Australian
Privacy
Foundation

p o s t: GPO Box 1196
Sydney NSW 2001
e m a i l: enquiries@privacy.org.au
w e b : www.privacy.org.au

20 March 2006

NSW Health*elink* – background information

NSW trials of electronic health records

*The two Health*elink *trials*

Trials of a consolidated shared electronic health record (EHR) are due to start in NSW on 23 March 2006.

The Health*elink* project involves trialling electronic health records for two populations:

- the elderly (over 65) in the Hunter area (commencing 23 March 2006), and
- children (under 15) in the Greater Western Sydney area (commencing 25 May 2006).

The purpose of the two trials (or 'pilots') is to test the system before it is rolled out to all people in NSW.

Privacy issues and risks with electronic health records

The Australian Privacy Foundation is not opposed to EHRs per se. We can see the great health benefits they can bring. However people will only gain the benefits of EHRs if they trust the system – and that means getting the privacy and security issues right.

These privacy and security issues include:

- consent – only enrolling people in an EHR system if they consent to be included
- transparency – allowing people to understand clearly how the system will work, and who can access what information in different circumstances
- control over the record – allowing patients to exercise some control over who can see which parts of their health record
- collection limitation – the system should only collect information that is relevant to a person's health record
- data security – ensuring the IT systems, policies and procedures in place is designed to minimise the chance of unauthorised access, modification, disclosure or deletion
- accuracy – ensuring the information in the record is correct, and is assigned to the correct person

- access and correction rights – ensuring people can access their own record easily, and can make corrections if they find mistakes
- use limitation – setting out who can access and use the health record, and who can add new information into it
- protection from disclosure – limiting the circumstances in which health information from the EHR can be disclosed by a clinician or by the organisation running the EHR database
- anonymity – not impinging on people's ability to seek healthcare anonymously
- identifiers – preventing unique identifiers development for an EHR system being used outside the health sector as a defacto 'national identification number'

Privacy risks inherent in any system of EHRs include:

- the system by which patients can access their own records has poor security, so that the wrong people may easily gain access to patient records by posing as the patient (e.g. through guessing passwords, phishing, intercepting mail or email, or stealing token 'keys')
- the system has poor online security, so that the wrong people may gain access to patient records by hacking into the database
- someone 'inside' the system accesses patients' records for inappropriate reasons (e.g. to find our their ex-girlfriend's new address)
- a clinician allowed the see patient records then uses or discloses the information for an unauthorised purpose (e.g. selling patient records to a pharmaceutical company)
- the very existence of a consolidated health record will lead a patient's employer or insurance company to demand a copy of the full record from the patient, before they get the job or insurance cover

It is the job of people designing EHR systems to minimise these risks as much as possible – by using the best technology, legal safeguards, policies, procedures, and training.

The Australian Privacy Foundation opposes the model being trialled in the Health*elink* project, because we do not believe it delivers the necessary levels of privacy or security, and thus leaves some of these risks unaddressed. We explain why below.

How Healthelink will work - FAQs

We've prepared the following FAQs based on our understanding of how the Health*elink* trials will work, from a demonstration of the system in January 2006, various discussions with NSW Health officials about the Health*elink* trials, presentations made by NSW Health officials at consultation events such as the NCOSS Healthelink Forum, and the two-page Fact Sheet issued by the Department in February 2006.

Q Who will be included in the trials?

Patients who meet the eligibility criteria will be included in the trials. The eligibility criteria relate to the patient's home address, and their age, at the date the trials commence.

The following people will therefore be included:

- people aged over 65 as at 23 March 2006, living in the postcodes 2320 to 2324 (the Hunter), and
- people aged under 15 as at 25 May 2006, living in the postcodes 2145, 2148, 2150, 2170, 2560, 2747, 2750 or 2770 (Western Sydney)

Patients who meet the eligibility criteria will be automatically added to the system, unless they opt out.

Q What information will be included in my EHR?

Your Health*elink EHR* will contain non-health information about you (such as your name, date of birth, address and home telephone number), as well as summaries of your health information, gathered from records kept by participating doctors, hospitals and community health centres.

Depending on the health services you have accessed since the start of the trial, this might include:

- a health diary containing your appointments and health questionnaires
- a summary of treatments you have received from participating health services such as:
    - hospital inpatient departments
    - hospital outpatient and emergency departments
    - community and allied health services (including social workers and psychologists)
    - GPs
    - dentists
- results from blood tests or x-rays
- discharge referrals

Q I've been told I can "opt out". Does that mean no information will be collected about me?

No – some personal information will still be collected about everyone who meets the eligibility criteria, even if you opt out from day 1.

Patients who opt-out will still have demographic information about them (name, sex, date of birth, address and home telephone number) kept on the central EHR database - because the Department needs to know who opted-out so that it knows not to keep collecting clinical data about them every time they visit a participating provider.

And patients who opt out more than 30 days after their first visit to a participating health service provider will still have their health information kept by the Department – it won't be deleted.

The following table summarises what information will be kept, and what information will be shared, depending on if and when you opt out.

	The Department will keep on the EHR database your:	**Clinicians / users will see:**
If you opt out between Day 1 and Day 30	• name • date of birth • sex • home address • home telephone number • Medicare card number • unique patient identifier	• nothing
If you opt out after Day 30	• name • date of birth • sex • home address • home telephone number • Medicare card number • unique patient identifier	Between Day 30 and the day you opt out: • name • date of birth • sex • home address • home telephone number

	plus: • health information gathered about you, collected from Day 1 until the day you opted out	• Medicare card number • unique patient identifier plus: • health information gathered about you, collected from Day 1 until the day you opted out After you opt out: • nothing
If you don't opt out at all	• name • date of birth • sex • home address • home telephone number • Medicare card number • unique patient identifier plus: • health information gathered about you, from Day 1 onwards	• name • date of birth • sex • home address • home telephone number • Medicare card number • unique patient identifier plus: • health information gathered about you, from Day 1 onwards

Q Is there any data security risk from using this "opt out" model?

Yes. The Health*elink* "opt out" system means retaining data even on people who "opt out".

This presents a data security risk from hackers, heightened for those people who have opted-out of Health*elink* not because of (or not only because of) concerns about the privacy of their health information, but because of privacy concerns about their contact details (e.g. victims of spousal abuse, people on witness protection, celebrities who fear stalkers etc - or anyone who just doesn't want to be a victim of identity theft or fraud).

In our view, this alone is an example of why the system should instead be "opt in" - then the security risks are at least only faced by the people who want to be included and will receive the benefits!

Q Can I see my own EHR?

Yes. Patients will be given a login ID and password, so they can see (and update) their own EHR over the internet.

Q Are there any privacy or security risks with this form of access?

Yes. Just like internet banking, you could be the victim of "phishing", in which someone attempts to find out your login ID and password by sending you a bogus email – or the victim of a trojan or virus which collects your login ID and password without you knowing it.

The Australian Privacy Foundation would prefer to see more robust authentication requirements than just a login ID and password.

Q Who else will be able to see my EHR?

Hundreds of health service providers will be participating in the two trials alone. These include:

- GPs

- hospital inpatient departments
- hospital outpatient and emergency departments
- community and allied health centres
- dentists
- pathologists
- social workers and psychologists

Q Can I say I don't want a particular person to see my EHR?

No. Any participating health service provider in the pilot areas will be able to see your EHR, unless you opt out of the system entirely.

This is contrary to various previous promises that people would be able to 'block' particular users of the system. (For example, a patient might not wish their dentist to see their sexual history, or might not want an ex-boyfriend working in a hospital to see their address or reference to a psychological report.)

Q Can I say I don't want my EHR to include particular information about me?

No. A summary of all new health information will be added to your EHR, unless you opt out of the system entirely.

So even health information you might regard as particularly confidential or sensitive, such as the results of a blood test or a record of attendance at alcohol counselling, will be readable by any health service provider who decides to read your EHR.

This is contrary to various previous promises that people would be able to 'quarantine' particularly sensitive health information, such as sexual or mental health issues.

Q Can I suppress my home address or telephone number on the EHR?

No.

Q How do health service providers see my EHR?

Like patients, participating health service providers will be given their own login ID and password.

Once in the system, users can search for the EHR of any patient who hasn't opted out, simply by searching on their name.

Health service providers do not need to prove that they are actually involved in your treatment or care, before they can access your EHR.

Q What security measures are there to stop unauthorised access to my EHR?

The Australian Privacy Foundation is concerned about the low level of security protections to prevent inappropriate access or misuse of your health information, by users of the EHR system.

Users of the EHR system (i.e. health service providers) do not need any kind of physical token (such as the patient's Medicare card or a smartcard or PIN) to be entered, to demonstrate that they are treating the patient, before accessing the patient's EHR.

There will be an audit log kept to show which health care provider has accessed a patient's record at what time, and the patient can see this, so that provides some level of accountability for any privacy breach.

But in our view this is an inadequate response to the risks of placing large numbers of people's name, home address and telephone number and date of birth (enough to start down the process of stealing someone's identity) on a central database, accessible by hundreds (and eventually thousands) of people.

Legal and ethical safeguards which encourage clinicians not to abuse this system are not enough - we should be examining the use of technological methods to more securely lock patients' information inside the database - and ONLY collect information on people who opt-in in the first place.

We are also concerned that health service providers could be subject to "phishing" or trojan attacks by hackers to gain their ID and passwords to enter the system; or that they simply don't protect the security of their ID and passwords (e.g. writing them on a note on their desk, or telling their admin assistant).

Q In what circumstances can my EHR be disclosed to third parties?

The Department of Health, which will be collecting personal information about you if you meet the eligibility criteria (even if you opt out), can then disclose information from your EHR under Health Privacy Principle 11.

This law allows your health information to be disclosed without your consent by the Department of Health for various purposes, including:

- to provide you with a related or further health service, *even if you object*
- to the Health Minister or the Premier, to inform them
- for law enforcement purposes
- as part of an investigation into professional misconduct or an employee disciplinary matter
- for approved research projects
- for complaint-handling purposes
- to inform your family about you, for compassionate reasons

The Department could also be forced by law to hand over your EHR to a third party, such as your boss or insurance company, if it is subpoenaed for your records.

What we think is wrong with the Healthelink trials

We've mentioned above a number of our concerns about:

- the poor data security design of the system for patients to access their own records
- the poor data security design of the system for health service providers to access EHRs
- the fact any participating health service provider can access any patient's record
- that patients can't block particular people from accessing their record
- that patients can't quarantine particularly sensitive information from the rest of their record, and
- the large number of reasons under which the Department of Health can disclose information from a patient's EHR

However what concerns us the most is the use of an "opt out" model, instead of "opt in".

Both "opt in" and "opt out" models rely on the Department of Health to clearly explain to people the benefits and risks of participating.

However only with an "opt in" system can you be sure that people have really been able to weigh up the risks and benefits to themselves, and make an informed choice. If the system is "opt out", there is a much greater chance that people will be enrolled on the system without even knowing about it, or without understanding that they can choose to opt out. This will particularly be the case with people of non-English speaking background, literacy problems, or other reasons not to have received or read the relevant information.

Why has the NSW Government changed its position from "opt in" to "opt out"?

We don't really know or understand why.

First the Department of Health argued it was all about the cost – that "opt in" was going to be too expensive. But no costings of "opt out" were done to prove it was demonstrably cheaper than "opt in".

Then the Minister for Health argued it was because the Commonwealth Government's HealthConnect project required them to adopt an "opt out" model (see pages 21-23 of budget estimates hearings in September 2005). We disagree – the HealthConnect project's website explicitly says EHR systems should be "opt in".

The Department has also said in consultation forums that it wanted to change to an "opt out" system "to overcome people's inertia", because "consumer consultation said that this was the best model", and/or because of "national and international experience".

None of these assertions have been backed up by any published documentation or research. The decision has been taken behind closed doors, without public discussion or scrutiny.

By contrast, there is plenty of published material explaining why the Government originally made its decision to enshrine "opt in" as a patient's "right".

By adopting an "opt out" model for the Health*elink* trials, the NSW Department of Health is therefore going against:

- NSW health privacy law (Health Privacy Principle 15 requires express consent, or "opt in", before a patient is placed on a shared EHR system)
- the recommendations of the expert Ministerial Advisory Committee on Privacy and Health Information (the Panacea or Placebo Report, 2000)
- the recommendations of the NSW Health Council (the Menadue Report, 2000)
- the bi-partisan support of Parliament
- the views of health consumers – particularly those involved in sensitive areas such as mental health, HIV and sexual health
- the views of medical professionals including the AMA
- the views of public interest advocates including NCOSS (see NCOSS's letter to the Department of Health, and NCOSS's media release of 15 March 2006)
- the views of privacy advocates

Why we want Parliament to debate the "opt in versus opt out" issue

The NSW Government made a very specific promise to the people of NSW, when it proposed a Bill in 2002, to allow for the introduction of electronic health records in this State.

That promise was that no patient would be added to a system which shared electronic health records, with that patient's express consent. The Government even described this as a patient's "right" to "retain control over the decision to participate in any such linkages" (see Michael Egan's speech in support of the HRIP Bill).

This promise was enshrined in the law as Health Privacy Principle 15.

The Opposition supported the Bill because of the assurances from the Government and the Privacy Commissioner that "the bill contains provisions governing the linkage of health records to other records to ensure that there is no inappropriate second party transfer" (see Shadow Health Minister Jillian Skinner's speech in support of the HRIP Bill.)

However the HRIP Bill (now the HRIP Act) also contained a provision which allows the Government to make regulations to exempt some practices from the health privacy principles.

The Opposition noted at the time the danger that the Government would undermine the promise of the legislation by making regulations to exempt itself. Dr Brian Pezutti suggested that Members of Parliament "must watch carefully what the Minister does by way of regulation. ... It is imperative that the process be subjected to the same level of scrutiny as that applied to the introduction of the bill".

Dr Pezutti also noted that the Parliament "will have the opportunity to amend the regulations if necessary. The AMA, NCOSS and the Privacy Commissioner can decide whether the regulations are fair and reasonable or otherwise."

The Australian Privacy Foundation believes this important issue should not be left to bureaucrats within the Department of Health to decide, by way of regulation. If the explicit promise in the current legislation - that health records would only be developed on an "opt in" basis - is to be undermined from the very start of trials, this decision should only be taken by Parliament following informed debate.

What consultation has been done on this issue?

When the NSW Government first proposed the introduction of electronic health records in this State, the then Health Minister convened a Ministerial Advisory Committee on Privacy and Health Information.

The Committee's public consultation process included:

- placing advertisements in leading metropolitan newspapers
- writing to over 500 individuals and organisations, calling for submissions
- considering 42 written submissions from a range of individuals and organisations
- two public forums held at the NSW State Parliament, and
- a workshop conducted as part of the Consumers Health Forum national consultation process regarding electronic health (*Panacea or Placebo*, 2000)

The Committee concluded that:

> ***The ability to transfer all or part of the information contained on an electronic health record must only occur with the expressed and informed consent of the health consumer.***

The NSW Government accepted that recommendation, and, in consultation with the NSW Privacy Commissioner and other key health consumer and clinician stakeholders, drafted Health Privacy Principle 15 in the Health Records and Information Privacy Act 2002.

By contrast, what public consultation or research has NSW Health done since changing its view about "opt in versus opt out"?

We have seen nothing published by the Department to prove their assertions that consumers and clinicians prefer “opt out” over “opt in”. In fact the published views of the two peak organisations representing health consumers in NSW (NCOSS) and doctors (the AMA) state the opposite – they are in favour of “opt in”.

While representatives of the Department of Health met with some health consumers in 2005 who expressed support for “opt out”, we are concerned that those results may have been biased with scare stories about how "opt in" takes 45 minutes of face-time the system can't afford. (We disagree that “opt in” should take any longer to explain to health consumers than “opt out”.)

Furthermore, even at that consultation, NCOSS has noted that “there is a divergence of opinion across this “broad church” about the desirability of using an “opt off” model as the basis of implementing electronic health records”. In particular, while “older persons organisations and groups representing the interest of people with more traditional chronic conditions” had fewer privacy concerns, many other health consumers, “especially in mental health, HIV and Hep C areas” expressed “strong concerns about privacy and discrimination matters”.

Although the trials of Healthelink are being used to make decisions about what consent model should be used for the entire NSW population, we understand that NSW Health has not consulted people aged between 15 and 65 and/or people who are *not* frequent health system users.

The rest of the population might have very different views to the under 15s and over 65s on the privacy risks versus the health benefits of EHRs, in particular concerns about:

- the sensitivity of sexual health information, including contraception, infertility, terminations, infectious diseases, and sexual abuse
- the sensitivity of drug and alcohol information, and
- potential employment and insurance uses of their health information.

We believe that a system of EHRs needs to work for everyone – both in terms of delivering the health benefits, but also in terms of minimising the privacy risks.

That is, the EHR model should be designed to promote the health benefits for those most likely to benefit, *and* be designed to minimise the privacy risks to those most likely to suffer a privacy impact.

What is wrong with just trialling “opt out”?

First, this is the first trial. We believe the first trial should be of “opt in” to test whether it is problematic and if so how the system could be fixed - instead of just assuming the decision made by Parliament to support “opt in” is just too difficult, without even bothering to test it.

Second, we don’t believe that patients in the Hunter and Western Sydney deserve any less privacy protection than patients elsewhere in the State, just because their area has been selected to run the trial.

Third, because the Department of Health has said they will use the results from this trial to determine what consent model will be rolled out for the rest of the State.

While trialling the EHR system on frequent health 'users' makes sense in terms of assessing the health benefits to those most likely to benefit, it does not make sense to also treat that as an appropriate trial of a consent model from which decisions can be extrapolated about the privacy needs of the entire population.

Fourth, because there has been no public notice or consultation about changing the law from “opt in” to “opt out”, and no independent Privacy Impact Assessment has been conducted.

Since the Acting Privacy Commissioner has not made a health public interest direction for Health*elink* (which is the way exemptions from the privacy law for temporary trial/pilot projects are usually handled), we cannot be sure that the public interest in the *Healthelink* trial proceeding on an "opt out" basis outweighs the public interest in protecting privacy to the satisfaction of the Privacy Commissioner.

Background to EHRs: where NSW fits into the national picture

For some time a national program called HealthConnect was co-ordinating various projects around Australia, with the aim of introducing a national scheme of electronic health records.

A number of State and Territory trials have already commenced, and in some cases finished. The NSW Health*elink* trials are listed as HealthConnect trials.

HealthConnect trials are supposed to follow the HealthConnect model of consent, which states:

"Consent must be informed and voluntary, with participation in Health*Connect* for both consumers and providers to be on an 'opt-in' basis."

The HealthConnect work agenda has in some respects more recently been taken over by the National E-Health Transition Authority (NeHTA). Created in July 2005, NeHTA's role is to develop national health information management and information and communication technology standards and specifications.

NeHTA is jointly funded by Australian the States, Territories and Commonwealth Governments, and its governance ensures equal participation by all jurisdictions.

NeHTA is working on a number of initiatives, many of which are the necessary first steps towards a national electronic health records system – things like ensuring different IT systems are interoperable, that there is a system for identifying patients and clinicians accurately, and that everyone uses the same 'language' when describing medical conditions, medicines, etc.

One of NeHTA's projects is to develop a national model of E-Health Consent for the States and Territories to follow when implementing their systems. That model has not yet been finalised. A key question will be whether the model will basically follow an "opt in" or an "opt out" model of consent.

The NSW Health*elink* trials are therefore proceeding before this key consent has been determined by NeHTA.

About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about us see www.privacy.org.au