

NSW Ministerial Advisory Committee on Privacy and Health Information

REPORT TO THE NSW MINISTER FOR HEALTH

PANACEA OR PLACEBO?

**Linked Electronic Health
Records and Improvements
in Health Outcomes**

NSW Ministerial Advisory Committee on Privacy & Health Information

Copyright NSW Government 2000

This work is copyright. It may be reproduced in whole or in part for study training purposes subject to the inclusion of an acknowledgement of the source and no commercial usage or sale.

ISBN: 0 7347 32570

A full copy of this report can be downloaded from the
NSW Health Web site:
www.health.nsw.gov.au

December 2000

PANACEA OR PLACEBO ?

Linked Electronic Health Records
and
Improvements in Health Outcomes

Report of
the NSW Ministerial Advisory Committee
on Privacy and Health Information

December 2000

Table of Contents

TERMS OF REFERENCE	1
MEMBERS OF THE ADVISORY COMMITTEE ON PRIVACY HEALTH INFORMATION	AND 2
EXECUTIVE SUMMARY	3
RECOMMENDATIONS	5
INTRODUCTION	8
PART ONE : ELECTRONIC HEALTH RECORDS	LINKING 9
Current Health Records	9
What is Proposed	9
NSW Health – Implementing the Health Council Reforms	10
Commonwealth Initiatives	11
Inter-relation of State and Commonwealth Proposals	13
Addressing Privacy	13
Overseas Experience	14
Benefits and Risks of an Electronic Health Record	15
Education and Training	18
PART TWO: FRAMEWORK FOR PRIVACY	LEGISLATIVE 20
Privacy Legislation in NSW	20
Commonwealth Privacy Legislation	21
Privacy Legislation – Other Jurisdictions	22
Concerns raised about current legislative framework	22
PART THREE: PRIVACY ISSUES	SPECIFIC 27

Possible Models for an Electronic Health Record System	27
Unique Patient Identifiers	27
Voluntary or Compulsory Model	30
Accountability, administration and responsibility for the EHR	32
Scope of and Information Contained on an EHR	32
Third party consent arrangements	36
Data accuracy and integrity	37
Access and amendment to health records by individuals	39
Transfer of data between health practitioners	40
Future possible uses of the data	41
Information technology issues	42
Rural Health	44
Timetable and Method of Implementation	45
APPENDIX 1 – THE OVERSEAS EXPERIENCE	46
APPENDIX 2 – WRITTEN SUBMISSIONS RECEIVED	55
APPENDIX 3 – CONSULTATIONS	57

Terms of Reference

The Terms of Reference for the Committee were determined by the Minister for Health, as follows:

- Deliver a report to the Minister that provides effective strategies to ensure NSW Health and its partners in health services delivery ensure personal health information is collected, stored and used in accordance with NSW and Commonwealth privacy principles, as applicable.
- The strategies will address issues such as:
 - a) NSW Health meeting its responsibilities under the Privacy and Personal Information Protection Act 1998, including its own Privacy Management Plan.
 - b) The implementation of Government Plan of Action for Health recommendations relevant to privacy and health information, such as the unique patient identifier and electronic health record taking into consideration work already initiated by NSW Health.
 - c) The impact of current and proposed Commonwealth legislation on privacy.
 - d) Education and training programs for health workers and consumers.
 - e) Effective privacy complaint handling programs covering access, process and service for consumers, taking into account existing processes and structures.
 - f) The promotion of excellence in privacy programs.
- The Committee will provide its final report by December 2000.

Members of the Advisory Committee on Privacy and Health Information

Mr Chris Puplick (Chair)

Privacy Commissioner and President of the Anti-Discrimination Board of NSW

Dr Andrew Wilson

Chief Health Officer, NSW Department of Health

Mr Robert Griew

Chief Executive Officer, AIDS Council of NSW

Prof Katherine McGrath

Chief Executive Officer, Hunter Area Health Service

Assoc Prof Lindsay Thompson AO

Chair, Canterbury Division of General Practice and Member, General Practitioner Advisory Committee, NSW Department of Health

Dr Kristen Kerr

Director, Missenden Unit, Department of Psychiatry, Royal Prince Alfred Hospital

Ms Char Weeks and Mr Geoff Sayer

Health Communication Network

Ms Amanda Adrian

Health Care Complaints Commissioner

Dr Norman Swan

Presenter of the Health Report, ABC Radio National

Ms Amanda Cornwall

Public Interest Advocacy Centre

Mr Tim Dixon

Baker and McKenzie, Solicitors and Attorneys
Chair, Australian Privacy Foundation

Executive Summary

Electronic health records are already a feature of the health system in both the public and private health sectors in NSW and their use is increasing. Their wider introduction is inevitable. The primary challenge of this development is to maximise both the protection of individual privacy and positive health outcomes.

While the mere existence of electronic health records poses limited privacy risks to the health consumer, this risk dramatically increases when health records in electronic format are linked.

An electronic health record residing on a stand alone computer in a general practitioner's surgery or other facility provides minimal opportunities for unauthorised, external access. However, when the stand alone computer is connected, especially via the internet, allowing all or parts of the electronic health record to be exchanged with other health service providers, control over access to and security of the information is compromised.

This is the primary privacy concern regarding electronic health records: not that the records are created but the fact the records can be transferred via communication links leaving the health consumer unable to be certain who is accessing their health information.

Controls and safeguards over access to electronic health records must be established to ensure that there is maximum public confidence in a health system where transfer of confidential information will become more routine.

The NSW Department of Health has in place a Health Information Privacy Code of Practice.¹ The Code applies to personal health information, which is held by: the Department of Health; the public health system; the NSW Ambulance Service; and non-government organisations receiving funding from the Department where compliance is included in the terms of their funding agreements. The Code also applies to any private health care agencies or practitioners, researchers or others who have authorised access to personal information owned by the public health system. While the Code sets very high standards of practice, the Report of the NSW Health Council found that there are "inconsistent standards about privacy and confidentiality" within the system.² One of the major shortcomings is that the penalties imposed for breaches are largely determined by each Area Health Service and are reliant on a complicated combination of internal disciplinary procedures, conciliation by the Health Care Complaints Commissioner and contractual law, depending on who is alleged to have committed the breach.

There is also a range of health related legislation which imposes privacy and confidentiality obligations on people working in the NSW Health System. This legislation includes the *Health Administration Act 1982* (s. 22), the *Mental Health Act 1990* (s. 289) and the *Public Health Act 1991* (ss. 75, 17). These provisions again vary in their coverage.

¹ NSW Health, *Information Privacy Code of Practice*, Second Edition, December 1998, available at <http://www.health.nsw.gov.au/fcsd/rmc/circulars/1999/cir99-18.pdf>

² *Report of the NSW Health Council - A Better Health System for NSW (the "Menadue Report")*, NSW Government, 2000, p. 21;

The information protection principles in the NSW *Privacy and Personal Information Protection Act 1998* cover only the public health system and the Committee believes that the recently introduced amendments to the federal *Privacy Act 1988* are inadequate in relation to the security of health information. This is due to the number and breadth of exemptions both to the Act in general and to specific provisions (especially access to and correction or annotation of information), the inconsistency of complaints handling mechanisms and the lack of meaningful and consistent penalties for breach. What is required for a system of linked electronic health records to work is a discrete piece of legislation which covers health information privacy in a comprehensive fashion. The legislation must cover all health information regardless who holds and maintains it, and must provide a strong, clear and transparent framework for privacy protection.

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

The Committee feels it should be the responsibility of the consumer to indicate to his or her health provider which data are restricted in relation to its transfer and this information must then remain non-transferable unless and until the health consumer consents to that information being shared and exchanged.

A system which is simple to operate is likely to be complied with more readily. The challenge for the health system and for software developers is to build computer systems that will allow such a consent regime to work in a simple manner. This will mean that health records may need to be maintained with different levels of data recording depending on the regime applicable to its potential transfer.

For the benefits of a system of linked electronic health records to be maximised, a unique patient identifier is necessary to facilitate the linking of different electronic health records and for the transfer of information between health care providers.

The unique identifier must be specific to an individual, and must be of the highest integrity.

A system of unique patient identifiers based upon proof of individual identity must not discourage contact with the health system or marginalise sections of the community. In particular, services currently available on an anonymous basis must continue to be so available.

The proposed health information privacy legislation must include safeguards to ensure that use of a unique patient identifier does not creep into other uses. It should be used to link electronic health records and nothing else, unless specifically authorised by legislation.

While it will be some time before a comprehensive system of linked electronic health records is established, it is important that the concept is adequately piloted and evaluated before widespread implementation.

It is important that the public is adequately informed of and consulted about the progress of implementation including the mechanisms to safeguard privacy of health information. This will assist in developing public confidence and understanding the ramifications of a linked electronic health record system.

RECOMMENDATIONS

1. That NSW Health proceed with the development of a system of linked electronic health records across the State which seeks to maximise both the protection of personal privacy and the positive public health outcomes which may be obtained.
2. That such a system be based upon the following principles:
 - (a) the system must operate for the measurable benefit of individual health consumers and the improvement of public health outcomes as its primary goals;
 - (b) the system must be designed so that all stages and operations reflect an appreciation of and a commitment to the maximum degree of protection for the privacy of individuals and communities;
 - (c) the patient/consumer must have the right to ensure that particular information on any health record is excluded from automatic transfer to other authorised recipients of such information except with the patient/consumer's express consent;
 - (d) the system must have the highest level of physical security and integrity incorporated in every component and level and at every point of access and transfer;
 - (e) that the data in the system be as complete, accurate and up to date as can be achieved.
 - (f) the system must have adequate and transparent audit trails which will allow for clear identification of all access obtained to the information contained therein.
3. That the system of linked electronic health records be governed by a separate and specific piece of State legislation entitled the Health Records and Information Privacy Act.
4. That the Health Records and Information Privacy Act:
 - (a) apply to all health records, in whatever form kept, in both the public and the private sectors of health care and health care delivery in New South Wales;
 - (b) specify the purposes for which health records may be linked and transferred so that no linkage or transfer may take place without specific legislative authority;
 - (c) incorporate the Information Protection Principles as set out in Part 2 of the *Privacy and Personal Information Protection Act 1998* modified as and if required to meet the specific needs of the health sector;
 - (d) establish protocols and provide mechanisms whereby linked electronic health records (or parts thereof) can be transferred between authorised parties;

- (e) provide for the right of inspection, access, copy, annotation and correction of any health record by any person who is the subject of such a record, except where exceptional circumstances (to be defined clearly in the legislation and which relate to the protection of the welfare of such a person) apply;
 - (f) vest in the Privacy Commissioner of New South Wales the powers to:
 - investigate and determine complaints made under the Act
 - initiate investigations and conduct enquiries and audits relevant to the conduct and administration of the Act
 - make reports and recommendations to the Minister and Parliament regarding the administration and operation of the Act.
 - (g) establish mechanisms for allowing complaints related to alleged breaches of privacy and other improper conduct to be made and determined
 - (h) impose significant penalties of both a civil and criminal nature for breaches of the Act;
 - (i) incorporate (either directly or by cross-reference) all existing privacy and confidentiality requirements present in various existing health-related statutes of New South Wales.
 - (j) give specific recognition to particular problems related to the capacity of children to withhold information from their parent or guardian in particular circumstances.
5. That relevant agencies, including Privacy New South Wales (the Office of the Privacy Commissioner), the Health Care Complaints Commission and relevant professional registration boards be resourced adequately for the discharge of responsibilities imposed under the Health Records and Information Privacy Act.
 6. That a comprehensive programme of community consultation be undertaken in the development of the Health Records and Information Privacy Act which should be introduced as soon as practical into the Parliament of New South Wales.
 7. That the introduction of the Health Records and Information Privacy Act be accompanied by a comprehensive education campaign directed at both the general public and health providers supported by adequate training being provided to users of the system of linked electronic health records.
 8. That such education, information and training campaigns be monitored and evaluated by the Privacy Commissioner on an on-going basis as part of his/her responsibilities under the Health Records and Information Privacy Act with regular reports being provided to the Minister.
 9. That the opportunity provided by the introduction of the Health Records and Information Privacy Act to improve the quality of health records generally be taken. This improvement should encompass issues such as data standards

and accuracy; uniformity of nomenclature and standardisation of recording and reporting requirements.

10. That a system of Unique Personal Identifiers be introduced to support the system of linked electronic health records on a State-wide basis. In that regard:
 - these Unique Personal Identifiers must be identifiers of the highest integrity;
 - they should be generated by either the Department of Health itself, or in a co-ordinated fashion by the Area Health Services;
 - the Medicare number should not be used for this purpose and the State-wide Unique Personal Identifier should not be linked directly to the Medicare number.
11. That the New South Wales Government and New South Wales Health recognise that there will be special circumstances in which people will, quite properly, seek to access health services on an anonymous basis. Nothing should be done to prevent, penalise or discourage such legitimate access to health services in the absence of any person using a Unique Personal Identifier.
12. That linked electronic health records not be accessible for data-matching and data-mining exercises outside the NSW health care system, unless such exercises are authorised specifically by New South Wales Health and the Privacy Commissioner.
13. That research projects seeking access to linked electronic health records be dealt with by a mechanism which reflects the provisions of sections 95 and 95A of the *Privacy Act 1998* (Cth) and the relevant *Guidelines* issued from time to time by the National Health and Medical Research Council.
14. That New South Wales Health publish a timetable consistent with the recommendations of the Health Council (Menadue) Report for the introduction of linked electronic health records in New South Wales and the enactment of the Health Records and Information Privacy Act.
15. That the recommendations of the Health Council Report in relation to the piloted, staged and progressive implementation of a State-wide system of linked electronic health records be endorsed and followed. At least one of the pilot projects should be based in an Area Health Service in rural or remote NSW.

Introduction

This report focuses on the privacy concerns which may arise from the implementation of the proposed new health system across NSW based on a unique patient identifier(s) and linked electronic health records.

The concerns exist because the advent of unique patient identifiers and linked electronic health records will make individual's health information much more accessible, not only to health practitioners and hospitals but to a wide range of interested third parties.

The NSW Ministerial Advisory Committee on Privacy and Health Information ('the Committee') was appointed by the NSW Health Minister in June 2000 to investigate and advise on privacy issues relating to health information, particularly those raised by the proposed linked electronic health record and the unique patient identifier.

The Committee met on seven occasions and consulted widely.

In August 2000, the Committee placed advertisements in leading metropolitan newspapers and wrote to over 500 individuals and organisations, calling for submissions.

The Committee received 42 written submissions from a range of individuals and organisations (The full list of individuals and organisations from whom the Committee received submissions is included at Appendix 3.). The submissions provided a valuable insight into the potential privacy issues posed by the implementation of linked electronic health records and some possible strategies for addressing such concerns.

Two public forums were held at the NSW State Parliament in November. The forums reinforced many of the views expressed in the submissions and highlighted additional issues for the Committee's attention.

A workshop was also conducted as part of the Consumers Health Forum national consultation process regarding electronic health.

The Committee was briefed fully by representatives of the Department of Health on the steps already undertaken by the Department to promote the use and linkage of electronic health records and the implementation of various parts of the Government's Action Plan for Health. The Committee also met separately with key personnel specialising in the complex areas of mental health policy and service delivery.

The recommendations of this Report reflect many of the concerns expressed in the various submissions and public meetings, together with the views presented by the Department of Health and the opinion of the Committee members. They have been distilled into recommendations which the Committee believes address all those concerns in a realistic and practical fashion.

PART ONE :Linking Electronic Health Records**Current Health Records**

Individual health records are held by a number of health providers, including public and private hospitals and individual practitioners. Records may be written, stored electronically or a combination of both. In some instances they are maintained in discrete locations (eg on a stand-alone computer, or practitioner's file), and in other situations may be held on a networked system accessible by a range of health providers.

In some cases a person may be able to take their records with them if they move (eg interstate), but in most cases the records remain the property of the hospital or health provider with continuity of care delivered via referrals or follow-up communication between providers.

In NSW, some Area Health Services have been working on new ways to link patient records within an area health service. Four of the Area Health Services (AHS) in NSW have developed Unique Patient Identifier systems to assist in managing their records. All of these Areas have set up different systems, but what they have in common is the possibility for linking individual health records across health providers within that particular area.

For example, Central Sydney Area Health Service (CSAHS) has introduced a Clinical Information System that provides clinicians with a comprehensive view of a patient's visit history and selected results. Over the next few years, CSAHS plans to extend the type of information held in this system to gradually replace the paper medical record.³

What is Proposed**NSW Health Council reforms**

In March 2000, the Report of the NSW Health Council (the Menadue Report) made a number of recommendations for reforming the health care system in NSW. These included proposals to improve access to health information for both health care providers and consumers.

To address shortcomings of the existing information infrastructure, the Council recommended that:

- The NSW and the Commonwealth Government work together to develop an Electronic Health Record for every individual in NSW
- As a first step towards developing Electronic Health Records, NSW Health take action to improve the links between patient information systems within hospitals (such as transferring information from an Emergency Department to the wider hospital), between hospitals and community health teams and between hospitals and GPs

³ Central Sydney Area Health Service, Submission no 27, pp 2 – 5

- NSW Health establish a Unique Patient Identifier (UPI) for every individual in NSW, so that health care providers can identify with certainty the particular patient they are dealing with, irrespective of where the patient has entered the health system.⁴

The Council outlined a number of possible features of the Electronic Health Record (EHR), including:

- It will be accessible to the individual consumer and their providers, regardless of location and with appropriate attention to privacy and security safeguards
- The individual will need to give consent about the type of information made available, and the transfer of information between providers
- The record will contain clinical records, advice, specialist referrals, pharmacy details, diagnostic tests and results
- The Electronic Health Record will be able to provide GPs, specialists, public and private hospitals, community health centres, and other health providers with access to relevant information about an individual's medical history with the patient's consent
- It will facilitate the use of computerised discharge summaries
- It will be linked to clinical protocols and clinical pathways and assist the health care provider in clinical decision-making
- An information system based on the Electronic Health Record will allow the collection of data that can be used to measure the quality and performance of health care provision, and to assist the consumer in making informed health choices.⁵

The Council outlined an implementation process based around demonstration projects to be established in at least two Area Health Services. It recommended that implementation of the Electronic Health Record should allow for proper evaluation and negotiation of relevant privacy issues, and its introduction must be on a voluntary basis for patients.⁶

As part of implementation of the Electronic Health Record, the Council raised the possibility of a Health Smart Card for each individual. The Health Smart Card would act as a pointer to how information could be accessed and identify the type of information that is held. The Council recommended that NSW Health investigate the use of a Health Smart Card as a means of increasing consumer control over information, and that consumer groups should be involved in its development and implementation.⁷

NSW Health – Implementing the Health Council Reforms

⁴ NSW Health Council, Report of the NSW Health Council, March 2000, p xvii

⁵ Report of the NSW Health Council, pp 23-24

⁶ Report of the NSW Health Council, p 27 and p 89

⁷ Report of the NSW Health Council, p24

Since the Health Council recommendations in March 2000, there have been a number of new developments with the proposed implementation of an Electronic Health Record (EHR) and Unique Patient Identifier (UPI).

In response to the Menadue Report and the Sinclair Report⁸, a Government Action Plan for health has been developed outlining the implementation process, including plans for the roll-out of an EHR and UPI.

The NSW Health Information Management Implementation Co-ordination Group (IMICG) has been established within the Department of Health to implement the Health Council recommendations relating to management of health information.

The following points from the IMICG submission reflect the current status of the NSW Health EHR proposal:

- NSW Health is proposing to implement a state-wide Unique Patient Identifier (UPI) by November 2002. This would be preceded by Area UPIs by June 2002. The approach being taken will support any initiatives undertaken at a national level to implement a national unique identifier. The introduction of a UPI is viewed as an essential precursor to the EHR.
- The NSW Health state-wide Client Data Linkage proposal is based on Area Wide identifiers supported by a statewide linkage mechanism. This linkage is two way and would allow patient event data to be made available across individual health services with informed consent.⁹

In November the IMICG produced a detailed strategy for the introduction of UPIs. Pre-eminent in the strategy's recommendations was to await the outcomes of the work conducted by the Ministerial Advisory Committee on Privacy and Health Information before proceeding further.

A Health Smart Card is no longer part of the proposed system. The view of the Department is that the current state of smart card technology is not sufficiently advanced to provide the necessary technical platform to support the data and security requirements of the electronic health record. As such, the Ministerial Advisory Committee has decided to make no further comments of its own in relation to health smart cards, but draws attention to an earlier report of the Privacy Committee of NSW on the broader issue of smart cards and privacy.¹⁰

Commonwealth Initiatives

At the same time as NSW Health is working on the reforms described, a number of parallel initiatives have been announced by the Commonwealth government.

⁸ Ministerial Advisory Committee on Health Services in Smaller Towns, Report to the NSW Minister for Health, *A Framework for Change*, February 2000; available at <http://www.health.nsw.gov.au/health-public-affairs/wayforward/sinclair.html>

⁹ NSW Health Information Management Implementation Coordination Group (IMICG) Submission no 30, p4

¹⁰ Privacy Committee of NSW, *Smart Cards: Big Brother's Little Helpers*, August 1995; available at <http://www.austlii.edu.au/au/other/privacy/smart/index.html>

HealthConnect

HealthConnect is a proposal put forward by the federal Department of Health and Aged Care and endorsed by all Australian Health Ministers for an Australia-wide network for exchanging health information online.

Under HealthConnect, health-related information about a person would be collected and held in a standard, electronic format at the point of care (such as a hospital or a GP's clinic). The information held will take the form of standardised event summaries. These would include information such as results of health treatments, hospital discharge reports, referrals, pathology test results, medication and diagnostic test results. With the consumer's consent, these summaries would then be exchanged via a secure network between health care providers authorised by consumers to access the information.¹¹

Five principles have been agreed to by the National Electronic Health Records Taskforce to ensure HealthConnect protects and enhances privacy. These are:

- Individuals must freely agree to participate in the network in the first place and on a continuing basis.
- An individual's information must only be used in a health care context
- People must have access to their own information and must be able to control who can see their information
- A stringent security framework must be in place wherever health information is collected, stored or exchanged, including audit trails and review mechanisms built into the network to track who has access the information
- Tight laws must be introduced to ensure, among other things, penalties for people who misuse the information.¹²

MedicineConnect

The other significant proposal by the Commonwealth Government is MedicineConnect (formerly known as the Better Medication Management System or BMMS). The MedicineConnect scheme involves the establishment of a database that records prescriptions written for individual patients by different prescribers and dispensed by different pharmacists. Under the provisions of the *National Health Amendment (Improved Monitoring of Entitlements to Pharmaceutical Benefits) Bill 2000*, a three stage scheme will be introduced which, by 1 July 2001, will provide for all prescriptions to be linked with a Medicare number. Pharmacists will be required to ask all consumers to provide their Medicare number for entry onto a prescription record and (with certain limited exceptions) pharmacists will be denied payment for prescriptions which are filled without a Medicare number being attached.

¹¹ National Electronic Health Records Taskforce, *An Introduction to Health Connect*, July 2000 pp 2-3

¹² National Electronic Health Records Taskforce, *An Introduction to Health Connect*, p 4

Inter-relation of State and Commonwealth Proposals

While both State and Commonwealth governments, and the Australian Health Ministers Advisory Council (AHMAC) have agreed to work together on the implementation of linked electronic health records in Australia, it is not yet clear exactly how this collaboration will operate in practice or how the NSW and Commonwealth initiatives will co-exist.

While the NSW Health Department has strategies in development for the co-existence of State and Commonwealth initiatives, clarification is still required as to whether the proposed Commonwealth initiative, *HealthConnect*, will draw upon the NSW electronic health record system being developed, or whether it is to be another system super-imposed over the State system. It also remains to be seen how a State Unique Patient Identifier (UPI) will co-exist with a possible national identifier implemented through the *HealthConnect* system and the Better Medication Management System.

In order to be clear about the privacy legislation which applies to the EHR proposal, it will be necessary to be clear about how the State and Commonwealth proposals interact. This is because there is different privacy legislation which applies to NSW and Commonwealth bodies, and to the public and private sector.

Even at the local level, it is not clear how an Area Health Service system will interact with the proposed NSW Electronic Health Record. For example, it is not understood whether the NSW EHR system will comprise of several smaller (for example, Area Health Service) systems linked together, or whether it will be a centralised system.¹³

A national system could either involve implementing the same system throughout Australia, or alternatively establishing a system of national standards to be agreed to and implemented by individual states.

Addressing Privacy

Apart from the work of the Committee, other processes have been established to ensure that the EHR system is not implemented until strategies are in place to ensure privacy standards will be met.

In NSW Health, the Information Management Implementation Coordination Group (IMICG) responsible for implementing the NSW health reforms has also established a Privacy Working Group with representatives from each of its sub-committees. The role of this Group is to identify and address privacy issues across all aspects of the implementation process.

The Australian Health Ministers Advisory Council (AHMAC) recently formed a joint Commonwealth/State/Territory Health Information Privacy Working Group. The aim of this group is to establish a nationally consistent regime for the protection of health information that applies to both the public and private sectors of the health industry.¹⁴

¹³ Central Sydney Area Health Service, Submission no 27, p4

¹⁴ See Commonwealth Department of Health and Aged Care, Submission no 8, p 3; Office of the Federal Privacy Commissioner, Submission no 34, p 3

Overseas Experience

(For more detail refer to Appendix 1)

In the United States, the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) outlines a process to achieve uniform national health data standards and health information privacy. Enacted with the widespread support of the health care sector and bipartisan support in the Congress, the law requires that the Secretary of Health and Human Services (HHS) adopt standards to support the electronic exchange of a variety of administrative and financial health care transactions.

On November 3, 1999, HHS published a proposed regulation to protect the privacy of health information.¹⁵ Once this health information privacy regulation is in effect, the Office for Civil Rights (OCR) within HHS will be responsible for enforcement. OCR's responsibilities will include issuing exception determinations and advisory opinions, providing technical assistance, receiving and investigating complaints, conducting compliance reviews, and seeking civil monetary penalties if voluntary compliance cannot be obtained. The final Rule and its related regulations were published in the US Federal Register on December 19, 2000 and will become effective on 18 February 2001 (sixty days later).¹⁶

The United Kingdom, Canada and New Zealand have all made some progress towards investigating and implementing an EHR system. However, none has yet implemented a comprehensive national system, and all look somewhat off achieving this goal.

What is in place is a number of local developments and numerous pilot studies which have been conducted of the broader proposals.

In all instances, the privacy of health information has been acknowledged as a key issue, though the extent to which privacy is being addressed as an integral part of the implementation processes varies.

In New Zealand, consistent privacy legislation in the health sector has been in place for a number of years and work on health privacy issues has been at the forefront of the concerns of the NZ Privacy Commissioner.¹⁷ This, together with the fact that New Zealand does not have the complexities of a federal system, mean that there are already well established and widely accepted standards for privacy in place across the country.

Both New Zealand and the United Kingdom have in place widespread unique identifier systems within the public health sector that are being given a role in the proposed electronic health systems, though in both instances it would appear that attempts are being made to limit the further use of this identifier outside the public health system.

Canada displays many similarities to the Australian situation. In relation to privacy legislation, there is a privacy framework that consists of a federal public sector Act, recently introduced private sector legislation and a patchwork of provincial legislation

¹⁵ Available at <http://aspe.hhs.gov/admsimp/nprm/pvclist.htm>;

¹⁶ see Appendix One, below ; the text of the final rule is available at <http://aspe.hhs.gov/admsimp/FINAL/Final%20Privacy%20Rule.pdf>

¹⁷ see <http://www.privacy.org.nz/shealthf.html>;

to work under this. The key difference appears to be in the way in which the e-health initiatives are being implemented, and the way privacy issues are being handled. The federal proposal for the Canada Health Infoway appears to have established a much clearer strategy for how such a system will be implemented across different levels of government than the Australian Commonwealth HealthConnect Proposal.

A common criticism of all the e-health proposals discussed appears to be the lack of widespread public consultation on what is actually proposed and the implications of this for how individual's information will be handled. Along with this is an acknowledgement that, without public support, the systems cannot work.

The possible lessons to be gained from overseas experience are salient and have strong relevance to the situation in NSW.

The lessons are:

- A consistent, strong legislative based health privacy regime which is widely accepted by health providers and consumers is essential
- Any unique identifier should be strictly limited in its use to the e-health system only (and prohibited by legislation against further uses) and it must be applied across the system
- Implementation of both the e-health initiatives and the privacy standards within those initiatives will be more successful if implemented from the local level in the first instance and not applied from above as a large, national system
- To be successful, any system must first of all be developed and implemented by a process in which public consultation and input is maximised to gain wide public support.

Benefits and Risks of Linked Electronic Health Records

During the Committee's consultation process it became evident that some groups support the electronic health reforms while others are not convinced that the benefits being put forward will in fact occur. This highlights the need for some objective analysis of the claims made about the potential impact of the proposed EHR on the provision of health care services. Despite the progress made already towards use of linked electronic health records and universal patient identifiers, the Committee does not believe such an analysis has yet been undertaken anywhere in Australia.

According to the Public Interest Advocacy Centre, public debate about privacy implications on linked patient records needs to have as its starting point an agreement as to the public benefits offered by an EHR and the risks involved. There needs to be open debate about whether such a significant diversion of funds from direct health service delivery is justified in terms of producing better health outcomes.¹⁸

As an example, consider the question: Will an EHR reduce the risk of adverse events, or potentially increase the risk of this? According to one view, an EHR provides a more complete and accurate record of a person's medical history, allergies and medications, and if other health care providers have access to this information, the

¹⁸ Public Interest Advocacy Centre (PIAC), Submission no 29, p 6

risk of adverse events (eg when prescribing medication, or treating a person in an emergency situation) is reduced. The other view is that although an EHR provides some information about a person's medications etc, it cannot be relied upon as a complete medical history as there are many reasons that certain data may be missing and/or inaccurate. Relying on information that is incomplete and inaccurate is in fact dangerous, and may in itself lead to serious adverse events. Interestingly, the groups arguing each of these positions provide some research or case studies to support their argument, but there does not appear to be detailed research which brings together both sides to assess or balance/evaluate the overall risk/benefit.

The uncertainty of the benefits of an investment in an electronic health record infrastructure was aired at both public forums and the question was asked of the opportunity cost and whether the considerable investment in the information technology infrastructure to implement pervasive electronic health records would result in better health care.

The NSW Branch of the Australian Medical Association, in its submission to the Committee, remarked that the many ramifications of electronic health records will only become apparent when such a system is in place and after a significant investment has been made.¹⁹

The following list provides a brief summary of the benefits and risks highlighted in the submissions received by the Committee.

Potential benefits

A system of linked electronic health records has the potential to:

- Improve health outcomes by increasing opportunities for coordinated and continuous of care within the health care system;
- Provide health providers with access to a more comprehensive patient history, and therefore improve clinical decision making;
- Allow consumers to access their own records;
- Be used as a tool for sharing information between health providers and consumers;
- Reduce the reliance on the patient's own memory to provide a medical history;
- Reduce possible errors in information transfer, and therefore preventable adverse events;
- Reduce duplication of diagnostic testing and imaging, and hence reduce costs;
- Improve accountability for health care decision making by making available a better quality of data
- Make more data accessible for research purposes;
- Bring together fragmented and dispersed information about an individual to a single accessible point;
- Track the use of critical implantable medical devices;
- Improve communication between practitioners and people with disabilities by providing a continuous medical record, particularly where the person has difficulty communicating or where the person has little family support.

¹⁹ Australian Medical Association (NSW), Submission no 41, p 1

Potential risks

Potential risks associated with the implementation of a system of linked electronic health records are:

- The threat to the confidentiality provided by the doctor/patient relationship;
- Sensitive data could be accessible to a wider range of health providers, thereby increasing the risk of misuse or unauthorised disclosure;
- With electronic format for health records, there may be increasing pressure and demands for access to the information by non-health care bodies (eg insurers, employers, law enforcement, some government agencies)
- That the 'continuity of care' benefits may not actually eventuate and that it is difficult to assess the research on this;
- The placing of a large amount of personal health data (and therefore power) in the hands of the government where it may be unnecessary and inappropriate for it to hold this information;
- Difficulty in identifying and correcting errors on the linked EHR;
- Consumers may be prevented from accessing genuine second opinions;
- Possible rationing of health resources;
- Factual 'summaries' of health diagnosis may present a subjective opinion in a factual manner because of the need to summarise, and information is open to mis-interpretation by another provider;
- The benefits for the community proposed by EHR may not produce best outcomes for some individuals, and the system may favour community outcomes over individual needs and interests; and
- Fear that some information (eg about mental illness or disabilities) may result in people being treated in a discriminatory manner if the information is more widely available.

Conclusions

The Committee recognises that the increasing use of electronic health records is a logical and inevitable part of the process of computerisation of information. However, whether, to what extent and how such records are linked can and should be controlled and regulated.

While the intention of the Committee's public consultation process was to focus on the issues of health information privacy, it was increasingly confronted by the broader issues associated with linked electronic health records and unique patient identifiers.

The Committee has formed a view that considerable work needs to be undertaken by the NSW Health Department to clearly and concisely communicate to and consult with the public about the proposal to introduce transferable electronic health records.

More importantly, work needs to be done to demonstrate and articulate the benefits of such a system and the reasoning behind the investment required.

This needs to be undertaken to both educate and engage the public.

The linking of electronic health records cannot proceed without gaining the confidence of the public that the introduction of such a system is in their best health interest and does not present unacceptable risks to privacy.

The Menadue report noted that the introduction of an electronic health record that can be shared and exchanged throughout the health system must commence with and be evaluated through a number of demonstration projects.²⁰

The outcomes of these pilot projects must be used to communicate the benefits and risks of the system to health consumers.

Education and Training

It is crucial for the success of any system of linked electronic health records that an extensive and ongoing program of education and training for users precedes and accompanies its implementation. This education and training should focus, not just on the effective operation and use of the system, but on the requirements of the recommended privacy legislation (see below). Such an exercise was undertaken with regard to the NSW public sector at the time of the introduction of the *Privacy and Personal Information Protection Act 1998*.

Moreover, significant resources will need to be devoted to any public education campaign about the benefits and potential risks of the system. This campaign will need to include education about the individual's right to "opt-in" (or not) to the system and of his or her continuing right to "opt out" of the system with respect to particular items of information or entirely. This campaign should also contain an explanation of the individual's right to access and correct or annotate records and to complain about privacy breaches.

Such a campaign should be designed by specialists in education and training, drawing upon the support of information technology and health experts. It should include training which will emphasise and promote excellence in privacy protection and will need to be subject to regular and detailed evaluation.

Recommendations

[Please note that, in the text, recommendations will be referred to according to the numbers assigned to them in the list of recommendations on page 6, above.]

1. *That NSW Health proceed with the development of a system of linked electronic health records across the State which seeks to maximise both the protection of personal privacy and the positive public health outcomes which may be obtained.*
2. *That such a system be based upon the following principles:*
 - (a) *the system must operate for the benefit of individual health consumers and the improvement of public health outcomes as its primary goal;*
 - (b) *the system must be designed so that all stages and operations reflect an appreciation of and a commitment to the maximum*

²⁰ Report of the NSW Health Council, p 25

degree of protection for the privacy of individuals and communities;

- (c) the patient/consumer must have the right to ensure that particular information on any health record is excluded from automatic transfer to other authorised recipients of such information except with the patient/consumer's express consent;*
 - (d) the system must have the highest level of physical security and integrity incorporated in every component and level and at every point of access and transfer;*
 - (e) that the data in the system be as complete, accurate and up to date as can be achieved; and*
 - (f) that the system must have adequate and transparent audit trails which will allow for clear identification of all access obtained to the information contained therein.*
6. *That a comprehensive programme of community consultation be undertaken in the development of the Health Records and Information Privacy Act which should be introduced as soon as practical into the Parliament of New South Wales.*
7. *That the introduction of the Health Records and Information Privacy Act be accompanied by a comprehensive education campaign directed at both the general public and health providers supported by adequate training being provided to users of the system of linked electronic health records.*
8. *That such education, information and training campaigns be monitored and evaluated by the Privacy Commissioner on an on-going basis as part of his/her responsibilities under the Health Records and Information Privacy Act with regular reports being provided to the Minister.*

Part Two: Legislative Framework for Privacy

Presently, there is no single, comprehensive piece of privacy legislation in NSW applying to the private and public sectors. Rather the legal framework applying to health care information consists of a number of layers, and includes:

- Privacy legislation in NSW applying to public sector agencies;
- Health-related legislation, with specific provisions on confidentiality;
- Federal privacy legislation for the private sector in Australia, which has not yet commenced;
- Common law medical confidentiality obligations applying to practitioner-patient relationship;
- Various laws requiring the mandatory reporting of information by practitioners, including public health and child protection legislation.

One of the key issues before the Committee is the adequacy of the current legislative framework for privacy and health information in NSW, and whether it provides sufficient privacy protection to support the proposed linked EHR system.

Privacy Legislation in NSW**Privacy and Personal Information Protection Act 1998**

The *Privacy and Personal Information Protection Act 1998* came fully into effect on 1 July 2000. The Act establishes the Office of the NSW Privacy Commissioner, and introduces a set of 12 Information Protection Principles which regulate the way NSW public sector agencies deal with personal information.

The definition of 'personal information' includes any information that relates to an identifiable person. It covers not only traditional paper files, but any other record that would reasonably allow a person to be identified including electronic files, video recordings, photographs, genetic material and biometric information such as fingerprints. Personal information would therefore also include blood and tissue samples, x-rays and pathology results.

Key features of the legislation include:

- Coverage - It imposes binding principles only on public sector agencies, not the private sector. There is however provision in the Act for people to complain to the NSW Privacy Commissioner about any alleged breach of privacy, including actions by private sector organisations or individuals.
- Codes of Practice – Under the Act, and agency can make a Privacy Code of Practice to allow an exemption from, or modification to, any of the Information Protection Principles in the Act. Codes must first be submitted to the Privacy Commissioner for comments, and approved by the Minister. The NSW Health has made a Code under the Act modifying the way a number of the principles apply to the activities of NSW Health.²¹
- Privacy Management Plans – Each agency covered by the Act is required to prepare a Privacy Management Plan outlining how it plans to comply with the

²¹ available at <http://www.lawlink.nsw.gov.au/pc/pages/pcphealth>

requirements of the Act. The Department of Health has its own Privacy Management Plan, issued as Circular 2000/62 on 26 July 2000.²²

- Internal Reviews – Individuals have the right to seek a review by an agency where the individual believes their privacy has been breached. The primary responsibility for the review lies with the agency, although the Privacy Commissioner can undertake a review on behalf of an agency if the agency requests.
- Remedies under the Act – If an individual is not satisfied with the outcome of an internal review, they can appeal to the Administrative Decisions Tribunal (ADT).

Commonwealth Privacy Legislation

The federal *Privacy Act 1998* applies to information held by Commonwealth and ACT *public sector* agencies. The Act is based around 12 Information Privacy Principles on collection, storage, use and disclosure of personal information, as well as providing individuals with a right to access and correct their own personal records.

The *Privacy Amendment (Private Sector) Bill 2000* was introduced into Parliament in April 2000. It was passed, as the *Privacy Amendment (Private Sector) Act 2000*, by the House of Representatives and the Senate in early December 2000. It comes into effect on 21 December 2001. The Act amends the federal Privacy Act 1988 to extend coverage to the private sector in Australia.

The Act introduces a 'light touch' legislative regime based around National Privacy Principles. However, there are a number of limitations in the Act, and therefore coverage does not extend to the handling of all personal information by the private sector. For example, the Act does not apply to:

- Small businesses with a turnover of less than \$3 million
- Employee records (including health information stored on those records)
- Media
- Collection, use and disclosure of information by political parties

The small business exemption does not extend to providers of health services, and therefore all health services providers *are* covered by the Act (except in relation to their employee records).

Most organisations, including all health services holding health information, will have twelve months to ensure they comply with the new scheme. The new provisions will start to apply in December 2001. Small businesses (except health services) covered by the new provisions have an additional 12 months and these provisions will commence in December 2002.

The federal Privacy Commissioner, in consultation with health consumers and professionals, will develop guidelines in regard to access to health information during the course of 2001.

²² available at <http://www.health.nsw.gov.au/iasd/hi/privacy/policies.html>

Privacy Legislation – Other Jurisdictions

Victoria

The Victorian Draft *Health Records Bill* is a companion to the (*Victorian*) *Information Privacy Act 2000*. The *Information Privacy Act 2000* applies to all personal information, except health information, collected by Victorian public sector agencies and organisations funded by the public sector.

The Health Records Bill applies to all health information collected and held in the public and private sectors in Victoria. It does not only apply to information held by “health service providers”, but to “health information” held by any organisation.

The Bill provides individuals with an enforceable right of access to their own health records held in the private sector, to complement the right that already exists for health records in the public sector.

Australian Capital Territory

The *Health Records (Privacy and Access) Act 1997* provides for the privacy protection of, and individual access to, personal health information in the ACT.

Concerns raised about current legislative framework

Concerns have been raised about the introduction of e-health reforms in the absence of comprehensive privacy laws applying in the public and private health sectors.²³

The main concerns highlighted in submissions about the current framework are:

- Inconsistency across state, territory and federal jurisdictions
- Inconsistency across public and private sectors
- Lack of adequate complaints mechanism
- The difficulty for consumers in understanding what regulations apply in certain situations and how to exercise their rights.

Consistent approach

A number of calls have been made for a consistent approach to privacy legislation across either NSW or Australia.

According to the Public Interest Advocacy Centre, a model privacy code is needed in NSW to cover the public and private sectors. Complaints about breaches of privacy should be able to be made to both Privacy NSW and the Health Care Complaints Commission (HCCC) to ensure effective cross referral of complaints and common reporting so that the nature of health privacy complaints can be identified.²⁴

The Federal Privacy Commissioner proposes that the ideal situation would be to have consistency across state and territory borders as well as public and private sectors.²⁵

²³ Public Interest Advocacy Centre, Submission no 29, p 2

²⁴ Public Interest Advocacy Centre, Submission no 29, p 2

²⁵ Office of the Federal Privacy Commissioner, Submission no 34, p 1

The Australian Health Ministers Advisory Council (AHMAC) is currently working on a national privacy code, and the Federal Privacy Commissioner will be encouraging the Council to develop a code that takes the form of a national 'health code' established under the proposed new federal legislation. States and Territories could then choose to recognise the code in their jurisdictions.²⁶

A number of other submissions argue that it is only through a national approach to legislation that consistency can be achieved.²⁷

The preferred view of some stakeholders is that health information should be removed from the coverage of the Privacy Amendment (Private Sector) Act, and new legislation should be prepared which would cover privacy and access of health information in both the public and private health sectors in Australia.²⁸ On this view, health records should be treated differently from other records, and therefore considered separately in another Act in recognition of the special place health has in the community. The current proposal fails to address the complexity of the health care system, and particularly the intermingling of public and private sectors.²⁹

Another view is that as the State government needs to maintain its powers and responsibility over the handling of health records in NSW, it is important that states do not refer their powers to the Commonwealth. The suggestion is that mirrored legislation is a more appropriate path for Commonwealth, State and Territory governments, and that drafting of this legislation be achieved as a collaborative effort between Commonwealth, State and Territory authorities.³⁰

Confusion created by different standards

According to one consumer group, discontinuity, differing jargon and different rules create havoc and confusion amongst both the legal profession and the layperson. For example, based on the Privacy Amendment (Private Sector) Act, complaints against the private sector may be investigated by a range of bodies, including industry bodies and the NSW Privacy Commissioner. This may lead to different standards of investigation, and it would be logical to resolve this confusion before a system of linked EHRs is introduced.³¹

The division between the public and private sector in health care is arbitrary, as consumers often deal with both sectors, and at a particular point in time may not even be aware whether they are dealing with the public or private sector. The fact that the Privacy Amendment (Private Sector) Act ends up creating different rules for each sector not only creates a legal nightmare, but also undermines the stated purpose of the Act, that is to achieve consistency.³²

Balancing privacy legislation and health care reforms

Another concern raised about the NSW legislation, is that compliance with this legislation may significantly impair the effective implementation of these information

²⁶ Office of the Federal Privacy Commissioner, Submission no 34, p 1

²⁷ Health Communications Network, Submission no 22, p 2; Illawarra Area Health Service, Submission no 19 p 1

²⁸ Consumers' Health Forum, Submission no 17, p 1

²⁹ Breast Cancer Action Group, Submission no 3, p 4

³⁰ NSW Nurses' Association, Submission no 13, p 2

³¹ Mental Health Coordinating Council, Submission no 32, p 1

³² Breast Cancer Action Group, Submission no 3, p 4

technologies in pursuit of better health care in NSW. That is, because privacy legislation is limited to the public sector, it may pose barriers to the transfer of health information between public sector agencies and private practitioners acting towards the care of the same individual. The provision of a patient-centred model of care is dependant on sharing information across professional and organisational boundaries. The development of a national health specific privacy protection legislation to facilitate inter-sectoral and intra-jurisdictional health care delivery is seen as highly desirable.³³

Coverage

There are a number of different approaches suggested by the above discussion. One question that arises is: Is it preferable for privacy legislation for health information to apply to handling of information by 'health service providers' [as in the Privacy Amendment (Private Sector) Act] or to the handling of all 'health information' by any organisation (as the Victorian approach)?

On either model, the definition of what is considered a 'health service provider' and 'health information' will need to be carefully addressed to ensure that the full scope of the system of linked EHRs is covered adequately by privacy legislation.

Complaints mechanism

A number of consumer groups have raised concerns about the adequacy of the complaints mechanisms which currently exist, including those under the federal Private Sector Act.

Some submissions recommended the need for an independent, external body to be able to handle complaints, and to be given the full force of law to ensure that privacy standards are enforced.

Keeping pace with technological change

Despite the current moves towards legislative reform in this area, it is important to be aware that technological changes will continue at a rapid rate. It is therefore likely that developments in technology will outpace even the most advanced legislation.³⁴

One important question is therefore what provisions can be made to cover future developments in software and communication technology?³⁵

Conclusion

It is the unanimous view of the Committee that separate and distinct legislation is required to cover the privacy of health information. The legislation must provide a clear and transparent framework for the introduction of transferable electronic health records.

The legislation must cover both the public and private sectors and include the provision of heavy penalties for breach of the legislation.

³³ NSW Health Information Management Implementation Coordination Group, Submission no 30 p 1

³⁴ Health Communications Network, Submission no 22 p 2

³⁵ Royal Australasian College of Physicians, Submission No 23, p 2

The legislation must include complaint handling and audit mechanisms with the establishment of an external body to handle this process.

Public confidence in electronic health records would be greatly enhanced by strong, robust health information privacy legislation.

Recommendations

3. *That the system of linked electronic health records be governed by a separate and specific piece of State legislation entitled the Health Records and Information Privacy Act.*
4. *That the Health Records and Information Privacy Act:*
 - (a) *apply to all health records, in whatever form kept, in both the public and the private sectors of health care and health care delivery in New South Wales;*
 - (b) *specify the purposes for which health records may be linked and transferred so that no linkage or transfer may take place without specific legislative authority;*
 - (c) *incorporate the Information Protection Principles as set out in Part 2 of the Privacy and Personal Information Protection Act 1998 modified as and if required to meet the specific needs of the health sector;*
 - (d) *establish protocols and provide mechanisms whereby linked electronic health records (or parts thereof) can be transferred between authorised parties;*
 - (e) *provide for the right of inspection, access, copy, annotation and correction of any health record by any person who is the subject of such a record, except where exceptional circumstances (to be defined clearly in the legislation and which relate to the protection of the welfare of such a person) apply;*
 - (f) *vest in the Privacy Commissioner of New South Wales the powers to:*
 - *investigate and determine complaints made under the Act*
 - *initiate investigations and conduct enquiries and audits relevant to the conduct and administration of the Act*
 - *make reports and recommendations to the Minister and Parliament regarding the administration and operation of the Act.*
 - (g) *establish mechanisms for allowing complaints related to alleged breaches of privacy and other improper conduct to be made and determined*
 - (h) *impose significant penalties of both a civil and criminal nature for breaches of the Act;*
 - (i) *incorporate (either directly or by cross-reference) all existing privacy and confidentiality requirements present in various existing health-related statutes of New South Wales.*
 - (j) *give specific recognition to particular problems related to the capacity of children to withhold information from their parent or guardian in particular circumstances.*
5. *That relevant agencies, including Privacy New South Wales (the Office of the Privacy Commissioner), the Health Care Complaints Commission and the relevant professional registration boards be resourced adequately for the*

discharge of responsibilities imposed under the Health Records and Information Privacy Act.

PART THREE: Specific Privacy Issues

Possible Models for an Electronic Health Record System

There are obviously many possible models for implementing a linked Electronic Health Records system in NSW, and it is beyond the scope of this report to consider them all. However, it is useful to discuss the privacy issues that may arise with different types of models, and identify which models offer the best privacy protection at the same time as delivering health benefits.

In broad terms, models for implementation include:

- De-centralised (or distributed) system. On this model, data could be stored at GP, public hospital, Area Health Service or other defined local level, and linked to other health care providers across and network when required. This approach minimises privacy risks by allowing the consumer and health care provider to have more control over information transmitted to other providers. The main questions centre around what information should be made available, who should have access to it and in what situations.
- Centralised database holding (eg by a State or Commonwealth Government body or independent regulatory body). On this system, data would be held on a single, centralised system and be accessible from any point in the State. The main privacy risk associated with this model is that it removes control of the information from both the individual and health provider, and increases the risk of the information being inappropriately accessed by other parties.
- Smart Card carried by the individual. There are a number of possible Smart Card models. The proposal in the Menedue report was for a Smart Card which acted as a pointer to certain data stored on a system elsewhere. An alternative Smart Card model is for the Card itself to hold the data, and the data be accessed via a card reader when the person visits their GP or hospital. On this system, if a back-up is required, this could be done at the local level (eg with GPs or hospital) to avoid the need for a centralised holding of data.
- A further option would be a combination of any of the above models, by networking and linking data across the system in different ways according to different individual health care needs.

Conclusion

The model used for linking electronic records is irrelevant as long as basic privacy principles are built into the system from the outset.

Unique Patient Identifiers

To effectively operate a linked electronic health records system, the health service provider needs to establish with certainty the identity of the person who is seeking access or treatment and to link their identity with existing health care records. It is proposed to introduce a unique patient identifier (UPI) for this purpose.

Unique Patient Identifiers offer a number of privacy benefits and risks to a linked Electronic Health Records system.

On the one hand, an individual UPI helps establish the identity of the individual and therefore allows health providers to ensure correct patient links are established. This benefit will only be forthcoming if the system developed is 100% accurate, as any error in the system could potentially lead to mis-matching of client data or lead to vital information not being included on a person's EHR.³⁶ It could also lead to an individual having access to another person's data, hence resulting in a breach of privacy.

Safeguards would need to ensure a high level of accuracy, and, for example, that there was no risk of an individual being issued with more than one UPI or of two individuals having the same UPI.

Local, State or National Unique Patient Identifier?

The Commonwealth Department of Health and Aged Care supports a national UPI that is strictly limited to use in the health sector, where participation by consumers and providers is on a voluntary basis.³⁷

NSW Health is proposing a multi-layer system based on individual Area Health Service UPIs, which can then be matched against a State UPI.

Given the need for accuracy, it is arguable that implementing a UPI system at the local level (at least in the first instance) would reduce the risk of errors occurring. For example, the Central Sydney Area Health Service (CSAHS) has developed a system based on a unique patient identifier to ensure correct patient links are established. It has taken extensive collaboration, staff training, standardising of systems and use of sophisticated information systems to achieve this solution within the local AHS. The emphasis has been on ensuring that only accurate data can enter the system, as any errors could lead to adverse clinical decisions. Given the complexity of undertaking such a project on a state-wide basis, CSAHS questions whether a similar model would work beyond the confines of a discrete organisation in a manner that would ensure individual privacy and comply with privacy legislation.³⁸

A look at Unique Identifier systems currently administered at the national level in Australia supports the notion that more errors are likely to occur with a wide-scale implementation than a local system. For example, the Australian Taxation Office (ATO) has estimated that there are approximately 5.3 million potentially inactive or excess tax file number registrations on the ATO database.³⁹ Clearly this huge margin for error would be unacceptable in the health care environment.

³⁶ Central Sydney Area Health Service, Submission No 27, p 3

³⁷ Commonwealth Department of Health and Aged Care, Submission no 8, p 3

³⁸ Central Sydney Area Health Service, Submission no 27, pp. 2-5

³⁹ House of Representatives Standing Committee on Economics, Finance and Public Administration, *Review of the ANAO audit report no 37 1998-99 on management of Tax File Numbers*, August 2000 p10

Any consideration of the use of the Medicare number (or the Health Insurance Commission identifier based on it) as a UPI needs to recognise that there are significant numbers of Australians who do not have Medicare numbers. For example, a 1997 study by Keys Young found that the proportion of indigenous people having no effective access to a current Medicare number or card ranged from about 15 to 20 per cent in some urban areas and to nearly 40 per cent in some remote areas.⁴⁰

Medicare number

There are specific privacy concerns raised if an individual's health record is linked to the same number as that used to administer the financial aspects of the health care system (ie the Medicare number). The main concern is that it gives a central government organisation (in this case the Health Insurance Commission) potential to access and link individual health records.

When the Medicare number was introduced into Australia, individuals were assured that the system was being established for administrative and financial purposes only, and that these records would never be linked with individuals' health data. Any extension of the Medicare number that involves linkage to individual health data would constitute a breach of trust with the Australian people.

It should be noted that while the Medicare number on a card may cover a number of different people, the Health Insurance Commission has a separate and distinct unique identifier for each individual covered under that card.

Conclusion

A UPI raises privacy issues because it allows information to be linked, and potentially accessed by a range of third parties who may have no right to that information.

It is probably not practical to use the Medicare number as the basis for a UPI because of the timeframe required to change legislation and the probable lack of community acceptance of the extension of its use.

The Committee has a preference for the introduction of a state wide UPI system with the identifier generated by Area Health Services or the Department of Health.

However any UPI that is generated must meet the same levels of security and integrity that are given to the allocation of medicare numbers/HIC identifiers.

Steps must be taken to ensure that clinical and financial information should never be linked by the same identifier.

Any administrative system relying on a UPI in the health field will need to limit the scope of its use, and have the backing of a strong legislative regime.

Recommendation

⁴⁰ Australian Bureau of Statistics, *The Health and Welfare of Australia's Aboriginal and Torres Strait Islander Peoples* (4704.0), 1999;

10. *That a system of Unique Personal Identifiers be introduced to support the system of linked electronic health records on a State-wide basis. In that regard:*
- *these Unique Personal Identifiers must be identifiers of the highest integrity;*
 - *they should be generated by either the Department of Health itself, or in a co-ordinated fashion by the Area Health Services; and*
 - *the Medicare number should not be used for this purpose and the State-wide Unique Personal Identifier should not be linked directly to the Medicare number.*

Voluntary or Compulsory Model

The highest level of privacy protection is provided by a system based on informed patient consent. The choice of how a health record is to be kept, i.e. in paper or electronic form, is the decision of the person of the person creating the record. However, it is clearly the right of the subject of that record to agree or to withhold agreement for that record to be linked with other records or transferred to or made accessible to other health service providers.

Based on the fundamental principle of medical confidentiality, a person assumes that when they seek treatment their medical data will remain confidential unless they give permission for it to be shared with other health care providers (eg for the purposes of continuing care, follow-up treatment).

Many health services involve collection of sensitive information, and individuals need to trust health providers to keep the information confidential so they can be confident in accessing the services they need.

HealthConnect – a ‘voluntary’ system?

In recognition of the importance of medical confidentiality as the overriding public concern, the Commonwealth government has reassured the public that participation in HealthConnect and BMMS would be entirely voluntary in order to protect individual privacy, and that steps would be taken to ensure this level of privacy protection applies.

The HealthConnect model is described as a national system where “individuals must freely agree to participate in the network in the first place and on a continuing basis.”⁴¹ However, in September 2000, press reports indicated that the Commonwealth government is considering an electronic system that would rely on every Australian having their own UPI and on a UPI being allocated to every newborn.⁴² Building up a system which compulsorily registers individuals from birth cannot be considered a ‘voluntary’ system, and the public statements on the Commonwealth proposal to date may be misleading.

It appears that what is emerging at the Commonwealth level is a combination of a ‘compulsory’ and ‘voluntary’ model. That is, it is compulsory for every person to be registered, but voluntary as to what information is included on the electronic network.

⁴¹ National Electronic Health Records Taskforce, An Introduction to Health Connect p 4

⁴² *The Age* ‘Electronic health records unveiled’ 22 September 2000; *Sydney Morning Herald* ‘Majority tipped to join health databank’, 22 September 2000

However, the true extent to which the proposal is voluntary or compulsory remains unclear.

Seeking genuine informed consent

For a system to be genuinely voluntary, individuals must not be disadvantaged if they choose not to allow their health records to be linked. For example, if the system was established so that a person had to pay for a service if they did not have a linked EHR, whereas the same service is provided free to someone with a linked EHR, then the system could not be said to be based on genuine consent as individuals may be forced to allow their records to be linked even if they do not wish to.

The Committee noted that in November 2000, reports appeared in the media suggesting that the medical records of more than 50 000 defence force employees were potentially available for sale to research and insurance companies without the explicit consent of the individuals to whom that data related.⁴³ It is precisely situations like this which are of particular concern to the Committee.

The Christian Science Committee has sought a religious accommodation to any EHR/UIP system that is introduced. Based on religious beliefs Christian Scientists oppose the involuntary and universal assignment of a UIP.⁴⁴

Opt-in vs Opt-out

If a model is to be based on informed consent, this is best achieved via an 'opt-in' model. That is, it is up to the individual to participate, and the role of the health care providers is to provide balanced information about the benefits and risks of using an EHR to inform the individual's choice.

On an 'opt-out' system, people need to specifically request *not* to be included on the system or they will be included by default. In this case, there is still an obligation on health providers to inform people that they are being included on an EHR system and of their right to choose not to participate.

The 'opt-out' model is viewed by some stakeholders as more effective as it means that more people will end up participating in the system. It also means that individuals who do not actively choose to participate will still be able to gain the potential benefits of the EHR system. On this view, one danger of an 'opt-in' model is that there is a risk that treatment and care may be compromised by the unintended withholding of clinical information.⁴⁵

However, more significant privacy issues are raised by an 'opt-out' model. While an 'opt-in' is clearly based on informed consumer participation, this is not necessarily the case with an 'opt-out' model. One reason is that individuals may enter the health system when they are vulnerable and not in a position to make an informed decision (eg in an emergency situation, when in poor health) about the extent to which they want their data shared across the health system, but are entered on the system by default. Another problem is that unless consumers are properly informed about the EHR, they may not even be aware that their records exist in electronic format and are

⁴³ Judith Whelan: "Military may sell health records database", *Sydney Morning Herald* 18 November 2000

⁴⁴ Christian Science Committee, Submission no 39, p1

⁴⁵ NSW Health Information Management Implementation Co-ordination Group, Submission no 30, p 6

therefore in no position to make a fully informed choice about the confidentiality of their medical information.

Conclusion

The basic assumption drawn from the Menadue report is that everyone in NSW is intended to be part of a future electronic health record system and it is therefore in many respects a compulsory “opt-in” system.

What needs to be built into the system is a voluntary process of then allowing and agreeing for all or some of the information contained on the health record to be transferred and exchanged.

The Committee is of the view that a linked EHR system must promote the active sharing of information, based on informed consent and not exist as a passive model.

Accepting that the creation of electronic health records is inevitable the key privacy issue is the consent of the individual to “opt-in” to a system that allows information transfer and how much information is transferred.

Recommendation

2. *That such a system be based upon the following principles:*

- c) the patient/consumer must have the right to ensure that particular information on any health record is excluded from automatic transfer to other authorised recipients of such information except with the patient/consumer's express consent.*

Accountability, administration and responsibility for the EHR

Given that the proposed linked EHR in NSW will to some extent overlap with the Commonwealth proposals, it will be important to clarify the lines of accountability for overall operation of the system.

The linked EHR will also bring together information held by both public and private sector health care providers, and will therefore open up questions of the lines between government and private sector responsibility. For example, clarity will be needed on establishing and implementing standards, dealing with errors on EHR, questions of liability as a result of incorrect information stored on the EHR, and the creation and disposal of records.

One key question is who will ultimately be responsible for overseeing the issue and/or administration of a linked EHR and UPI? At present, this is being dealt with through NSW Health. If the Commonwealth also implements its proposal, how will this impact on the extent to which NSW Health is responsible for the handling of the EHR in NSW?

Scope of and Information Contained on an EHR

During the Committee's discussions and through the submissions received, the issue of the scope and information to be recorded on an electronic health record was raised continually.

One of the key issues impacting on how privacy issues will be managed is the scope of the linked EHR. That is:

- What information will it contain – only summary information, or more detailed consultation and observation notes? Is this the type of decision that would be left to the health service providers themselves, or would it be subject to certain standards?
- Which health providers will access the information and use it to deliver services? For example, will it be used by all types health professionals including, GPs, physicians, physiotherapists, nurses, complementary health practitioners, health service providers on the Internet, community workers (eg drug and alcohol workers and counsellors), emergency and hospital services, pharmacists etc? Or will access to the EHR be limited to certain categories of health professionals?
- Will people from overseas or interstate be required to have an EHR for the duration of their stay?
- Will the EHR be able to be accessed by health providers in other States and Territories?
- Will other types of electronic health records, such as telemedicine or Internet services be integrated or linked into a patient's records system?
- How will the EHR be linked to billing and administrative activities?

Health Information

There is a broad range of data that constitutes 'health information'.

For example, health professionals not only collect details of medical diagnoses and treatment, but also information on social and lifestyle factors that may impact on a person's health, including information on domestic violence, child abuse, cultural and religious beliefs, illicit drug use, sexuality and sexual practices, economic factors such as poverty or housing conditions and a range of other indicators.

Some 'event' information collected by hospitals or providers may also reveal sensitive information about the person's health condition or history. For example, the fact that a person was treated in a particular hospital or location, such as a prison or sexual health centre, could indirectly reveal information about the person. Similarly, medication information or history can often reveal details about a person's medical condition. Therefore, even though summary information such as name of hospital and health provider may not appear to be 'health information' as such, to the extent that it reveals something about a person's health status it may need to be treated with the same sensitivity as other health information.

There is an extremely broad range of health information, much of which is highly sensitive and which individuals may wish to remain confidential. This needs to be kept in mind when considering what types of data should be held on an EHR.

Types of 'non-health' data that could be included on an EHR

One of the benefits of a linked EHR is the capacity to hold important information that may be needed in case of an emergency, and that might not be otherwise accessible.

For example, other data stored on the EHR could include:

- contact details
- information on next-of-kin
- consent arrangements (eg if a guardian has been appointed or the individual has a preferred “person responsible”)
- organ donation preferences
- preferences for treatment in life-threatening situations (i.e. “living wills”).

Third-party data

Data about other family members and individuals may at times be collected to assist in providing a health service for particular person. For example, details of partners, children, carers, other family members with a particular medical history or genetic disposition and names of individuals used for contact tracing of infectious diseases could be collected by a health provider.

In these situations, information about third parties, although often collected without the individual’s consent, is held (if at all) in strict confidence. If such information is included on an EHR there may be privacy implications to be explored here, given that the data may be more widely available and the individual providing the information is not in a position to make decisions on behalf of others as to how the information should be handled.

Types of data that should *not* be included on a linked EHR

In the submissions received by the Committee, certain types of information were identified that should not be included on an EHR, or only with the *written* informed consent of the person.

Specialist sexual health and HIV services attract people who are highly sensitive about confidentiality to the point where they will avoid health services if they believe their privacy is threatened. Any threat to privacy of individual information may therefore pose a health risk to both the individual and the wider public.

The experience of HIV testing has shown that, due to privacy concerns, individuals choose to access some services anonymously or under a pseudonym. While it is important that this option is maintained, it should not be seen as a solution to dealing with privacy-sensitive issues. People should still be able to access such services assured that their consultation is kept confidential without having to resort to finding a way to bypass the system.

Recommendation

11. *That the New South Wales Government and New South Wales Health recognise that there will be special circumstances in which people will, quite properly, seek to access health services on an anonymous basis. Nothing should be done to prevent, penalise or discourage such legitimate access to health services in the absence of any person using a Unique Personal Identifier.*

It has been argued that the following types of information should not be included on a linked EHR without written consent of the individual:

- Sexual health
- HIV status
- Family history
- Family planning issues, including contraception and termination of pregnancy
- Needle and syringe exchange, and other information on illicit drug use
- Health services accessed by sex workers
- Health services targeting high risk young people
- Sexual assault⁴⁶
- Counselling on key psychological episodes, eg. family violence, etc.

There is a portion of the population who are often discriminated against on the basis of a disability. One submission to the Committee gave examples where employers and insurers frequently discriminate against people with a visual disability on the basis of health information they demand from individuals.⁴⁷

Another submission similarly reported that people with mental illness often fear being unfairly judged and treated differently if information about their mental illness is more widely known. People seeking treatment or medication for mental illness may be reluctant to provide information to a health care provider if they are told their records will be kept on an electronic database that may be accessed by other health providers.⁴⁸

The Guardianship Tribunal in its submission also raised concerns about data being included on a networked system that could have a stigmatising affect on the person and may result in discrimination against them by health professionals. The examples cited included HIV test results, terminations of pregnancy and psychiatric history.⁴⁹ The issue of health-related discrimination is real and needs to be recognised. In April 1992 the NSW Anti-Discrimination Board released its report, *Discrimination - The Other Epidemic* which resulted from its enquiry into discrimination against people with HIV. This Report outlined numerous instances of such discrimination across a wide spectrum of activities, ranging from employment and insurance to housing and the provision of medical services.

In November 1998 the NSW Legislative Council Standing Committee on Social Issues published a further report, *Hepatitis C - the Neglected Epidemic* where similar instances of gross discrimination against people with Hepatitis C were outlined. The Parliamentary Committee called for the issue of Hepatitis C - related discrimination to be made the subject of a formal enquiry by the Anti-Discrimination Board. The Board itself announced in November 2000 that such an enquiry would be held commencing in February 2001.

Most recently there have been numerous reports of people suffering discrimination as a result of certain genetic information about themselves (and members of their families) being made available to other than their medical practitioners⁵⁰. The level of

⁴⁶ Sexual Health Services Medical Directors Committee, Submission no 28, p 2

⁴⁷ Retina Australia (NSW) Inc, Submission no 10, p 1

⁴⁸ Mental Health Coordinating Council, Submission no 32, p 3

⁴⁹ Guardianship Tribunal, Submission no 16

⁵⁰ Natasha Bitá : "Curse of the unclean genes", *The Australian*, 14 December 2000. See also

concern about this new form of discrimination has led to specific moves to outlaw such genetically-based discrimination in the United States and Europe⁵¹; to proposed genetic privacy legislation in Australia⁵²; to specific regulations in relation to the insurance industry being authorised by the Australian Competition and Consumer Commission⁵³ and to the federal government announcing an enquiry into the issue to be conducted by the Australian Law Reform Commission and the Australian Health Ethics Committee⁵⁴.

Clearly if people believe that details of their health or genetic status will be used against them or be used to subject them to discriminatory treatment, then they will very properly resist any attempts to widen accessibility to this personal health data. This in turn could compromise the value of a system of linked electronic health records. Such concerns merely serve to reinforce the critical need for privacy issues to be addressed as a central element in the development of such a system.

Conclusion

After considering all the issues the Committee has formed the view that it is not practical for a health record to be limited in the health information contained about an individual.

However, to safeguard the privacy of the individual, stringent controls must be placed on access to this information and the information can only be transferred or exchanged with the individual's explicit consent.

The Committee recognises that there may be some emergency circumstances, involving a serious and imminent threat to the life or health of a person and where the person is unable to give or withhold consent, where EHRs could be accessed without explicit consent.

Third party consent arrangements

There are a number of situations where a person may not be able to consent on their own behalf. This could be an ongoing requirement (such as for some people with an intellectual disability or people suffering severe dementia), or it may be a one-off situation (such as in an emergency where someone is unconscious, or a person experiencing a psychotic episode who is temporarily unable to make an informed decision).

collection of papers from NSW Young Lawyers Continuing Legal Education seminar published as *Dolly McBeal : Genetics and the Law*, August 2000

⁵¹ United States Government, Presidential Executive Order 8 February 2000; G. Apenes, (Privacy Protection Commissioner of Norway) : "Genetics and Privacy Protection", paper at International Privacy Commissioner's Conference, September 2000.

⁵² Senate Legal and Constitutional Legislation Committee : *Provisions of the Genetic Privacy and Non-Discrimination Bill 1998* (March 1999)

⁵³ Australian Competition and Consumer Commission : *Draft Determination on Application for Authorisation lodged by Investment and Financial Services Association in relation to the implementation of a draft policy on genetic testing*, 14 June 2000

⁵⁴ Joint News Release, Attorney General and Minister for Health and Aged Care, *Gene Technology*, 9 August 2000, available at:

http://www.law.gov.au/aghome/agnews/2000newsag/joint10_00.htm

At present, these issues are either handled through formal arrangements (such as with the appointment of a guardian) or at the level of individual consultations where the health care provider makes an assessment of the capacity of the person to act autonomously.

With the introduction of an EHR, it will be necessary to look any implications this raises for consent arrangements.

The Guardianship Tribunal made a number of recommendations on this issue in its submission to the Committee. It proposes a move away from a substitute consent model of decision-making because of the difficulties this poses, and favours an approach whereby disclosure of health information is made in the interests of the person in accordance with a set of ethical principles and guidelines.⁵⁵

Children's records

There are principles that currently guide health professionals when making decisions about whether or not a child or teenager requires parental consent to receive certain treatment, or whether the child is capable of making an informed decision in their own right.

The EHR needs to support the way in which decisions are made on this issue, and not (for example) apply an automatic right of access by the parent to their children's records. Respecting confidentiality and autonomy, and assessing what is in the best interests of the child, should remain guiding principles in this area.

There are a range of circumstances in which a child or young person may wish information contained on an EHR not to be accessible to other people, including (sometimes especially) his or her parents. These circumstances may include seeking advice about contraception, sexuality, drug and alcohol abuse, eating disorders, suicidal feelings, or depression. In the view of the Committee, children and young people should have the right to choose which information will be available on a linked EHR.

Conclusion

The Committee is strongly of the view that consent to the transfer and exchange of health information must be express and informed.

There needs to be legislative protection of a young person's right to seek care and treatment without parental consent or knowledge and of his/her right to privacy.

Data accuracy and integrity

If one of the aims of the EHR system is to improve the accuracy and integrity of patient data, it is important to look at how this can be achieved, and any risks in the event that inaccurate data finds its way into the system.

How will historical data be handled

⁵⁵ Guardianship Tribunal, Submission no 16

Many issues associated with data accuracy and integrity, stem from the historical nature of a person's medical history, and the extent to which this will be recorded on the EHR.

For example, it is unlikely an EHR will represent a complete history, and it may not be evident from the record which aspects of the information may be missing/incomplete.

At present, records systems rely on a combination of historical record keeping and patient memory/recall. It appears some reliance on patient memory, as well as the need to check the accuracy or completeness with historical records, will still be needed with a linked EHR system.

There is also the question of whether the EHR will be used as a new record keeping system, or rather another system superimposed over the written record system.⁵⁶

Data accuracy and adverse events

This is also discussed earlier under Risks and Benefits of an EHR.

One of the most frequently argued benefits of a linked EHR is the fact that it will make information such as medication and treatment regimes available to health providers, and in doing so, will greatly reduce the risk of adverse reactions. The main problem is that, in order for this benefit to be realised, the data on the original EHR must be accurate, up to date and provide some indication as to whether there may be any data or records missing from the records.

According to one consumer group, a record of prescriptions and medications will only be of benefit if it is complete, otherwise it poses dangers. A record will also pose risks if it is assumed to be complete when it is not. There is also the question of consumer behaviour and response to medications. For example, if a consumer chooses to discontinue a course of medication, how will this be reflected in the record?⁵⁷

It is difficult for any consumer who is treated by many health professionals to determine whether or not records are accurately kept and whether they contain any information that may adversely affect their future treatment.⁵⁸ While an EHR may assist in this process, it may also lead to problems if data is recorded incorrectly.

Data standards

For the EHR to operate effectively, it will be necessary to have some standards on how and what data should be entered.

Simply producing a set of standards that are then taken up by all health care providers may not by itself produce a uniform language across the health care system. Where the diagnosis or treatment process is complex, it may not be fully captured in a single 'event summary'. A diagnosis may involve some subjective as well as factual elements, and there is the question of how this information can be reflected in an EHR.

⁵⁶ Royal Australasian College of Physicians, Submission no 23, p 3

⁵⁷ Wollongong Health Consumers Advisory Group, Submission no 7, p 4

⁵⁸ Breast Cancer Action NSW, Submission no 3, p2

Who enters data on to the EHR?

Obviously the more people who are able to enter data on to the EHR, the wider the scope for errors and misinterpretation of the data entered. This in turn will impact on the overall integrity of the data entered on the EHR.

Also, if the linked EHR can be accessed and altered by a large number of parties, this may reduce its overall usefulness and integrity.

Professional Liability

There may be legal liability issues for health practitioners if decisions are made on the basis of incorrect, incomplete or unreliable information that was previously entered (eg by another practitioner) on the EHR. The EHR provides no guarantee of a complete patient history. This could perhaps be addressed by some legislative protection for practitioners who rely, in good faith, on information contained in a linked EHR.

Recommendation

9. *That the opportunity provided by the introduction of the Health Records and Information Privacy Act to improve the quality of health records generally be taken. This improvement should encompass issues such as data standards and accuracy; uniformity of nomenclature and standardisation of recording and reporting requirements.*

Access and amendment to health records by individuals

One of the main benefits for consumers presented by the EHR system as it is currently proposed, is that it will allow easier access to their own health information.

At present, privacy legislation provides an individual with the right to access their medical records held by the NSW public sector, the Commonwealth public sector and the ACT Government. The new federal legislation for the private sector, when it is in force, will also provide individuals with a right to access their records held by private sector bodies.

While both the EHR and the proposed legislation may assist in making medical records more accessible, the introduction of the technology itself will not bring about a radical change in the culture of the health sector towards access to records by consumers.⁵⁹ Therefore, implementation of the EHR must ensure that, in practice, consumers are able to access the information on their EHR that they need, and that the information is presented to them or discussed with them in a way they can understand.

It is not clear from the EHR proposal whether a person would be able to access their records from any point in the system, or for example, only via their general practitioner or local hospital.

⁵⁹ Public Interest Advocacy Centre (PIAC), Submission no 29, p 7

It should be noted that the rights to access, correction and/or annotation are a fundamental part of the principles enshrined in existing federal and State privacy legislation. Information Privacy Principles 6 and 7 in section 14 of the *Privacy Act 1998* (Cth) and Information Protection Principle 7 and 8 (sections 14 and 15) in the *Privacy and Personal Information Protection Act 1998* (NSW) respectively, grant these rights. In over a decade of practice in the federal public sector, the Office of the Federal Privacy Commissioner has reported no major difficulties with the operation of these principles. The State and Commonwealth principles are based on the Organisation for Economic Cooperation and Development's (OECD) 1981 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

Transfer of data between health practitioners

Varying opinions on sharing of information

The extent to which data on an EHR should be shared amongst health professionals appears to be a major source of disagreement about how the EHR system should operate. Differences of opinion have been expressed amongst health professionals as well as within consumer groups.

The basic issue open to question is: In what situations might it be justified to transfer data to another health provider without the individuals' express consent?

On one view, the over-riding principle is that information should not be transferred to another health provider without the person's consent. That is, medical confidentiality remains an important underlying principle of health care. For example, unless a person's right to privacy is respected, people may not seek treatment for STIs, and people will not be truthful for fear of judgement or discrimination by others in the health system. On this view, a health records system that ignores the need for medical confidentiality is putting both individual and public health at risk.

On another view, health professionals require all the health information that is available about an individual in order to provide treatment. This is regardless of what the treatment is for and irrespective of the patient's wishes; the reasoning being that any information they can access may assist them in clinical decision making and the individual themselves would not be able to judge what information should be made available or withheld.

Who will have access to data on the EHR?

A key issue is the extent to which the individual is able to control the different levels of access to information on EHR by various persons and organisations seeking access to the records. The individual must be able to have some say about who has access to certain information, and also what type of information is transmitted where.

Conclusions

As previously indicated, the Committee's preference is for an active information sharing model as opposed to a passive system of health information transfer.

Future possible uses of the data

There are many uses of data on the EHR that are not envisaged at the time the information is entered.

Use for research purposes

The information will be highly valued for health research purposes. The ability of linked EHRs to potentially provide a cradle-to-grave record has been highlighted as one of the key advantages of the EHR system.

At present, most medical research is conducted in accordance with the *National Health and Medical Research Guidelines*, issued under section 95 of the *Privacy Act 1988* (Cth). These state that an individual's consent should generally be obtained for the use of potentially identifying data for research, but also outline situations where a health research ethics committee may approve access without consent. This approach attempts to balance the individual's right to privacy with the interests of health research.⁶⁰

Law enforcement

Demands on the data by law enforcement bodies may increase. Already there has been some compromise on the level of medical confidentiality for the purpose of investigating serious offences, with, for example, the introduction of mandatory reporting of child abuse.

In future, this could extend to other areas of the law, particularly with the growing demands for access to DNA data as a law enforcement tool.⁶¹

Insurance companies and Employers

Insurers and employers may also make demands for increasing levels of access health data. As discussed above such demands are raising new issues about the security of personal health data and people's willingness to have such data recorded.

It would be useful to explore whether or not the introduction of an EHR will change the extent to which the health system comes under pressure to disclose information in unrelated areas such as this.

With an increasing number of people being employed by health care providers and organisations, the rights of individuals currently employed or seeking employment within the health system is an area of concern. The risk of inappropriate use of their data by managers or other health care workers must be strictly protected.⁶²

Recommendation

13. *That research projects seeking access to linked electronic health records be dealt with by a mechanism which reflects the provisions of*

⁶⁰ Australasian Epidemiological Association, Submission no 35, p 1

⁶¹ see *Crimes(Forensic Procedures) Act 2000* (NSW), Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Model Forensic Procedures Bill and the Proposed National DNA Database*, February 2000;

⁶² NSW Nurses Association, Submission no 13, p 2

sections 95 and 95A of the Privacy Act 1998 (Cth) and the relevant Guidelines issued from time to time by the National Health and Medical Research Council.

Information technology issues

Security, authentication and data integrity

An individual's identity will in some way need to be linked to their EHR so that the health professional can be sure of the identity of the individual.

Technology is available and already in place which grants varying degrees of access to a patient's health record.

For transmission of information between practitioners, appropriate standards of security (eg encryption) and authentication mechanisms (eg digital signatures) will be necessary to protect and validate the information.

The role of encryption (for example by Public Key) and messaging standards (for example the HL-7 system) will play an important role in the functionality of any proposed systems.

Data mining

The development of an EHR system opens up new opportunities for extracting information from clinical records.

For example, there may be much to be gained from monitoring health outcomes resulting from the use of particular drugs or therapies. This process relies on assessing de-identified, aggregated information about drug prescribing. This means that information has to first of all be 'mined' from the individual records.⁶³ To achieve this, there would need to be appropriate authority to conduct the research (for example, individual consent or ethics committee approval), and an appropriate level of security to ensure privacy of individuals and practitioners is protected.

De-identified or aggregated data has great value for the purposes of epidemiological studies and health planning. The Committee has no desire to see those purposes thwarted by unreasonable restrictions on access to valuable health data. On the other hand, it does not believe that commercial or industry-based interests should have access to such data. The Committee believes that a clear distinction can be drawn between those uses of such aggregated data as will be of benefit to the public health system and those which are sought merely for commercial purposes. This distinction should be recognised in the access rules for the system. Where special cases can be made out for access to such data outside the confines of the NSW health care system (other than for bona fide research purposes as discussed above), clear authorisation should be sought from NSW Health and the Privacy Commissioner.

⁶³ NSW Therapeutic Assessment Group, Submission no 20, p 3

Recommendation

12. *That linked electronic health records not be accessible for data-matching and data-mining exercises outside the NSW health care system unless such exercises are authorised specifically by New South Wales Health and the Privacy Commissioner.*

Audit and compliance mechanisms

Audit mechanisms are essential for ensuring the overall integrity of the system, and for undertaking investigations in the event that information is mishandled. For example, a built in audit trail can assist in providing information on when and who accessed certain data on an Area Health Service system.

There will be a need to include an alert mechanism to notify of a breach or attempted breach into an unauthorized part of the system.

However, audit trails will only be really effective if there is an independent body which uses them to examine how the system has been used or accessed in practice and which can identify and respond to instances of improper use or access. Recommendation 4(f) of this Report suggests such a mechanism.

Internet

Health care services are increasingly being provided over the Internet.

The internet is a low cost alternate to distribute information, when compared with direct exchanges between two parties. Using the internet allows multiple data exchanges to take place and requires no additional infrastructure. The internet, however is a potentially most insecure method of information exchange. There are numerous instances of internet communications being improperly accessed or intercepted. As a result, assuming that a separate and dedicated NSW health intranet system is not developed, security of information exchange over the internet will need to be a matter of the highest priority.⁶⁴

Conclusion

There appears to be no information technology system that is completely foolproof or completely safe from unauthorised attack.

However it is imperative that in the design of electronic health record systems appropriate attention is applied to the security aspects of access, transfer and storage.

With the internet being regarded as perhaps offering a low level of security, a secure private network may be worth considering to again build public confidence in a EHR system.

⁶⁴ see Department of Communication, Information Technology and the Arts, *From Telehealth to E-Health: The Unstoppable Rise of E-Health*, Commonwealth of Australia, 1999;

Rural Health

The Report to the NSW Health Minister by the Ministerial Advisory Committee on Health Services in Smaller Towns, known as “the Sinclair Report” after its Chairperson, the Right Hon. Ian Sinclair, was a companion report to the Menadue Report.⁶⁵ It found that the traditional hospital structure and models of care need to change to reflect the changed demographic and social environment. For small rural communities, integrated flexible service models need to be developed which are client-focused and responsive to communities’ needs. A linked EHR and UPI could argueably form an important part of this.

However, there are some different and additional privacy concerns in rural NSW compared to metropolitan NSW. These include:

- In small towns it is difficult (and sometimes impossible) to access health services confidentially or anonymously. This may be an issue when it comes to sensitive health issues such as HIV or termination of pregnancy, and individuals may have to travel a great distance to access such services in confidence. Even if they choose to do this, the issue of what is included on a linked EHR still needs to be addressed
- There may be less choice about which health provider to attend, and also less choice for obtaining genuine second opinions
- This is where many proposals for implementing new initiatives (eg telemedicine, Internet consultations) are directed, so there may be more issues arising from non-face-to-face consultations
- Health employees (eg in hospitals, community health centres) may have more difficulty accessing the health system with some degree of privacy than in larger cities
- Some health services may be delivered through non-health outlets in remote NSW (eg pharmacy supplies)
- In very small towns, statistical or demographic data (eg from hospital records) may reveal the identity of individuals (eg with a rare condition) more readily than in larger populations
- Rural towns are one area where there is the potential for disadvantage in terms of access to latest technology infrastructure – and hence an area to be addressed to prevent widening of advantage-disadvantage gap with a linked EHR.

Recommendation

15. *That the recommendations of the Health Council Report in relation to the piloted, staged and progressive implementation of a State-wide system of linked electronic health records be endorsed and followed. At least one of the*

⁶⁵ see Ministerial Advisory Committee on Health Services in Smaller Towns, Report to the NSW Minister for Health, *A Framework for Change*, February 2000; available at <http://www.health.nsw.gov.au/health-public-affairs/wayforward/sinclair.html>

pilot projects should be based in an Area Health Service in rural or remote NSW.

Timetable and Method of Implementation

The Committee is strongly of the view that the staged, graduated approach for the introduction of a linked HER system, as recommended in the Health Council (Menadue) Report should be adopted by the NSW Government and NSW Health. This staged, graduated approach must be preceded and/or accompanied by the drafting and enactment of the Health Records and Information Privacy Act and by widespread community consultation and user education about the introduction of a UPI and a linked EHR.

Recommendation

14. *That New South Wales Health publish a timetable consistent with the recommendations of the Health Council (Menadue) Report for the introduction of linked electronic health records in New South Wales and the enactment of the Health Records and Information Privacy Act.*

One Committee member, Assoc. Prof. Lindsay Thompson AO, does not accept the general approach of the Committee's recommendations in this regard. He does not believe the rapid passage of comprehensive privacy legislation is a necessary first step and prefers a gradual introduction of UPIs, linked EHRs and privacy protections after extensive consultation and trial with both consumers and health providers.

Appendix 1 – The Overseas Experience**Privacy, Electronic Health Records and Unique Patient Identifiers****New Zealand**

There are a number of e-health initiatives underway in New Zealand. The main bodies responsible for developing and implementing these initiatives are:

Ministry of Health

New Zealand Health Information Service (NZHIS) – A group within the Ministry of Health responsible for the collection and dissemination of health-related information.

Health Funding Authority - The HFA allocates resources to enhance and maintain the health and independence of New Zealanders. Most publicly funded health and disability support services receive their funding from the Health Funding Authority.

The National Health Index (NHI) and NHI number

One of the major information systems supported by the NZHIS, is the National Health Index (NHI). The NHI provides a mechanism to uniquely identify healthcare users. It was developed to help protect personally identifying health data, particularly data held on computer systems, and to enable linkage between different information systems whilst still protecting privacy.

Access to the NHI is restricted to authorised users, and is permitted by the Health Information Privacy Code of Practice under the *Privacy Act 1993*. The use of the NHI ensures that when health information is communicated between healthcare facilities within the health sector, easily recognisable identifying details such as name and address can be removed. The NHI database does not contain any clinical information.

The National Health Index (NHI) number is a unique identifier that has been used in New Zealand for about 20 years. Established in 1977, the NHI number has been used as an identifier for recording hospital admissions and important medical warnings for hospitals. Since 1991, all babies have been given a NHI number at birth, and numbers are now allocated to over 90% of New Zealanders.⁶⁶

Recent developments may extend the use of the NHI number to potentially linking all health care transactions, not just those relating to hospital admissions.

E-health initiatives

A recent e-health project underway in New Zealand is Health Intranet.

The Health Intranet was launched in July 1998 starting with a pilot project. The Intranet aims to provide a secure means of nationwide communication between organisations in the health sector, including transfer of data between health professionals. It also aims to provide all health care providers with access to the

⁶⁶ Bill English, Health Minister, *Wellington GPs to trial use of Health Intranet*, Press release 28 July 1998

National Health Index (NHI). Following the pilot project, the Health Intranet is now being implemented more widely across all hospitals.

The Health Intranet must meet the requirements of relevant privacy legislation, and has been developed to international standards of communication and security suitable for exchange of sensitive health information.⁶⁷

In April 1998, a Privacy Impact Assessment was conducted on the Health Intranet project by barrister, Mr Robert Stevens who found a number of shortcomings with the way in which privacy issues were addressed.⁶⁸

The main points highlighted in Mr Steven's Privacy Impact Assessment were:

- Confirmation that the Privacy Act 1993 does apply to information referenced by an NHI number, as the number constitutes "information about an identifiable individual".
- Use of NHI number more widely may improve accuracy and therefore promote privacy, but it could also be used to collate data from different sources and of a different nature thus raising privacy issues.
- Lack of evidence of any research supporting better patient health outcomes as a result of centralised medical records. Therefore, it should not be assumed that a full and accessible patient record is necessarily good for the patient.
- Common law has respected confidentiality in professional relationships, and in some cases is protected by legal professional privilege. It is unlikely this privilege would apply to individual health information held by government bodies such as the Health Funding Authority and NZHIS.
- As the HFA proceeds down the track of assembling a large database of health information, there are fears that this is happening without widespread public debate or knowledge.
- There are a number of 'health informatics' initiatives in NZ, which require coordination and leadership to avoid the problem of incompatible or competing systems.
- A reappraisal of the role of Privacy Officers in organisations in NZ may be needed.

The NZHIS advises that the Ministry of Health has acted on the recommendations in this assessment.⁶⁹

Privacy framework

⁶⁷ NZHIS Health Intranet information at www.nzhis.govt.nz/projects/hi_userinfo.html

⁶⁸ Robert Stevens, (Barrister, Auckland), *Medical Record Databases. Just what you need? A survey of practice and plans in NZ for the collation and retention of health records about identifiable individuals, with particular reference to the implications for privacy arising from the increased use of NHI numbers*, April 1998

⁶⁹ NZHIS Health Intranet information at www.nzhis.govt.nz/projects/hi_security.html

In New Zealand, the *Privacy Act 1993* applies to information handled by all organisations in both public and private sectors.

Under the Act, a Code of Practice may be issued by the Privacy Commissioner to cover specific agencies or activities. Soon after the Act was passed, a Code was issued to cover the health sector (both public and private). This Code, the *Health Information Privacy Code 1994 (Revised edition, July 2000)*, has been drafted to operate in harmony with other legislation impacting on the health sector such as the Health Act and the Medicines Act.⁷⁰

The Health Information Privacy Code covers all 'health information' collected, used, held and disclosed by 'health agencies'. The 12 rules in the Code substitute for the 12 Information Privacy Principles in the Privacy Act and are enforceable - a breach of a rule is deemed to be a breach of a privacy principle under the Act. The code contains a number of more stringent standards than in the Privacy Act in recognition of the sensitivity of health information.

Information Privacy Principle 12 in the Privacy Act places limits on the use of unique identifiers, and generally prohibits the re-assignment of unique identifiers by agencies where another agency already uses that identifier. Rule 12 in the Health Information Privacy Code continues this, but contains some exceptions in relation to the NHI number.

United Kingdom

The National Health Service (NHS) and the NHS number

In the UK, one feature of health service delivery is that each person is assigned to a GP by the Local Health Authority. This allows the health system to be able to reach the vast majority of the population through direct contact with the GPs, local hospitals and clinics within the NHS. When patients change to another GP, they are able to take their records with them.⁷¹

Everyone in England and Wales has been given a new NHS number. New numbers are issued by the NHS Central Register that holds demographic information on all persons who are registered with a GP in England and Wales.⁷² The NHS number is used as the primary identifier on medical records, and is being implemented to replace any existing local identifiers overtime. A key feature of the NHS number is that it is a randomly generated number that does not include any patient-identifiable data.

All newborn babies are also issued with a number when the parents register the birth.

The number is intended for use by all NHS organisations that hold or transfer patient information. Its primary purpose is to support the provision of health care within NHS, but it is also to assist in the coordination and transfer of care outside the NHS. Within the NHS system, the number is the primary identifier, but outside the system its use

⁷⁰ NZ Privacy Commissioner, *Centralised Databases: People, Privacy and Planning*, A paper presented to the NZ-Australia Health IT Directors Meeting, 18 February 1998

⁷¹ Chris Puplick, *UK Trip Report, Part 6 Electronic Health Records and Unique Patient Identifiers*, July 2000

⁷² NHS Executive, *General principles in the use of the NHS number* April 1998

is strictly limited to uses that support the delivery of health care to patients and it cannot be used more widely than this.⁷³

The fact that a nationwide NHS number already exists provides an important foundation for integrating and sharing information across the NHS.

E-health initiatives

In September 1998, the NHS Executive published *Information for Health: an information strategy for the modern NHS 1998-2005*. This outlines a strategy to ensure health information is used to help patients receive the best care possible. It aims to ensure professionals have access to the information they need, and that patients and the public have information necessary to make decisions about their own treatment and care.

Central to the strategy is to achieve a common goal of seamless care through creation of an electronic health record (EHR). This will provide the basis of lifelong core clinical information with eventual electronic transfer of patient records between health providers. Initially, the EHR is most likely to be constructed on the basis of data transfers across the NHS network, but in future other developments such as browser and intranet technology, and smart cards, may be used.

The aim is to implement the system of EHRs by 2005.⁷⁴

The Caldicott Report

In December 1997, the Caldicott Committee published its *Report on the review of patient-identifiable information*.

This Report was commissioned by the Chief Medical Officer of England due to increasing concern about how patient information was being handled within the NHS, and in particular to ensure confidentiality was being respected.⁷⁵

The Report reviewed all patient identifiable information passing between NHS organisations or from the NHS to non-NHS bodies. The purpose was to ensure that information was only transferred for justifiable purposes, and that only the minimum information necessary was being transferred.

The Committee made a number of recommendations that the NHS have accepted, and will be subsequently implementing as part of its information strategy. For example, each health institution is required to appoint a designated officer (known as a "Caldicott Guardian") to be responsible for ensuring the institution's compliance with all privacy requirements.

Privacy legislation

The *Data Protection Act 1998* came into effect in the UK on 1 March 2000. This Act replaces the Data Protection Act 1984. The office of the UK Data Protection Commissioner was established in March 2000 under the Act.

⁷³ NHS Executive, *General principles in the use of the NHS number* April 1998

⁷⁴ NHS Executive Information Policy Unit, *EHR Options – A discussion paper*
www.doh.gov.uk/nhsexipu

⁷⁵ NHS Executive, *The Caldicott Committee: Report on the review of patient-identifiable information*, December 1997

This legislation gives effect in the UK to the European Commission Directive 95/46/EC requiring member states to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data.

There are 8 Data Protection Principles in the *Data Protection Act 1998*, and these apply to all businesses and organisations that are 'data controllers'. Data controllers will have to comply fully with the Act from October 2001. The Act gives legal rights to individuals in respect of personal data held about them by others, and ensures those who hold personal information have corresponding obligations.

Canada

Developments in e-health

In Canada, work is underway on the development and implementation of a national strategy for a Canadian Health Infrastructure (Canada Health Infoway).

An Advisory Council on Health Infrastructure was established in 1997, and in February 1999, issued its final report entitled *Canada Health Infoway – Paths to Better Health*, including recommendations on privacy and health information.⁷⁶

In this report, electronic files were identified as a crucial element to strengthening and integrating the health care system. The Canada Health Infoway system proposes the use of privacy-enhancing technologies to ensure medical records are secure. As an extra privacy protection, the Canada Health Infoway report rejected the concept of a unique personal identifier that could be used for health purposes as well as other government identification purposes.

The Canadian approach does not propose a single massive structure, but rather aims to build on diverse federal, provincial and territorial initiatives. The proposed system takes into account the information requirements of consumers, as well as other participants in the health sector, and provides a useful model for implementing electronic health records.⁷⁷

The initiatives of the Health Infrastructure being implemented by Health Canada are all undergoing privacy impact assessments, and a working group with representatives from federal, provincial and territorial governments is working on a national, harmonised approach to protecting personal health information.

However, despite these efforts, the Canadian Privacy Commissioner believes that not enough is being done to consult with the public about health information privacy and the implications of the Health Infoway for patient privacy. The Commissioner states that health-related organisations must explain the existing flows of health information so that the public understands the privacy implications. Another barrier is the fact that in the transition to electronic health records, there is still some opposition to obtaining patient consent on how these records are made available.⁷⁸

⁷⁶ Advisory Council on Health Infrastructure, Press Release 3 February 1999

⁷⁷ Meredith Carter, *Integrated electronic health records and patient privacy: possible benefits but real dangers*, *Medical Journal of Australia*, 2000; 172: 28-30

⁷⁸ Brian Foran, Director, Issues Management and Assessment, Office of the Privacy Commissioner of Canada *Reaching a Consensus on the Privacy of Health Information: Looking Down the Road* March

Privacy framework

Canada's *Privacy Act 1983* was brought in to deal with the growing impact of computers on government record keeping. The Act only applies to federal government departments and agencies.

In April 2000, the *Personal Information Protection and Electronic Documents Act* received Royal Assent and comes into force on 1 January 2001 to govern the handling of personal information in the private sector in Canada.⁷⁹

In addition, there are a number of state and local Acts that regulate the privacy of personal information.

The Privacy Commissioner and the Advisory Council on Health Infrastructure have both called for harmonised privacy protection across different jurisdictions; the Privacy Commissioner has called for the establishment of a "high benchmark for the protection of health information across the country".⁸⁰

In the health sector at present, the *Canadian Medical Association (CMA) Health Information Privacy Code* articulates principles for protecting the privacy of patients, the confidentiality and security of their health information and the trust and integrity of the therapeutic relationship. The CMA has issued this Code to provide a consistent standard for the handling of health information in the health care community. The CMA acknowledges the challenges posed by the patchwork of privacy legislation applying in the health sector, and has issued the Code as an ideal to strive for.⁸¹

The Canadian Privacy Commissioner wants any national consensus on the handling of health information to embody the principles of the CMA Code, as unless this is done Canadian's rights to privacy will be diminished.⁸²

United States

In the United States, the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) outlines a process to achieve uniform national health data standards and health information privacy. Enacted with the widespread support of the health care sector and bipartisan support in the Congress, the law requires that the Secretary of Health and Human Services (HHS) adopt standards to support the electronic exchange of a variety of administrative and financial health care transactions. All health plans, health care clearinghouses, and those health care providers who elect to conduct the specified transactions electronically are required to comply with the

2000

⁷⁹ available at http://www.privcom.gc.ca/english/02_06_e.htm

⁸⁰ Brian Foran, Office of the Privacy Commissioner of Canada *Reaching a Consensus on the Privacy of Health Information: Looking Down the Road* March 2000

⁸¹ Canadian Medical Association, CMA Health Information Privacy Code, August 1998 at www.cma.ca/inside/policybase/1998/09-16.htm

⁸² Brian Foran, Office of the Privacy Commissioner of Canada *Reaching a Consensus on the Privacy of Health Information: Looking Down the Road* March 2000

standards within 2 years of their adoption, except that small health plans are required to comply within 3 years. Among these standards are:

- Certain uniform transactions and data elements for health claims and equivalent encounter information, claims attachments, health care payment and remittance advice, health plan enrolment and disenrolment, health plan eligibility, health plan premium payments, first report of injury, health claim status, referral certification and authorisation, and for coordination of benefits.
- Unique identifiers for individuals, employers, health plans, and health care providers for use in the health care system.
- Code sets and classification systems for the data elements of the transactions identified.
- Security standards for health information.
- Standards for procedures for the electronic transmission and authentication of signatures with respect to the transactions identified.

Privacy and confidentiality protections for health information play a prominent role in the law. The Secretary is required to adopt security standards to safeguard health information, during transmission and while stored in health information systems, to ensure the integrity of the information, and to protect against unauthorised uses and disclosures. Further, the law requires the Secretary to make detailed recommendations to the Congress for protection of individually identifiable health information. These recommendations were delivered to the Congress on September 11, 1997. If the Congress did not enact legislation for health record privacy by August 21, 1999, the law required the Secretary to issue regulations to protect the privacy of individually identifiable health information transmitted in standard transactions. These regulations were to be finalised by February 21, 2000.

On November 3, 1999, HHS published a proposed regulation to protect the privacy of health information (Standards for Privacy of Individually Identifiable Health Information).⁸³ The Office for Civil Rights (OCR) within HHS will be responsible for enforcement. OCR's responsibilities will include issuing exception determinations and advisory opinions, providing technical assistance, receiving and investigating complaints, conducting compliance reviews, and seeking civil monetary penalties if voluntary compliance cannot be obtained

The proposed rule was published in the Wednesday, November 3, 1999 edition of the *Federal Register* (Vol. 64, No. 212, pp. 59918-60065). The comment period ended on February 17, 2000. The Department received more than 52,000 comments on this regulation. HHS reviewed and analysed these comments, and prepared a final rule. The final Rule and its related regulations were published in the US Federal Register on December 19, 2000 and will become effective on 18 February 2001 (sixty days later).⁸⁴ Covered entities must comply with the rule two years and two months following the publication date of the final rule.

Under the Rule, covered entities would not be able to use or disclose an individual's protected health information except as provided under the regulation. The regulation also requires health plans and health care providers: (1) to provide individuals with a notice of their privacy policies and procedures; (2) to allow individuals to inspect and obtain a copy of health information in their medical records; (3) to provide individuals

⁸³ Available at <http://aspe.hhs.gov/admsimp/nprm/pvclist.htm>;

⁸⁴ see Appendix One, below ; the text of the final rule is available at <http://aspe.hhs.gov/admsimp/FINAL/Final%20Privacy%20Rule.pdf>

with an accounting of disclosures of their health information; and (4) to either correct errors in an individual's record or to allow the individual to include a statement of disagreement in that record.

Individuals who believe a covered entity has violated these or other privacy rights under the regulation would be able to file a complaint with OCR. There is no private right of action, so an OCR complaint will be the only recourse for aggrieved parties.

Concluding remarks

Overall, the countries discussed above have made some progress towards investigating and implementing an EHR system. However, none has yet implemented a comprehensive national system, and all look somewhat off achieving this goal.

What is in place are a number of local developments and numerous pilot studies that have been conducted.

In all instances, the privacy of health information has been acknowledged as a key issue, though the extent to which privacy is being addressed as an integral part of the implementation processes varies.

In New Zealand, consistent privacy legislation in the health sector has been in place for a number of years. This, together with the fact that New Zealand does not have the complexities of a federal system, mean that there are already well established and widely accepted standards for privacy in place across the country.

Both New Zealand and the United Kingdom have in place widespread unique identifier systems within the public health sector that are being given a role in the proposed electronic health systems, though in both instances it would appear that attempts are being made to limit the further use of this identifier outside the public health system.

Canada displays many similarities to the Australian situation. In relation to privacy legislation, there is a privacy framework that consists of a federal public sector Act, recently introduced private sector legislation and a patchwork of provincial legislation to work under this. The key difference appears to be in the way in which the e-health initiatives are being implemented, and the way privacy issues are being handled. The federal proposal for the Canada Health Infoway appears to have established a much clearer strategy for how such a system will be implemented across different levels of government than the Australian Commonwealth HealthConnect Proposal.

A common criticism of all the e-health proposals discussed appears to be the lack of widespread public consultation on what is actually proposed and the implications of this for how individuals information will be handled. Along with this is an acknowledgement that, without public support, the systems cannot work.

Possible lessons to be gained from overseas experience:

- A consistent, strong legislative based privacy regime that is widely accepted by health providers and consumers is essential
- Any unique identifier should be strictly limited in its use to the e-health system only (and prohibited by legislation against further uses) and it must be applied across the system

- Implementation of both the e-health initiatives and the privacy standards within those initiatives will be more successful if implemented from the local level in the first instance and not applied from above as a large, national system.
- To be successful, any system must first of all be open to public consultation and scrutiny, and gain wide public support

Further information

New Zealand

NZ Ministry of Health: <http://www.moh.govt.nz/>

New Zealand Health Information Service: <http://www.nzhis.govt.nz/>

New Zealand Health Funding Authority: <http://www.hfa.govt.nz/>

Health Research Council of New Zealand: <http://www.hrc.govt.nz/>

New Zealand Office of the Privacy Commissioner: <http://www.privacy.org.nz/>

United Kingdom

National Health Service (NHS): <http://www.doh.gov.uk/nhs.htm>

NHS Information Strategy: <http://www.nhsia.nhs.uk/strategy/full/contents.htm>

Caldicott Report: <http://www.doh.gov.uk/confiden/crep.htm>

UK Data Protection Commissioner: <http://www.dataprotection.gov.uk/>

Canada

Health Canada: <http://www.hc-sc.gc.ca/english/index.htm>

Office of Health and the Information Highway: <http://www.hc-sc.gc.ca/ohih-bsi/>

Privacy Commissioner of Canada: http://www.privcom.gc.ca/english/01_e.htm

United States

Electronic Privacy Information Center: www.epic.org

Department of Health and Human Services: www.dhhs.gov

The Privacy Page: www.privacy.org

Legal Information Institute, Cornell Law School: www.law.cornell.edu

Appendix 2 – Written Submissions Received

Submissions were received from the following individuals and organizations:

1. K.H. Thomas
2. Brendan Mills
3. Breast Cancer Action NSW
4. Social Policy Research Centre
5. Carol O'Donnell
6. E. D. Webber
7. Wollongong Health Consumers Advisory Group
8. Commonwealth Department of Health and Aged Care
9. Medical Consumers Association Inc
10. Retina Australia
11. Hornsby Ku-ring-gai Ryde Division of General Practice Ltd
12. The Royal College of Pathologists of Australasia
13. NSW Nurses Association
14. New England Area Health Service
15. TAFE NSW
16. Guardianship Tribunal
17. Consumers Health Forum of Australia
18. Commonwealth Attorney Generals Department
19. Illawarra Area Health Service
20. NSW Therapeutic Assessment Group
21. Far West Area Health Service
22. Health Communication Network Ltd
23. Royal Australasian College of Physicians
24. Barbara Wright
25. Hunter Urban Division of General Practice
26. Medical Industry Association of Australia
27. Central Sydney Area Health Service
28. Sexual Health Services Medical Directors Committee
29. Public Interest Advocacy Centre
30. NSW Health Information Management Implementation Co-ordination Group
31. Helen Poynten
32. Mental Health Co-Ordinating Council
33. Voluntary Euthanasia Society of NSW

34. Malcolm Crompton, Federal Privacy Commissioner
35. Australian Epidemiological Association
36. Wendy Keys
37. People Living With HIV/AIDS
38. Mark Paul
39. Christian Science Committee
40. Health Information Management Association
41. Australian Medical Association (NSW Branch)
42. Adam Johnston
43. Stan Stanfield

Appendix 3 – Consultations

Public Consultations

Consumers Health Forum workshop held at the YWCA Conference Centre on Friday 3rd November 2000.

Public forums, advertised in the Sydney Morning Herald and Daily Telegraph, and held at the State Parliament House Theaterette on Wednesday 8th November and Thursday 9th November.

Consultations held directly with the Committee

Mr Peter Williams
Director Information Management and Clinical Systems
NSW Health Department

Dr Diana Horvath AO
Chief Executive Officer
Central Sydney Area Health Service and co-chair NSW Health Information
Management Implementation Co-ordination Group

Emeritus Professor Beverley Raphael AM
Director, Centre for Mental Health

Professor Marie Bashir AO
Area Director of Mental Health Services
Central Sydney Area Health Service and Chair, Mental Health Implementation Group

Consultants used by the Committee

Stuart Oliver

Tonya Rooney