

The draft National Health Privacy Code: unresolved issues for health records

Cassandra Gordon

Abstract

While the need for a consistent national privacy framework is well recognised, it has become even more pressing in light of the development of online health information networks which transcend existing state and territory borders. The Commonwealth Government's draft National Health Privacy Code attempts to address this need by providing a single mechanism for governing the privacy of health records nationally. This paper identifies the privacy challenges posed by e-health records and the importance of proper safeguards to protect this information. The draft Code, including a number of unresolved problems underpinning its implementation, is discussed. Although a stakeholder consultation process has been undertaken, it is argued that further debate and development is required before such an untested and fundamental change to Australia's health privacy framework can be effectively implemented.

Key words: *Confidentiality; computer security; medical records; privacy.*

Introduction

A robust privacy framework is critical to the protection of patient records from inappropriate and unauthorised access, and the handling of paper-based records is governed by such protocols in federal and state-based legislation. However, the move to collect and store clinical records electronically and access them online as part of broader health information networks means the existing matrix of privacy laws that impose different standards on different parts of the health system is not only confusing, but also outdated in the context of electronic records. In an attempt to address the self-evident need for a consistent protocol, both nationally and across the public and private sectors, a working group appointed by the Australian Health Ministers Advisory Council (AHMAC) has developed a draft National Health Privacy Code.

This paper examines the significant risks to patient privacy presented by e-health records, establishes the importance of proper controls for accessing records, and explores the suitability of the proposed Code in meeting these privacy requirements. It analyses the proposed implementation mechanisms of the Code and discusses a number of potential problems and unresolved issues of the proposed model. It is argued that because of these challenges, the Code in its current form will not provide a policy or regulatory framework to adequately meet the significant challenge of applying consistency to Australia's health privacy framework.

Protecting privacy in the e-health environment

The duty of confidentiality is a core tenet and legislative requirement of medical practice to protect patient privacy. It was traditionally based on an intimate client-professional relationship, where an individual divulged personal information to their doctor, who was responsible for any third party access to that information (Gerber 1999). While this common law requirement is clearly a necessary part of providing high quality medical care, it is becoming outmoded in the context of modern health care. The increasing use of e-health records in hospitals and general practice

means a far greater number of clinicians can access and share patient records. The global availability of medical records is needed beyond the walls of the facility where a patient is usually seen, and patients want their records to be available wherever they present themselves to seek care (Gibby and Schwab 1998). During a hospital stay it is likely that several staff will need to access patient information simultaneously, and e-health systems offer the flexibility to do this (Schoenberg and Safran 2000).

Compared with a paper-based system, e-health records can significantly increase the security of health information. This can be done by restricting access to authorised users who must prove their identity and by ensuring that information cannot be amended, lost or destroyed. Audit trails enable tracking of user access and identification of improper activity such as attempts to access unauthorised information (National Electronic Health Records Taskforce 2000).

Despite these security features, in comparison with a paper registry, storing information electronically can create a greater privacy risk, as an act of intrusion by a 'hacker' or an error by an administrator could compromise the records of a much larger number of people (Carter 1999). An important feature of protecting privacy in the context of e-health records is that consumers should be able to control and monitor access to their health information, including the level of disclosure of information appropriate to the type of care received. Unless proper privacy safeguards are in place, it is more difficult for individual patients to control the flow and exchange of e-health records, given they are likely to be accessed by a wide range of clinicians. This is considered to be a fundamental requirement for empowering consumers to take greater responsibility for managing their own health care (National Electronic Health Records Taskforce 2000). It has been observed that while the public generally has a high level of trust in existing practices for protecting the privacy of paper-based information, there is some anxiety about who can access their records if they are stored electronically (National Electronic Health Records Taskforce 2000).

This tension is magnified by the concerted effort to develop online health information networks and to

capture systemic, longitudinal health data on patients, including summaries of all interactions with the health care system. These networks would enable all health providers involved in a patient's care to access their health records, so they are instantly available when and where they are needed. In July 2000, the National Electronic Health Records Taskforce proposed a coordinated national health information network for Australia, named *HealthConnect*. The system is being developed by the federal, state and territory governments to allow summaries of health events to be collected at the point of care and exchanged electronically with authorised health care providers. Patients who suffer chronic conditions or have complex health needs would be among the first to benefit from a national system, given they often use multiple providers; however, all consumers would clearly benefit from improvements in the safety and quality of care (National Electronic Health Records Taskforce 2000).

Similarly, the federal government's *MediConnect* (formerly the Better Medication Management System) is being developed to link prescription information provided by doctors with dispensing pharmacists. This is expected to lead to better decision making and subsequently reduce adverse drug events as well as fraud, and would ultimately form the medicines component of the *HealthConnect* network (Department of Health and Ageing 2003)

The need for a nationally consistent framework

There is no single piece of privacy legislation for managing health information that applies nationally in Australia. Instead, there are different standards that apply across jurisdictions and public and private sector boundaries. This framework is complex and consists of a number of layers. Firstly, the common law requires health professionals to uphold a duty of confidentiality with respect to patient information. At the Commonwealth level, the *Privacy Act 1998* sets out the Information Privacy Principles that apply to Commonwealth agencies and, since 21 December 2001, the National Privacy Principles apply to private sector organisations. At the state and territory level, generic privacy legislation applies to public and private sector organisations in Victoria and the public sector in NSW. Health-specific privacy legislation also applies to both the public and private sectors in Victoria and the ACT (Magnussen 2002; Australian Institute of Health Law and Ethics 1998).

Clearly, this matrix of laws is confusing and inconsistent. There is an obvious need for a national approach to privacy legislation that applies to both private and public sectors. The collocation of health services, or the delivery of services collaboratively between public and private sectors, exemplify the difficulties of pragmatically applying existing privacy standards. It may be unclear to consumers what standards actually apply when receiving care, and health providers could also be uncertain of which legislation they are bound to in a particular setting (AHMAC 2002). According to the Federal Privacy Commissioner, the proposed National Health Privacy Code is the key to addressing such lack of cohesion and achieving the

required legislative consistency (Office of the Federal Privacy Commissioner 2002).

The need for national consistency has become even more critical given the substantial resources being invested in developing and implementing e-health records at both the federal and state levels (AHMAC 2002). The development of the national *HealthConnect* network is a particular impetus for the drive to finalise the development of the Code, given that a rigorous privacy framework will be fundamental to its success (AHMAC 2002). To achieve high participation rates, consumers will need to feel satisfied that appropriate safeguards are in place to protect their personal information. It is intended that patients will be able to choose whether their data is used in *HealthConnect* and control who has access to it (National Electronic Health Records Taskforce 2000). By having *HealthConnect* and *MediConnect* operating within the same national framework, it is expected that individuals can be assured that when their information is transferred to another provider who operates outside these systems, it will be handled in accordance with appropriate privacy standards. The Department of Health and Ageing recognises that unless such a framework is in place, consumers and providers will simply not use the network (Briggs 2000).

The draft National Health Privacy Code

The AHMAC Health Privacy Working Group, comprising government, provider and consumer representation, developed a draft National Health Privacy Code, released in December 2002 for five months of public consultations. The accompanying Consultation Paper states that the aim of the Code is to achieve the required consistency in protecting health privacy, while specifically taking into account initiatives proposed under *HealthConnect*. It introduces a set of rules broader than the existing legislative framework to cover all methods and situations for handling health information. These have been designed to regulate how information should be managed in the patient-health care provider relationship, and how it should be exchanged on a wider scale between sectors of the health system such as hospitals, pharmacies, insurance companies, government departments and researchers (AHMAC 2002).

To cater for e-health records, the Code has been drafted on the basis that standards for handling all forms of health information would be the same, regardless of whether they are kept in hard copy or electronic format (AHMAC 2002).

Proposed implementation mechanisms

To achieve the required national consistency, the Health Privacy Working Group proposes that the implementation of the Code should be based on one set of rules which would govern how health information is handled. These rules are outlined in the National Pri-

vacancy Principles, which stipulate standards with which all health service providers in the private sector need to comply when handling personal information.¹ It would also use a standard process for dealing with requests by individuals for access to their health information.²

While the mechanisms for implementing the Code are yet to be defined in detail by the Privacy Working Group, the Consultation Paper outlines three possible approaches:

- Option One: The application of the Code would be limited to information handled by health services only. The National Privacy Principles and/or applicable state or territory law would cover other private and public sector organisations. The advantage of this approach is that clear boundaries for the operation of the Code would apply. The disadvantage is that health organisations could not disclose information to non-health organisations that do not have adequate standards of privacy protection in place to meet the cross-border requirements set out under National Privacy Principle 9.³
- Option Two: The Code would apply to all information regardless of whether it is held in the health sector, or by other private and public sector bodies such as schools, employers and insurers. The benefit of this option is that consumers would be assured that their information is protected by universal rules, regardless of where it is held. The disadvantage to this approach is that non-health organisations would have to consider different privacy standards for different types of information.
- Option Three: A combination of Options One and Two. The Code would apply primarily to the health sector, with limited coverage of other organisations that have significant holdings of health information, such as health departments, insurance companies, and housing and welfare organisations.

The draft Code adopts Option Two, the broadest scope possible, so it would apply to all health information held by any organisation. However, the Health Privacy Working Group has stated it would revise the draft Code if health ministers decide coverage will be limited to the health sector (AHMAC 2002). If this is the case, it would contradict the original intention of developing a Code that incorporates a robust nationally consistent framework to protect the privacy of individual health information in all sectors that handle and manage this information.

¹ See *Privacy Act 1988* (Cwlth), Schedule 3, National Privacy Principles, Office of the Federal Privacy Commissioner, pp 194-203.

² This process is set out in Part 5 of the proposed Code, which is Part B to the National Health Privacy Code (Draft) Consultation Paper, pp 63-88.

³ See *Privacy Act 1988* (Cwlth), Schedule 3, National Privacy Principle 9; Office of the Federal Privacy Commissioner 2001, pp 202-203.

Unresolved issues in the draft National Health Privacy Code

In its current form, the draft Code has a number of complex political, legislative and practical issues that should be resolved before it can be finalised.

The consultation process

Policy makers need to be mindful of the requirement under section 18BB(2)(f) of the *Privacy Act 1998*⁴ which requires that the Privacy Commissioner must be satisfied that the public has been provided with adequate opportunity to comment on a draft of the Code before it can be approved.

The opinions of policy makers and consumers differ as to whether the five month consultation process has been adequate. Some commentators believe that this is an insufficient amount of time for the thorough consideration of this major policy issue that will have fundamental implications for consumers and government and private sector bodies responsible for managing health information (I-Privacy Health Privacy Consultants 2003). While this should be borne in mind, it should be noted that widespread and active consultations have occurred, including a series of public forums in state and territory capital cities and Townsville. These forums comprised representatives from the AHMAC Privacy Working Group, the Australian Government Department of Health and Ageing and the Attorney-General's Department. Several hundred participants took part in the forums and the Working Group received one hundred written submissions (Utkin, T. pers. comm. 2003). Policy makers need to be committed to continuing dialogue with key stakeholders even though the formal consultation period has been finalised. Ministers agreed at the Australian Health Ministers' Conference (AHMC) in November 2003 to refer the proposed code and implementation options to relevant state and territory departments for consideration. It is expected that these views will be tabled at an AHMC meeting at an unspecified time in 2004 (Department of Health and Ageing 2004).

Adherence to the Code

It is unclear whether the application of the Code would be mandatory or voluntary. The Consultation Paper seeks views on which would be more appropriate; however, it was clearly the original aim in developing a national health privacy code that providers and organisations would be bound by it, at least when using the proposed HealthConnect network (Briggs 2000). The former NSW Privacy Commissioner has supported the view that the Code will only be effective if it is a nationally enforceable standard (Weule 2003).

It should be noted however that there is a legislative barrier preventing the implementation of a mandatory code; the *Privacy Act 1988*⁵ excludes compulsory adherence to a Code. Under the legislation, the

⁴ See Part IIIA, Office of the Federal Privacy Commissioner 2001, p 67.

⁵ See Part IIIA, section 18BB (2)(c), Office of the Federal Privacy Commissioner 2001, p 67.

Federal Privacy Commissioner can only approve a code if membership is either by consent or voluntary (I-Privacy Health Privacy Consultants 2003). This is a fundamental issue underpinning the scope of a national framework that could hamper or prevent its implementation. If ministers do decide that the Code will be mandatory, then consideration will have to be given to the amendment of the *Privacy Act 1988* to ensure this can be achieved. It is also likely that many health providers will be unwilling to be bound by a new code, as they have already invested time and resources into conforming with existing federal, state and territory privacy regimes when delivering care.

Absence of penalties

The draft Code does not propose using penalties for breaches of health information privacy. Instead, the Privacy Working Group suggests using a balance between promoting compliance through means such as positive endorsement for organisations that are compliant, and measures such as publishing details of organisations that practice serious or repeated breaches (AHMAC 2002). Such mild measures are at variance with the view of Briggs (2001) that there should be firm sanctions and that an appropriate legislative framework for e-health records should provide rights of redress and hold liable those who misuse health information. A number of stakeholders also support the view that without appropriate penalties, the Code may not allow for adequate redress through common law to individuals whose privacy has been breached (AHMAC 2002).

Additional legislation required for e-health record initiatives

The development of online health information networks like HealthConnect means that an additional layer of regulation will probably be required to support the specific requirements of the system. The format of an electronic record itself may require additional or revised standards, particularly in relation to obtaining consumer consent for forwarding information to a national repository or linking records containing personal information (AHMAC 2002). Such standards would also need to regulate the responsibilities and obligations of providers, the purpose for which information can be used, and governance arrangements. Additional legislation would need to be carefully considered to ensure it marries with the Code and does not create additional confusion.

Difficulties in attempting to unify existing privacy regimes

Australia's health privacy framework is a complex matrix of four Commonwealth Acts and legislation in eight states and territories. It is foreseeable that the implementation of the proposed Code will create confusion given many separate and different privacy regimes already operating, some of which are incompatible and may not be able to be accommodated in a national code. For example, unlike the *Privacy Act 1988*, there

is no statutory basis in either the Health Records Acts in Victoria or the ACT for the approval of a separate privacy code, whereas the *Health Records and Information Privacy Act 2002 (NSW)* does contain a mechanism for implementing health privacy codes (I-Privacy Consultants 2003).

Achieving national consistency will require significant organisational changes. Governments would need to consider whether changes to their existing laws and administrative arrangements are required to ensure uniformity in governing health information across the public and private sectors. Additional legislation may also be required at all levels of government to enable legislative frameworks to meet the objectives of a national Code (I-Privacy Health Privacy Consultants 2003).

The confusion that could result from introducing a national regime is a challenge also encountered by the United States. Dixon points out that one of the strongest drivers of a national framework in both countries is to avoid a patchwork of inconsistent, state-based privacy laws, given their historically similar piecemeal approaches taken to privacy rules (Dixon 2001).

Conclusion

The implementation of a nationally consistent privacy framework will inevitably be fraught with obstacles. Consumers have traditionally shown scepticism that governments will use their personal information in the most appropriate way. However, before consumer confidence in a national health privacy framework can be achieved, there are several problems with the draft Code that need to be debated and resolved before it can be finalised. These include application to a limited range of sectors managing health information, application on a voluntary basis, and a possible lack of penalties and redress measures. It is also uncertain whether the consultation period satisfies the requirement for adequate consultation set out under the *Privacy Act 1988*. Nevertheless, it is critical that the key stakeholder groups, particularly consumers and health care providers, are directly engaged in further development of the Code.

A key driver for the development of the Code is to provide a national privacy framework for the operation of the HealthConnect network. While this is necessary to ensure health information is being used in the most appropriate way, there are a number of problems with the proposed Code in its current form that indicate its potential impact on existing health privacy practices would probably be limited. The draft Code lacks the precedent of a national privacy regime successfully operating alongside existing state and federal regimes; it is therefore untested and likely to encounter significant resistance and difficulty from the private and public sectors before it could be properly implemented. At the very least, fundamental organisational changes will be required to unify the Code with federal and state arrangements. Clearly, a common commitment and agreement of all governments to administer a national regime will be critical to its success. In the context of e-health records, a solution that ensures patient records are subject to clear and practical privacy rules that afford patients the discretion to deter-

mine who can access their records should remain the principal concern of policy makers.

Acknowledgments

Thanks to Dr Simon Barraclough, Senior Lecturer at the School of Public Health, La Trobe University, for his valuable comments.

The views expressed in this article are solely those of the author.

References

- Australian Institute of Health Law and Ethics (1998). *Public health law in Australia: new perspectives*. Canberra, Commonwealth of Australia.
- AHMAC (2002). *National Health Privacy Code Consultation Paper*. National Health Privacy Working Group. Canberra, Department of Health and Ageing.
- Briggs L (2000). A national approach to electronic health records. *Proceedings of the National Health Online Summit, 3-4 August 2000*, National Health Information Management Advisory Council, Canberra; online version available at <http://hima.org.au/members/journal/30_01_2001/briggs/briggs.asp>
- Carter M (1999). Protecting consumers' interests in their health records. *Australian Health Law Bulletin* 8(2): 13-16.
- Department of Health and Ageing (2003). *MediConnect website*, viewed 20 May 2003, <<http://www.mediconnect.gov.au/what.htm>>
- Department of Health and Ageing (2004). *HealthConnect website*, viewed 28 May 2004, <<http://www.healthconnect.gov.au/publications.html>>
- Dixon L (2001). Preparing for the new privacy legislation. *CyberL Res* 7, point 5.1.
- Gerber P (1999). Confidentiality and the courts. *Medical Journal of Australia* 170: 222-224.
- Gibby GL and Schwab WK (1998). Availability of records in an outpatient preanesthetic evaluation clinic. *Journal of Clinical Monitoring and Computing* 14(6): 395-391.
- I-Privacy Health Privacy Consultants (2003). *The National Health Privacy Code: when can we expect delivery?* Viewed 22 April 2000 at: <<http://www.i-privacy.com.au/?id=128.htm>>.
- Magnussen R (2002). Regulating genetic privacy in the online health information era. *Health Information Management Journal* 30(4). Electronic journal, viewed 19 June 2003, online version available at: <http://www.himaa.org.au/members/journal/30_04_2002/magnussen.asp>
- National Electronic Health Records Taskforce (2000). *A health information network for Australia: report to health ministers by the National Electronic Health Taskforce*. Canberra, Department of Health and Ageing.
- Office of the Federal Privacy Commissioner (2002). 'Commissioner Crompton welcomes draft Health Privacy Code', Media release 5 December.
- Schoenberg R and Safran C (2000). Internet based repository of medical records that retains patient confidentiality. *British Medical Journal* 321:1199-1203.
- Weule G (2003). Federal privacy legislation inadequate. *Medical Observer* 14 March: 22.

Cassandra Gordon MPH

Assistant Director
National E-Health Systems Branch
Department of Health and Ageing
Australian Government
Canberra, ACT
Email: cassandra.gordon@health.gov.au
Tel: 02 6289 8198
Fax: 02 6289 8295