

Shared electronic health records systems: The significance of the privacy dimension.

Moira Paterson*

Many countries are in the process of implementing systems of shared electronic health records (SEHRs). This paper explores current developments and highlights the privacy concerns raised by those systems. Three areas of privacy concern relating to consent, disclosure limitation and access to records by third parties including health administrators, researchers and law enforcement agencies are examined. It is argued that, unless SEHRs are firmly grounded in identified policy and technological designs based on good privacy practice, they are likely to encounter resistance by both patients and medical practitioners and to be counterproductive to their objectives of improving healthcare outcomes.



Introduction

Currently in Australia health information is collected and stored locally in paper-based or electronic systems, with information about each individual held by a number of different entities in different information silos. This is obviously inefficient and potentially dangerous but it offers a measure of privacy protection in that an individual can control the extent to which a complete picture of his or her medical history is available to any person.

As noted by Terry and Francis,

EHRs are not like paper records writ larger. The differences for patient privacy and confidentiality and data security are matters of kind, not simply matters of degree. The irony is that the more inefficient a health records system, the more it is silo-based and makes interoperability difficult, the fewer confidentiality and security issues it will pose.¹

Part of the reason for this lies in the potential for silos to quarantine information which may result in stigma or discrimination such as information about treatments for sexually transmitted diseases. For example, there is evidence that 'psychiatric treatment is often paid for by patients out-of-pocket, precisely to avoid creating a record over which a patient has little or no control'.²

In February 2006 the Council of Australian Governments (COAG) agreed to 'accelerate work on a national electronic health records system to build the capacity for health providers, with their patients' consent, to communicate quickly and securely with other health providers across the hospital, community and primary medical settings'.³ The system which is envisaged will be what is commonly referred to as a shared electronic health record (SEHR) system based on the sharing of a common summary record separate from the records kept by individual practitioners. It differs from distributed systems which involve the one-to-one sharing of information by health providers.⁴

SEHR regimes have been advocated on the basis that they can make available to treating professionals a more complete medical history for each patient, thereby improving the overall quality of healthcare and facilitating a more holistic and integrated approach to the treatment of patients. They are also attractive to governments because of their potential to reduce the cost of healthcare budgets and to provide a more useful source of information for public health policy planning and medical research.

There are two key elements to the proposed new Australian system: first, the allocation of unique identifiers for the identification of patients and health providers⁵ and, second, a SEHR consisting of 'a longitudinal collection of key pieces of information that are most important to clinical decision making and ensuring high quality and better continuity of care'.⁶

Background

To date there have been two key bodies involved in the development of electronic health records in Australia: the Commonwealth Department of Health and Aging (via the *HealthConnect* project) and the National E-Health Transition Authority Ltd (NEHTA), a not-for-profit company established by Australian Health Ministers to develop national e-health standards and infrastructure requirements for the electronic collection and secure exchange of health information

HealthConnect had its origins in a report of the National Electronic Health Records Taskforce which recommended its creation to oversee a nationally coordinated and distributed network of SEHRs based on a common electronic health records architecture.⁷ Its key role was to develop a program for the practical implementation of a SEHR via a staged rollout, following trials in several states. Key initiatives in the states include the New South Wales Healthelink Electronic Health Record pilot⁸ and the development of a South Australian electronic planning and referral system for health consumers with chronic disease.⁹ In addition, the Northern Territory government has agreed to a framework to collaborate with the Commonwealth on the progressive implementation of HealthConnect across the Territory.¹⁰

Over time it has become clear that the actual implementation of the program (including procurement activities) will be carried out and substantially paid for by the states and territories and there has been a transition of most significant design activities relating to e-health to NEHTA.

NEHTA's primary role is to develop standards for adoption by the Australian, State and Territory Governments in their own e-health systems, with a view to creating the necessary foundations for the adoption of e-health developments, including SEHRs.

Healthcare providers and organisations will be able to contribute information to an individual's SEHR by keeping electronic records of patient interactions, and using software which is compatible with the SEHR Service(s). This software will allow healthcare providers to maintain their own detailed records, while ensuring that the most critical information can be easily included in the individual's SEHR, without the need for double data entry. Providers will also be able to see summarised views from the individual's SEHR.¹¹

NEHTA's work program for 2007 focuses on producing SEHR specifications and standards for adoption in the Australian health sector and defining requirements for a national approach to SEHRs.¹² It aims to ensure what it describes as a 'balanced outcome' which enhances quality of care while ensuring that privacy and other legal obligations are met and providing a solution that is both 'practical and pragmatic'.¹³ As a preliminary to the development of a Shared EHR Business Case for consideration by COAG in 2008 NEHTA has prepared a Shared EHR Privacy Blueprint (the Preliminary Privacy Blueprint)¹⁴ for targeted consultation via a Shared EHR Privacy Roundtable. The Roundtable comprised a group of privacy and related

experts, clinicians and consumer representatives and jurisdictional representatives with specific privacy expertise. That blueprint provides some clarification concerning the scope of the SEHR proposed by NEHTA although it is possible that this may alter in the light of the feedback received.

An issue that has created some uncertainty concerns the relationship between these initiatives and the proposed National Access Card regime. In an interview given in January 2007, NEHTA CEO, Ian Reinecke has stated that it is his understanding that the access card will operate quite separately from the healthcare identifier.

At this point there's really no place where the projects intersect. The access card is a Commonwealth initiative, the healthcare identifiers is pan-government, involving all states and territories.¹⁵

It would seem at this stage that the difference between the two initiatives is that the access card is about a citizen's relationship with the government, while the UHI is about an individual's relationship with a healthcare provider. However, that may change given that the Access Card proposal is itself still a work in progress.

Privacy and its significance

Information privacy is essentially concerned with an individual's ability to exercise control over the disclosure and use of their identifiable personal information.¹⁶ As described by the Victorian Law Reform Commission, it -

reflects the belief that individuals should be able to exercise control over their own lives and have some say in the extent to which other individuals, governments or corporations obtain access to information about them or intrude in their life in other ways.¹⁷

It is frequently confused with the duty not to misuse confidential (or secret) information (breach of which gives rise to right to sue). However, while the two concepts overlap, they are quite different from each other.

The determining factor in relation to the equitable duty not to misuse confidential (or secret) information is the acceptance of the information on the basis that it will be kept secret. That acceptance affects the conscience of the recipient of the information, thereby creating a fiduciary relationship.¹⁸ In contrast, the concept of privacy is grounded in the notion of a personal right to self-determination¹⁹ and respect for individual autonomy and integrity.²⁰

Privacy serves an important role in enabling people to formulate 'goals, values, conceptions of self, and principles of action' by providing them with a space where they are free to decide for themselves without having to give account to others.²¹ Furthermore, as noted by Gostin, 'intrinsic harms result from the mere fact of an unwanted or unjustified disclosure of personal information. Many moral views recognize the desirability of protecting individuals against the insult to dignity and the lack of respect for the person evidenced by such disclosures.'²²

However, privacy also serves a more utilitarian function not only in terms of protecting individuals from discrimination and stigmatisation but also in promoting better health outcomes. There are many studies which show that lack of privacy affects the willingness of patients to seek medical treatment and the extent to which they are prepared to be fully frank and open with treating professionals. For example, it has been established that confidentiality in consultations with their doctors is of prime importance to young people²³ and that some adolescents are reluctant to ask their doctors for advice about sensitive conditions because of anxieties about confidentiality.²⁴ Collins and Knowles, in a study of the views of adolescents and adults, found that participants expressed a strong desire for respect for their autonomy.²⁵ They also found that 98% considered that absolute confidentiality was either essential or at least important.²⁶ Likewise, it has been found that individuals receiving psychotherapy place a high value on the importance of confidentiality to the therapeutic relationship.²⁷

Research also shows that failure to reveal the limits of confidentiality seriously threatens the therapeutic relationship and the provider's credibility, potentially compromising treatment and leading the patient to terminate treatment prematurely.²⁸

While the sharing of health records may not amount to a breach of confidence in the legal sense, it may create similar responses. A study conducted in South Australia found that ordinary information sharing within treating teams may be an important source of misunderstandings between patients and health care providers.²⁹

The fact that they are designed for sharing (and not only amongst treating professionals but also with third parties, including healthcare administrators) and that they involve the use of web-based technologies means that SEHRs raise obvious privacy issues.

A submission by the Commonwealth Department of Health and Aging to the Australian Privacy Commissioner has commented in relation to HealthConnect that privacy and security issues had been consistently identified as a key building block for HealthConnect. It further states that ‘unless consumers and providers have confidence in the way that their personal health information is handled, they may well choose not to participate in such initiatives’ or ‘may not seek the health care they need which may in turn increase the risks to their own health and the health of others’.³⁰

Likewise, NEHTA’s Preliminary Privacy Blueprint acknowledges that privacy is fundamental for community acceptance of the project. NEHTA’s *Approach to Privacy* identifies six privacy tenets which are intended to guide its work program.³¹ These include a commitment to privacy as the starting point of initiatives involving the collection and handling of personal information and individual participation by maximising individuals’ control over the collection and handling of their personal health information

The General Legal Context

The extent of privacy protection available in respect of an SEHR will be affected by the nature of any privacy-related provisions in the legislation which creates the necessary legal infrastructure for its operation. For example, such legislation might impose requirements concerning audit trails, criminal sanctions for unlawful access or disclosure and so forth. However, it is likely that most legal aspects will be determined by the legal framework which regulates personal health information more generally.

Relevant laws include information privacy and health records laws and provisions in statutes which prohibit disclosure (including imposing sanctions for unlawful disclosure) and provisions which authorise or mandate the disclosure of information in specific circumstances (for example, provisions which mandate reporting of specific diseases or authorise access by law enforcement bodies).

Information privacy/health records laws are based on sets of principles which regulate the collection, use, storage and disclosure of identifiable information as well as conferring rights of access and amendment. Problematically from the perspective of the implementation of a nation-wide SEHR, they do not operate uniformly across

all sectors and jurisdictions, are incomplete in their coverage and to some extent overlap with each other.

At present the national privacy provisions (NPPs) of the federal *Privacy Act 1988* (Cth) do not distinguish between health information and other types of personal information although they are given enhanced protection under specific NPPs as a species of 'sensitive information'. Private sector health records are generally protected by the private sector provisions in the *Privacy Act 1988* (Cth). Public health sector records are protected under the public sector provisions in the *Privacy Act 1988* (Cth),³² the *Information Act 2002* (NT), *Personal Information Protection Act 2004* (Tas) and under sui generis health records laws in Victoria, New South Wales and the ACT.³³ The latter also protect private records, thereby creating dual protection for private sector health records in those jurisdictions. States other than New South Wales, Tasmania and Victoria do not have either public sector privacy laws or sui generis health records laws.³⁴

In an attempt to remedy this situation a Privacy Working Group appointed by the Australian Health Ministers' Advisory Council has developed a draft *National Health Privacy Code* based on a set of National Health Privacy Principles (NHPPs). It would seem that, while much of the content of the draft Code has apparently been finalised, it is yet to be formally endorsed at ministerial level.³⁵ Furthermore, it remains unclear how the Code might be implemented. Options discussed by the ALRC, in its recent Privacy Issues Paper, include the enactment of national legislation and cooperative regimes based on a referral of power by the states to the Australian Parliament, the enactment of mirror legislation or applied legislation, where one jurisdiction passes legislation which is then applied by the other jurisdictions as a law of those jurisdictions.³⁶

Privacy-protective system design features

Arguably, if patients are to be able to exercise meaningful control over their information, they should have some say in whether or not it is collected in the first place and also as to the ways in which it is subsequently used and disclosed.

The Preliminary Privacy Blueprint suggests a number of mechanisms which should go some way to achieving a measure of patient control.³⁷ However, while it seems clear that the any SEHR will be made available on a voluntary basis and that patients

will have some elements of control, the precise details still remain to be finalised and are in any case subject to approval by COAG.

Voluntary participation

The most basic and fundamental mechanism is one ensuring that participation in an SEHR is voluntary (and that people may choose to cease to participate if they do decide to register). However, this raises the vexed issue of opt-in versus opt-out.

It would seem from its Preliminary Privacy Blueprint that NEHTA remains committed to an opt in model (as well as an option to opt out once in). This is very important from a privacy perspective as it ensures that participation results from an act of informed volition rather than a default. As explained by the Australian Privacy Foundation -

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 in 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.³⁸

However, there is a perception that it is easier both technically and administratively to provide for opt-out. This was illustrated in the case of the recent *Healthelink* trials in New South Wales where a late decision to use an opt-out model was justified in Parliament by the Minister for Health on the basis that; 'research on international experience in the United Kingdom and Canada identified significant problems with the use of an opt-in model'.³⁹

It is to be hoped that similar concerns do not bring about a last minute rethink on the part of NEHTA or COAG.

Non-reporting restricted views and masking

Other features which enhance patient privacy by giving them control over their information can include an option not to record specific events in the summary electronic record or to restrict what information can be seen by specific treating professionals. The latter can be achieved either by tailoring views so that each

category of user is able to see only an edited version of the summary on a need to know basis or by giving patients the option of masking more sensitive data.

Evaluation

Factors which may be relevant in assessing the pros and cons of each of these features include the extent to which it detracts from the collection of a complete set of summaries and therefore from the overall efficiencies which the SEHR is designed to achieve, the extent to which it exposes patients to additional dangers in the event of function creep and the extent to which, and the form in which, the summary record is subject to compulsory disclosure to other users.

Non-reporting provides for flexible way in which to achieve meaningful control over the collection of data and is also likely to increase the chances that individuals will be willing to opt in to a SEHR scheme. However, it creates practical difficulties in terms of its administration because of the need to ensure that patients understand the risks of non-reporting and are able to make an informed choice. In addition, it potentially undermines the usefulness of the SEHR from the perspective of researchers and other secondary users such as health administrators.

A system of restricted views provides for a more nuanced form of control by restricting the parts of the record that can be viewed by different health providers. It can address the concern frequently expressed that patients may not wish an ancillary health provider (such as a podiatrist, for example) to access sensitive information that is not relevant to the services provided by them. However, that approach may be at odds with the new emphasis on multi-disciplinary treatment teams and there are practical difficulties in determining precisely which categories are relevant to different classes of providers. Furthermore, patients need to understand that restricted views are unlikely to be applicable in respect of secondary users.

A related, but alternative, approach is to allow for the masking of more sensitive items of information. According to how the system is set up that data would be viewable only on a 'need to know' basis with the express consent of the patient or, alternatively, by pre-nominated practitioners. To the extent that masking is available, it may both increase the willingness of patients to opt into the system and reduce the extent of non-reporting. However, the ability to mask information is more difficult to achieve in a technical sense, although this task can be made simpler by providing predetermined categories which can be specified in advance. In addition, as with

restricted view, masking may be of limited value if it restricts access by other health providers but not (in a deidentified form) by secondary users.

One specific scenario which is likely to create particular difficulty is where the patient is currently receiving medication for an illness or disorder that they would like to be kept secret. In some cases the fact that they are on specific medication may be sufficient to reveal the nature of their illness or disorder. However failure to make this information available to other health providers may present difficulties in terms of the need to avoid adverse drug interactions.

An different, and arguably more controversial approach,⁴⁰ which has been suggested by Terry but was not posited in the Preliminary Privacy Blueprint would permit patients to access their records and remove or request removal of specific data, or to place restrictions on its dissemination. As he notes, this has the –

disadvantage for patient care that patients may use idiosyncratic judgment in securing records, but the concomitant advantage that patients will be able to exercise individualized preferences in this regard.⁴¹

Further privacy issues

It is important to bear in mind that the information on the shared electronic health record, although summary in nature, may be more extensive and more sensitive than the other information that might have been stored within the practitioner's record system in the absence an SEHR and the fact that the consequences of its disclosure may therefore be more serious for the patient. Take, for example, information about a mental illness or a sexually transmitted disease which migrates onto a practitioner's system or onto a hospital system where it may potentially be accessible by a range of persons (including administrative staff).

In addition, aggregated information of the type accumulated on a SEHR creates a rich mine of information for a range of third parties, including secondary users (such as health administrators and researchers) and law enforcement/national security agencies. In the context of the United States, Gostin comments that:

Advocates have long recognized that the most serious threats to privacy come from authorized users of health information. Providing a reasonable measure of privacy for the individual requires, at the very least, some control over the number of individuals that have access to health information. Once

large numbers of individuals and organizations have access to sensitive and often highly valuable information, it becomes difficult to prevent uses that stigmatize or harm the subjects of those data.⁴²

There are of course already laws and procedures in place which provide for disclosure of identifiable health information to a wide range of users.⁴³ These include procedures authorising flows of patient data to insurers for payment and monitoring functions and from insurers to government and professional agencies.⁴⁴ What is important is to ensure that the introduction of a SEHR does not result an expansion of the amount of data available.

There is also an issue concerning the more extensive pool of information which will potentially be accessible by third parties such as employers who are in a position to require a patient to give consent to access or even to require them to obtain access to, and make available, a copy of their health record.

A final broader issue relates to the threat of function creep. Once the system is in place and there is an increased awareness of the potential value of the store of information within it, there will be an inevitable pressure to make that information available for new uses and also to alter the system in ways which increase its efficiency. Magnusson suggests that: "The factors motivating the massive investment in health informatics, 'population health' and associated 'secondary use' claims are almost certainly likely to water down the level of 'individualised' control individual patients may wish to exercise over the distribution of their health data'.⁴⁵ He also points to a wider long term trend in which the regulation of medical privacy 'goes beyond the allocation of rights and responsibilities within private therapeutic relationship and *enhances the power of the state* as the broker for information flows within health care settings'.⁴⁶

Concerns about future function creep are partially addressed by the inclusion of an option to cease to participate. However, there is a possibility that future governments may be pressured to make the exercise of that option unattractive, or to remove it altogether. That may also be the case with any option for non-reporting of events. Arguably therefore what is called for is some mechanism which requires Parliamentary debate and approval for any extension of existing uses or weakening of existing privacy safeguards and for ensuring that any such changes are notified to patients.

Conclusion

In conclusion, finding appropriate and workable privacy solutions for SEHRs is important if they are to achieve their promised benefits without undermining the relationship between patient and health provider. This presents a very difficult dilemma. Part of the justification for the substantial monetary investment that they require is based on their potential to produce efficiencies resulting from the integration of records. However, they pose substantial privacy risks which can best be addressed by measures which reduce their overall efficiency. Arguably finding an appropriate balance requires placing an appropriate emphasis on the objective of improving healthcare outcomes rather than on broader efficiency objectives.

* Associate Professor, Faculty of Law, Monash University.

Presented at the Fifth Greek Conference, *Challenges in Law, Medicine and Science*, Kos, Greece – 15 to 21 September 2007.

- 1 N Terry and L P Francis, 'Ensuring the Privacy and Confidentiality of Electronic Health Records' (2007) *University of Illinois Law Review* 681, 700.
- 2 S Alpert, 'Health care information: Access, confidentiality, and good practice'. in K W Goodman (ed), *Ethics, computing, and medicine: Informatics and the transformation of health care* (1998) 89.
- 3 See <http://www.coag.gov.au/meetings/100206/index.htm#health>. It was agreed that the Commonwealth would contribute \$65 million and the States and Territories \$65 million in the period to 30 June 2009.
- 4 For example, the New Zealand Ministry of Health's Health Information Strategy is based on developing a distributed electronic health records system linked by a nationwide, secure broadband network rather than creating a centralized system: see #.
- 5 For details concerning the Individual Healthcare Identifier (IHI) and Healthcare Provider Identifier (HPI) see http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=153&Itemid=139
- 6 Based on NEHTA's Preliminary Shared EHR Privacy Blueprint it would seem that the SEHR currently envisaged will include a shared health profile at its centre, containing information about allergies, alerts and adverse reactions, current medications and problems and diagnosis.
- 7 The National Electronic Health Records Taskforce, *A Health Information Network for Australia*, Taskforce Report, Commonwealth Department of Health and Aged Care (2000).
- 8 See <http://www.healthlink.nsw.gov.au/>.
- 9 HealthConnect South Australia, *HealthConnect South Australia: Health Information When You Need It* (2007) www.healthconnectsa.org.au/.
- 10 See <http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/nt-11p>.
- 11 NEHTA, *Fact Sheet: A National Approach to Sharing Health Information* accessed at http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=130&Itemid=139.
- 12 NEHTA, *Fact Sheet: A National Approach to Sharing Health Information* accessed at http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=130&Itemid=139.
- 13 NEHTA, *Paths to Benefits: NEHTA's approach to modelling the benefits of investment in national e-health infrastructure* (2006) 17 accessed at http://www.nehta.gov.au/index.php?option=com_docman&task=doc_download&gid=110&Itemid=139

14 I had access to this document via my participation at the Privacy Roundtable and have
 permission to discuss some aspects of it in this paper. NEHTA envisages publishing a revised
 Shared EHR Privacy Blueprint in 2008 for public consultation purposes.

15 K Dearne, 'Doing the numbers on e-health' *Australian IT*, 20 August 2007 accessed at
<http://www.australianit.news.com.au/story/0,24897,21124569-24172,00.html>.

16 See, for example, C Fried, 'Privacy' (1968) 77 *Yale Law Journal* 475, 482.

17 VLRC, *Privacy Law: Options for Reform* (2001) 3-4 accessed at
[http://www.lawreform.vic.gov.au/CA256902000FE154/Lookup/Privacy/\\$file/Information_Paper.pdf](http://www.lawreform.vic.gov.au/CA256902000FE154/Lookup/Privacy/$file/Information_Paper.pdf).

18 *Stephens v Avery* [1988] 2 All ER 477, 482.

19 See D Mendelson, 'Travels of a Medical Record and the Myth of Privacy' (2003) 11 (2)
Journal of Law and Medicine 136.

20 See Australian Law Reform Commission, *Privacy* (1983) [1032].

21 H Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 101, 131.

22 L O. Gostin, 'Health Information Privacy' (1995) 80 *Cornell Law Review* 451, 490.

23 For example, see J S Thral, L McCloskey, S L Ettner et al. 'Confidentiality and adolescents'
 use of providers for health information and for pelvic examinations' *Archives of Pediatrics &*
Adolescent Medicine 2000;154:885-92; G Scally, 'Confidentiality, contraception and young
 people' (1993) 307 *British Medical Journal* 1157-8.

24 T L Cheng, J A Savageau, A L Sattler et al, 'Confidentiality in health care. A survey of
 knowledge, perceptions, and attitudes among high school students' (1993) 269 *Journal of the*
American Medical Association 1404-7.

25 N Collins and A D Knowles, 'Adolescents' Attitudes Towards Confidentiality Between the
 School Counsellor and the Adolescent Client' (1995) 30 *Australian Psychologist* 179, 182.

26 Ibid 181.

27 See J M McGuire, P Toal and B Blaux, 'The adult client's conception of confidentiality in the
 therapeutic relationship' (1998) 16 *Professional Psychology, Research and Practice*, 375-384

28 T G Kremer and E L Gesten, 'Confidentiality limits of managed care and clients' willingness
 to disclose' (1998) 29 *Professional Psychology, Research and Practice* 553-558.

29 See M Paterson and E Mulligan, 'Disclosing Health Information Breaches of Confidence,
 Privacy and the Notion of the 'Treating Team'' (2003) 10 *Journal of Law and Medicine* 460.

See also E Mulligan and M Paterson, 'Breaches of Confidence were infrequent but some
 patients were offended by Routine Information Exchanges in a
 Commonwealth Government Department of Health and Ageing, *Submission to the Review of*
the Private Sector Provisions of the Privacy Act 1988 accessed at
<http://www.privacy.gov.au/act/review/revsub99.doc>.

31 NEHTA, *Approach to Privacy* (2006) 5 accessed at
http://www.nehta.gov.au/index.php?option=com_docman&task=doc_download&gid=88&Itemid=139

32 These treat health information in same way as other types of personal information.

33 The Health Records Act 2001 (Vic), the Health Information Privacy Act 2002 (NSW) and the
 Health Records (Privacy and Access) Act 1997 (ACT).

34 Public bodies in Queensland, South Australia and Tasmania are, however, subject to the
 operation of administratively imposed privacy rules: see
<http://www.justice.qld.gov.au/dept/privacy.htm>,
<http://www.archives.sa.gov.au/privacy/index.html> and
<http://www.justice.tas.gov.au/legpol/privacy/index.htm> accessed on 21 April 2005. See also
 Information Privacy Bill 2007 (WA).

35 See ALRC, Issues Paper 31, *Review of Privacy* (2006) [8.42].

36 See [8.43] - [8.54].

37 For a more extensive discussion these features in the context of the HealthConnect model see;
 M Paterson, 'HealthConnect and privacy: A policy conundrum' (2004) 12 *Journal of Law and*
Medicine 80.

38 Australian Privacy Foundation, *NSW Health E Link: NSW trials of electronic health record*
 (2007) accessed at http://www.privacy.org.au/Campaigns/E_Health_Record/HealthElink.html.

39 NSW, Legislative Council Hansard, 29 March 2006, *Debate on Disallowance of Health*
Records and Information Privacy Regulation accessed at
<http://parliament.nsw.gov.au/prod/parliament/hansart.nsf/5f584b237987507aca256d09008051f3>

[/8bb294064d9c5e32ca25714c000ecedf!OpenDocument](#). It should be noted that Canada has not chosen to adopt an 'opt out' model.

40 The approach is controversial because it raises considerable safety issues and undermines the integrity of the record.

41 N Terry and L P Francis, 'Ensuring the Privacy And Confidentiality of Electronic Health Records' (2007) *University of Illinois Law Review* 681, 728.

42 L O. Gostin , 'Health Information Privacy' (1995) 80 *Cornell Law Review* 451,485.

43 See D Mendelson, 'Travels of a Medical Record and. the Myth of Privacy' (2003) 11 *Journal of Law and Medicine* 136.

44 See for example the National Health Act 1953 (Cth) ss 73AB (disclosure of data to the Commonwealth Health Department and the Private Health Insurance Administrative Council) and s 73BD(2).(disclosure to health funds) as discussed in R S Magnusson, 'Privacy: The Changing Legal and Conceptual Shape of Health Care Privacy' (2004) 32 *Journal of Law, Medicine and Ethics* 680, 684. See also D. Mendelson, 'Health Legislation (Private Insurance Reform) Amendments Act 1995 (Cth) and the Question of Medical Confidentiality: the Money or the Ethics?' (1996) 4 *Journal of Law and Medicine* 101.

45 R S Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review*. 5, 52.

46 R S Magnusson, 'Privacy: The Changing Legal and Conceptual Shape of Health Care Privacy' (2004) 32 *Journal of Law, Medicine and Ethics* 680.