Beyond the Tomb: Privacy, confidentiality, and long-term preservation of and access to electronic health records in national systems – a case study of Australia's Health*Connect* project*

Livia Iacovino

Dr Livia Iacovino is an Honorary Senior Research Fellow in the Centre for Organisational and Social Informatics and the Records Continuum Research Group, in the Faculty of Information Technology, Monash University. She has taught in the recordkeeping courses of the Faculty, and developed the legal and ethical curricula. Her research is focused on interdisciplinary perspectives of archival science, law and ethics; in particular ownership, access and privacy of networked electronic records. She has been a Chief Investigator, for *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework,* an Australian Research Council Discovery Grant (2002-05), together with the Faculty of Law, Monash University and the School of Law, Deakin University. Livia's awards include the Australian Society of Archivists' *Mander Jones Award* 1999, and the Monash University Mollie Holman Medal of Excellence 2003 for her PhD thesis published in 2006 as *Recordkeeping, Ethics and Law: Regulatory Models, Participant Relationships and Rights and Responsibilities in the Online World.*

***

National electronic health record systems such as Australia's Health*Connect* are designed to capture every encounter with the health system and to keep records for the life and beyond of the patient. This paper considers the extent to which the 2004-05 Health*Connect* model for secondary uses of identifiable as well as de-identified health data would

have satisfied the patient's and his or her descendents' requirements for long-term privacy and confidentiality within the framework of privacy and archival law. It also identifies the difficulties of managing long-term access to electronic health records held in multi-layered distributed systems such as the one proposed for Health*Connect*. Finally, it makes a number of recommendations necessary for such systems to ensure long-term confidentiality, privacy, and accessibility.

Introduction

National electronic health record systems such as Australia's Health*Connect* have been designed to collect key information about a specific health care event, whether it is a visit to a general practitioner or a hospital admission, and to be retained over and beyond an individual's lifetime. Whilst these systems offer enormous potential for large-scale research into health issues both actual and preventative, there needs to be a fine balance between the usage of the data for its original purpose with unlimited secondary uses to which the patient has not explicitly consented. Privacy infringements may occur when personal information from many systems is electronically linked to one person via a unique personal identifier and made available to a range of third parties. The federal government's proposal for a national social benefits access smart card which will include emergency health data raises many similar privacy and confidentiality concerns as those illustrated by the analysis of Health*Connect*. Despite the fact that Health*Connect* will not proceed in the form originally envisaged, it provides a valuable case study of the potential difficulties in preserving records held in distributed systems over long periods, and of re-assuring patients and providers that their health and other personal data will not be monitored by government, employers and insurers without their consent.

Shared health information systems

'Sharing' or exchanging of patient health information electronically has been driven by a number of factors, the most important being changes in healthcare policy focused on patient safety and healthcare delivery methods, as well as health economics and technology.[1] Health informatics specialists claim that technically all healthcare information can be shared if computing infrastructure is shared. The impediments are said to be 'only cultural and political'.[2] Privacy and confidentiality

are seen as 'barriers' to powerful technological and economic arguments for shared health record systems. However, medical confidentiality remains essential to a patient's openness with his or her health practitioner. Openness may be jeopardised if the patient is made aware that the information imparted to his or her practitioner is shared with third parties without his or her consent.

The development of the 'electronic health record' (EHR) has occurred within what is termed the 'health information domain' or 'health infostructure', a business model which places the health record in the context of relevant stakeholders, health technologies and health standards.[3] Yet these and other health informatics standards initiatives have failed to address many recordkeeping issues including the requirement to preserve not only the EHR as an information entity, but also its metadata stored in many diverse parts of the system such as the one envisaged for Health*Connect*.

Health*Connect*: an Australian shared health record system

Health*Connect* has been a complex cross-jurisdictional project between the Australian federal, state and territory governments originally established to oversee a nationally coordinated and distributed network of electronic health records.[4] The shared funding and governance arrangements have been due to the Commonwealth's limited constitutional power over the practice of medicine and thus its requirement to work with the cooperation of the states which run public medical services and set the standards for private practitioners.[5] In early 2005 Health*Connect* was set to move from its research and development phase to a proposed state-by-state implementation phase, in some cases building on top of state EHR projects as well phasing in the national medication record module of the system (Medi*Connect*).[6] By mid 2005[7] it began to move away from this plan and in early 2006 its initiatives were absorbed by the National E-Health Transition Authority (NEHTA), a not-for-profit company that has effectively become the major driver in the government's electronic health record systems.[8] NEHTA is aligned closely with state and territory electronic health record projects.[9]

Central to the Health*Connect* system has been the requirement for nationally maintained patient and healthcare provider identifiers, which have privacy implications in terms of linkages to other health data and

other government identifiers. Unique patient identifiers remain part of NEHTA's agenda.[10] Although a voluntary 'opt-in' rather than an 'opt-out' system for both the patient and healthcare provider, Health*Connect* identification would have been triggered through the national health insurance smart card of all Australians, therefore everyone would by default have been registered once the smart card became operational.[11] Records would be kept indefinitely, even if one elected to opt-out or died, and would remain available for research indefinitely. As its data principles stated: 'Health*Connect* will be a repository service for consumers' lifetime health records'.[12] As research purposes were primary objectives of the system, the regulatory framework would have had to be able to protect personal health records of long-term research value. A national repository of personal health records can provide valuable research data in de-identified form and the identifiable data over time will lose most of its sensitivity. This latter aspect has depended on a robust government archival legislative and procedural framework to protect identifiable health records of long-term value for at least one hundred years. However for Health*Connect*'s records there has been a question as to which legislation and common law remedies apply.[13]

The HealthConnect record

The Health*Connect* record was designed to capture an event summary at the time of the health event (for example, in a hospital or a general practitioner's surgery) from a pre-determined set of patient health data to be uploaded by a participating health provider (an individual or an organisation as defined by the project) at the point of care. Event summaries would form part of a series of event summaries pertaining to a uniquely identified patient who had consented to participate in the system. These summaries would not replace providers' clinical records, although they could be incorporated with them. They would be stored in identified form in a Health Record System (HRS) to which a participating patient had been assigned, and subject to consent arrangements, made available to participating health service providers on the patient's access control list. They would also be copied and stored in a National Data Store (NDS), in clinical systems (at the discretion of the healthcare practitioner) and in the patient's own records (at the discretion of the patient). Event summaries in the form of reports would be made available in de-identified form to authorised third parties, including researchers and health administrators from the NDS. Identifiable data would also be

available subject to a set of access requirements, but no policy decision had been made on which secondary purposes would be authorised.

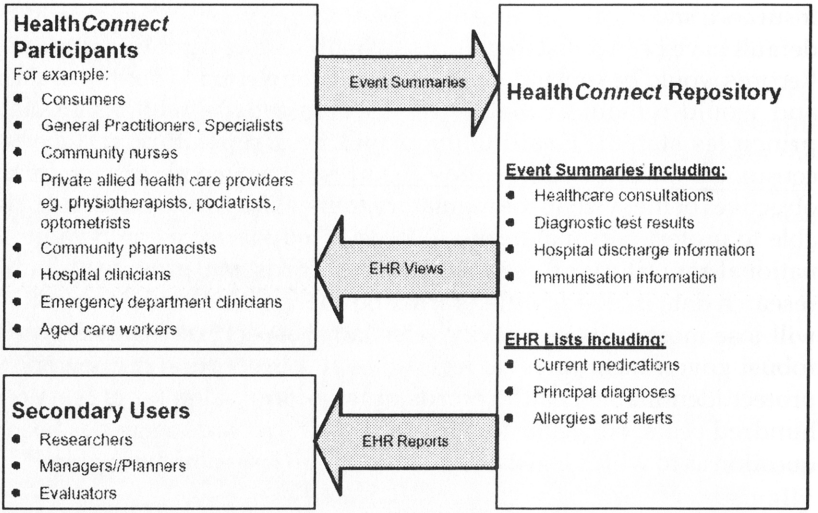

Figure 1. Key Components of HealthConnect[14]

HealthConnect participants were to be grouped either as primary users (providers and consumers/patients) or secondary users (researchers, planners, managers and evaluators). Significantly, secondary uses were subsumed into the primary purposes of the project's objectives. On the one hand the model appeared to provide patients with control over the providers who could see their record, and even the ability to contribute to their record, while on the other hand, depriving them of control over who saw their data in either de-identified or identified form for secondary research purposes. Detailed secondary use mechanisms had been left to the implementation stage.

HealthConnect system architecture

HealthConnect has had a complex system architecture which evolved over three years. The technical architecture envisaged for HealthConnect

consisted of a set of third party hosted Health Records Systems operating as a national network. Each HRS would hold and manage the shared electronic health record (EHR) for a patient registered in that system. Records would have been created by processes at three levels of the architecture – the national coordination layer, the HRS layer and the user layer – and the interactions between these levels.

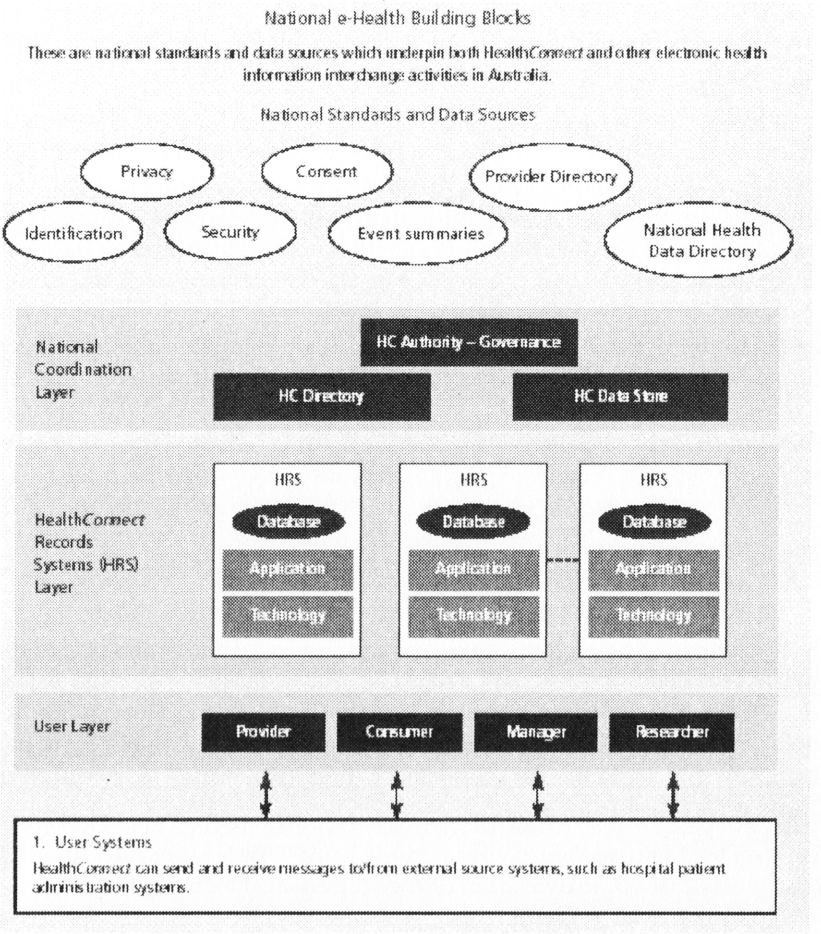

Figure 2. Components of National e-Health Building Blocks[15]

The National Coordination Layer incorporated the maintenance of the National Data Store (NDS), provider and consumer directories, access portals for consumers and providers, and maintenance of a national Health*Connect* metadata repository, and most importantly, it managed secondary access to Health*Connect* records.[16] The HRS performed the functions of EHR storage, update and access control, including keeping audit trails and access logs and recording all access, outputs and changes involving consumer/patient information held in the HRS.[17] Less formalised requirements in the business architecture were to be defined for the user layer. It included automatic transmission of event summaries to providers, and the records of these processes.

As a result of this architecture, identifiable data would be stored in various parts of the system - in registration records and indexes, audit logs, provider and consumer directories and in individual transactions - not all of which would need to be retained permanently as proposed by Health*Connect*. Records retention would have had to address a patient's record from the perspective of her or his encounters with the whole Australian healthcare system, as well as at the provider level. Management of records in the various layers of system had not been adequately included in the Health*Connect* system requirements.

Long-term retention: preservation issues

> The EHR data will be permanently recorded and preserved subject to legal constraints. Upon a consumer's death, processes will be put in place to limit access to those with a need, eg for activities in relation to death certificate issue, autopsy or coroner investigation and for secondary uses.[18]

If, as envisaged by Health*Connect*, the EHR is retained for the life of the patient and beyond, it must be readable and accessible over successive data formats. The necessity to put into place backward compatibility and other measures for the system to preserve records can be found in a number of Health*Connect's* 2004 technology principles. A selection of these principles include:

> The Health*Connect* data model must be extensible to accommodate evolution of the content and format of EHR information over time.[19]

> HealthConnect data structure, systems and processes must be designed to maintain backward compatibility and integrity of the stored data so that information may be reproduced through time.[20]
>
> Within 24 hours of an EHR being updated (and preferably much earlier), a copy of the updated EHR material is to be transmitted in a standard format by the responsible HRS/AEM to the National Data Store for archiving and long-term retention. Together, the EHR information held in each HRS and the National Data Store comprise the HealthConnect EHR repository.[21]

There are a number of factors that would have affected the implementation of these principles. Firstly, the EHR is a not a physical record, but is only brought together logically by software applications. Secondly, preservation of all its metadata would be very complex as they would exist in many parts of the system, and thirdly, the lack of a clear governance structure would make it difficult to have a responsible person in charge of its preservation.

Shared networked health records, in which there are multiple record creating agents, and which reside in many systems, require managerial and technological intervention to preserve their integrity and confidentiality. In relation to HealthConnect, the process of identification of the information entities or data that is created, used and amended in the different processes, and where the information resides and who is responsible, had been difficult to track.[22] The challenge of maintaining technology-dependent electronic records for long periods was recognised only briefly in the statement 'the very scale of HealthConnect represents a significant challenge to its ability to acquire, configure and manage underlying processing technologies for the long term'.[23] The 2004 business specification did specify the need to maintain an appropriate set of metadata templates reflecting changes over the life of the system encompassing emerging changes to structures, requirements for backwards and forwards compatibility, requirements to enable time-bound version controls and changes to supporting terminologies over time.[24] Although there was a gradual incorporation of a long-term preservation perspective into the HealthConnect business requirements, a lack of attention to overall recordkeeping requirements would have

compromised the authenticity, reliability and integrity of the HealthConnect system.[25]

In Australia, retention and disposal of personal information has been managed through archival legislation, although over the past few decades this has been made more complex with the introduction of general privacy and health-specific privacy legislation mandating destruction or de-identification of personal information once the purposes for which it was collected have passed. If the de-identification process is permanent it impinges on record authenticity.[26] Recordkeeping authenticity involves the ability to reconstruct the record and includes preservation of its recordkeeping metadata including personal identification details, controls on record creation, transmission and storage. It is critical that metadata needed for a record's identity remains persistently linked with the record to which it relates.

HealthConnect's blanket retention policy also raised the issue as to which legislation would be appropriate to control such long-term preservation. The Commonwealth, and therefore the National Archives of Australia would most likely have had responsibility for the HealthConnect records in the national data store and for access arrangements for personal health information over thirty years old.

Health privacy and confidentiality issues in HealthConnect

Confidentiality is a legal duty whereby those who agree to receive information on the basis that it will be kept secret, come under the obligation of confidentiality. The concept of confidentiality is already strained in relation to health records generally and has been further eroded through legislative exceptions such as mandatory reporting of diseases.[27]

In the medical context, the duty of confidence is imposed on the medical practitioner, but in HealthConnect would any form of confidential duty exist and on whom? The legal consultants to HealthConnect argued that:

> While it may be possible to infer an implied licence to use confidential information supplied to the HealthConnect database for purposes related to the treatment of a patient, in our view, given the nature of the information being disclosed, it would not be safe to rely on implied licences or

> technical legal arguments to defeat a claim that confidentiality has been breached. Instead, it is anticipated that providers and consumers who elect to join Health*Connect* will, as a condition of joining, give such authorisation.[28]

Confidentiality in a system like Health*Connect*, which would require a medical practitioner to release confidential data not only to other practitioners but also to health administrators and researchers as part of the condition of joining the system, effectively destroys the patient's right to confidentiality. In addition, the government could simply legislate to disclose Health*Connect* data to authorised users. Health*Connect* most likely would have spelt the death knell for medical confidentiality, except in very limited circumstances.

Unlike confidentiality, which is concerned with the disclosure of information, privacy is concerned primarily with an individual's ability to exercise control over his or her own identifiable personal data. International conventions on human rights, case law and privacy legislation in many countries recognise the special sensitivity of health information and classes within.[29] Shared health records systems by their nature lead to an increased demand for third party access.[30] Identifiable health information, if it is disclosed inadvertently can result in distress and embarrassment, social stigma and discriminatory decisions, and requires the data subject's explicit consent to its release to a third party.[31]

Access to a Health*Connect* record would have been available to the patient, to healthcare practitioners or organisations to whom the patient had given consent via an access control list and other authorised secondary participants for 'approved secondary uses' subject to Health*Connect* rules to which the patient had *not* given consent. As Barbara Reed has stated:

> It transfers a significant degree of control over use of personal and personally identified health information away from the explicit control of the consumer, onto the body responsible for assuring 'approved secondary uses'. However, this type of transfer of responsibility is against the spirit of the privacy protections now enshrined in legislation and similarly in contrast to the encouragement of individuals to take more active role in the management of their personal health information.[32]

Patient privacy requires that only those who are authorised to do so can access and add to a patient's record and that any unauthorised access is tracked and recorded.[33] Concerns over access to sensitive personal information had driven the HealthConnect requirement for an audit trail associated with the individual EHR (presumably the cumulative resource consisting of event summaries, views, lists and access control lists linked to a single unique identifier), providing a record of all accesses to the specific material linked to the unique health identifier. Although an access log was to be maintained of all access to the NDS there did not appear to be a patient right to view secondary users or uses of their EHR from within the NDS, as opposed to the right to view access logs in the HRS.[34] Given the breadth of secondary users, this was a significant gap in patient access and privacy rights.

A major issue has been that Australian privacy law does not operate uniformly across all sectors and jurisdictions.[35] To overcome this lack of consistency, it was envisaged that the implementation of HealthConnect would be preceded by the development of a set of National Health Privacy Principles embodied in the National Health Privacy Code (NHPC).[36] HealthConnect's legal consultants recommended that even if the Code was implemented there should be separate HealthConnect legislation to accommodate privacy and access rules for the whole system.[37] This would most likely have diminished existing privacy rights as the enactment of HealthConnect-specific legislation would have expanded cases in which personal information could be collected, used and disclosed. In addition, if privacy regimes in Australia and the states in particular were amended to comply with the NHPC, privacy rights would have been significantly diminished. Until the NHPC was in place, privacy arrangements were to be tailored to each jurisdiction for each implementation,[38] resulting in uneven privacy protection in relation to HealthConnect's records.

HealthConnect also intended to rely on participating providers entering into a legal agreement which included abiding by specific HealthConnect privacy protocols, covering access, contribution to and use of information from HealthConnect records,[39] leaving individual organisations responsible for ensuring the compliance of staff of the organisation with these privacy provisions.[40] This left the patient subject to the procedures of individual organisations, particularly if the HealthConnect record was brought into the organisation's own records system, as had been anticipated.[41]

Unique identifiers and privacy

> Each consumer and their EHR information will be uniquely identified within Health*Connect* by use of a single unique identifier able to be linked to any future National Health Identifier.[42]

To implement a national EHR system across different jurisdictions, there is a requirement for unique identification of patients and healthcare providers. This is needed to ensure that all event summaries are appropriately linked to the correct EHR. The smart card initiative within the Medicare domain and more recently the social benefits access card had already raised concerns for privacy advocates.[43] Control of the identifiers would have been at the national level but the nature of the national organisation had not been resolved.[44] Therefore legal ownership and responsibilities for protecting identifiers could not be established. Nor would the National Health Privacy Code have provided sufficient controls over the use of identifiers. Unlike HPP 15 of the *Health Records and Information Privacy Act 2002* (NSW) which specifically requires an individual's express consent to the use of his or her identifier for record linkages, NHPP 7 of the NHPC, as well as NPP 7 of the *Privacy Act 1988* (Cth) which cover identifiers, do not contain provisions dealing expressly with the sharing of records. There is a need to include in all health privacy legislation a requirement for the data subject's explicit consent to the linking of his or her health data through the use of unique identifiers.

Private sector

The proposed outsourcing to the private sector not only of operational functions such as registration, identification and access services for patients and providers, but in some instances also the running of the HRS, would have caused major privacy, confidentiality and legal liability issues for Health*Connect*.[45] Moreover, there was no guarantee that the processing of the Health*Connect* data would not be outsourced to overseas subcontractors.[46] Given the role of the private sector in Health*Connect*, one of the essential issues would have been the adequacy of legislation to regulate the activities of contractors delivering aspects of Health*Connect* functionality. 'Contracted service providers' to Commonwealth and state agencies are bound by the public sector Information Privacy Principles of the Commonwealth or state equivalent laws, and are also required to comply with the National Privacy Principles (NPPs) where there is no

clause in the contract corresponding to the NPPs (or relevant approved code, whichever is applicable).[47] This means that government agencies continue to have contractual remedies against a contractor who breaches a privacy clause in a contract, but not necessarily against the subcontractor. When contracting offshore, agencies may not be able to enforce the provisions of the contract.[48] The added layers of contractors and subcontractors would have complicated the investigation of privacy breaches.

Secondary uses: The HealthConnect model

While privacy and data protection law is concerned with secondary uses of personal information that refers to 'any information relating to an identified or identifiable individual (data subject)',[49] HealthConnect's secondary uses included both identifiable and de-identified personal information. Secondary users who accessed HealthConnect for purposes other than direct care delivery were to include a wide range of researchers. Within the HealthConnect specifications the reasons listed were 'research and planning of health service delivery'[50] serving 'researchers, planners, managers and evaluators'[51] who 'will access data through "reports" that are extracts of EHR information that have been predefined as part of the HealthConnect secondary use approval process' using the National Data Store.[52] Secondary use was to be managed by the NDS within the HealthConnect architecture. It was a component which caused considerable public concern for privacy, and had received specific attention in the specifications of HealthConnect.[53]

The HealthConnect architects expected that as implementation progressed, advisory groups would be introduced, including a privacy and access control advisory group, which would be composed of patients/consumers and professional bodies representing healthcare providers; other national agencies involved in the provision and use of national data collections; and the National Health and Medical Research Council (NHMRC).[54] The privacy and access control advisory group would monitor privacy protocols, define consent options and rules, approve research requests and act as an independent monitor in authorising and managing access to information for secondary uses.[55] However, the independence and transparency of the monitoring group would be open to question if it was answerable to a HealthConnect Board.

Secondary users' responsibilities had also been specified. These included a commitment to using information only for purposes stated; participation in line with HealthConnect confidentiality and privacy arrangements; commitment to abiding to HealthConnect processes and rules relating to circulating and publishing information; and provision of a secure environment for storage of HealthConnect supplied information.[56]

There was clearly more work that needed to be done in order to finalise these complex arrangements, which placed considerable responsibility onto the secondary users themselves. However, user responsibilities are an accepted ethical approach in research contexts.

Rather than adopting procedures that look at the type of information and its sensitivity, the proposals for secondary use of HealthConnect data would have been assessed against ethical and legal principles which had yet to be established.[57] The HealthConnect governing body would have had the task of enforcing the policies and guidelines for secondary uses.[58]

The HealthConnect secondary uses model for de-identified health data

Secondary use was generally anticipated as being access to 'aggregated or de-identified' data from the HealthConnect system.[59] Reporting based on anonymised records included analyses such as occurrences of patients who had received a particular treatment regime (potentially to evaluate effectiveness of the regime) or clinical audit and benchmarking studies, and statistical reporting of aggregated HealthConnect data.[60] The possibility of reconnecting de-identified information to its identifying details, whether by small cell inference or by other means should not be discounted.[61] Depending on the anonymisation method adopted, HealthConnect unique identifiers could have been used to re-identify the individuals in the redacted record.

In 2005 a number of reports appeared in the media regarding doctors in Australia having sold patient information with names and addresses removed. Following an investigation by the Office of the Federal Privacy Commissioner into alleged privacy breaches by the doctors and the companies involved, the Federal Privacy Commissioner allowed the sale of de-identified health records of patients on the following grounds:

> The Privacy Act applies to information where the identity of the individual is apparent, or can reasonably be

> ascertained, from the information. The Office is bound to make its decision about matters it investigates on the basis of the meaning of personal information as set out in the Privacy Act. Following my Office's investigation it was found that the identity of patients could not reasonably be ascertained. Therefore, the Privacy Act does not apply in the circumstances of this particular case.[62]

Therefore 'identifiable' personal information is narrowly interpreted in Australian federal privacy law. However, in Health*Connect* the use of de-identified data would have been subject to guidelines of the *National Statement on Ethical Conduct in Research Involving Humans* which forms part of the NHMRC guidelines referring to 'potentially identifiable' personal information.[63] It could be argued that researchers using de-identified data that can be re-identified may be subject to the limitations of these standards which go beyond identifiable personal information as defined in the *Privacy Act 1988* (Cth).

Even if Health*Connect* does not breach privacy when it authorises the use of anonymised data, it may breach confidentiality. In the United Kingdom the duty of confidentiality has been expanded by case law.[64] The English High Court in 1999 in *R v Department of Health, Ex Parte Source Informatics Ltd* found that the disclosure of de-identified patient data without the consent of the patient breached confidentiality, unless a high public interest value in its disclosure could be demonstrated by the user. However in an appeal by *Source Informatics*, the United Kingdom Court of Appeal made a controversial decision overturning the High Court decision.[65] It decided that disclosing anonymised patient data, even though the patient had not consented, was not breach of confidentiality on the part of the confidant. The decision in this case limited the legal duty of medical confidentiality to information that reveals the identity of the patient. Although it can be argued that if third party access is only given to de-identified data the risks of disclosure of sensitive information will be substantially reduced, patients do expect to be informed if their health information is to be used for purposes not related to their treatment, even if identifying details have been removed.[66] The requirement for patient consent for access to his or her de-identified data is consistent with recommendations of medical codes of practice. For example, the Australian Medical Association recommends that patients are informed that their de-identified data may be sold or used for non-clinical

purposes.[67] Therefore, there is considerable support in both the medical practitioner and patient community for consent to the disclosure of de-identified data.

The HealthConnect secondary uses model for identifiable data

Some research use of identified information would have been permitted in plans for Health*Connect*. Amongst those nominated was the evaluation and review of particular performances such as specified medical procedures and medication regimes of patients that meet certain criteria.[68] This leads to the inevitable conclusion that the data set that comprised the Health*Connect* information base in the NDS would have been capable of much greater monitoring of particular provider services than is currently available. For the health providers this should have been an issue of considerable concern, particularly given the fact that this type of monitoring and any protections for providers were not specified at all; the model only referred to consumers (patients).

Health*Connect* had proposed that the use of identified personal data would be in accordance with the *Privacy Act 1988* (Cth) and the National Health and Medical Research Council, as well as other strict protocols and approval processes for researchers.[69] The *Privacy Act 1988* (Cth) s95 provides that the NHMRC may, with the approval of the Privacy Commissioner, issue guidelines for the protection of privacy in the conduct of medical research. The guidelines need to be read in conjunction with the *National Statement on Ethical Conduct in Research Involving Humans,* which forms part of the *National Health and Medical Research Guidelines* requiring patient consent before use of any identified data. There are exemptions for research without the data subject's consent. Section 95A of the *Privacy Act 1988* (Cth) provides a framework for human research ethics committees to assess proposals to access health information for research (including without the consent of the subject), to compile or analyse statistics or to conduct health service management. Approval for research without the consent of the subject is only given if the public interest in that research substantially outweighs the public interest in the protection of privacy.[70] Therefore at the Commonwealth level there is a legislative framework for researchers applying for access to identifiable health data, which would most likely have applied to Health*Connect* identifiable data in the National Data Store. The extent to which the legislation would have applied to identifiable data held in other parts of

the Health*Connect* system is uncertain; hence there would have been a need for Health*Connect*-specific protocols.

Consent to secondary uses over time

Consent by patients and providers to participate in Health*Connect* and the process of registering and recording their consent preferences have been pivotal to the Health*Connect* scheme. The initial consent models took into account the ability to change consent settings, but they did not include consent to access patient data for secondary uses, or to further linkages with other external databases.[71] Patients would not have been made aware that on registration they also consented to secondary uses which did not expire should they revoke participation, and that there would be no capacity to opt-out of the secondary use provisions.[72] Managing access to records of patients who left the system had only partially been covered by the requirement to mask or withdraw the information from viewing.[73] If patients were alive they had a right to nominate who could see their record for treatment; upon their death the records were to be retained in the NDS and in the HRS subject to the retention requirements of the regime(s) that would apply to records in different layers of the architecture. The indefinite retention and continued use of the information for secondary purposes appeared beyond the scope of consent permission supplied at registration.

The only patient control in Health*Connect* that may have been available for secondary uses would have been via a consumer representative on an undefined privacy and access advisory governance structure (see above). With a generalised consent process for secondary use, which had no limitations on period, type or whether it would be for identified or de-identified information, patients had lost considerable control over the use of their personal information.

Blanket consent for all future uses does not constitute informed consent. Health*Connect*'s legal consultants argued that it was unworkable to ask for express consent for every use.[74] The legal right to consent to secondary uses of health data is already limited under existing Australian privacy law. As a general rule, the Australian federal National Privacy Principle (NPP) 2(b) requires that the patient must consent to the *use* of health information provided by her or him. However, under NPP 10.3(a)(iii) and NPP 10.3(d)(ii), no consent is required for the *collection* of health information if it is necessary for 'the management, funding or monitoring

of a health service' and if 'the information is in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation'.[75] The Health*Connect* scheme would fall within both of these descriptions.[76] As in the United Kingdom, broad exemptions for monitoring health services would most likely undermine explicit consent requirements from patients for secondary uses. In fact, according to the *Data Protection Act 1998* (UK) research is a legitimate use of medical records.[77]

A major issue of patient autonomy is determining the range of uses and the persons to whom information may be provided and used. Under the proposed Australian National Health Privacy Code (NHPC), secondary uses that were closely related to primary uses would not have required consent of the data subject.[78] The recommendation of the *Legal Issues Report* was that the full range of potential secondary uses be identified and legislated. This would have led to less privacy protection as more exceptions were likely to be added, but at least they would have been made public. The Report also pointed to a need to control patient privacy in the data downloaded in providers' clinical systems.[79]

In the Health*Connect* model with its many outsourced services, a breach of system security at any one of the three layers would have opened up widespread possibility of inappropriate disclosures. The legislative framework would have needed to be consistent to cover records held by all three levels of the system architecture.

Given the lack of explicit consent by patients to secondary uses of their Health*Connect* records, and the absence of a right to view access logs of secondary users and of any constitutional protection for privacy, there would have been nothing to prevent the government from legislating to undermine the privacy protections which were stated to underpin the Health*Connect* system.

Long-term uses of Health*Connect* identifiable data: Protective legislative regimes

The Health*Connect* consent implementation model offered limited flexibility in terms of the extent to which patients could control access to unspecified future uses of their identifiable health information. Secondary

uses, in particular the use of identified information presents a dilemma: the genuine need for access to personal health data for health research, as well as non-health research (law enforcement requirements or family history), which may need to identify an individual (including a deceased patient), and the continuing protection of the individual or family from harm even decades later. Social and genealogical research ethical guidelines would need to take account of particularly sensitive medical conditions that may be hereditary, as well as the purpose of the research. Models such as that of Gostin and Hodge provide a legal and ethical framework for balancing privacy and common goods which maximise privacy interests where they matter most to the patient and maximise communal interests where they are likely to achieve the greatest public good.[80]

Archival regimes have focused on preservation of records for general public disclosure, which may include personal information of data subjects or other record participants once the information has lost its sensitivity. Health*Connect* did not address long-term access for non-medical research purposes. Privacy legislation also excludes this perspective. Archival and health records legislation in Australia includes provisions for authorised destruction of categories of personal health data and places extensive time limits on access to its use if retained permanently.[81] Each access use of personal data whether authorised by the record creator or the archives must be captured as metadata, and retained as part of the record, essential to its authenticity, as well as to track privacy infringements.

Cessation of privacy and confidentiality

Whether privacy and confidentiality persist after the death of a person is a contentious issue. There is no sunset clause in the common law principle of confidentiality.[82] In relation to privacy rights these may not be extinguished with the death of the individual, unless legislated otherwise (for example the United Kingdom and Sweden). This line of argument leads to the conclusion that long-term access to personal information should be restricted, and in some instances the data destroyed. On the other hand, it could be argued that on utilitarian grounds long-term access to patient information is unlikely to harm the person once he or she is dead or if a number of years have lapsed. Other factors, such as the dead patient's genetic disposition to particular diseases, could affect

descendants and lead to discrimination if made available to health insurers or employers.

The definition of 'personal information' in the proposed NHPC states that it 'does not include information about an individual who has been dead for more than thirty years'. This approximates to limits on access to identifiable health records that are more than one hundred years old, commonly provided through archival legislation or practice. An alternative approach is to narrow the definition so that personal data is confined to living persons, which would follow the Swedish data protection regime, and thus provide some sort of sunset clause for personal health data.[83]

A way forward

Uniform health privacy law is a prerequisite for any national health record system.[84] Health*Connect* had endorsed a national health privacy code that included provisions of a lower standard than some existing Australian state privacy laws. Until a national health privacy code was approved, Health*Connect* conceded it would have had to tailor privacy implementation separately for each Australian jurisdiction which would have resulted in an uneven legal protection for patients and provider responsibility in each state. The potential for selling off outsourced medical data and the extent to which private contractors would be subject to privacy regulations would have needed further investigation. While Commonwealth archival legislation would have applied to records in the national data store, the overall privacy framework as it currently stands would not have sufficiently protected current and future uses of identifiable information in the various layers of the Health*Connect* system.

The Health*Connect* model provided neither informed nor explicit patient consent to secondary uses. Secondary uses of the national data store would have required strict research protocols that went beyond the *National Health and Medical Research Guidelines* to include patients' consent to particular uses of their records. Privacy and archival law would have needed to be reconciled so that long-term use, retention and preservation of electronic health records were properly balanced with privacy, confidentiality and public interest.

Preserving the EHR in the proposed Health*Connect* system would have been complex because the specifications had limited requirements for

managing the metadata and underlying record technologies over a long period. The management and appraisal of the records in the National Data Store were likely to be deemed to be a Commonwealth responsibility, and consequently under the national archival and records regime. Yet there remained the issue of the status and legislative control over the EHR held by local health providers and the HRS.

A national health records system would need to address the issues of which digital preservation strategies to adopt, what and who will preserve the records, and for how long. Each Health*Connect* record would need to be appraised from the perspective of the functions of Health*Connect*'s central authority, the health records systems and the clinical system to ensure that the retention of all records is appropriate to their purposes.

Other recommendations for a national health record system that respected privacy and confidentiality would be to ensure that:

- Patients and descendants were given access to logs of secondary uses of both identifiable as well as anonymised information.
- Explicit consent had been provided by patients for secondary uses of identified data and informed consent for de-identified data.
- Clarification of when confidentiality and privacy cease had been stipulated.
- Consent to data linkage via identifiers was uniformly applied.

Conclusion

Health*Connect* and similar multi-jurisdictional networked systems holding sensitive personal information are likely to falter on political and technical grounds. The project had been politically fraught from its inception with strong criticism from the Federal Privacy Commissioner.[85] Other factors that contributed to its overall failure included the absence of a national health privacy regime, an appropriate governance structure and the complexity of the various iterations of its business specification. The 2004-05 draft business specifications had attempted to resolve many

technical and policy issues. One can only speculate whether the specifications will be resurrected in another form.

There is still public concern surrounding the introduction of a national social benefits smart card[86] which includes health data and the National E-Health Transition Authority's development of patient identifiers for a national system. The more mature shared health records projects in Australian states underpinned by privacy and health records legislation are now at the forefront of developments with a national system likely to ride on state developments, particularly in New South Wales. Whether the federal strategy focused on common standards for health record systems in all states will build a viable 'bottom up' national system is uncertain. This strategy must also address the variation in privacy rights between the states, and the preservation of and access to personal health records across many jurisdictions and organisations over and beyond an individual's lifetime.

Endnotes

* This article is a substantially revised version of 'Beyond the Tomb: Privacy, Confidentiality and the Long Term Preservation of EHRs in National Systems: a Case Study of Australia's Health*Connect* Project', paper presented at *The Long-term Curation and Preservation of Medical Databases*, International Workshop, Digital Curation Centre, University of Glasgow and Electronic Resource Preservation and Access Network (ERPANET), Calouste Gulbenkian Foundation, Lisbon, Portugal, 13-14 October 2005. It is based on the author's research as a Chief Investigator, School of Information Management and Systems, Faculty of Information Technology, Monash University and Faculty of Law, Monash and Deakin University, Australia, *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework*, Australian Research Council, Discovery Grant, 2002-05. The article also acknowledges the work of the Grant's Research Associate, Barbara Reed.

1 Nicolas P Terry, 'Electronic Health Records: International, Structural and Legal Perspectives' *Journal of Law and Medicine*, vol. 12, no. 1, August 2004, pp. 26-39. In the United Kingdom, encouraged by the needs of its national health system, the idea of a health record that aggregates all encounters of a person with the health system had been mooted since the 1980s. See Bernard Benjamin, *Medical Records*, 2nd edn, William Heinemann Medical Books Ltd., London, 1980, Chapter 16.

2 ISO/TC 215 *Ad Hoc* Group Report, *Standards Requirements for the Electronic Health Record & Discharge/Referral Plans, Draft V 2.1*, 31 May, 2002, Peter Schloeffel and P Jeselon EHR *Ad Hoc* Group Co-Chairs, 2002, p. 33.

3 Canada, Australia and the United States have been at the forefront of the business health domain view of the EHR. For example HealthConnect's national health infostructure included 'the national provider directory, national health consumer identifier, health metadata repositories, health information standards, approved terminologies and health data sets.' HealthConnect, *Business Architecture v1.9*, November 2004, Department of Health and Ageing, 2004, p. 3, <http://www.healthconnect.gov.au/pdf/BArc1-9.pdf> (accessed November 2005). This version remained publicly available until early 2006 but has since been withdrawn from HealthConnect website. It was intended to be the consultation draft for the first full implementation of HealthConnect. *ibid.*, p. 172.

4 National Electronic Health Records Taskforce, *A Health Information Network for Australia, Taskforce Report*, Department of Health and Aged Care, Commonwealth of Australia, July 2000, <http://www.healthconnect.gov.au/pdf/ehr_rep.pdf> (accessed November 2005).

5 See Livia Iacovino, Danuta Mendelson and Moira Paterson, 'Privacy Issues, HealthConnect and Beyond', in *Disputes and Dilemmas in Health Law*, Ian Freckelton and Kerry Petersen (eds), the Federation Press, Sydney, 2006, p. 614. There have been many different groups involved in the governance and funding of HealthConnect; some of these bodies have been specifically set up for the project, while others have been part of a broader government E-health agenda often from state jurisdictions. The recommendation of the *Legal Issues Report* in relation to governance was that 'the simplest structure should be adopted, at least initially. That would be retention as a government departmental function'. HealthConnect, *Legal Issues Report*, January 2005, prepared by Clayton Utz for the Department of Health and Ageing, Commonwealth of Australia, 2005, August 2005, p. 94, <www.healthconnect.gov.au/pdf/lirsummary_web2.pdf> (accessed January 2006). Despite this recommendation, a corporate entity, the National E-Health Transition Authority was established to govern HealthConnect.

6 HealthConnect, *Business Architecture v1.9, op.cit.*, 'Foreword', p. 1.

7 HealthConnect, *Implementation Fact Sheet*, June 2005, <http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/8B76541C5CD5ADC1CA257128007B7E92/$File/HealthConnect_implementation_Jun05.pdf> (accessed July 2006). The Australian Productivity Commission's criticism of HealthConnect's benefits study, the federal Privacy Commissioner's concern with HealthConnect's privacy provisions, and its association with the Medicare smart card, abandoned in June 2006 for a generic access benefits card, have made HealthConnect politically untenable. Renai LeMay, 'HealthConnect Gets Productivity Check-up', *ZDNet Australia*, 22 April 2005, <http://www.zdnet.com.au/news/business/soa/

HealthConnect_gets_productivity_check_up/0,39023166,39189218,00.htm> (accessed July 2006).

8 Karen Dearne, 'PM Backs Off E-health', *The Australian*, 24 Jan., 2006.

9 National E-Health Transition Authority, 'About NEHTA', <http://www.nehta.gov.au/content/view/1/103/> (accessed July 2006) and Health*Connect*, 'Introduction', <http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/intro> (accessed July 2006).

10 In a statement by the federal Department of Health and Ageing to a federal Senate Estimates Committee, Medicare and NEHTA intend to develop patient identifiers. See Karen Dearne, 'Health Plan Just a Series of Trials', *The Australian, IT Today*, 6 June 2006.

11 There were a number of incentives to be offered to both patients and practitioners (eg providing additional services such as free broadband to Health providers) to entice them to join the Health*Connect* system. The Health Minister had stated that: 'After a suitable transition period, participation in Health*Connect* and HIC (Health Insurance Commission) Online could become mandatory'. Minister for Health and Ageing, Tony Abbott, 'Speech Notes for the Health Informatics Conference', Melbourne Convention Centre, Melbourne, 2 August 2005, p. 4, <http://www.health.gov.au/internet/ministers/publishing.nsf/content/health-mediarel-yr2005-ta-abbsp020805.htm/$FILE/abbsp020805.pdf> (accessed July 2006).

12 Health*Connect*, *Business Architecture v1.9*, *op. cit.*, p. 37.

13 Iacovino, Mendelson and Paterson, *op.cit.*, pp. 614-21.

14 Health*Connect*, *Business Architecture v1.9*, November 2004, Figure 1: Key Components of Health*Connect* p. 2. © Commonwealth of Australia reproduced by permission.

15 Health*Connect*, *Legal Issues Report*, January 2005, p. 21, Figure 3: Components of Health Connect National e-Health Building Blocks. © Commonwealth of Australia, reproduced by permission.

16 Health*Connect*, *Business Architecture v1.9*, *op.cit.*, p. 20.

17 *ibid.*, p. 110.

18 *ibid.*, p. 34.

19 *ibid.*, p. 34.

20 *ibid.*, p. 35.

21 *ibid.*, p. 110.

22 Hans Hofman, 'Report on a Preliminary Analysis of Dataflows in the Health*Connect* System', April, 2005, for *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework*, *op.cit.*, (unpublished).

23 Health*Connect*, *Business Architecture v1.9*, *op.cit.*, p. 127.

24 *ibid.*, p 145; *Business Architecture v1.9*, Barbara Reed, 'Report: Issues Arising From Analysis of the Health*Connect*, *Business Architecture v1.9*', July 2005, for *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework, op.cit.*, (unpublished).

25 The *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework* project, gauged the extent to which recordkeeping best practice was found in the three versions of the specification of the Health*Connect* business requirements using key recordkeeping industry standards. The final analysis found that the business specifications did not adequately incorporate recordkeeping requirements. Barbara Reed, 'Report on Recordkeeping Standards Analysis', June 2005, for *Electronic Health Records: Achieving an Effective and Ethical Legal and Recordkeeping Framework, op.cit.*, (unpublished).

26 Livia Iacovino, 'Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and Health*Connect*', *Journal of Law and Medicine*, vol. 12, no. 1, August 2004, pp. 49-50.

27 Danuta Mendelson, 'Travels of a Medical Record and the Myth of Privacy', *Journal of Law and Medicine*, vol. 11, no. 2, 2003, p. 136.

28 Health*Connect, Legal Issues Report, op.cit.*, p. 33.

29 For example, mental health is a subset of health that is of particular sensitivity. See Livia Iacovino, 'The Patient-Therapist Relationship: Reliable and Authentic Mental Health Records in a Shared Electronic Environment', *Psychiatry, Psychology and Law*, vol. 11, no. 1, 2004, pp. 63-72.

30 Moira Paterson, and Livia Iacovino, 'Health Privacy: The Draft Australian National Health Privacy Code and the Shared Longitudinal Electronic Health Record', *Health Information Management*, vol. 33, no.1, 2004, pp. 5-11.

31 Moira Paterson, 'Health*Connect* and Privacy: A Policy Conundrum', *Journal of Law and Medicine*, vol. 12, no. 1, August 2004, p. 82.

32 Reed, 'Report: Issues Arising', *op.cit.*

33 Tracking provides an auditable trail of record transactions, ensuring that event histories are part of the record. 'Tracking' is defined in the *ISO records management standard* as 'creating, capturing and maintaining information about the movement and use of records'. International Standards Organisation, *International Standard: Information and Documentation – Records Management ISO 15489-1-2001 Pt 1*, p. 3.

34 'Access logs detail individual access to EHR records by providers including emergency override access, consumers, Health*Connect* registration agencies and Health*Connect* system administration functions'. Health*Connect, Business Architecture v1.9, op.cit.*, p. 141. The access log of the HRS would have been archived to the National Data Store (*ibid.*, p. 155). Similarly, the National Data Store itself was to maintain an access audit log (*ibid.*, p. 113). It was not

clear whether these two records, which should have existed independently, would actually be consolidated into one log at the National Data Store level ('a consolidated access log is also to be maintained as part of the national data store data collections', *ibid.*, p. 157), nor is it clear whether use of a particular EHR for secondary use purposes would write an entry to the audit log for the specific individual's records, nor whether a consumer could access audit logs of the National Data Store. All reference to consumer access to their EHR was through the HRS layer of the architecture (*ibid.*, p. 62 and p. 110). See Reed, 'Report: Issues Arising', *op.cit.*

35 Private sector health records are generally protected by the private sector provisions in the *Privacy Act 1988* (Cth). It is unclear whether all Health*Connect* records would have qualified for protection under these private sector provisions. Public health sector records are protected under the public sector provisions in the *Privacy Act 1988* (Cth), the *Information Act 2002* (NT) and under sui generis health records laws in Victoria, New South Wales and the ACT. See *Health Records Act 2001* (Vic), *Health Information Privacy Act 2002* (NSW) and *Health Records (Privacy and Access) Act 1997* (ACT). The latter also protect private records, thereby creating dual protection for private sector health records in those jurisdictions.

36 Australian Health Ministers' Advisory Council, *National Health Privacy Code Draft Consultation Paper*, National Health Privacy Working Group, Canberra, 2002. However, the NHPC does not specifically address the unique issues raised by shared electronic health records. In fact it broadens the classes of disclosure. See Paterson and Iacovino, *op.cit.*

37 Health*Connect*, *Legal Issues Report*, *op.cit.*, p. 4.

38 Health*Connect*, *Business Architecture v1.9*, *op.cit.*, p. 32.

39 *ibid.*, p. 5. Private healthcare providers, in addition to specific Health*Connect* privacy rules, would be bound by the 10 National Privacy Principles (NPPs) of *Privacy Act 1988* (Cth) which require, *inter alia*, consent for collection and use of health information; secure data storage; and impose limitations on transborder data flows.

40 Health*Connect*, *Business Architecture v1.9*, *op.cit*, p. 107, 120. Also 'consumers will not be able, through Health*Connect* to deny access to an individual provider within an authorized provider organization, though it may be possible for the consumer to address this requirement with the relevant provider organization'. *ibid.*, p. 56.

41 The Health*Connect*, *Legal Issues Report*, *op.cit.*, p. 48 however recommended that this level of registration would not be sufficient, recommending individual registration and tracking of actions at the individual level.

42 Health*Connect*, *Business Architecture v1.9*, *op.cit.*, p. 58.

43 Australian Government, Office of the Privacy Commissioner, 'Submission on the Health*Connect* Business Architecture Version 1.9', February 2005, p. 14, <http://www.privacy.gov.au/publications/hlthcnnctsub.pdf> (accessed July 2006); Renai LeMay, 'Hackers on Medicare Smart Card Waiting List' *ZNet Australia*, <http://www.zdnet.com.au/news/security/0,2000061744,39182294,00.htm> (accessed July 2006); Bob Brewin, 'Australia Health IT Faces Privacy Fears', *Gov Health IT*, 17 June 2005, <http://govhealthit.com/article89294-06-17-05-Web> (accessed July 2006).

44 Health*Connect, Business Architecture v1.9, op.cit.*, p. 108 and p. 162.

45 Health*Connect, Business Architecture v1.9, op.cit.*, p 110-11, pp 115-17 and p. 163.

46 For a discussion of outsourcing of medical data processing see Danuta Mendelson, 'Electronic Medical Records: Perils of Outsourcing and the *Privacy Act 1988* (Cth)' *Journal of Law and Medicine*, vol. 12, 2004, pp. 8-14. Also see 'Indian Call Centre Sell Off Australians' Details', 'Four Corners', *ABC News Online*, 15 August 2005, <http://www.abc.net.au/news/newsitems/200508/s1437366.htm> (accessed July 2006).

47 A contractor under a Commonwealth contract is defined as a 'contracted service provider' (CSP) in section 6(1) of the *Privacy Act 1988* (Cth) which includes a 'subcontractor'.

48 Australian Government, Office of the Federal Privacy Commissioner, *Information Sheet 14 - 2001*: Privacy Obligations for Commonwealth Contracts, <http://www.privacy.gov.au/publications/IS14_01_print.html> (accessed July 2006).

49 'An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, 1980, Annex to the Recommendation of the Council of the 23 September 1980, Part 1 General Definitions (b).

50 Health*Connect, Business Architecture v1.9, op.cit.*, p. 2.

51 *ibid.*, p. 3.

52 *ibid.*, p. 7.

53 *ibid.*, pp. 96-98.

54 *ibid.*, p. 96.

55 *ibid.*, p. 164.

56 *ibid.*, pp. 95-96.

57 *ibid.*, pp. 96-97. For further discussion of ethical principles that could be adopted for secondary uses, see Bernadette McSherry, 'Ethical Issues in

HealthConnect's Shared Electronic Health Record System', *Journal of Law and Medicine*, vol. 12, no. 1, Aug. 2004, pp. 60-68.

58 HealthConnect, Business Architecture v1.9, *op.cit.*, pp. 107-8.

59 *ibid.*, p. 46.

60 *ibid.*, pp. 93-95.

61 *ibid.*, p. 97. Currently de-identified claim records of Medicare and Pharmaceutical Benefits Scheme are held permanently by Department of Health and Ageing but can be re-identified by the Health Insurance Commission's Medicare pin. Australian Government, Office of the Privacy Commissioner, *Review of the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines*, Issues Paper, November 2004. The public meeting held on 7 December 2004 in relation to the review of these Guidelines expressed concern about the ability to re-identify health records that had been de-identified. The HealthConnect *Legal Issue Report* suggested that de-identification should be irreversible (p. 10) but as the identifiable record will continue to exist in NDS and the HRS, the anonymised version is another record, albeit a redacted version.

62 Australian Government, Office of the Privacy Commissioner, 'Commissioner Clarifies Media Inaccuracies That Doctors are Selling Patient Information to Drug Companies', *Media Statement*. 26 May 2005, <http://www.privacy.gov.au/news/05_05.html> (accessed July 2006).

63 Colin Thomson, *The Regulation of Health Information Privacy in Australia*, National Health and Medical Research Council, Privacy Committee, Canberra, 2004, p. 4.

64 Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State*, LexisNexus Butterworths, Chatswood, NSW, 2005, p. 17.

65 In a 1999 English High Court case, *Source Informatics Ltd* requested permission from the UK Department of Health to allow general practitioners and pharmacists to provide it with statistical information on their prescribing habits extracted from their patient data in de-identified form, in order to sell the information to drug companies. As the disclosure was not found to be in the public interest the application for judicial review was dismissed, but the appellant successfully appealed against the decision. See *R v Department of Health Ex Parte Source Informatics Ltd* [1999] 4 All ER 185, and *R v Deptartment of Health, Ex parte Source Informatics* [2001] QB 424, [2000] 2 WLR 940. The reasoning in this latter case could apply to similar Australian cases.

66 McSherry, *op.cit.*, p. 64; Donald J Willison, et al, 'Patient Consent Preferences for Research Uses of Information in Electronic Medical Records: Interview and Survey Data', *British Medical Journal*, vol. 326, 2003, pp. 373-6. The *Legal Issues Report* was of the view that there was no privacy obligation regarding

the use or disclosure of de-identified data, but it did recommend that patients be advised that their de-identified data might be used. *Legal Issues Report, op.cit.*, p. 10 and p. 55.

67 Australian Medical Association, 'AMA Advises Doctors To Be Vigilant With Patient and Prescribing Information', AMA, *Media Release*, 21 Jan 2005, <http://www.ama.com.au/web.nsf/doc/WEEN-68U9YB> and 'AMA Poll Shows Patients Are Concerned About the Privacy and Security of Their Medical Records', AMA, *Media Release*, 20 July 2005, <http://www.ama.com.au/web.nsf/doc/WEEN-6EG7LY> (accessed July 2006).

68 HealthConnect, *Business Architecture v1.9, op.cit.*, p. 93.

69 *ibid.*, p. 38.

70 Australian Government, National Health and Medical Research Council, *Guidelines Approved Under Section 95A of the Privacy Act 1988*, 2001, <http://www.nhmrc.gov.au/publications/synopses/e43syn.htm>

(accessed July 2006).

71 The patient's right to deny access to specific data was rejected by HealthConnect as unwieldy at an early stage of its research. The 2004-05 model allowed patients to nominate and amend at any time the providers and provider organisations (but not individual providers in organisations) who could access their EHRs and to limit the reporting of specific events, either in full or in part. Access control lists would operate, at least partially, to the level of the healthcare provider organisation, leaving a large area of potential exposure to inappropriate disclosure of personal information (HealthConnect, *Business Architecture v1.9*, November 2004, p. 106). Access control lists were to be subject to an override in the case of a request by a provider for emergency access and would be issued without time limitations, valid until a consumer changed them (*ibid.*, p 56).

72 HealthConnect, *Business Architecture v1.9, op.cit.*, p. 53 and p. 95.

73 *ibid.*, p. 61.

74 HealthConnect, *Legal Issues Report, op.cit.*, p. 9, and 56.

75 The *Privacy Act 1988* (Cth) distinguishes between 'collection' and 'use' of information, and NPP 2, as well as NPP 10 regulate the 'collection' but not the 'use' of information.

76 Similarly in *Health Information Privacy Act 2002* (NSW), HPP 11 'Limits on disclosure of health information' there is an exemption for secondary uses if 'the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services'. <http://www.austlii.edu.au/au/legis/nsw/consol_act/hraipa2002370/sch1.html> (accessed November 2005).

77 *Data Protection Act 1998* (UK), Sch 3, cl 8.

78 '2.2. An organisation must not use or disclose health information about an individual for a purpose (the "secondary purpose") other than the primary purpose for which the information was collected unless - (a) both of the following apply - (i) the secondary purpose is directly related to the primary purpose; and (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; ...' Australian Health Ministers' Advisory Council, *op.cit.*, p. 17.

79 Health*Connect, Legal Issues Report, op.cit.*, p. 11.

80 Lawrence O Gostin and James G Hodge Jr, 'Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule', *Minnesota Law Review*, vol. 86, 2002, p. 1439.

81 Livia Iacovino and Malcolm Todd, 'The Long-term Preservation of Identifiable Personal Data: a Comparative Archival Perspective on Privacy Regulatory Models in the European Union, Australia, Canada and the United States', *Archival Science*, (in press 2006).

82 Heather MacNeil, 'Information Privacy, Liberty, and Democracy', in *Privacy and Confidentiality Perspectives: Archivists and Archival Records*, M Behrnd-Klodt and P Wosh (eds), Society of American Archivists, Chicago, 2005, pp. 67-81.

83 For example, the *Personal Data Act 1998* (Sweden), s 3 defines 'personal data' as 'all kinds of information that directly or indirectly may be referable to a natural person who is alive'. See also Australian Health Ministers' Advisory Council, *op.cit.*, p. 42.

84 Australian Government, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, Office of the Privacy Commissioner, Sydney, 2005, p. 9.

85 Australian Government, Office of the Privacy Commissioner, *Submission on the HealthConnect Business Architecture Version 1.9*, February 2005, <http://www.privacy.gov.au/publications/hlthcnnctsub.pdf> (accessed July 2006).

86 The Consumer and Privacy Taskforce Report on the access card became available after this article was submitted for publication. See Australian Government, Department of Human Services, *Health and Social Services Access Card*, Consumer and Privacy Taskforce, Report Number One, Sept 2006, pp. 49-51 <http://www.accesscard.gov.au/various/Consumer_privacy_rp2.pdf> (accessed November 2006). The Privacy Commissioner in her *Media Release* indicated a number of concerns with the report's recommendations. *Media Release: Privacy Commissioner Welcomes Release of the Access Card Task Force Report*, 8 November 2006, <http://www.privacy.gov.au/news/media/06_6.html> (accessed November 2006).