a great initial attraction, but others clearly require that much greater deliberation be carried out in a public setting [4].

References

[1] Berwick, D.M. 2002, Escape fire: lessons for the future of health care, The Commonwealth Fund, New York, http://www.members.cox.net/trustmemedblog/escapefire.pdf, (viewed 1 October 2004).

[2] Cornford, T. & Klecun-Dabrowska, E. 2003, Images of health technology in national and local strategies, Methods of Information in Medicine, vol. 42, no. 4, pp. 353–9.

[3] National Centre for Policy Analysis 2000. Patient dissatisfaction, <http://www.ncpa.org/ba/ba311/ba311.html>, viewed 30 September 2004.
[4] Griener, G. (2005) Electronic Health Records as a Threat to Privacy, Health Law Review, Volume 14, Number 1, Canada
[5] New South Wales Ministerial Advisory Committee on Privacy and Health Information 2000, Report to the NSW Minister for Health: Panacea or Placebo? <http://www.health.nsw.gov.au/policy/gap/privacy/eprivacy.pdf>, viewed 15 May 2004.
[6] Clarke, R. 2001, Research challenges in emergent e-health technologies, <http://www.anu.edu.au/people/Roger.Clarke/EC/eHlthRes.html#Ben>, viewed 12 September 2004.
[7] Schoen, C., Blendon, R., DesRoches, M., Osborn, R., Raleigh, E., Huynh, P., Ho, A. & Zapert, K. 2003, Commonwealth Fund International Health Policy Survey of Hospital Executives, Summary Chartpack, http://www.cmwf.org/usr_doc/2003_IHP_Survey_Chartpack.pdf, viewed 23 June 2004.
[8] Bajkowski, J., 2006, Abbott crash tackles e-health program. Computerworld, http://www.computerworld.com.au/index.php?id=1737192765&eid=-6787 Viewed 4 December 2006.
[9] email communication from a Victorian Primary Care Partnership Project Officer, 2006
[10] Delegate, National Health Information Summit, Melbourne December 2004
[11] *Curtis, Consumer Group, 200*4:62
[12] Horsfield, B. & Peterson, C. 2000, 'The hierarchy of discourses in the current diffusion of e-health, telemedicine and telehealth in Australia', Communications Research Forum. http://www.crf.dcita.gov.au/papers2000/horsfield.doc Viewed 15th December 2004
[13] IMIA Code of Ethics http://www.imia.org/English_code_of_ethics.html
[14] Ross, J.W. and Weill, P., 2004. IT Governance: How Top Performers Manage It Decision Rights for Superior Results, Idea Group Publishing, Hershey, PA, USA
[15] Booth, N., Martin, M., Smith, S., and Bell, S. (2002) Durham & Darlington ERDIP Demonstrator Project: Frameworks for Ethics, Security and Governance for the Electronic Health Record. http://www.nmconnect.nhs.uk/doclib/DuDa%20info%20governance.doc
[16] Phillips, G. 2003, 'Guthrie cards', *Catalyst*, ABC http://www.abc.net.au/catalyst/stories/s867619.htm
[17] Johnson, A., 2006, in Dearne K., Watchdog accused of cringing to Hockey, The IT Australian, Tuesday November 14th
[18] Warner, T., 2006 in Dearne K., Watchdog accused of cringing to Hockey, The IT Australian, Tuesday November 14th

Address for correspondence

Sue Whetton
Sue.Whetton@utas.edu.au
Ph: 03 6324 4025
Fax: 03 6324 4040
University Department of Rural Health
Locked Bag 1372,
Launceston TAS 7325