Patient Privacy and Security – Not a zero sum game!

Stephen Wilson[1], Chris Connolly[2] & Elizabeth Denney-Wilson[3]
[1]Lockstep Consulting
[2]Galexia Consulting
[3]NSW Centre for Overweight and Obesity, University of Sydney
Email: swilson@lockstep.com.au

Invited paper for Australasian Epidemiologist Special edition on Ethics and Privacy, April 2005 Vol 12.1

Abstract

All too often in the debate over electronic health records, the interests of the individual and of the broader community are thought to be at odds. The patient's fundamental right to privacy is generally assumed to be best served by an *opt-in* rule requiring their explicit up-front consent to participate. Yet the benefits to population health and medical research of a comprehensive record depend on the completeness of the data and a freedom from bias, both of which may be compromised unless the vast majority do in fact opt-in. Is this tension between individual and community unavoidable? The answer may lie in new security technologies such as smartcards, which can help de-identify event summaries written into the record, while preserving the patient's explicit control over the process. If fundamental privacy protections can be built into the architecture of electronic health record systems and health identifiers, then the de facto rule might be safely changed from opt-in to opt-out, with significant improvements in participation rates and consequentially the usefulness of population health data.

Introduction

Electronic health records constitute a rich vein of complex ethical and privacy issues. Consumers typically fear for their privacy in EHR systems and yet remain divided over whether the benefits are worth the risks.[1] Lawyers and legislators are weighing the need-to-know of researchers versus the legal and ethical rights of patients.[2] Much academic research is ongoing as to whether or not important biases are introduced into population health data should patients be systematically opting out.[3] Furthermore, comprehensive electronic health records are going to be very expensive;[4] such major allocations of the public health dollar make it arguably unethical not to take active steps to ensure the full potential benefits can be delivered.

Much of the privacy and security tension in electronic health records turns on one simple technical fact: all data stored in EHR systems must be ultimately tied to individuals. Typically, a unique health identifier (UHID) is assigned to each individual, and included with each item of saved data. Yet the uniqueness of a numerical UHID is also its greatest privacy weakness, for on its own it is merely a pseudonym. If the UHID is used to index someone's records, and if the linkage between their name and their UHID becomes known, then their entire stored history becomes identifiable.

Relatively little research has been done to date on the detailed handling of health identifiers. It is assumed by many that UHIDs are basically no more than numbers[5,6] and, as such, can be stored and handled in a variety of technologically neutral ways. Further, by fostering a range of UHID storage mechanisms and thereby offering a wide range of options,[7] some EHR architects would appear to believe they are serving the ethical interests of consumers in respect of freedom of choice.

Identifiers in Health*Connect* – Australia's national EHR project

Health identifiers are listed by the Department of Health and Aging as amongst the seven most crucial building blocks of the emerging national e-health environment.[9] Contemporary work on public policy and management of UHIDs in Australia can be traced back to the late 1990s with the National Electronic Health Records Task Force, which laid the foundations[10] for the project we now know as Health*Connect*.[7] Amongst many other things, the task force report started the process of outlining the technological and management options for a national UHID. It suggested three alternatives:

1. options not requiring universal identification; e.g. Patient Master Indexes
2. biometrics, and
3. the assignment of a number unique to each individual, "either entirely new or based on an existing one, such as the Medicare number".[11]

The task force preferred the third option, for a number of non-controversial reasons which need not be reviewed again here. The same conclusion has been confirmed several times since, and is now an accepted part of the Health*Connect* Business Architecture.[8] The new National Electronic Health Transition Authority (NEHTA) has recently begun detailed work on a national identifier.[12] In the meantime, the Health*Connect* project has advanced through requirements, pilot and architecture phases. In 2004, the Commonwealth committed $128M over four years to the project.[13]

The benefits of electronic health records

There are five broad areas where e-health records can deliver benefits:

1. ***Clinical care***
   Ready access to complete medical histories can be expected to improve the way healthcare providers work with their patients; adverse interactions may be spotted before prescribing drugs; complications and adverse hospital events should be reduced; post-operative care should be enhanced when General Practitioners have access to electronic hospital discharge data.
2. ***Administration***
   Keeping track of patient's and family member's contact details; automating Medicare and insurance claims and settlements; generating reminders for routine interventions such as pap smear tests; automating chronic care plans; generally allocating health resources in a more timely and efficient manner.
3. ***Cost***
   Major time and cost savings can result from reducing the need to take repetitive patient histories, decreased readmission rates as a result of better post-operative care, and reducing over-servicing or over-prescribing on an individual as well as community basis.
4. ***Population health***
   Communicable and non-communicable disease surveillance; monitoring of health indicators and complications of chronic conditions; enhanced post market surveillance, including rapid identification of adverse events of medications, surgical procedures and medical devices.
5. ***National health programs***
   Feedback on performance of preventative health programs (such as immunisation); fine tuning the allocation of preventative health resources; enhanced response to outbreaks.

To date, most political and media interest has concentrated on the first benefit; that is, clinical care. However, all five categories of benefit should be considered, and most EHR implementations will lead to benefits in the other categories many years before clinicians are routinely relying heavily on electronic patient files.

Attitudes to electronic health records and privacy in Australia

Australians register a high level of concern about issues of personal privacy. As the strong public opposition to the proposed Australia Card in 1987 demonstrated, Australians are sensitive to government initiatives that are seen as a threat to individual privacy. Since that time, concerns have increased in response to growing privacy threats, in particular from new technologies.

Escalating privacy concerns is a well established global trend, reflected both in the spread of regulation in Europe, Australasia and America, and in numerous surveys over the past decade. For example, the regular Harris-Westin consumer privacy survey in the USA has recorded a jump in the number of "privacy fundamentalists" – those worried about personal control, data use and regulation – from 25% in 1995 to 37% in 2003, while 'privacy unconcerned' respondents dropped from 20% to 11%.[15]

The most comprehensive survey of attitudes to privacy in Australia was conducted by the Office of the Federal Privacy Commissioner (OFPC) in 2004.[16] Health information was confirmed as one of the most sensitive categories of personal information. It was, for example, ranked fourth in terms of sensitivity in the OFPC's survey; similar results have emerged in the United States.[17]

However, community attitudes on health privacy are nuanced. Although individuals are acutely concerned in principle about the privacy of their health information, it seems that few have experienced direct privacy breaches. In fact, health-related organisations enjoy a higher level of public trust than any other in Australia. The OFPC's survey revealed that health service providers scored 4.43 out of 5.00, well ahead of financial organisations, placed second on 3.54, and the government on 3.52. Overall, 89 per cent of respondents regarded health service providers as "trustworthy".[16]

In other words, while people expect a high standard of privacy from health service providers they do not have significant concerns that these expectations are not being met. This may reflect the fact that high standards are followed, or perhaps individuals are unaware of shortcomings in health information handling because they have limited visibility of clinical and administrative practices. We would caution at this stage that, given the disparity in trust scores between healthcare organisations and governments, a perception of excessive government interference in the way healthcare is delivered, in the process of introducing Health*Connect*, may be expected to erode trustworthiness rather suddenly. It is clearly important that Health*Connect* be perceived first and foremost as a *healthcare* and not a government programme.

Consumers' main concern over Health*Connect* is that they want to know that they can exercise control over their health information. The OFPC's survey found that 64% of respondents believe they should be able to choose whether they are included in any national health database. Individuals want to decide how much information they provide, when it can be disclosed to other healthcare stakeholders – including insurers, drug companies, employers and government departments – and they want access to personal records that a health service holds. Finding ways to meet these expectations will be critical for ensuring public support for Health*Connect*.

The perceived conflict between privacy and electronic health records

Recent telephone polling by Harris Interactive[1] of over a thousand American adults showed a nearly even split between those who believed that the benefits of EHR outweigh the privacy risks (48% of respondents) and those who believe the privacy risks outweigh the benefits (47%). [Notes: sample size was 1,012; sampling related error was quoted as +/- 3 % points at 95% confidence limit].

We suggest that a deeper message in the survey is that many people appear to believe that *significant privacy risks are inevitable*. It is likely that some proportion of those who believe benefits to outweigh the risks are prepared to live with those risks, no matter how high they may be in absolute terms. That is, people have come to believe that they probably cannot have privacy and electronic health records at the same time. The construction of the Harris Interactive survey itself follows the presumption of a dichotomy: minimal privacy risk *or* beneficial electronic health records, but not both.

The Opt-In Privacy Model

The quasi-standard way to ensure privacy in electronic systems is to have participants explicitly opt-in before any of their information becomes part of the system. In an opt-in EHR, the default is that individuals do not have any of their health information entered until they give explicit consent. One risk in the opt-in model is that it can focus on a once-only choice of participating or not, and may not be able to address adequately the complexity of individuals' concerns about privacy issues, and their desire to be able to exercise control over their personal information.

Similarly, EHR consent models may need to take account of the specific choices that patients may want to exercise in the course of its use; that is, when they want a specific encounter to form part of their record, when they want clinicians to be able to access their medical history, or when they want to modify their medical record. So while the opt-in approach is regarded as almost axiomatic by many, it carries significant risks if used as the sole privacy protection for EHRs, including:

– ***One-time only consent***
  Opt-in systems rely on the one-time provision of consent for participation, yet this is not an accurate reflection of a typical person's interaction with health services over their lifetime. Attitudes to privacy, health records and even the individual or organisation they are dealing with at any particular moment may not reflect overall attitudes, nor future views.

– ***Promotion of bundled consent***
  An opt-in approach may promote "bundled consent", where the patient's EHR consent is sought at the same time they are trying to access an important health service. In the financial services context, the Federal Privacy Commissioner has criticised the practice of obtaining bundled consents.[20] In contrast, with opt-out schemes, consent decisions are more readily separated from provision of health services, and can be made at any time, under less pressure.

– ***Over-reliance on a single privacy measure***
  Reliance on a single safeguard can weaken overall privacy protection. In practice, privacy concerns raised by consumers down the track are sometimes met with the blanket response 'if you have concerns, you shouldn't have consented', or 'if people don't like it, they don't have to join'. This is lazy privacy protection, and it removes the motive to manage all aspects of privacy responsibly.

In addition to these privacy risks, the opt-in approach can limit the potential benefits of EHRs, not only by shrinking the size of the population data set, but possibly also biasing the data. For instance, Canadian researchers have argued that "[strict] consent laws can introduce an important authorization bias when patients who release personal health information for health research differ significantly from those who do not. Such a bias may result in an inaccurate estimate of the health status of the population".[3] Important research is ongoing regarding the question of consent and bias.

Let us revisit the five major benefits of EHR and examine the impact of an opt-in approach:

– ***Clinical care***
Clinicians might not see a sufficient volume of full participants to justify changing their current practices to rely more on electronic records.

– ***Administration***
Health administrators would have to maintain major paper-based and electronic systems in parallel.

– ***Costs***
Financial managers would have to maintain parallel paper-based and electronic systems. Moreover, efforts to manage over-servicing would be limited to sub-populations; we should expect persistent "doctor shoppers" to not opt-in and so self-limit their fraudulent activities.

– ***Population health***
Australia's small size means that an inability to use national data may impede population health monitoring and surveillance. This will be exacerbated if the number of EHR participants is small, or if there is a bias in the electronic records towards particular population sub-groups who are more likely to participate (e.g. the chronically ill).

– ***National health programmes***
An opt-in scheme could be seen to be inconsistent with the strategic objectives of some national preventative health programs where high levels of compliance are required (such as childhood immunisation) and may also impede the country's ability to respond quickly to new national health issues such as changes in tropical diseases purportedly associated with global warming, and novel outbreaks such as bird flu or SARS).

The Opt-Out Model

In an opt-out EHR, health information is collected, stored and, within limits, distributed, unless the individual concerned explicitly elects not to participate. That is, the default is that patient data is entered into the EHR.

An opt-out model does not mean that individual choice is removed. In particular, it is expected that patients should always have the opportunity to withdraw from an EHR, or more subtly, to exercise fine-grain control over how their records are made available to third parties. The essence of the opt-out approach is an assumption that the great majority of individuals can reasonably be expected to willingly participate, and that it is ethically sound therefore to enter their medical data without first gathering explicit consent.

Any workable opt-out model demands a host of additional privacy protection measures, including:

– ***Prohibition on use of the EHR outside health***
This is critical for addressing "function creep". The OFPC has raised this concern repeatedly, and has advocated the use of active technical controls in system design to limit function creep, rather than relying solely on legislation.

– ***Simple and clear opportunity to opt-out***
Many consumer rights advocates are concerned that patients' current experience of consent processes – being asked to sign a consent form before a procedure – does not enhance their sense of autonomy or choice; typically they are left feeling that they may have waived some of their legal rights. A proper opt-out system must provide easy and ever-open opportunities to modify one's consent elections.

- ***Partial opt-out elections***
  The system must let individuals make their own choices as to the collection of data from different types of encounter, and how that data is stored, processed, used, and to whom it may be disclosed. Participants ought to be able to selectively opt-out of certain aspects of the EHR, while remaining a participant in others.
- ***Strengthened privacy governance***
  Finally, under opt-out models, if we are to reasonably presume that consumers will be happy to be included by default, then clearly they deserve clear privacy protections in legislation and in binding codes of conduct. In this context, encouraging progress has been made in the last 24 months on a National Health Privacy Code.[21]

The principle benefits of the opt-out model for EHRs in Australia should be that a higher proportion of the population will participate, and the make-up of participants will be less likely to be biased. This would lead to obvious benefits in all five categories of benefits as discussed above, while still allowing a sophisticated response to privacy concerns, consistent with legislation and codes of conduct.

We note that a number of significant EHR programmes have already adopted the opt-out approach, including the Central Hampshire (UK) EHR Demonstrator,[22] the Walsall (UK) EHR,[23] and South Australia's Open Architecture Clinical Information System (Oacis).[23] The UK National Health Service is adopting opt-out in general,[25] and has the cautious support of some privacy advocates. For instance, the patient rights body, the UK General Medical Council, advised the Central Hampshire Electronic Health Record Project as follows:

> *"[Our] guidance says that where patients have consented to treatment, express consent is not usually required before relevant personal information is shared to enable the treatment to be provided. Patients should, however, be told that information will be shared unless they object … In our view it clearly follows that, for an emergency EHR, or for the provision of care to which a patient has consented, an opt-out system will be sufficient in respect of consent for* access to or use of *the data. There is one proviso to that. A fundamental principle of confidentiality is that disclosures should be kept to the minimum necessary"*.[22]

Smartcards to protect patient privacy in EHRs

We propose that significant structural improvements can be made to patient privacy within EHR systems by taking special care of health identifiers. Rather than the prevailing technology neutral position which sees UHIDs stored in more or less any fashion, we suggest that smartcards have an untapped potential to mask an individual's UHID, thus de-identifying patient data before they are written into the EHR.

Smartcards are perhaps best known for their resistance to identity theft. Unlike regular magnetic stripe cards which can be "skimmed" if they fall into the wrong hands, smartcards protect stored data against unauthorised access. To merely read, let alone modify, the data in a smartcard, it is necessary for an intelligent card reader to positively identify itself to the microchip on the card, and to satisfy various security criteria. One thing that makes smartcards "smart" is their ability to be programmed to make decisions about when and where they will exchange data with the outside world. If the correct conditions do not obtain – including the proper terminal equipment, the proper security protocols, and the presentation of a recognised PIN – then the smartcard will simply refuse to "talk".

In considering how best to convey patient identifiers, we observe that cryptographic smartcards have the capability to "tag" stored data with an essentially incorruptible *digital signature*. This signature can be unique to the smartcard chip without giving away any information at all about the card holder. This provides a powerful means for eliminating data linkages and de-identifying transactions carried out using the smartcard. In particular, a health event summary can be indelibly linked (by another digital signature) to the smartcard chip, which as indicated, can be linked in turn to a UHID programmed into the chip. Nothing in such an event summary would directly identify the patient; it could only be linked back to an individual through their smartcard and therefore with that person's explicit consent. Third parties such as researchers, policy analysts and administrators could safely access more or less the entire EHR without being able to identify the individual.

Benefits

Smartcard protection of health identifiers brings potential benefits for the privacy of participants – and by extension, for the population health purposes of the EHR – as follows:

– enables secure, de-identified health records, with high levels of trust and safety, perhaps sufficient to support the opt-out consent model, thus driving higher participation rates

– one smartcard, programmed with multiple UHIDs, can index multiple EHRs, facilitating the mapping of personal records from one system to another, maximising the population-wide benefits of what would otherwise be isolated data stores

– helps to quarantine EHR systems from each another, and so defuse fears that function creep might lead in effect to an "Australia Card"

– provides patients with clear, physically tangible consent mechanisms, and explicit control over linkages between disparate EHRs

– simplifies de-identification of research or administrative data because event summaries are not identifiable in the first place.

Implications and conclusions

If digital signatures can be used to link health identifiers to smartcards, and smartcards in turn to EHR entries, such that card holders cannot be re-identified without their smartcards, then we suggest that the time has come to get more specific about precisely how identifiers will be managed. The privacy advantages and the resulting possibility of a trustworthy opt-out model may be sufficiently large that the historical perceived downsides of smartcards – chiefly their cost and relative lack of accessibility – should be re-visited.

A new Medicare smartcard is currently undergoing evaluation in Tasmania.[24] To date, the Health*Connect* project team has not envisaged integrating the smartcard closely into the EHR system; Health*Connect* has only made some generic statements about optionally storing a UHID 'on the card'.[8] We recommend that consideration now be given specifically to using digital signature technology to manage Health*Connect* identifiers with the Medicare smartcard. Furthermore, we urge caution with regard to any other form of storage of identifiers, because of the privacy risks should they be exposed.

Another possibility arises from the fact that modern smartcards can act as general purpose "containers" for digital credentials. Any sufficiently capable smartcard could be used to convey private identifiers as described here. Examples of such smartcards include the New Qld Driver Licence[26] and the debit/credit smartcards that have appeared in the tens of millions across Europe[27] and parts of Asia. We recommend that EHR system architects in general consider the option of loading secure health identifiers onto such smartcards, which will become increasingly available to the general public over the next few years.

References

1. *Health Information Privacy (HIPAA) Notices Have Improved Public's Confidence That Their Medical information Is Being Handled Properly* Harris Interactive 24 February 2005. Available: www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=894 (accessed February 2005).
2. *NHS Confidentiality Consultation – FIPR Response* Foundation for Information Policy Research 2003. Available: www.cl.cam.ac.uk/users/rja14/fiprmedconf.html (accessed March 2005).
3. Upshur REG, Morin B, Goel V *The privacy paradox: laying Orwell's ghost to rest* CMAJ August 7, 2001; 165.
4. Dearne K, *Feds hunt HealthConnect head* The Australian, January 12, 2005.
5. Netter W *Curing the Unique Health Identifier: A Reconciliation of New Technology and Privacy Rights* American Bar Association Jurimetrics, V43 pp 165-186, 2000.
6. *Unique Health Identifier for Individuals: A White Paper* United States Department of Health and Human Services, July 1998. Available: http://ncvhs.hhs.gov/noiwp1.htm (accessed January 2005).
7. *HealthConnect Business Architecture V 1.9* Commonwealth Department of Health and Aging, November 2004.
8. *HealthConnect Business Architecture Version 1.9 Specification of HealthConnect Business Requirements* Commonwealth Department of Health and Aging, November 2004.
9. *Progress Report: E-health building blocks* Commonwealth Department of Health and Aging, April 2003. Available: http://tinyurl.com/2gr33h (accessed March 2007).
10. *A Health Information Network for Australia*, Report to Health Ministers by the National Electronic Health Records Taskforce, July 2000. Available: http://tinyurl.com/yrh8fw (accessed March 2007).
11. *Health Identifiers: Options In An Electronic World* Appendix H of the Report to Health Ministers by the National Electronic Health Records Taskforce, July 2000. Available: http://tinyurl.com/yrh8fw (accessed March 2007).
12. *National E-Health Transition Authority Work Program* 2005.
13. *Highlights of the 2004 Federal Budget* People With a Disability E-Bulletin Issue 11, May 2004. Available: www.pwd.org.au/e-bulletin/pwd_e-bulletin_11.html (accessed March 2005).
14. *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)* American Society for Testing and Materials, ATSM E1714, 2003.
15. Westin, A *Consumers, Privacy and Survey Research*, CASRO Annual Conference, 2 October 2003.
16. *Privacy and the Community*, Office of the Federal Privacy Commissioner 2004.
17. *Public Attitudes Toward Medical Privacy*, Institute of Health Freedom September 2000. Available: www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.pdf (accessed February 2005).
18. *EHR Community Consultation Research Report* NSW Health December 2002.
19. *A Report of Qualitative Research into the Health Online Concept* Commonwealth Department of Health and Ageing. February 2000.
20. *Bundled Consents and the Privacy Act* Office of the Federal Privacy Commissioner, Media Release 22 May

2002. Available: www.privacy.gov.au/news/media/02_8_print.html (accessed February 2005).

21. *Proposed National Health Privacy Code* The National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, August 2003.

22. *Central Hampshire Electronic Health Record Demonstrator* Report T35 Hampshire and Isle of Wight Strategic Health Authority, November 2002. (accessed March 2005).

23. *Electronic health information systems case studies* (Health*Connect* Interim Research Report Volume 3 Part Two) Commonwealth Department of Health and Ageing, April 2003.

24. Medicare smartcard home page: www.hic.gov.au/yourhealth/our_services/medicare_smartcard.htm (accessed March 2005, no longer available at March 2007).

25. Cross M *IT gurus attempt to win doctors' hearts and minds* BMJ.2005; 330: 276, 5 February 2005.

26. New Queensland Driver Licence www.transport.qld.gov.au/new_driver_licence (accessed March 2005).

27. *Chip and PIN now 'part of everyday life';* Chip and PIN press release, 8 November 2005. Available: www.chipandpin.co.uk/reflib/part_of_everyday_life.pdf (accessed March 2005).