Magnusson (2002) makes the point that:

tient.

to facilitate the sharing of information and they gener-

increase.

health records regimes which involve the re-use of

privacy because of their ability to electronically link

longitudinal record, once compiled, “is likely to

be of interest to many other parties, quite outside

one such initiative, the Australian HealthCon-

ect project, is designed to provide for the collection, stor-

age and exchange of health information on a national

basis via the creation of a longitudinal contact record

for each patient detailing all interactions with the

health system. The government report published in

July 2000 (National Electronic Health Records Task-

force 2000), which recommended its development, iden-

tified a number of key building blocks as being

required to underpin all other activities. These in-

cluded the development of legal data protection and

security frameworks that were regarded as necessary

to facilitate electronic transfers and storage of health

information (National Electronic Health Records Task-

force 2000). Core components of the policy-design

work of HealthConnect include the development of

national privacy rules; they also include consent and

identification arrangements and a security framework.

To facilitate this task the Australian Health Minis-

ters’ Advisory Council appointed a Privacy Working

Group to develop a nationally integrated framework

for privacy protection of personal health information.

The latter states that the principles in the Draft Code

extend beyond the context of a person’s one-to-one

relationship with a health provider to “the exchange of

individual health information on a much wider scale

between hospitals, pharmacists, other health informa-

tion providers, health researchers, law enforcement

agencies, government departments and individuals”

(Australian Health Ministers’ Advisory Council 2002).

This article reports a joint submission made by its

authors to the Privacy Working Group in March 2003,

which focuses principally on the capacity of the Draft

Code to protect health information in a shared longitudi-

dinal electronic health record. It also discusses further

privacy research in 2004 in relation to the code as ex-

pressed in the technical requirements of business

processes of HealthConnect.

Scope

Currently, private sector health records are protected

by the private sector provisions in the Privacy Act

1988 (Cwlth), except to the extent that they fall within

the exception for employee protection. The national

Key words: medical records systems; computerised/legislation & jurisprudence; medical record linkage;

confidentiality/legislation & jurisprudence; access to information; health information management

Introduction

It is generally accepted that health information has a

special quality of sensitivity. This is reflected in the

fact that it is almost always listed as one of the cat-

egories of information which it is most easy to identify

as private (see, for example, Gleeson’s comments in

ABC v. Lenah Game Meats (2001) 185 ALR 1.13). As a

consequence people are more likely to cooperate with

public health strategies if they trust the health system

not to act in a way that would undermine their inter-

ests and that such trust is undermined by uses of in-

formation “in ways that the individual does not expect

and has not been consulted about” (Health Issues

Centre et al 2002 p. 13; see also Australian Health


In recent years, governments world-wide have en-
couraged the development of integrated electronic

health records regimes which involve the re-use of

personal health data in shared networked environ-

ments by using personal or entity identifiers coupled

with authentication techniques to link personal data

across jurisdictions and institutions for online delivery

of services (Cornwall 2002). Those regimes pose an

increased threat to privacy because their objective is

to facilitate the sharing of information and they gener-

ally involve the retention of data for the life of the pa-

tient.

Magnusson (2002) makes the point that:

As medical records move “on-line” and the cen-

tralisation and coordination of health data becomes

possible, the demands for third party access, the

potential benefits of providing such access, as well

as the privacy risks for individual patients, will all

increase.

Those developments pose a substantial threat to

privacy because of their ability to electronically link

and integrate information that was previously segre-
gated within individual health records (Terry 2000).

Furthermore, as explained by Carter (1999), an inte-

grated, longitudinal record, once compiled, “is likely to

be of interest to many other parties, quite outside

those who might be considered to have legitimate

public health interests”.

One such initiative, the Australian HealthConnect

project, is designed to provide for the collection, stor-

age, and management of health information. It is

aimed at improving the quality and efficiency of

health care by facilitating the sharing of informa-

tion across jurisdictions and institutions. The

Draft Australian National Health Privacy Code

was developed to provide a framework for the pro-

tection of personal health information in a shared

environment. It includes a number of key principles

that balance the need for privacy with the potential

benefits of shared health information.

Abstract

An explicit distinction between shared electronic health records and those at the point of care is required

when referring to electronic health records. The former raises particular privacy issues discussed in this

paper in relation to HealthConnect and the Draft Australian National Health Privacy Code. In addition to a

number of revisions to the code, the analysis recommends that related legislation such as archival and

freedom of information law should be reconciled as much as possible within the code, so that a long-term

view of the uses, retention and preservation of the longitudinal electronic health record is balanced with

privacy, confidentiality and public interest.

Health privacy: the draft Australian national health privacy code and the shared longitudinal electronic health record

Moira Paterson and Livia Iacovino
privacy provisions (NPPs) which form the basis for that protection 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. Public health sector records are protected under the public sector provisions in the Privacy Act 1988 (Cwlth), the Information Act 2002 (NT) and under sui generis health records laws in Victoria, New South Wales and the ACT, such as the Health Records Act 2001 (Vic), the Health Information Privacy Act 2002 (NSW) and the 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. States other than Victoria and New South Wales do not have either public sector privacy laws or sui generis health records laws. (Public bodies in Queensland, South Australia and Tasmania are, however, subject to the operation of administratively imposed privacy rules. (See www.justice.qld.gov.au/dept/privacy.htm, www.archives.sa.gov.au/privacy/index.html and www.justice.tas.gov.au/legpol/privacy/index.htm.)

The Draft Code was designed to provide a national framework for the development of consistent state and federal rules for the protection of health information. However, the Discussion Paper leaves open for discussion whether it should be voluntary or compulsory and the extent to which it should apply to health records outside the health sector.

The Discussion Paper suggests three possible options concerning the code’s scope of coverage. The first would limit its application to health services and would have the consequence that personal health information in the possession of bodies other than health services would receive protection only as a species of personal information. This would mean that such health information would receive no protection in those jurisdictions that lack public sector privacy laws. It would also receive no protection under the private sector provisions in the Commonwealth Privacy Act to the extent that it falls within the exception for employee records. There would also be a risk that the restrictions on the transfer of data contained in the code would create difficulties for a health organization wishing to transfer health information to organizations other than health services (Australian Health Ministers’ Advisory Council 2002).

The second option would be to extend the code’s coverage to the handling of all health information no matter where it is held. This would have the consequences that organizations would be required to comply with different privacy standards for health data than for other categories of personal information.

The third option represents a combination of the other two approaches. It envisages that the code would apply primarily to the health sector, with some limited coverage of organisations outside the health sector that might also have significant holdings of health information (Australian Health Ministers’ Advisory Council 2002). There is no information provided concerning the criteria that might be used in determining whether a body has a significant holding of health information.

Arguably, there are two important reasons why a national code should offer mandatory and across-the-board protection. The first is that the unique sensitivity of health information is sufficient to warrant a mandatory and comprehensive approach. The second is that the code will fail to achieve its objective unless such an approach is adopted.

One reason why health information is accepted as being uniquely personal is that our sense of self is intricately bound up with our health status. It is also the case that specific health-related events, such as terminations of pregnancy or the receipt of treatment for a sexually transmitted disease, shed light on other intimate aspects of our lives. A third and related reason is that disclosure of health information may result in adverse consequences for an individual, including discrimination (for example, in the context of employment), or in stigmatisation and social isolation. It should be noted, however, that stigmatisation may not necessarily be reflected in discriminatory action; instead, it may lead to withdrawal of vital social support, thereby having a degenerative effect on the individual’s self esteem (Harris 1997). The risk of adverse consequences is greatest in the case of conditions that involve mental or emotional instability and those which are perceived to be caused by life choices or behaviours (for example the use of illegal drugs or engagement in certain forms of sexual expression) which are not viewed with favour by the general community (Gostin et al 1995). This special sensitivity arises irrespective of the context in which a record is generated or held. Arguably, therefore, health records warrant an individualised treatment that operates across the board, and, in fact, the code as drafted follows the second option.

The stated objectives for the development of the Draft Code specifically include the achievement of national consistency between public and private sectors and across jurisdictions. The lack of a single uniform national framework creates unnecessary complexity for health providers who operate in different jurisdictions or who need to transfer data across different sectors or jurisdictional boundaries. It also creates difficulties for individuals who may receive no protection in some contexts and be required to navigate different and mutually independent review mechanisms.

Although the Discussion Paper provides no explanation of how precisely the Draft Code might contribute to a uniform scheme, one obvious role for it is to serve as model law for those states which currently lack health privacy legislation and as a voluntary private sector code under the Privacy Act. Since the Draft Code draws heavily from the existing sui generis health records laws, this could ultimately result in a regime that is reasonably uniform except in relation to its coverage of health records in the Commonwealth public sector and any records that fall outside the scope of any private sector privacy code. It should be noted in respect of the latter that the exclusion of employee records is currently under review (Commonwealth Attorney-General’s Department 2004). It should, however, also be acknowledged that there are significant differences both between existing sui generis laws and between provisions in the draft code and the principles contained in the sui generis laws (see, for example, the submission

Reviewed articles

Health Information Management 2004  ISSN 1322-4913  Vol 33 No 1  Page 6

Coverage of HealthConnect
The stated objectives for the development of the Draft Code refer to the need to take into account the initiatives proposed under the HealthConnect network (Australian Health Ministers’ Advisory Council 2002, p. 11). In addition, the Privacy Working Group’s Discussion Paper acknowledges that a robust and consistent privacy framework is needed “... to achieve a viable and secure national health information network that facilitates the exchange of health information between and within health service providers – as proposed under HealthConnect...” (Australian Health Ministers’ Advisory Council 2002, p. 10).

It is currently unclear whether all HealthConnect records will qualify for protection under the private sector provisions in the Commonwealth Privacy Act. That uncertainty arises because of the three levels within its conceptual model: a national coordination layer, a state or area health record system and a provider’s clinical information system (HealthConnect 2003c). Third party access authorisations are within the processes of the health record system that stores the individual’s record at state level. The national level will consolidate into one database all the summaries for secondary and other uses and provide an archival recovery service with archival control at the Commonwealth level (HealthConnect 2003b). Consent information will be held in both the local clinical system and the area or state health record system (HealthConnect 2003a). Therefore, different jurisdictions will be involved from the point of view of the HealthConnect system architecture.

Despite the fact that the code aims to provide rules for networked health systems, it does not make an explicit distinction between shared electronic health records and those at the point of care. The former raises particular privacy and linkage issues. Legislation that also impinges on privacy, including archival and freedom-of-information law, and standards and guidelines should be reconciled as much as possible within the code, so that a long-term view of the uses, retention and preservation of health information and records is balanced with privacy, confidentiality and public interest.

Definitional Issues
Key terms, including health information, health service, and health service provider are defined in Part 4 of the code. However, a definition of a record is also needed. A record, as defined in the International Standards Organisation (ISO) records management standard, is “information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business” (International Standards Organisation 2001, p. 3). The standard includes tracking, which is defined as creating, capturing and maintaining information about the movement and use of records (International Standards Organisation 2001, p. 3). Tracking provides an auditable trail of record transactions (event histories/audit trails) as part of the record. Consumers require access to information on who saw their health record, what they saw, and when, in particular in the HealthConnect context where secondary uses are extensive. Adding a definition of a record will improve consumers’ rights to a full record and supports the draft national health privacy Principle 5, which deals with access to health information by consumers. This definition would apply to any record, which includes health information.

The definition of organisation is left unclear, as this will depend on the mechanism selected for implementing the code, although there is clear intention that it will include public and private health service providers. This matter requires careful attention as there is confusion when the code switches to responsibilities of an individual health service provider who is defined within the meaning of organisation, and then refers to an organisation which includes more than one health service provider, as well as occasional references to a record keeper. Individuals in an organisation do not register separately to participate in HealthConnect. It is envisaged that “Organisations will manage the access entitlements of the individuals within the organisation and may have a range of clinical and non-clinical users” (HealthConnect 2003d, p. 78). As an organisation may control a large number of users via its own rules, there is a danger that privacy controls may be undermined unless such rules are consistent with the code.

The definition of personal information states that it “does not include information about an individual who has been dead for more than 30 years”. This effectively protects personal information to a length of time applied to medical information in archival legislation. However, access to public health records that are more than 100 years old is commonly provided through archival legislation or practice. For example, the State Records Act 2000 (WA) s. 49 contains a special provision for access to a medical record that is at least one hundred years old that is a State archive (ie, a State record that is to be retained permanently). An alternative approach is to narrow the definition so that it is confined to living persons, which would be consistent with the Commonwealth Privacy Act and most European law; for example, the Personal Data Act 1998 (Sweden), s. 3 defines personal data as “kinds of information that directly or indirectly may be referable to a natural person who is alive”. (See also Australian Health Ministers’ Advisory Council 2002, p. 42).

A final definitional issue relates to the definition of publicly-available health information in cl. 3. Paragraph (c) of that definition refers to “a public record under the control of the Keeper of Public Records” (see also Australian Health Ministers’ Advisory Council 2002, p. 56). The Keeper of Public Records is a term only used in the Public Records Act 1973 (Vic), so there needs to be general wording to cover other public archival authorities throughout Australia. An alternative term could be the relevant public archival authority. Control is also defined differently in different archival legislation, so once again there is a need to provide a more precise meaning.
The adequacy of the NHPPs as a standard for protecting shared electronic health records

The Draft Code covers records in all media, not just those in electronic form, with exemptions only for information collected or held for the purposes of, or in connection with, personal, family or household affairs (Australian Health Ministers’ Advisory Council 2002, p. 66 cl. 1).

As explained above, it is an objective of the Draft Code to enhance HealthConnect and e-health exchange of personal health information between jurisdictions and across health information networks. However, the eleven National Health Privacy Principles (NHPPs) in the Draft Code arguably fail to sufficiently address the unique issues raised by electronic health records, and shared electronic health records in particular. For example, shared records provide access to the whole health history of a patient over his or her lifetime, compiled from a range of individual health records across the health sector. Arguably therefore, NHPP 1.4 (c), which requires that an individual should be made aware of the purposes for which his or her health information is collected, should also require notification of the fact that health information will be shared and the provision of appropriate details concerning any such sharing. Likewise, NHPP 7, which deals with identifiers, and NHPP 9, which deals with trans-border data flows within Australia as well as overseas, should contain provisions that deal expressly with the sharing of records within the context of a shared electronic health record.

Another issue of concern is the matter of security. The electronic storage of data, irrespective of whether or not they are linked for the purposes of access by a multiplicity of persons, increases the potential risks to privacy, but these are magnified by the provision for sharing which is integral to systems such as HealthConnect. Arguably therefore, there is a need for the inclusion of some discussion concerning the appropriate use of privacy enhancing measures such as encryption of messages and virtual private networks via the drafting of suitably worded guidelines which could form the basis for developing requirements in standards governing specifications for shared electronic health systems.

Another important issue relates to the autonomy of patients in determining the range of persons to whom information may be provided and the uses to which it may be put. The draft principles provide that a person’s health information may be used or disclosed for the main reason it was collected, or for another directly related purpose if he or she would reasonably expect this, otherwise further consent is required for its use or disclosure. However, as long as the purpose for collection is made clear there is no limitation as to what it may entail, so that the person may essentially have no choice but to withdraw from the medical consultation, as they may be reluctant to provide the information that is sought.

In the absence of an integrated electronic health records regime, there is scope for flexibility in terms of establishing the uses and disclosures that the patient is willing to accede to and scope for the quarantining of information by consulting different practitioners.

Theoretically, an electronic health records system could be set up so that not only is participation voluntary but also so that participating individuals can decide for themselves on an individual basis precisely which categories of access should apply to each item of information included in their electronic record. Patients may wish to quarantine certain more sensitive types of information; for example, information about a sexually transmitted disease, so that it cannot be accessed by all of the health professionals and administrators who would normally have access to their records. These are implementation issues, which include access permissions that must be built into electronic health systems. Quarantining can be achieved, for example, via the use of passwords and/or alphanumeric identifiers (Schoenbery & Saffran 2002). However, in the absence of specific principles requiring such flexibility there is a danger that it may give way to “arguments focusing on clinical necessity, administrative burden and the economic and public health benefits of administrative and research access” (Magnusson 2002). Such principles can, of course, be overridden by legislation, but they have the benefit of requiring Parliament to deal explicitly with the issue.

HealthConnect summaries will be available to primary and secondary user groups. Primary user groups consist of consumers who may wish to review and add to their own health records, and health service providers seeking information about the consumer they are treating. Secondary users are persons and organisations seeking to conduct analysis and research to support several of the objectives set out by the National Electronic Health Records Taskforce. The provision of data for secondary uses will only be allowed under strict protocols requiring the aggregation or de-identification of information and the obtaining of authorisation from a central access authority for the requested use. Secondary users are expected to include researchers (including clinical, health service, administrative, statistical, consumer and epidemiological researchers) seeking information to assist clinical decision making, and managers (including administrators, planners, policy makers and funders) seeking information to assist management decision-making (HealthConnect 2003a, p. 14).

As far as HealthConnect secondary users are concerned, they are all covered in the code under a very wide scope for secondary uses in NHPP 2.2. Although HealthConnect differentiates between secondary uses that are aggregated from those that are de-identified, it recognises that personal information may be inadvertently released regardless of the method of access employed (HealthConnect 2003d, p. 84).

As a minimum, the code should provide that health information cannot be collected for inclusion in an electronic health record without voluntary consent and that inclusion of information within an electronic health record should occur only if the record provides patients with some genuine choice as to its potential uses and disclosure. The current HealthConnect business processes address this by using rules to flag data not available for secondary use (see HealthConnect 2003d, p. 86: “Eliminate those who have indicated that they do not wish their information to be available for the requested secondary use” [Major System Process 4.2]).
Another important issue relates to linkages. A shared electronic health record provides a unique linkage of medical information relating to the treatment of an identifiable individual, which in HealthConnect is envisaged as part of a national identifier database. If it is accepted that participation in a shared electronic health record system should be voluntary, then it follows that there should be limitations imposed on use of unique identifiers which link information contained in that record with information contained in records generated in other contexts. Unless such limitations are imposed, then it may be possible to use the electronic record as the basis for producing a record that is more comprehensive than the record that the patient has agreed to contribute to, thereby substantially undermining patient autonomy. It is therefore imperative that a national code should include provisions that specifically limit linkages without specific consent.

The principle in the Draft Code that deals with identifiers allows an organisation to disclose its own identifier to another organisation without the individual’s consent where this use or disclosure is necessary for it to fulfil its obligations to, or the requirements of the other organisation and does not otherwise contravene NHPP 7.2(a) of the Draft Code. NHPP 7.2(b) also allows for the use and disclosure without consent of an identifier used by another organisation where this is reasonably necessary to fulfil a primary or secondary purpose of collection and does not otherwise contravene the principles. Arguably, what is required in addition is a principle along the lines of HPP 15 of the Health Records and Information Privacy Act 2002 (NSW). This precludes the inclusion of health information in a system that links health records without the individual’s express consent and the disclosure of identifiers for the purpose of allowing for the inclusion of an individual’s health information in such a system.

The appropriateness of requirements concerning the retention of records
Records retention currently depends on legislative and business requirements in different states, including archival legislation. Current state-based record disposal schedules do not adequately cover lifetime healthcare. Although the Draft Code recognises continuing business, legal and research uses in personal health records in NHPP 2.2, the purposes specified do not cover non-medical research of the kind envisaged in archival legislation.

Likewise, NHPP 4, which deals with data security and data retention, applies only in an organisational setting and not in a shared record environment. It proposes that information related to a child can be deleted once the individual attains 25 years, or in any case, 7 years after the last occasion on which a health service was provided to the individual. However, it is unclear whether the seven years applies to discrete data or to the patient’s whole record or history. Some health information may not need to be retained and is covered in disposition schedules issued by archival authorities based on triggers for removing particular types of medical information from the record. In terms of potential litigation, medical practices keep patient records even longer than seven years. Clause 4.2 (b) (ii) could instead be redrafted to read “7 years after the last interaction or encounter with the health system”, effectively for the normal expected lifetime of a person, plus 7 years. Alternatively, a longer period could be considered; for example, “30 years after the death of the patient”, which would be consistent with the code’s definition of the end of privacy.

The extent to which an individual should be able to request deletion of health information
NHPP 4 follows the approach in the Health Records Act 2002 (Vic) and the Health Records Act 1997 (ACT) and includes provision for a record found to contain inaccuracies to be held separately from the “active” record in use by the treating team. In the case of the Commonwealth Privacy Act the deletion principle is contained in NPP 10, which regulates the collection of sensitive data. That principle distinguishes between the collection of health information for the purposes of the provision of a health service, which is governed by NPP 10.2, and its collection for other purposes, which is governed by NPP 10.3. Only the latter is subject to NPP 10.4 which requires reasonable steps to be taken to “permanently de-identify” the information before disclosing it.

The question as to whether data should ever be totally deleted (as opposed to being amended or annotated) and the scope of the circumstances in which such a course might be appropriate has previously arisen for consideration in the context of applications for amendment under freedom of information legislation. The Freedom of Information Acts differ in the way in which they deal with data deletion. The Freedom of Information Act 1982 (Vic), for example, implicitly allows for data deletion using controlled authorised destruction by requiring the concurrence of the Keeper of Public Records where a correction or amendment “has the effect of deleting or expunging the information”. At the other extreme, the Freedom of Information Act 1982 (Cwlth), s. 50(3) has been amended so as to preclude deletion.

The general approach taken in Victoria and in those jurisdictions where the position is less clear is that deletion is generally inappropriate. (That approach was endorsed by the New South Wales Court of Appeal in Crewdson v. Central Sydney AHS [2002] NSWCA 345). In most cases the information privacy rights of individuals can be substantially protected by adding an appropriate amendment or annotation and ensuring that this is provided to any person who accesses or makes use of the information for decision-making purposes. This ensures that individuals are protected from the adverse consequences of decisions based on incorrect data, while preserving the historical integrity of the document. For example, the fact that incorrect data was relied upon may be relevant in the context of litigation for malpractice.

On the other hand, there may be some circumstances where information is demonstrably wrong, and its preservation, even with appropriate corrections or annotations, may result in ongoing harm to the individual whose information has been recorded. In some such cases, the relevant review bodies have required
total erasure (see, for example, re Foster & Victoria Police (1989) 3 VAR 110). Paragraph 6.7(a) of the code is apparently designed to deal with this contingency. However, it would be preferable to replace the words it is likely with the expression there is a real risk and that this should be supplemented with guidelines which make it clear that the potential harm which must be included includes potential discrimination resulting from the making of decisions which may impact adversely on the individual.

**Issues posed by the interaction between freedom of information legislation and the Draft Code**

Although the Draft Code makes it clear that it is subject to the operation of the Freedom of Information Act, the significance of this fact may be lost on those not familiar with that regime, especially patients. It is therefore vital that there should be specific guidance provided at least by way of guidelines. Persons wishing to exercise access and amendment rights contained in the code need to first of all be aware that public sector bodies are generally subject to freedom of information and that access and amendment rights in respect of personal information, including health records, held by them needs to be exercised via that mechanism.

They also need to be aware that:

- The Commonwealth public sector and the public sectors in each of the Australian states and territories are subject to the operation of Freedom of Information Acts, which, although similar in their basic structure, vary in their details.
- There may also be bodies which would appear to belong within the private sector but which are prescribed bodies for the purposes of freedom of information legislation, for example because they receive government funding.
- Conversely there are a number of public sector bodies or bodies on the periphery of the public sector which are excluded from the operation of freedom of information legislation.
- Freedom of information laws contain rights of access to documents, including health records which may be exercised by persons who are the subject of such records as well as by third parties. They also contain rights of amendment which may be exercised only in relation to the applicant’s own personal information.
- These rights of amendment are dependent on first having obtained access to the document under freedom of information legislation. (A person who has a right of amendment under the code and has not obtained access to the record under freedom of information legislation must therefore exercise this right outside of the freedom of information mechanisms.)
- The rights of access under freedom of information legislation are subject to a number of exemptions, including exemptions designed to protect personal privacy. These differ between freedom of information acts and are not identical to the exemptions in the code.
- There are requirements under freedom of information legislation to consult with persons whose personal information is contained in documents to which access is sought by other persons.
- The freedom of information acts do not deal specifically with capacity, although it has been held that a person who lacks capacity is precluded from making a request for access on their own behalf (see Wallace v. Health Commission of Victoria [1985] VLR 403). As a result, the issue of who has capacity to make a request for access or amendment of a health record may be resolved differently where the application is made under freedom of information legislation.

In summary, there is a need to address the immense complexity of the interaction between the freedom of information and information privacy laws and to provide mechanisms to assist individuals in navigating the system.

**Conclusion**

The HealthConnect Interim Research Report of August 2003 states that the development of core components of policy design work, including specific privacy arrangements, is near completion (HealthConnect 2003b). This is a matter of concern, given that the Privacy Working Group is yet to respond to the various submissions that identified weaknesses in the Draft Code (see, for example, the submission by Privacy New South Wales mentioned previously). Arguably, a national health privacy code that applies to health records that are created from many source systems and that may need to be retained for the lifetime of the patient must take account of the interaction of all relevant legislation to both protect the patient’s privacy and ensure an accurate and reliable record is available for their healthcare. It is our view that more work needs to be done on the Draft Code, and more attention given to the precise mechanisms for its implementation, before this objective can be achieved.

**References**


Reviewed articles


Acknowledgments

This article draws on research carried out in respect of a project *Electronic health records: achieving an effective and ethical legal and record keeping framework* funded by an Australian Research Council Discovery Grant, 2002-2004. Administering Institution: Deakin University. Chief Investigators: Associate Professor Danuta Mendelson, School of Law, Deakin University; Dr Livia Iacovino, School of Information Management and Systems, Monash University; Associate Professor Bernadette McSherry and Moira Paterson, Faculty of Law, Monash University.

Moira Paterson BEd, LLB(Hons), LLM (London)
Senior Lecturer and Associate Director of the Centre for Law in a Digital Economy (CLIDE)
Faculty of Law
Monash University

Livia Iacovino BA(Hons), GradDipInfoMan, MA(Archives and Records), PhD
Lecturer and Principal Researcher Records Continuum Research Group
School of Information Management and Systems; Monash University
Website: www.sims.monash.edu.au/research/rcrg/about/people.html#lv

Contact
Dr Livia Iacovino
School of Information Management and Systems
Monash University
26 Sir John Monash Drive
Caulfield East, VIC 3145
Tel: +61 3 9903 2551
E-mail: Livia.Iacovino@sims.monash.edu.au