A Health Information Network for Australia

Report to Health Ministers by the National Electronic Health Records Taskforce

July 2000

ISBN 0 642 44668 7

First published: July 2000

Requests for copies and inquiries regarding *A Health Information Network for Australia* may be made to the following address.

Director
Information Policy Section, MDP 12
Department of Health and Aged Care
GPO Box 9848
Canberra ACT 2601
Email: NHIMAC.Secretariat@health.gov.au

TERMS OF REFERENCE

The Taskforce's terms of reference were to:

- Evaluate the benefits and difficulties of a national approach to electronic health records that respects the dignity of each health consumer and allows them to enjoy improved health outcomes delivered more effectively by health providers.

- Consult widely with stakeholders to identify the form and key components of an effective electronic health records system suitable for Australia.

- Develop specifications (including the functions – administrative, clinical and policy/planning uses – core data items etc) for the key components of electronic health record systems, drawing on work in progress and seeking advice from relevant sources.

- Describe the building blocks that will need to be put in place to enable electronic health record systems to operate (such as issues concerning record linkage, security/authentication, telecommunications, messaging, imaging standards and coding).

- Review progress that has already been achieved, define the additional work program that needs to be undertaken and determine who should undertake the work, including, where necessary, the creation of new working partnerships:

    - to develop and implement the key components of electronic health records;
    - to develop and establish the building blocks that will underpin the operation of electronic health records; and
    - to define the implementation and ongoing governance arrangements for electronic health records.

- Develop a plan, nominate priorities and provide a timetable to develop electronic health records in Australia.

- Cost the plan and provide an indicative timetable.

- Report to Health Ministers by July 2000, recommending a way ahead for the development of nationally coordinated and integrated electronic health records for Australia.

NATIONAL ELECTRONIC HEALTH RECORDS TASKFORCE

20 June 2000

Professor Richard Smallwood
Chair, National Health Information Management Advisory Council

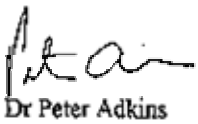
Dear Professor Smallwood

It is with pleasure that members of the National Electronic Health Records Taskforce forward to the National Health Information Management Advisory Council our report *A Health Information Network for Australia*. We propose that the report be referred to the upcoming Australian Health Ministers' Conference for consideration and decision.

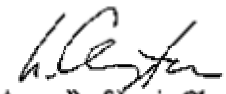
Yours sincerely

Ms Lynelle Briggs
Chair

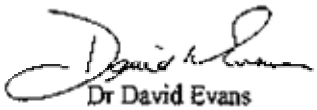
Mr Peter Williams
Deputy Chair



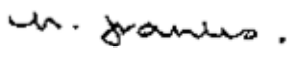
Dr Peter Adkins
Member



Assoc Prof Lexie Clayton
Member

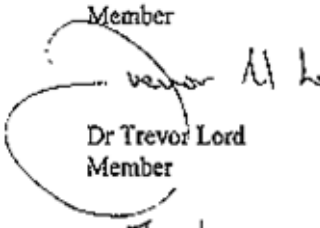


Dr David Evans
Member



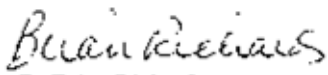
Ms Natalie Franks
Member

Mr Keith Kranz
Member



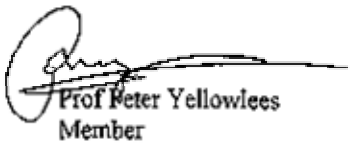
Dr Trevor Lord
Member

Dr Richard Madden
Member



Dr Brian Richards
Member

Dr Tom Stubbs
Member



Prof Peter Yellowlees
Member

Prof Neville Yeomans
Member

FOREWORD

The health sector is on the threshold of great changes as a result of new and evolving information and communication technologies and their power to improve the health and wellbeing of Australians by transforming the way health care is delivered in this country. We are now embarking on a complete re-shaping of the way in which we use information in the health system to turn the focus back to where it should be — on consumers and the communities they live in.

Over recent years there has been a great deal of resources committed to improving the integration of care and reducing the isolation and sense of powerlessness that health consumers experience all too often in a health care system marked by artificial boundaries, both professional and sectoral. However, despite the substantial gains to date, consumers and providers are still having to go over the same old ground each time a person presents to a new service or provider, and critical information is not available when and where it's most needed — at the point of care.

New technologies such as integrated electronic health records can provide the tools with which consumers can more readily share their valuable health information with the health care providers of their choice, and thereby improve the quality of their care and their health outcomes. Having access to such information means that consumers and providers will be in a better position to make more informed decisions in partnership, based on solid information and not just 'best guesses' and imperfect recall.

Already, we are witnessing a multitude of innovations in the health information management and information technology arena. Until recently, however, cohesiveness and a strategic purpose has been missing from much of this activity, resulting in less than optimal use of scarce health care resources. To this end, in November 1999, the National Health Information Management Advisory Council released *Health Online: A Health Information Action Plan for Australia*. A key area of work to emerge from this national strategic plan has been the establishment of the National Electronic Health Records Taskforce by Australian Health Ministers through the Council. The Taskforce has been charged by Health Ministers with developing a co-ordinated approach to electronic health records in Australia.

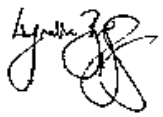
Over time, electronic health records will be adopted by most providers of health care — and used by health consumers — regardless of the existence of a national framework. However, we run the very real risk of wasting substantial resources through duplication of effort and the creation of incompatible systems that could endanger people's health through an inability to transfer critical information in a timely way. A national approach is both preferred and recommended by the Taskforce.

An integral part of the work of the Taskforce is a commitment to ensuring that a robust framework is created to protect the privacy of personal health information. Such information is extremely sensitive, and consumers need to be confident that their information is valued, that their privacy will be respected, and that such information will be used to both improve their own health and that of the community as a whole.

Initially, thought was given to the possibility of creating a single electronic health record system. This idea has been replaced by a proposal to build an information 'network' that can evolve from work already being undertaken by the many stakeholders in the health sector. The proposed information network will allow great flexibility to collect, exchange and store information for those who consent to participate — both consumers and providers. The Taskforce has also been mindful in its recommendations of the need to put in place necessary 'building blocks' that will allow a network to function: privacy, consumer identification, standards etc. Governance will also be crucial and the Taskforce has recommended a separate access control authority to provide independent scrutiny and regulation. Lastly, the Taskforce has been cognisant of the need to plan for the future, but hasten slowly. This is an exciting proposal but one that will need to be developed with the engagement of the Australian community. The report also recommends the establishment of a lead implementation site (or sites) to test the concept and provide an opportunity for people to see it working in practice and demonstrating its worth.

I would like to take this opportunity to thank all those people who contributed to the work of the Taskforce: first, my fellow members who contributed their time and expertise and their considerable personal efforts in preparing important briefing papers; second, the many individuals and organisations who attended the public consultations and made submissions to the Taskforce (and whose contributions significantly shaped the final proposal); third, the consultants who produced several major papers — particularly the work of the team from Flinders University led by Dr Sam Heard. Finally, I would like to thank the members of the secretariat (Phil Hagan, Paul Fitzgerald, Jane Aitken, Chris Mount, Chris Kelman and Jarrad Houghton) who not only supported the Taskforce but contributed substantially to the intellectual content and the writing of the report.

This report represents a landmark in bringing together the evidence and opinions from around the country and from overseas, to build a better health care system for the Australian people. I am therefore very honoured to present to Health Ministers, on behalf of the National Electronic Health Records Taskforce, the *Health Information Network for Australia* report.



Lynelle Briggs
Chair, National Electronic Health Records Taskforce

20 June 2000

CONTENTS

Part C: How do we get there?

Part D: Appendixes

Tables

Figures

Boxes

Acronyms and abbreviations

A glossary of terms is located at the end of the report.

ABS	Australian Bureau of Statistics
AHMAC	Australian Health Ministers' Advisory Council
AHMC	Australian Health Ministers' Conference
AIHW	Australian Institute of Health and Welfare
AIM	Advanced Informatics in Medicine
ANSI	American National Standards Institute
CEN	The European Committee for Standardisation
CHDM	Conceptual Health Data Model
CHIME	Community Health Information Management Enterprise
CHIPP	Canada Health Infostructure Partnerships Program
CHN	Canadian Health Network
CIHI	Canadian Institute for Health Information
CORBAMed	Common Object Request Broker Architecture for Medicine
CPR	Computer-based Patient Record
CPRI	Computer-based Patient Record Institute
DES	Data Encryption Standard
DHAC	Department of Health and Aged Care
EC	European Community
EDI	Electronic Data Exchange
EHR	Electronic Health Record
EPR	Electronic Patient Record
EU	European Union
GALEN	Generalised Architecture for Languages, Encyclopaedias and Nomenclatures in Medicine
GDP	Gross Domestic Product
GEHR	Good Electronic (formerly European) Health Record
GP	general practitioner
GPCG	General Practice Computing Group
GUI	Graphical User Interface
HIC	Health Insurance Commission
HIN	Health Information Networking
HINA	Health Information Network Australia
HISP	Health Infrastructure Support Program
HL7	Health Level 7
HMRI	Hospital Medical Records Institute
HTML	Hyper Text Mark-up Language
ICD	International Classification of Diseases
ICIDH	International Classification of Impairments, Disability and Handicaps
ICTs	information and communication technologies

IOM	Institute of Medicine (USA)
ISO	International Standards Organisation
IT	Information Technology
LOINC	Logical Observation and Identifier Names and Codes
MB	Megabyte
MWS	Medical Warning System
NCCH	National Centre for Classification in Health
NHDD	National Health Data Dictionary
NHI	National Health Index (NZ)
NHIMAC	National Health Information Management Advisory Council
NHIMG	National Health Information Management Group
NHMRC	National Health and Medical Research Council
NHS	National Health Service (UK)
NHSnet	National Health Service Network (UK)
NICE	National Institute for Clinical Excellence (UK)
NZHIS	New Zealand Health Information Service
OACIS	Open Architecture Clinical Information System
OHIH	Office of Health and the Information Highway (Canada)
OHPA	Ontario Health Providers Association
PCN	Primary Care Network
PIN	Personal Identification Number
PIT	Pathology Information Transfer
PKAF	Public Key Authentication Framework
PKI	Public Key Infrastructure
PMI	Patient Master Index
PROREC	PROmotion Strategy for European electronic health care RECords
RACGP	Royal Australian College of General Practitioners
RAS	Remote Access Server
RIM	Reference Information Model
SNOMED	Systematised Nomenclature of Medicine
UMLS	Unified Medical Language System
UN/EDIFACT	United Nation Directories for Electronic Data Interchange for Administration, Commerce and Transport
USA	United States of America
VPN	Virtual Private Network
WHO	World Health Organisation
XML	Extensible Mark-up Language

SUMMARY

Australia now has a unique opportunity to invest in the health of its people by building a national health information network to support a system of electronic health records for those who want to share potentially vital information with their various health care providers. Such an investment holds the promise of better health, higher-quality care while improving personal privacy because the information that providers need to know will be accessible when and where it is needed (in contrast to the existing situation with paper-based records). The aim is to ensure that information is used to help consumers receive the best possible care. Building such a network will be a challenging task, not just because of the complexity of modern health care practice but also because consumers will demand control over their personal health information, including that it is only made available to authorised people on a need-to-know basis and that their privacy and dignity is respected at all times.

The principal reason for building a system to support the sharing of electronic health records in Australia is to improve the health and wellbeing of those Australians who want to participate. Better health outcomes, better quality of care and better consumer safety will be achieved by such a system as a result of such things as:

- better consumer access to their own health information and therefore consumers being able to make more informed decisions about their own health care;
- better provider access to information (with consumer consent) at the point of care;
- fewer diagnostic tests (including elimination of redundant tests);
- improved warnings and alerts to counter avoidable error (eg adverse drug interactions); and
- better planned and co-ordinated care (including the capacity to develop comprehensive care plans that providers and consumers alike would use).

Electronic health records will also be a significant contributor to increased consumer safety. As a recent US report points out,[1] the annual toll from preventable errors exceeds the combined number of deaths and injuries from road and air crashes, suicides, falls, poisonings and drownings.

[1] Kohn LT, Corrigan JM, Donaldson MS (1999), eds. *To err is human, Building a safer health system*, National Academy Press, Washington DC.

This report, prepared by the National Electronic Health Records Taskforce, investigates the potential of electronic health records to improve the health of Australians via access to accurate and immediately accessible information. The report concludes electronic health records will be an important underpinning to quality health care and improved personal privacy in Australia in the future. The report of the Taskforce develops a proposal for electronic health records in Australia, including the necessary building blocks (privacy, security, messaging standards etc) and governance arrangements to implement a national approach.

Background and context

Even in a materialistic world, health comes before wealth as Australians' most prized possession. We all wish for the very best of health for ourselves, our family and our friends (ie to be fit and well). Accordingly, the goal of health departments is usually cast in terms of securing better care for consumers and improved health and wellbeing for all.

Thus, governments around the world are increasingly concerned not just with growing the economy but also with improving living standards broadly defined. When it comes to health, most Australians would agree that the fruits of what modern health care has to offer should be shared widely within the community and not be confined, for example, to those able to afford the very best of care.

Any general health objective needs to be pursued, however, within the constraints of available resources. The necessarily limited resources a society can afford to devote to health imply having to choose between competing priorities at every level: from how much to spend on preventive versus curative versus palliative measures at the highest level right down the line to detailed operational decisions — such as how much of an individual organisation's budget to devote to gathering information and deploying modern information and communication technologies versus satisfying other pressing demands. And since so much of health care spending is funded from general taxation in Australia, it is understandable that the community wants to participate meaningfully in what are, in effect, collective decisions with so much potential to affect individuals' wellbeing.

Health improvement also needs to be pursued in a way that respects individual's human dignity. A system which gives individual health consumers a feeling of powerlessness is unacceptable. This report is about leveraging in a cost-effective way new technologies to achieve better health while at the same time improving personal privacy for all Australians irrespective of their personal circumstances or where they live. In particular, it advocates devoting considerable time, effort and expense to building a health information network for Australia. With such a valuable resource in place, no longer would those seeking health care have to repeatedly recount their health histories at every turn, nor be worried about inappropriate use of their personal health information — their (electronic) health

records would follow them and be available every time they encounter the health system (if that is their wish). Indeed, the availability of health information where and when it is needed will revolutionise the health care system as we know and experience it today.

This report charts a way forward in order to bring new information and communication technologies to bear on the ongoing challenge of providing the best of care at affordable cost, setting out two and five-year milestones along the way to building a cost-effective health information network for all Australians.

What are electronic health records?

There are several definitions of just what constitutes an electronic health record (sometimes also called a computer-based patient record). The Taskforce favours the following view of electronic health records:[2]

> An electronic longitudinal collection of personal health information, usually based on the individual, entered or accepted by health care providers, which can be distributed over a number of sites or aggregated at a particular source. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of the consumer and is stored and transmitted securely.

The following is typical of other definitions that have been advanced:[3]

> An electronic health record is any information relating to the past, present or future physical/mental health, or condition of an individual which resides in electronic system(s) used to capture, transmit, receive, store, retrieve, link, and manipulate multimedia data for the primary purpose of providing health care and health-related services.

A *system* of electronic health records would include all the infrastructure necessary to bring such records online so that, with the consent of the individual concerned, authorised users (eg medical practitioners) could gain access to those parts of the record that will aid decision making at the point of care. Advice on care options could also be informed by other decision-support applications using both personal and other health information (eg best practice guidelines) to automatically generate aids like alerts and reminders of various kinds.

Information from specified parts of the record would also be valuable for other authorised purposes (eg for medical research and for administrative and statistical purposes) — many of which could use de-identified information from the record (ie information which is not traceable to the individual to whom it relates). An obvious health application for de-identified data from electronic health records would be to strengthen the evidence basis of health care interventions (ie what seems to work under what circumstances?). Such applications for the information contained in

---

2 This definition is based on discussion with stakeholders at the public consultations and feedback received through a public submission process (see Chapter 8).

3 Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.5).

electronic health records would, of course, have to be authorised (eg via expressed permission of the individual or declared by an independent access control authority to be in the interests of the community as a whole).

Given that the necessary infrastructure would not only have to support a system of electronic health records but also applications which add value to the basic data in various ways, what is effectively involved is building a trusted *network* dedicated exclusively to health information.

The Taskforce settled on the following statement as a basic set of objectives for a national approach to electronic health records. The statement consists of three key parts. The first part describes the overarching objective, which focuses on securing better health outcomes for Australians while enhancing their personal privacy. The second part highlights key areas in which a national health information network can contribute to efforts to realise the overall objective. The final part describes the mechanism through which these contributions will be achieved — emphasising the need for a national approach.

Objectives Statement

Improved delivery of health care and better quality of care, consumer safety and health outcomes for all Australians while enhancing the privacy and respecting the dignity of health consumers by:

- empowering consumers to be able to take a greater responsibility for their own health care and be better informed about the choices available to them in respect of their health care;
- ensuring better decision making which is shared by both consumers and health providers at the point of care;
- providing a flexible, seamless and integrated process of care through the sharing and better exchange of information;
- providing better access to health care, particularly in rural and remote areas;
- building a best-practice, evidence based health system;
- encouraging better, more targeted health initiatives; and
- informing research, learning and training;

through developing a nationally coordinated and distributed system of electronic health records, which is based on the greater use of online technologies.

Benefits of electronic health records

Consumers of health care services have the most to gain from the successful introduction of electronic health records on a national basis. Indeed securing better health outcomes for all Australians than is currently possible with paper-based records is *the rationale* for building a health information network Australia-wide.

In order to thus attain good health and make informed health care decisions, people need accurate and up-to-date information. As the introduction to this summary points out, the ability to exchange personal health information (provided the consumer consents) and other kinds of health information (eg 'best practice' guidelines) via a secure network will improve health outcomes by, for example: enabling better co-ordination of care at the point of care; eliminating any need to have diagnostic tests redone unnecessarily; and reducing the potential for medical misadventure.

An important initiative in this regard is the recently announced *Better Medication Management System for Australia*. Seen by the Taskforce as an integral component of the future electronic health record, the proposal is to create an electronic record of medications dispensed to an individual and make that information available to medical practitioners and pharmacists — provided that that is the expressed wish of the individual concerned. Knowing what medications a consumer has had prescribed will greatly assist prescribers to avoid potential adverse drug interactions. Indeed, such alerts could be generated automatically and brought to the attention of both provider and consumer alike, in the process encouraging active participation in pharmaceutical prescribing on the part of the provider, the pharmacist and the consumer. Of course, such a system must incorporate the privacy and security safeguards advocated for the electronic health record more generally in this report.

To secure the promised benefits of electronic health records, consumers will need convincing evidence that the system has been designed to meet their needs and works to their advantage. Importantly, their records must be accessible when required for any purpose they deem necessary for their health and wellbeing. These purposes are likely to vary considerably from person to person, with older people and the chronically ill likely wanting more open communication and continuity of care, and younger people likely to place more emphasis on privacy and security considerations. A necessary pre-condition will therefore be to involve health consumers in the design of the network.

The necessary level of consumer confidence is only likely to be established when they can check both the content of their records and who has accessed them, when and why. They also need the reassurance that, should breaches of confidentiality occur, they will be able to seek redress via a complaints mechanism and suitable sanctions for unwarranted breaches of their privacy.

It is important to establish what users actually want, for example what applications and services health care providers believe are important and which could be provided in a more timely and cost-effective way electronically. For example, health care providers should be able to easily send and receive information electronically about consumers they are treating. This will save them time, effort and the frustration they often feel when at the mercy of manual methods in a paper-based system.

Tools like secure electronic communications (eg e-mail), ready access by providers to the health history of their patients, and just as ready access to the latest research findings and suggested best practice in treating their patients will make life a lot easier for providers.

Health care providers will be key users of the network and will need to accept the system if it is to fulfil its promise. As is the case for consumers, it will be essential to involve health care providers in the design of the network. Even so, achieving provider acceptance will not be straight forward and will certainly require training and support. Nevertheless, once operational and having gained the acceptance of both consumers and health care providers, the worth of the network will manifest itself in better health for consumers with providers able to spend more time actually providing care and counsel because the information-gathering side of things will be far less time consuming with the advent of the network.

To develop a better understanding of the interaction between health care delivery and the health of the population and to develop a more strategic approach to health care delivery requires bringing together public health information (such as births or cancer registry data) with information gathered from individual health encounters subject to individual consumer consent (such as would become available via a system of electronic health records). Making the necessary connections between these various kinds of data will provide a more complete picture of health care than decision makers have had access to so far, contribute to the evidence basis for health care interventions (by establishing what works; for whom and under what circumstances), and where additional resources should be targeted to secure the greatest health gains.

Risks in implementing electronic health records

Systems of electronic health records have proved very difficult to design and implement successfully. Issues to be overcome include: reassuring consumers that their privacy will be protected; the need to stick to agreed terminology; the challenges surrounding entering data on the record; providing decision-support tools which health care providers value; and ensuring access only to authorised users.

There are also moral, legal and ethical issues to be considered. Health records contain highly sensitive information (eg they may contain information about mental health, sexuality, drug use, genetic test results and HIV/AIDS and hepatitis status). Although the public has a high level of trust in current practices designed to protect the privacy of their medical records, new technologies and associated media attention have heightened consumer concern about privacy in the information age. Consumers are thus understandably concerned that use of new information and communication technologies may mean that their personal health information may

fall into the wrong hands (eg that it may be used to discriminate against them in areas like the workplace or in taking out insurance).

Gaining the acceptance of consumers in a world of electronic health records will mean reassuring them that they will control who will have access to the record (or to just parts of it if that is their wish) and, for what purposes — and that appropriate mechanisms are in place to ensure this. They will also expect that, in the event that their confidentiality is breached, offenders will be identified and appropriate penalties imposed.

As primary users of electronic health records, health care providers and health consumers must be intimately involved in the design of the system. That is why they have been represented on the Taskforce and must be totally involved in the specifics as the proposal progresses (eg in the nature and content of the various health summaries which would feed into the individual record). Providers will also have to 'champion' the proposal to their peers, if it is to be successful and make a difference on the ground to the health of Australians.

Gaining the acceptance of health care providers in a world of electronic health records will mean reassuring them that, provided the necessary permissions are in place when it comes to personal health information, they will have access to all the information that they would want to aid in decision making at the point of care. Such information would extend beyond that contained in the individual health record to encompass access to relevant 'knowledgebases' and decision-support tools (such as recommended guidelines and treatment protocols). Ultimately, provider acceptance will only be won if having access to the network makes their jobs easier eg by cutting down on the time spent on gathering information and thus increasing the time providers can spend on the actual task of caring for consumers of their services.

There are also lessons to be learned from implementing complex systems:

- implementation needs to be incremental;
- it needs to be flexible enough to adjust to the emergence of new technology;
- electronic health record systems significantly alter work practices and potentially, consumer habits;
- it is preferable to start with a sound system that has been evaluated in its development;
- it can take many years to implement an effective system;
- involvement of users, including health consumers, is essential in design and testing;
- the implementation team must have a leader who is clinically orientated, understands the problems, is available to users; and
- projects must have an ongoing evaluation component to justify costs.

Although systems may not deliver all they promised (especially from the beginning) because of technical difficulties, most implementation issues revolve around human rather than technical considerations, and can thus be addressed. Thus 'people problems' are recognised as more important than 'technical problems'. The following are typical conclusions:

- most providers and consumers anticipate enough benefits to be willing to use the system;
- computers must be accessible, easy to log onto, and provide for interrupted sessions;
- many providers and consumers are concerned about losing eye contact with each other;
- it is unrealistic to expect even good keyboard operators to enter their own lengthy notes;
- staged implementation, with order entry introduced first, may help providers and consumers adapt gradually;
- training should include dedicated time for instructional sessions for providers, simulated consumer encounters to help providers adapt their practice patterns, and tutors available to answer questions in the clinical setting; and
- corresponding training and learning opportunities should also be provided to interested health consumers.

As well as implementation challenges, building complex systems — such as a system of electronic health records — inevitably involves overcoming numerous technical issues, in this case including:

- devising effective and efficient ways of getting health care providers to enter the information from which the record is constructed, which can involve a combination of fact, opinion and intuition/guesswork/deduction;
- presenting and tailoring 'views' of information from the record in ways that health care providers and health consumers find valuable, which can range from simple repackaging of data through to sophisticated transformation of the basic information to provide new insights;
- striking an appropriate balance between free text (permitting maximum freedom of expression) and use of an agreed, structured vocabulary so that, for example, information from individual records can be aggregated and analysed without risking 'apples and oranges' comparisons; and
- encoding information such as sounds and images requires a very large amount of digital data compared to text, which will likely stretch the installed storage capacities beyond their limits — for example a typical US medical centre generates 3.5 terabytes of data a year.

Building complex systems also costs a lot of money. This can be a sticking point even when other necessary resources (such as the skills and commitment of the people who can deliver the system) can be marshalled. That is why the Taskforce

proposes a staged approach, construction of a 'lead implementation' site to trial the full proposal on a small-scale, periodic milestones for the full implementation, and reviews of progress and demonstrated value for money invested.

It is also why the Taskforce proposes to start by automating existing health summaries which providers regularly use at the moment (or would dearly like to have access to), and to gradually incorporate more sophisticated solutions over time once the value of the system has been demonstrated.

Need for a nationally co-ordinated approach

Systems of electronic health records have already been implemented in Australia at a local level (eg individual hospital departments) and more ambitious ones are planned, if not on the verge of being rolled out. The opportunity to build a national system — rather than ending up with a series of incompatible implementations that cannot talk to one another — may therefore soon pass. That would be a pity given that there are only 19 million of us, we are a highly mobile population and as a community can ill afford to squander scarce resources.

Thus, a national approach to electronic health records in Australia is almost certainly warranted based on experience with their development so far in this country and overseas, and given the divergent approaches that have been implemented to this point. However, the future will be determined to a great extent by decisions made in the present. Charting a national approach to electronic health records and health information more generally requires a creative but cohesive vision, along with the necessary leadership backed by a determination to succeed.

The Taskforce urges Health Ministers to seize the opportunity to agree on and jointly commit to a national approach to electronic health records to provide universal access to the information contained in them, if that is the wish of the individuals concerned.

What is being proposed?

The Taskforce’s deliberations led it to think in terms of a general framework for health information exchange, rather than a structure purpose built just to support electronic health records — something more in tune with what came out of the public consultation and submissions process, and also something that can be used flexibly and be adapted to the evolving needs of multiple users.

Specifically, what the Taskforce proposes is the building of a national health information network (proposed working title Health Information Network Australia (HINA)) which provides for the systematic collection of clinical and demographic information at the point of care. This information would take the form of event summaries (which themselves will require definition and agreement about standard

data items) rather than the full set of information that providers may collect for each episode of care. Event summaries would include basic information about the outcome of a general practitioner consultation, a hospital discharge report or referral, a summary of pathology investigations, etc.

Information would be collected only for those consumers and providers who agreed to participate. Furthermore, the data collected in event summaries would need to be agreed with the potential users of the health information network — that is, consumers, providers and health care administrators, researchers and planners. As indicated by the proposed working title, these event summaries would be nationally agreed documents.

The scheme would also provide for the storage of these event summaries in a standard format — so that they can be retrieved at a later time and also so that the information they contain can be assembled in a different format, according to the requirements of the network's authorised users.

The nature and location of storage facilities proposed as key components of the network is such as to allow storage to be as close as practicable to the point of care that generated the event summary in the first place. In the case of a hospital, for example, the hospital discharge summary or referral could be expected to be stored at the hospital itself. This would also almost certainly be the case for pathology records. In the case of general practice, providers are likely to choose to store information in a secure host facility at a regional level. The Health Insurance Commission (HIC), the private sector or the Divisions of General Practice could be involved in establishing and maintaining such facilities.

The final decision on storage arrangements would be left to participating providers and would be influenced by issues such as cost and the ability of individual providers to meet the standard storage format requirements, mandated security standards and functional specifications, such as provider speed of access to information.

Finally, the proposal includes provision for accessing the information held in the standard format repositories. This is where the real value of the network will be realised — as users of the network (consumers, providers and planners) will be able to assemble different views of the information according to their needs, provided that consumers consent to meeting those needs.

As well as providing for the creation and storage of electronic health records and access to information contained in them by authorised users (including health consumers), the proposed national health information network would facilitate other types of transactions as well — including such things as:

- electronic booking and reminder systems (eg consultations with and hospital admissions);
- provider access to 'best practice' guidelines, the latest research findings and other kinds of knowledgebases;

- telehealth services;
- secure provider-provider communications;
- ongoing education and training for providers;
- decision-support applications to assist providers in care delivery (eg medical alerts and reminders); and
- access for consumers to their own health information.

Necessary building blocks

Health Information Network Australia (HINA) cannot come into existence without the necessary 'building blocks' being put in place first. The most important of these the Taskforce sees as:

- privacy, confidentiality and security;
- standards;
- telecommunications infrastructure; and
- encouraging uptake and use of information technology.

People reveal highly sensitive information to health care providers. If this information were used inappropriately, it might lead to serious consequences for the individual — such as being refused insurance, a job or a bank loan. Furthermore, in these circumstances, it may be difficult for the individual to recover from such disclosure or hold anyone accountable. Any new health data record-keeping system — such as a system of electronic health records — must therefore ensure that information is used appropriately or people will not use it.

Several issues are involved. First, personal health information needs to be kept *confidential* — it should be used only for approved purposes and shared only among authorised people (typically associated with the consumer by a special relationship, such as the provider-consumer relationship).

Second, an appropriate level of *privacy* for the information must be established — to ensure that an individual's right to keep his or her personal health information confidential is maintained while also realising the benefits that can accrue to society if the information is shared more broadly.

Finally, electronic health records must be protected by adequate *security* — that is, administrative and technical measures must safeguard them against loss, modification, or inappropriate dissemination.

Measures that need to be put in place to satisfy privacy, confidentiality and security imperatives are discussed in Chapter 10.

More generally, lack of widely agreed and implemented standards for health information is a factor that has hindered implementation of health records in electronic form. Until health care providers collect data in a standard format

according to widely accepted definitions, it is virtually impossible to connect data generated in various parts of the health care system in any meaningful way. This is a challenging task, if only because the health care system has highly heterogenous data and information needs.

In addition to the security standards under the collective heading of privacy, confidentiality and security, the Taskforce considers that agreed standards need to be implemented in the following areas to allow HINA to operate (see discussion in Chapter 10):

- data standards;
- classification and coding standards;
- messaging standards; and
- information storage standards.

A system of electronic health records will require appropriate infrastructure on which to run. Networks provide a physical channel for exchange of data between computers and have become commonplace in most settings heavily dependent on computer-aided assistance (now most sectors of the economy). What health needs is its own 'virtual network' which takes advantage of the existing, installed telecommunications infrastructure but adds the necessary security to what is basically an insecure public system (eg the Internet).

Additional investment in telecommunications and information storage infrastructure is almost certain to be needed to support the capabilities required by HINA. The Taskforce proposes that work be undertaken to:

- identify an affordable and cost-effective strategic direction for health telecommunications over the next 3 to 5 years, identifying and describing service requirements, infrastructure requirements, key projects, management and organisational arrangements (including staffing and training); and
- assist the development of communications infrastructure options with a standard approach to enable health care providers to link to each other to form regional, state-wide and, eventually, a national information network.

Health care providers, who will bear the main responsibility for entering the information to form the basis of a national system of electronic health records, will need to be supported and encouraged in this vital work. This will mean assistance in acquiring the necessary computer hardware and software to connect to HINA, along with appropriate training and support.

Network governance

The Taskforce considers that there are three broadly defined areas of activity involved in setting up the network. The first concerns defining the detailed operational policy, setting the business rules and managing the process. The second concerns the actual implementation of the network and developing the underpinning building blocks. The third involves access — determining access rules, how consent will operate, appropriate uses etc, and regulating access (including sanctions for breaches of privacy/security).

The Taskforce has proposed two alternatives for governance of policy and delivery functions. The first is based on using existing structures — hence the National Health Information Management Advisory Council (NHIMAC) (through a continuation of the Taskforce) could take on the role of overseeing the development of HINA. The work (policy, planning, overall management, service level agreements with delivery agencies, monitoring progress etc) would be undertaken in an existing agency, possibly the Commonwealth Department of Health and Aged Care. The second alternative is the establishment of a not-for-profit company. This would provide the necessary independence from any one jurisdiction, allow appropriate representation from all sectors and at the same time could have a sufficiently robust constitution to allow it to function with a reasonable level of autonomy. In each model, the governance body would contract out construction of HINA (to the HIC and other delivery agencies).

The Taskforce sees the access control function to be the responsibility of a separate body similar in nature to the Office of the Federal Privacy Commissioner.

Staged implementation of the Network

Implementing HINA is clearly not a simple task. The building blocks alone are complex. Much of the work in this area is relatively undeveloped. Some elements, including, for example, the standard format data storage arrangements, are untried in a large-scale operational environment. Accordingly, the Taskforce proposes that a separate health information network lead implementation project be established to prove the concepts and technical feasibility of the Network and its underpinning building blocks in an experimental environment that can be closely monitored and managed.

Apart from these technical issues, the implementation of HINA in its fully developed form is a major undertaking and one that will require a substantial cultural change. The Taskforce therefore also proposes that a significant investment be made in educating consumers and providers and publicising the benefits for consumers and the wider community through their increased participation in HINA.

In recognising these complexities, the Taskforce proposes a three-staged approach to the full implementation of the Network, with the view to having HINA operationalised within five years. The three stages are:

Stage 1 — Design and development (years 1-2);

Stage 2 — Construction and initial operationalisation (years 2-5); and

Stage 3 — Growth and expansion (beyond 5 years).

Estimated benefits and costs

Work is still underway concerning the nature and dimensions of the savings that could be realised from the introduction of the health information network. However, initial modelling of savings (see Chapter 13) that could be attributed to positive impacts such as: reduced deaths from adverse events; reductions in the costs of care through reduced hospitalisations; increased productivity through reduced days absent from work; reduced costs of disability resulting from adverse events; and product registries — suggests that annual gains could be in the billions of dollars.

The Taskforce has also had an independent costing consultant working on the costs side of the equation. Again work remains indicative only (see Appendix G). Nevertheless, indications are that for a relatively small investment, in the order of $120 million over 10 years, much in the way of the governance and the building blocks can be developed —including privacy, confidentiality, security and authentication, standards development, a telecommunications strategy, uptake of technology and community liaison — as well as the development of the lead implementation site(s) and communications strategy.

The establishment and operation of the information storage facilities, communications costs and investment in source systems would bring the network into full operation (takeup rate estimated to be in the order of 80% by year 10) and by then the savings would be expected to be clearly evident. The all up costs, currently estimated to be in the order of $440 million over 10 years, would therefore be offset by measurable savings by that time. Costs will also need to be apportioned because the costers have provided a full system cost. Costs will need to be attributed to the private sector and to the public sector on an agreed Commonwealth/State cost shared basis.

Necessarily evolutionary nature of the Network

Of necessity, developments in electronic health records are evolutionary. This is inevitable because of:

- the evolutionary nature of the technologies which make them possible (including the emergence of completely new technologies);

- changing disease patterns and our understanding of them; and
- evolving uses to which the information contained in electronic health records will be put.

Successful initial applications will breed greater acceptance of later, more complex applications because the attitude of users towards computer access to various systems will already be positive.

RECOMMENDATIONS

Objectives Statement

The Taskforce has articulated the objectives for a national approach to electronic health records as follows:

> Improved delivery of health care and better quality of care, consumer safety and health outcomes for all Australians while enhancing the privacy and respecting the dignity of health consumers by:
>
> - empowering consumers to be able to take a greater responsibility for their own health care and be better informed about the choices available to them in respect of their health care;
> - ensuring better decision-making which is shared by both consumers and health providers at the point of care;
> - providing a flexible, seamless and integrated process of care through the sharing and better exchange of information;
> - providing better access to health care, particularly in rural and remote areas;
> - building a best-practice, evidence based health system;
> - encouraging better, more targeted health initiatives; and
> - informing research, learning and training;
>
> through developing a nationally coordinated and distributed system of electronic health records, which is based on the greater use of online technologies.

In accordance with the above statement of objectives, the Taskforce recommends that Health Ministers agree:

Need for a national approach

1. to affirm the need for a national approach to electronic health records in Australia, and to the secure networking of health information more generally (Section 7.3).

A health information network for Australia

2. to the establishment of a health information network for Australia (working title Health Information Network Australia, or HINA) as described in Chapter 9 (Section 9.7).

Necessary building blocks

3. to the establishment of a uniform data protection regime across Australia to apply to personal health information — a regime which enhances privacy and respects the dignity of individuals (Section 10.1).
4. to having individual participation based on informed consent. That is, that a framework of uses or use categories as described in Section 9.5 for the information contained within the network should be developed and communicated to consumers of health services so that they are informed about exactly what they are consenting to – in terms of what information they agree to being transferred (via HINA), to whom, and for what purposes. Only those uses that are specifically consented to should be permitted without seeking further consent. This will require that legislation be developed that sets out the way consumer consent should operate and also specifies the responsibilities and obligations of providers in respect of network operation. This would be at the core of legislation that may be required to establish HINA and its governance arrangements (Section 10.1).
5. to the establishment of a sound security framework (including public key infrastructure technology), which mandates minimum security standards for the health sector, to ensure the confidentiality of personal health information and to prevent unauthorised access to, and misuse of, the health information stored in the form of electronic health records on the network (Section 10.1).
6. to the establishment of a national health identifier to be used only in the health sector under strict privacy protocols and which is implemented concurrently with HINA. Similarly, providers and facilities/locations need to be reliably identified to eliminate any uncertainty about who was involved in an episode of care and where that care was provided (Section 10.1).
7. that the National Health Data Dictionary form the basis for an expanded set of data definitions needed for the development of the network (Section 10.2).
8. to the establishment of an expert group (which includes key players in health classification in Australia, health consumers and expert representatives of users for clinical, planning, statistical and research purposes) under the auspice of the National Health Information Management Group to be tasked to:
    - establish (by June 2001) a sustainable process for the national maintenance of classifications and terminologies, and mechanisms to facilitate interoperability through the use of an appropriate national reference terminology.
    - agree (by June 2002) upon national classification systems for all sectors identified within the framework (taking the World Health Organisation Family of Health Classifications work as a starting point); and

- establish (by June 2002), a national mechanism for the assessment and accreditation of interface terminologies in use in all health care settings. (Section 10.2).

9. that further work proceed in the area of messaging standards and, in particular, that:
   - Health Level 7 (HL7) and UN/EDIFACT be promoted in international standards forums;
   - HL7 be adopted as the messaging standard in Australia for the transfer of information within the health environment;
   - XML be investigated as the preferred technology medium to exchange health information; and
   - a message usage model be defined whereby HL7 and UN/EDIFACT can be used in a complementary way in Australia (Section 10.2).
10. that further work proceed in the area of information storage standards and, depending on evidence coming from the General Practice Computing Group (GPCG) trial, that the Good Electronic Health Record (GEHR) architecture be further tested in work associated with HINA (Section 10.2).
11. that further work be undertaken to develop comprehensive policies and standards for records management (Section 10.2).
12. to work proceeding under the auspices of the agreed governance structure for the network to:
   - identify an affordable and cost-effective strategic direction for health telecommunications over the next 3 to 5 years, identifying and describing service requirements, infrastructure requirements, key projects, management and organisational arrangements (including staffing and training); and
   - assist the development of communications infrastructure options with a standard approach to enable health care providers to link to each other to form regional, state-wide and eventually a national information network (Section 10.3).
13. that the education and training of health care providers will be vital to the success of the network, as will be gaining the acceptance and trust of health care consumers. These will be major tasks that will take time and require appropriate resourcing. The body tasked with operating the network should be charged with these education, training and consumer acceptance responsibilities (Section 10.4).

Governance

14. that governance for the HINA be based either on existing structures (NHIMAC and a governance unit in the Commonwealth Department of Health and Aged Care) or through the establishment of a not-for-profit company. Delivery of HINA be contracted out by the governance body (Section 11.3)

15. that a HINA access control authority be established within the Federal Health portfolio with similar independence to that of the Office of the Federal Privacy Commissioner (Section 11.3).

Staged implementation

16. to a staged implementation of the network in accordance with the Taskforce's proposed timetable set down in Chapter 12, noting an early focus on those applications that will create maximum impact at modest cost, namely:
    - secure communication between providers;
    - medication management;
    - pathology reporting;
    - hospital/community communication; and
    - immunisation reporting (Section 12.1).

Making a modest start

17. to the establishment of a 'lead implementation' site as a small-scale version of the full network, along with simultaneous trialing of particular network features in other settings — as a way of informing the full-scale implementation of HINA (Section 12.2).

Transition arrangements

18. that interim HINA governance arrangements be based on continuation of the Taskforce and the establishment of a special HINA Unit in the Commonwealth Department of Health and Aged Care, and that the Unit be jointly staffed and resourced by the Commonwealth and State/Territory jurisdictions (Section 12.4).

Education and publicity

19. to a network marketing model being adopted for HINA education and publicity, and that publicity be given high priority in the lead up to (and beyond) any announcement by Health Ministers (Section 12.5).
20. to the establishment of a mechanism (such as the establishment of a widely representative consumer group) to enable widespread consultation with consumer and provider organisations on announcement of HINA by Health Ministers and to the engagement of consumers and providers during the implementation of HINA (Section 12.5).

Necessary resources and review of progress

21. to set in train work, in co-operation with other jurisdictions, to further refine the likely costs of HINA, given the uncertainties that necessarily attach to the costing exercise that has been possible for this report (eg in terms of what infrastructure is already in place, or in prospect, which HINA can use) (Section 13.2).
22. to commit resources (on an agreed Commonwealth, State and Territory cost-share basis) to the first stage of implementation (as per estimated costing at Chapter 13), with a review of the network's value for money after two years (Section 13.1).

PART A

BACKGROUND AND CONTEXT

1 NATURE OF REPORT

This report examines the case for introducing a nationally consistent system of electronic health records for Australians, considers what barriers would have to be overcome in order to put such a system in place, and advances a costed proposal for consideration by Health Ministers.

The terms of reference for the Electronic Health Records Taskforce (the Taskforce) are set out on page iii. In brief, the Taskforce was asked to evaluate the benefits and difficulties of adopting a national approach to electronic health records in Australia and to propose a costed plan to Health Ministers for the introduction of such a system (including the building blocks that will need to be put in place for it to be viable).

1.1 Approach

The approach adopted by the Taskforce was to inform itself of the merits of introducing a system of electronic health records nationally by:

- commissioning an assessment of both the benefits and difficulties of introducing a national approach to electronic health records in Australia from researchers at Flinders University who are experts in the field (and whose report constitutes an accompanying paper to this report — see Appendix B), and indicative costs of the Taskforce's proposal (Appendix G);
- engaging in a process of public consultation by releasing an Issues Paper (reproduced in Appendix C), calling for written submissions and convening a series of meetings with interested parties around the country;
- learning from others' attempts to put such systems in place — both in Australia and overseas; and
- relying on its own research and the considerable expertise and experience of Taskforce members.

1.2 Information sources

There is now an extensive literature on the subject of electronic health records on which to draw, along with considerable practical experience in implementing such systems mainly on a local but also on a national scale — both in Australia and in other countries. The work of the Taskforce therefore builds on previous work undertaken here and elsewhere.

In March 2000, the Taskforce circulated an Issues Paper seeking public input into its deliberations. A summary of views expressed at the public consultations and in written submissions is incorporated into Chapter 8 of the report.

Thus, this report to Health Ministers has been developed from the first-hand knowledge and experience of members of the Taskforce, from studies commissioned by the Taskforce, from other available reports and studies (both Australian and overseas), from feedback on the Issues Paper and consultations held thereon, and from advice from various organisations with expertise in the area, including:

- the Health Insurance Commission;
- the Commonwealth Department of Health and Aged Care;
- the Australian Institute of Health and Welfare; and
- the General Practice Computing Group.

Appendix A contains a full list of the organisations and individuals with whom Taskforce members consulted and/or from whom it received written submissions. The Taskforce gratefully acknowledges the time and effort people went to in order to contribute their ideas on a system of electronic health records for Australia, especially in view of the short period available for canvassing views for incorporation in this report.

1.3 Report structure

The report begins with a summary, which concludes with the Taskforce's consolidated recommendations. The report itself is divided into four parts:

- Part A sets the scene with some background and context with regard to electronic health records, describes what they are, their benefits and difficulties which would have to be overcome in order to successfully introduce them on a national basis in Australia. This part of the report also addresses what can be learned from both Australian and overseas experiences with such systems. Part A concludes by explaining why it is in everyone's interest to adopt a national approach to electronic health records in Australia.
- Part B contains the Taskforce's specific proposal to create a national health information network which, *inter alia*, would capture, communicate and store the health records of individual Australians who choose to participate in the arrangement in a way which maintains the confidentiality of personal health information and respects the privacy and dignity of health consumers. This part of the report also spells out what needs to be done to build such a network (on which a system of electronic health records would reside), who would be responsible for building the network, how the network would operate and what security measures would be necessary to gain the trust of both consumers and health care providers.

- Part C spells out how to realise the Taskforce's proposal, dealing with the implementation phase, attempting to quantify some of the benefits, as well as addressing estimated costs of the various stages of what would constitute a significant national project.
- Finally, Part D comprises supporting material on which the report has drawn, including specially commissioned work. The report concludes with a glossary of terms and list of references.

2 BACKGROUND

> *Although the practice of medicine in Australia is increasingly 'hi-tech' (with advanced technologies being deployed in support of consumer care) new information and communication technologies have so far struggled to make a similar impact on health records (and in integrating health information more generally). This is likely to change as the barriers — which have so far militated against the use of such technologies in support of better care for Australians and a better-functioning health care system — are progressively overcome.*

Governments, on behalf of the people, pursue many objectives. Progressively raising per capita incomes in a sustainable way is a central one. But improving the quality of life enjoyed by Australians involves other, less materialistic, goals as well, including:

- improving the health status of our community by providing better health services and educational opportunities;
- encouraging greater participation in the life of local communities; and
- protecting the environment.

Thus, better health is just one aspect of the kind of living standards to which we all aspire. Ethical care, which acknowledges consumer autonomy, should be an integral component of policies and institutional arrangements designed to reward desired outcomes, eliminate perverse incentives, encourage initiative and innovation, and nurture consumer and community participation.

Widespread community and consumer participation in decision making about Australia's health system and how Australians want it to evolve in the future needs to be specially encouraged. While expert input from health care providers, administrators and policy makers is clearly necessary, consumers need to shape the system so that it operates principally for their benefit.

There are many reasons for a general lack of participation to date: consumers are not generally experts in the health sciences, and many have been happy to leave the decisions to people they trust (eg their general practitioner) — especially when they are sick and thus not in their best decision making frame of mind. But as in other areas of our lives, consumers want to have more of a say in health care decisions — and many are taking steps to be in a position to make informed decisions jointly with what is becoming an array of health care providers (rather than just the family general practitioner).

The key to greater consumer participation in health care decision-making is better information. More informed consumers will be in a better position to approach the consumer-provider relationship as more of a partnership of shared decision making (rather than the responsibility for care decisions falling disproportionately on the

provider). While some consumers may want to continue to leave all decisions to the provider, those who want to take a more active role in their health can only do so effectively if they are in a position to make informed decisions.

But how can we go about empowering consumers of health care with the right information? For that matter, is it even true that health care providers are in possession of all the information that they would want to have at the point of care in order to do the best they can for people they are trying to help?

These are challenging questions, and the issues they raise are not necessarily amenable to simple solutions. Also, there are many initiatives being pursued to improve the situation. One such initiative was the establishment of the National Health Information Management Advisory Council (NHIMAC) — an expert body set up to advise Health Ministers on the most effective and efficient use of information and communication technologies in the health sector. The Council, which met for the first time in April 1999, is rapidly becoming an important body for progressing key issues relating to information management and the use of information technologies in the health sector.

2.1 Health Online: A Health Information Action Plan for Australia

Health Online: A Health Information Action Plan for Australia (*Health Online*) was developed and published by NHIMAC in response to the need for a national plan of action for information management in the health sector.[4] Endorsed by Health Ministers at their August 1999 meeting, *Health Online* sets out both a framework for future work and details of projects that are already under way or are planned to be implemented over the next five years.

Health Online promotes new ways of delivering health services that benefit both consumers and health care providers, by harnessing the enormous potential of new information and communication technologies. Most importantly, the plan will be updated and monitored over time under the direction of NHIMAC as new initiatives and possibilities emerge.

One of the actions proposed in *Health Online* was to "develop a national framework for the use of electronic health records for service delivery purposes"(p. 52). The context described in *Health Online* for the initiative was as follows (pp 52-3):

> Currently the majority of health care records exist as discrete paper-based entities held at a variety of different locations, resulting in a fragmented picture of the individual's health needs and history. They cross traditional and non-traditional health care sectors and health

[4] National Health Information Management Advisory Council (NHIMAC 1999), *Health Online: A Health Information Action Plan for Australia*, Commonwealth of Australia, Canberra. *Health Online* is available at www.health.gov.au/healthonline.

Formatted

and related community support services. The quality of information contained within them varies enormously and problems often arise with illegibility and issues about quality, appropriateness of content and loss of information.

Access to the appropriate information at the time of care delivery is central to good clinical decision making – practitioners and consumers need the right information at the right time. The greater focus of health care policy on providing a 'seamless delivery of care', particularly for the frail aged, the chronically ill and those with other complex care needs has highlighted the need to improve information exchange between different types of services and providers. The increasing shift in health care out of hospitals and into the community has also led to a wider range of services being utilised, often resulting in duplication of time and effort through repeat assessments and history-taking.

Increasingly, the potential benefits of electronic health records in improving efficiency, safety and quality of care over paper-based systems are being recognised across the health sector. As far back as mid-1996, the Taskforce on Quality in Australian Health Care advocated the use of a consumer-centred, computerised, clinical information system with links between different health care providers as the only practical way of ensuring that relevant health information is made available to practitioners.

Electronic records and transmission can provide powerful tools to link the isolated islands and fragments of information that currently exist between services and allow practitioners almost instant access to a comprehensive picture of an individual's health record and status. The potential benefits to health consumers are substantial, including:

- reduced numbers of adverse events caused by lack of information about the individual consumer at the point of care;
- reduced duplication of diagnostic tests due to unavailability of previous test results;
- enhanced decision making for practitioners and consumers (and therefore increased quality of care and health outcomes) through online access to decision-support tools such as clinical practice guidelines, prescribing alerts and recent information on diagnoses, treatment and prevention;
- greater coordination and integration of care across the care continuum through increased exchange of information between service providers in the health and community sectors;
- individual consumers being confident that, subject to appropriate privacy protection and their consent, regardless of where they seek or need health care, the health care professional treating them has full access to relevant clinical histories and treatment information. This will mean they don't have to go over the same questions and assessments each time they see a different provider; and
- efficiency gains through time saved in retrieving information and reduced duplication in ordering tests. Ordering of tests and treatments and arranging appointments and referrals can be substantially sped up with direct electronic requests. Data will be collected and made available more quickly, thereby increasing the time available for direct consumer care.

At their August 1999 meeting, Health Ministers agreed to set up an Electronic Health Records Taskforce to look into the possibilities of establishing a system of electronic health records in Australia, what would be entailed and what it would cost.

2.2 The National Electronic Health Records Taskforce

Appointed by the federal Health Minister with agreement from his state and territory colleagues, the National Electronic Health Records Taskforce first met on 30 November 1999 and had seven meetings in total. At these meetings, Taskforce members sought to address the many issues raised by the terms of reference, including:

- the various uses to which a system of electronic health records could be put;
- the various building blocks that would have to be put in place to build such a system;
- what would have to be done to make the system sufficiently attractive to both consumers and providers that most would welcome and use such a system; and
- how such a system could come into being and under what governance arrangements.

More fundamentally, however, the Taskforce sought to establish the likely benefits and understand the risks that would be involved in introducing a system of electronic health records for Australia — in order to reach a consensus on whether advocating such a course would represent a cost-effective use of scarce health resources. In order to inform itself on this overarching issue, the Taskforce commissioned several studies (one on benefits and risks and one on likely costs). On balance, the Taskforce is convinced of the merits of embarking on setting up such a system, in spite of the considerable likely cost — and advocates a staged approach to implementation (refer Parts B and C of the report).

2.3 Characteristics of the Australian population and their interest in online information

By taking advantage of new information and communications technologies, Australians are rapidly changing the ways in which they go about their daily lives and do business. Better use of such technologies can also change the ways in which health care is managed and delivered, for the benefit of all Australians. Already, there is much activity under way in every State and Territory and across the public and private sectors, which is aimed at using these new technologies to build a better health care system. Indeed, Australians have a reputation for being early adopters of new technologies.

But new ways of doing things are not the only forces for change impinging on Australia's health care system. Others include the changing size, distribution and composition of Australia's population — which will have implications for service provision, including health care. Like other industrialised countries, Australia has an ageing population structure and it is instructive to look at what is likely to happen over a realistic time horizon for implementing and properly bedding down a national health care network of, say, a decade.

According to the Australian Bureau of Statistics, in 2010:

- there will be 1,745,200 more Australians than there are now;
- the proportion of children in the 0-14 age group will have fallen from 20.53 per cent to 18.45 per cent of the population (largely because there will actually be 75,700 fewer in this age group);
- the over-65 years age group will have grown from 12.29 per cent now to 13.78 per cent (involving 525,100 more people in this age group than there are now);
- the over 85 year olds will have grown the fastest (1.70 per cent compared to 1.29 per cent now — representing an increase of some 107,500 people).[5]

On the affordability-of-health-care side of the equation, if Australia manages to maintain growth over the decade of at least 2.5 per cent per annum (well below its long-term average of around 3.9 per cent), we will be some $184,400 million richer (equivalent to some $8,840 more per person in today's dollars). According to figures from the Australian Institute of Health and Welfare, health spending per person in 1997-98 was around $2,500 and growing in real terms at around 3 per cent per annum.[6] If this growth rate were to persist, as a society we would have to devote an extra $1000 dollars out of our increased incomes of an extra $8,840 per annum in 2010 (ie nearly 11.3 per cent) to health care. This is higher than the proportion of Gross Domestic Product (GDP)/national income currently devoted to health (of some 8.5 per cent of GDP) and thus there would be some 'crowding out' of other claims to the current tax take from GDP/national income of around 30 per cent if all the increase were to be publicly funded. Nevertheless, government's ability to finance its share of the health care dollar (currently around 66 cents) should not be completely unmanageable over the next ten years.

However, these averages do not take account of the ageing of the population, and this will place some additional stress on the ability of government to finance its historical share of health care outlays. The outlook, therefore, over the next decade is likely to be one of continuing government restraint on the growth of health care spending (or at least the publicly financed component of that spending). This means that big and expensive initiatives — such as the introduction of a national health information network — will have to demonstrate that they can make a cost-effective contribution to securing better health outcomes for Australians in such an environment.

Reference was made above to Australians' preparedness to be early adopters of new technologies. Online technologies are a case in point as Australians' use of the Internet illustrates (see Box 2.1). Overseas experience is that health information ranks highly as a subject on which people scour the Internet for information. That is

---

5 Australian Bureau of Statistics (ABS 1998), *Population Projections: 1997 to 2051*, Cat. no. 3222.0, Canberra.

6 Australian Institute of Health and Welfare (AIHW 1999), *Health Expenditure Bulletin No. 15: Australia's Health Services Expenditure to 1997-98*, AIHW Cat. no. HWE 13, Canberra.

why, for example, the Commonwealth Department of Health and Aged Care has built the Health*Insite* web site[7] — so that Australians would have somewhere to go to obtain authoritative information on a subject dear to their hearts.

As the recent Report of the Australian Information Economy Advisory Council (Bandwidth Report 1999) points out (p.2)[8]:

> Currently, Australia ranks sixth in the world in terms of Internet users at 37 per cent of the population. This is just three percentage points behind the US, which holds first place. Australian consumers and businesses have repeatedly demonstrated their willingness to be early adopters of new technologies and have done so again in this case.

The Report also points out that, during the course of its inquiry, "the transformation from discrete voice telephony and data communications systems to a fully integrated data based 'Internet' type of system will be largely complete" in Australia.

As with other bandwidth-hungry applications[9] bringing health online will rely on the availability of adequate, high-quality and affordably priced communications bandwidth (a key enabler of the emerging 'information economy' more generally).

---

7 http://www.healthinsite.gov.au

8 National Bandwidth Inquiry Report (1999), Australian Information Economy Advisory Council (T. Cutler, Chair), Commonwealth of Australia. Document available at http://www.dcita.gov.au.

9 Historically the term *bandwidth* was used by engineers to refer to the amount of radiocommunications spectrum available or necessary for carrying an (often analogue) signal for a particular purpose. For example, a telephone call normally uses in the order of 4 KHz of bandwidth, while a television signal in Australia requires 7 MHz. With the advent of digital communications systems, and in particular the Internet, the term bandwidth is a term capable of different meanings. Bandwidth has been used more generally to refer to the measure of throughput capacity of a given communications network link or transmission protocol. In relation to digital transmission of data, the amount of bandwidth between sender and recipient determines how much data can be transmitted per unit of time. It is measured in bits per second (bps) or Kbps, Mbps and so on. A typical residential modem for example, may transmit in the range of 28.8 Kbps through to 56 Kbps. Assuming there were no other impediments, this would determine the rate of flow for the data being sent. In the case of larger businesses, their data connections might operate at 2 Mbps, 10 Mbps or higher transmission rates. It is fairly common to talk about the size of the *pipes* available to carry data, with *larger* pipes having capacity to transmit higher volumes of data per second. While the analogy with, say, gas or water pipes is a useful way to depict flow rates, this analogy can be misleading if it gives rise to the inference that data carrying capacity is somehow related to the physical size of the transmission medium. The size of transmission media such as copper wire, optical fibres and microwave radio transmission is not a relevant consideration in relation to data carrying capacity. While the available bandwidth may be equal in both directions or symmetrical (as for example, in a voice call) this is not necessarily the case. Broadcast, for example, is essentially a one-way transmission system, while nominally 56 Kbps modems typically provide a higher data rate inbound than outbound (that is, asymmetrical bandwidth). Bandwidth services can be provided in a variety of ways depending on the degree of value added. These range from transmission services such as private leased circuits, wholesale virtual networks to a variety of packaged wholesale services such as asynchronous transfer mode (ATM) and frame relay. (Source: National Bandwidth Inquiry Report (1999), Australian Information Economy Advisory Council

Formatted

Box 2.1: Australians' use of the Internet

At November 1999 an estimated 25% of all households (1.7 million) had home internet access — an increase of nearly 37% over the corresponding figures for a year earlier (19% or 1.3 million households). However, the proportion of households with a home computer has risen only slightly to nearly 50% of households (3.5 million) in November 1999 from 47% of households (3.2 million) in November 1998.

An estimated 6 million adults, 44% of the Australian population, accessed the internet at some time during the 12 months to November 1999 (up from the corresponding figures of 4.2 million or 31% of Australia's adult population a year earlier).

Work and home were the sites of internet access most likely to be reported by adults (2.8 million for both work and home). Other sites included: friend's or neighbour's house (2.1 million adult internet users); TAFEs or other tertiary institutions (1.2 million); public libraries (0.8 million); shops, stores or telecafes (0.3 million); schools (0.2 million); and government agencies or departments (0.2 million).

Of the 1.7 million households with internet access at November 1999, 75% (1.3 million) were located in capital cities (representing just under 30% of all capital city households — with the corresponding figure for households in other parts of Australia being 17%).

Younger age groups had the greatest proportion of internet users, with 73% (1.3 million) of 18-24 year olds accessing the internet in the 12 months to November 1999. For persons aged 25-39 the estimate was 56% (2.4 million); for 40-54 year olds, the figure was 44% (1.7 million) and for those aged 55 or more the figure was an estimated 16%.

Approximately 48% of adult males (3.3 million) had accessed the internet in the 12 months to November 1999, with the corresponding figure for females at 39% (2.7 million).

Nearly 60% of adults employed full-time (3.7 million) accessed the internet in the 12 months to November 1999, with the corresponding estimates for other labour force categories being: adults employed part-time 50% (1.3 million); unemployed adults 50% (0.3 million); not in the labour force 16% (0.7 million).

Nearly 6% of Australian adults (803,000) used the internet to purchase or order goods or services for their own private use in the 12 months to November 1999 (up from 2% a year earlier). 74% of internet shoppers paid for their purchases online (down from an estimated 83% a year earlier). Nearly 54% internet shoppers made their purchases only from Australia, 33% made them only from overseas and 13% from both Australia and overseas. Purchases were (in order of popularity): books or magazines 27%; computer software or equipment 19%; clothing or shoes 14%; music 13%; tickets to entertainment events 12%; sporting equipment 9%; holidays 7%; and alcohol 7%.

In the 3 months to November 1999: 4% of all adults (530,000) used the internet to pay bills or transfer funds; 2% (227,000) used an electronic information kiosk to pay bills; 41% (5.6 million) used a telephone to pay bills or transfer funds; 62% (8.5 million) used EFTPOS; and 72% (9.8 million) used an ATM.

(T. Cutler, Chair), Commonwealth of Australia. Document available at http://www.dcita.gov.au (pp.6-7)).

Source: ABS (1999) Use of the Internet by Householders, Cat. No. 8147.0, AGPS, Canberra.

Overseas trends: a sign of the times

In the USA, health information is the most sought after personal information on the Internet. There is a veritable explosion of individuals seeking medical information from sources other than their general practitioner. This is a sign of the information society in which individuals routinely seek information to address issues in their daily lives.

More generally, information and communication technologies are dramatically transforming many aspects of economic and social life, such as working methods and relations, the organisation of companies, the focus of training and education, and the way people communicate with each other. They are resulting in major gains in productivity in industry, and in the quality and performance of services. A new 'information society' is emerging, in which management, quality and speed of information are key factors for competitiveness: as an input to industry as a whole and as a service provided to consumers, information and communication technologies influence the economy at all stages. The health sector is not, and will not in the future, be immune from such trends.

2.4 New technologies and health care

The twentieth century has been characterised by a revolution in the provision of health care services. Advances in medical science and management have created an entirely new system of health care. People are not cared for by a single general practitioner any longer. Instead, it is increasingly a collective process that includes nurses, a variety of specialist medical practitioners, laboratory technicians, diagnostic technologists and administrative staff. Moreover, people are no longer treated by one organisation. For example, a person can be admitted to one facility, transferred to another for treatment, and then require extended care in the community or at home. In these circumstances, it is necessary to be able to safely identify consumers across multiple care settings and to be able to assemble relevant information on them from multiple sources in order to provide continuity of care.

Thus, health providers increasingly perform a wide variety of tasks, including rapidly changing combinations of 'hands-on' care, inductive and diagnostic thinking, detailed record keeping, consumer education, and communication with colleagues. Although 'high-tech' equipment is increasingly common in clinical practice, automated information systems are not. Thus, computers are not yet as useful, ubiquitous, and handy as the stethoscope and other common medical technologies.

In addition, medical practice is extraordinarily complex and can change rapidly. Systematising even the process of performing medical procedures — much less rationalising the language and scientific knowledge underlying those procedures —

is therefore a formidable challenge. Largely because of the complexities involved, the much-anticipated 'expert systems' of the past have largely yielded to 'decision-support systems' which alert providers to possible problems rather than attempt to solve them.

Information and communication technologies tend to flatten organisations and may not mesh well with the rigidly defined job roles and hierarchical structure of current medical practice. Many types of organisational changes will emerge throughout the health care system if information technologies are widely adopted. In other industries, changes associated with the introduction of information technologies have included large reductions in the demand for some types of workers (eg mid-level managers and bank tellers), increased responsibilities for workers in jobs that traditionally involved little decision-making (eg line workers in manufacturing industries), and an increase in competition for local experts from non-local sources (eg discount stockbrokers). Similar changes are likely to occur for health professionals, along with a redistribution of status, responsibilities, and remuneration associated with the various health disciplines.

Deploying information and communication technologies also facilitates alliances between geographically separate parties (eg telehealth), and can be expected to not only redefine jobs but to exert more subtle influences as well. Also, the widespread adoption of integrated information systems will challenge the legal system (eg who 'owns' an electronic health record — and is ownership still a relevant concept — when the record may be constructed from the contributions of numerous care providers, and may not in fact even 'exist' in its entirety at any one location).

Finally, information and communication technologies tend to be expensive to implement and their benefits may be difficult to directly measure, even when all parties are happy with the results. This may delay their deployment in an industry whose sophisticated technological base is seen by some to be a driving force in making health care more expensive.

Nevertheless, if past trends continue and the experience of other sectors of the economy is any guide, there will be an increasing imperative for all aspects of health care documentation and clinical communication among health care providers to be by electronic means.

2.5 Health information and supporting systems

Need for consumer health information

Consumer health information is any information that enables individuals to understand their health better and be in a better position to assume greater responsibility for making health-related decisions for themselves (or on behalf of members of their families). This includes information supporting individual and

community-based health promotion and enhancement, self-care, shared (provider-consumer) decision making, consumer education and rehabilitation, using the health care system and choosing whether to take out private health insurance (and with whom).

From the perspective of the consumer, such information can be actively sought or it can be provided through public or private education campaigns targeting specific health issues (eg media campaigns aimed at combating the transmission of AIDS).

People need good information if they are to make sound decisions about how to keep healthy and about, when, how and where to use health care services when they need them. That an informed consumer is essential to an improved health care system is predicated on the following principles and assumptions:

- personal behaviours are an essential component of health promotion and disease prevention. Of the many factors influencing individual health status, (eg genetics, environment, lifestyles, medical care) one of the most important is personal behaviour. Most premature morbidity and mortality is associated with individual risk behaviours. These include: unhealthy eating habits; lack of exercise; alcohol, tobacco and other drug abuse; unsafe sexual practices; and activities, which place one at risk of accidental injuries;
- consumer health information is necessary for self-care. Minor illness or injury is much more common than more serious illness or injury. How an individual or family member manages these problems through self-care can often mean the difference between simple resolution of the problem or progression towards more serious illness requiring outside intervention;
- consumer health information can improve the quality and cost of care. For example, a recognised failure of the health care 'market' is inadequate information on the part of consumers (who are regularly faced, for example, with decisions about health insurance, who to turn to among heath care providers, and what kind of care to agree to);
- management of ill health often requires the availability of consumer health information to return to a state of health. For example, once a person is seen and treated by a health care provider, consumer information may be needed to be acted upon to return to good health and to prevent a re-occurrence of the problem. In many circumstances, the need is great for ongoing, comprehensive and readily available information to help people to cope with what has become an ongoing problem (eg a chronic illness);
- an important aspect of consumer health information is community health. Many issues related to health happen at the population level (eg the spread of communicable disease or the impact of temporary environmental hazards). Individuals need to be as informed as possible about these issues, often in a timely and universal way; and
- because of the environmental, social, and behavioural determinants of health, the base of information that can help improve or maintain health is much

broader than that of information solely about medical problems. An individual's ability to readily obtain and use information in this wider spectrum of human needs must also be recognised as critical to health.

Health information systems past and present

Health care information systems, like most other large computer applications, were designed for many years around the capabilities of powerful mainframe computers. Users gained access to information stored in the large databases of a central computer using relatively slow, text-based terminals. Although the central computer might be very fast, it had to perform many tasks — so that its performance in responding to a user's request for a consumer's admission records, for example, might be slow if it were occupied with other calculation-intensive tasks.

As the speed and capabilities of desktop computers and networks has increased, the centralised, hierarchical structure associated with mainframe computers has progressively been replaced with distributed computing using a client-server architecture. Under this approach, the many tasks formerly performed by a monolithic central computer are dispersed among a series of programs running on a set of smaller computers, or servers. Each server handles a specific task, according to requests made by other programs, or clients, on the network.

Typically, users interact with client programs running on desktop computers with relatively sophisticated graphics capabilities. A client program for scheduling surgery, for example, might issue requests for information to servers throughout a hospital. The client program gathers the necessary information from the various sources and displays it to the user in a way that the user wants. The data and the computational resources of the information system are distributed throughout the institution rather than being localised in a central computer. In these circumstances, failure of any one computer may not bring down the entire system. In addition, if one server comes under heavy use, some of the load may be passed to another, less busy server. Another plus for a client-server network is that storage and computing capacity can be added incrementally.

Thus client-server computing replaces large, central computers with interacting networks of servers, each accomplishing specific tasks and communicating with standardised messages.

These kinds of technologies are now widely used for collecting, distilling, storing, protecting, and communicating data throughout Australian industry. In the health care sector, however, their application has been confined to scattered islands of automation — often limited to discrete departments within major teaching hospitals, for example. Computers are widely deployed in parts of the health sector, but tend not to be widely connected via any kind of network. The result is that the health sector in Australia is lagging badly behind other parts of the economy in its

use of computers and online technologies more generally. Compared to, say, the financial sector, health is still largely stuck in a world of the pen, paper and post when it comes to health records.[10]

Current situation with consumer records

Most of the clinical and administrative information that currently flows through Australia's health care system is paper-based, although some information is captured and disseminated electronically (eg some diagnostic tests). And many of these pieces of paper are masterpieces of idiosyncratic functionality (ie only decipherable, if at all, by 'insiders' in the system). In most cases, health care providers and organisations are free to determine what information is relevant and what form it should take. As a result, paper records tend to be individualistic (even down to individual annotations) because much of the information is handwritten and individual providers may phrase entries using their own terms and conventions.

Different types of providers might assemble records with different content. For example, ambulatory care records generally have fewer categories of information than hospital records, but they may span a much greater time period because they are historical records documenting many encounters. Consumer records also incorporate administrative records such as letters, insurance claims, and bills, although these may be stored separately from clinical records.

Paper records within a single folder have traditionally been kept either in the chronological order of collection or in source-oriented or problem-oriented formats. Source-oriented records are organised with forms from nurses, physicians, laboratories, and other sources in separate sections. Problem-oriented records organise the various notes into a brief database of information identifying the consumer, a problem list of the aspects of the consumer's condition that require treatment, an initial plan for treating the problems, and progress notes detailing actions engendered by the problems and plans.

This non-standardisation of consumer records is not necessarily a symptom of poor design; instead, it is a reflection of the main task that consumer records once served. They were a highly detailed, consumer-centred documentation of the care process and a record of everything that happened with respect to a consumer during a particular episode of care. In ambulatory care settings, they were also repositories of historical information about an individual's previous care. The records mediated communications and conveyed instructions and responsibilities among members of the medical team. In this context, designing a standard format for documenting consumer-provider encounters made about as much sense as trying to enforce a standard format for phone conversations or diary entries.

---

[10] A similar diagnosis was made of the UK's National Health Service (see *Information for Health* available at http://www.doh.gov.uk/dhhome.htm.)

The problem is that the functionality required of consumer records has grown far beyond the bounds of record keeping and communication within a limited team because of changes to both the delivery system and clinical practice. Consumer records are now widely used for legal, administrative, and research purposes. They have become sources of information for determining eligibility for insurance payments and for documenting the extent of injuries or the quality of care for use in legal proceedings. They may be used to provide data for evaluating the quality and appropriateness of care for peer review, accreditation, or other quality-assurance programs and for reporting communicable diseases and other required data to relevant authorities.

Paper records are thus becoming increasingly inadequate for the information demands of modern health care systems. A number of weaknesses of paper records have been noted:

- *Paper-based consumer records document the care-giving process inadequately:* Medical record keeping tends to be a hurried, ancillary activity to the care process. Providers may not, for example, have sufficient time to completely and accurately fill out the forms comprising the paper records, and the required health information is sometimes unavailable or of questionable accuracy. Providers' notes may be illegible if handwritten, or inaccurate if dictated and then transcribed. Detailed descriptions of the consumer's health problem and the reasoning behind diagnoses and care choices may be left out or abbreviated because they are hard to summarise and tedious to record. The voluminous data from continuous monitoring systems cannot be easily summarised manually, while other components — such as laboratory and radiological reports — may be missing because of filing or communication errors.
- *Paper-based consumer records hinder the free flow of information:* Once information has been recorded within a set of bulky paper records, it may not be readily accessible later. Efforts to compile a more complete paper record are likely to exacerbate this problem. The data are bound to the paper itself and individual pieces cannot be sorted for relevance, making the record difficult to use when dealing with multiple problems or extended treatments. Collecting and aggregating data from multiple records for purposes of quality monitoring or clinical research involves an expensive and time consuming manual search. Paper records can be in only one place at a time. Short of laboriously photocopying and then shipping them by courier, records may frequently be unavailable to a caregiver who needs them. When the record is unavailable, new data cannot be entered in a timely manner; entries must often be made from memory or copied from other forms or informal notes. This can lead to the creation of secondary records that are difficult to coordinate with the primary record set and which may contain conflicting or superseded data. Finally, the data are only as secure as the paper itself, and entire records, or individual pages within a record, can easily be misplaced, damaged, lost, or stolen.

- *Paper records impede the integration of health care delivery, research, and administration:* The wide variety of formats, styles, and organisational systems for paper records frustrates the coordination of care between different providers, or even between departments or providers in the same institution. The impenetrability of the record means that there are few tools that can use information in the paper records to generate things like reminders and decision support more generally.

In many settings, the traditional paper record has become large, unmanageable, illegible, and frequently unavailable. As Murphy points out:[11]

> In complex organisations, several conditions create constraints on the effective clinical use of the manual record:
>
> - The records may not be available because other practitioners are using them.
> - If available, they may not be complete — particularly if they rely on manual filing for diagnostic test results.
> - The reliability of the record is often compromised because it is fragmented. There may be separate medical records that are maintained by practitioners to keep data handy for their individual clinical needs. Inevitably, relevant clinical data will be placed in one record and not transferred to the main record.
> - Paper records often cannot be used effectively for research and educational purposes.
> - Paper records are limited by boundaries of time sequence. Data manipulation for comparisons and study requires significant additional work to access and abstract their content for this purpose.
> - Quality monitoring is limited in the paper record system.

[11] Murphy, GF *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia.

3 WHAT ARE ELECTRONIC HEALTH RECORDS?

The notion behind electronic health records is simple enough: changing the form in which the health record is held from paper to electronic means. But building useful systems to support them is quite challenging. This not only reflects the complexity of having to cope with many contributions to the record (both from multiple providers and over time) in a way that will prove valuable to others but also the necessity of incorporating into systems design aspects such as a safe way of identifying the consumer, secure means of transmission and storage of what is highly sensitive personal information, and mechanisms to ensure that access to records is confined to authorised users. Otherwise, such systems will simply not be used.

3.1 Definitions of electronic health records

There are various definitions of just what constitutes an electronic health record.[12] The Taskforce favours the following definition, which has been developed after the Taskforce's consultation process:

> An electronic longitudinal collection of personal health information usually based on the individual, entered or accepted by health care providers, which can be distributed over a number of sites or aggregated at a particular source. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of the consumer and is stored and transmitted securely.

The following is typical of other definitions that have been advanced (see Box 3.1 for a selection of others):

> … any information relating to the past, present or future physical/mental health, or condition of an individual which resides in electronic system(s) used to capture, transmit, receive, store, retrieve, link and manipulate multimedia data for the primary purpose of providing health care and health-related services.
>
> Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.5).[13]

---

[12] Other terms in use include computer-based patient record, electronic medical record and computerised medical record.

[13] Secondary purposes include support for provider business operations and health care policy and research. The authors point out that their definition is a synthesis on a number of definitions that have been proposed over the past decade, and focuses on the most inclusive terminology including individual health status and condition (to encompass preventive medicine, illness, and patient-contributed information), system functions (to reflect the broadcast capability for using and linking information) and multimedia (to identify the scope of possible electronic tools).

Box 3.1: Other electronic health record definitions

… an electronic consumer record that resides in a system specifically designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge, and other aids.

US Institute of Medicine

Computer-based patient record (CPR) systems: computerised information systems maintained by providers to capture, store, retrieve, transmit, and manipulate consumer-specific health care — related data, including clinical, administrative, and payment data. Using standard definitions, codes, and formats that enable data to be universally recognised and processed, CPR systems would be linked (with appropriate mechanisms allowing consumers and their providers to control access to information) through high-speed communication highways capable of transmitting multimedia data (including voice, image, and text) electronically. We distinguish the computer-based patient record — which would consist of all the information necessary for managing that consumer's care — from health information infrastructure which would also include decision support applications, reference data bases and linkages between CPR systems.

US Work Group on Computerisation of Patient Records

A computer-based patient record is electronically maintained information about an individual's lifetime health status and health care. The computer-based patient record replaces the paper medical record as the primary source of information for health care, meeting all clinical, legal, and administrative requirements.

US Computer-based Patient Record Institute

Source: Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.6).

Creating electronic health records

An electronic health record is built-up as a collation of selected digital data captured each time an individual interacts with the health care system. Typically, one (or more) entries for the record are created for each interaction with a health care provider. Examples of individual entries would be a general practitioner prescribing a drug for a patient, and a pharmacist filling the prescription.[14] To be able to construct the record, each entry needs to include an agreed set of information (eg time and date; identification of the provider, the consumer and the location of the health care service; any coding system(s) used; and who is permitted to access the entry). Authorised people must be able to update the record but it must

[14] Increasingly, consumers will have the ability to contribute their own entries to their records, such as recording blood glucose levels, via personal computers — and such contributions to the record will need to be accessed by providers no differently from those generated in more traditional health care settings.

Deleted: insulin

be impossible to alter or erase previous entries. Finally, electronic health records must be secured against such things as unauthorised use, tampering or destruction.

Electronic health record properties

The various definitions of the electronic health record have been framed with an eye to the following widely shared properties which proponents see as valuable aspects of the electronic health record:

- individual/consumer centric focus in support of personal health care;
- longitudinal nature;
- flexibility for users;
- timeliness for decision support;
- as source material for various kinds of studies (eg epidemiological);
- confidentiality of stored information (apart from authorised uses); and
- record stored and transmitted securely.

Depending on the extent and complexity of an individual's encounters with the health care system, the medical record may contain lengthy contributions from a multiplicity of health care providers (eg general practitioners, specialists, dentists, nurses and a variety of allied heath workers — such as physiotherapists, dietitians and social workers), what medications have been taken, as well as the results of diagnostic tests (radiology, pathology, electro-cardiology etc).

Thus, the content of an electronic health record comprises personal health information — information that has meaning in the context of the evolving health status of a particular individual. The usefulness of such information in turn reflects the value-added nature of the health care delivery system: it is outcome-oriented, with the desired outcome being the continued health of the individual, the restoration of health (if possible) or palliation (if restoration of health is not possible). Thus, the principal reason for collecting consumer-specific health data is to help maintain that person in as good health as possible and the value of the data is in its derivative capacity to serve that end (see Box 3.2). The implication of this is firstly, attention should focus on collecting personal health information that consumers and health care providers find most useful and secondly, to present that information in a form that the consumer and the provider finds most convenient (and, from a provider's perspective, this is likely to depend on the type of health care provider wanting to access information held in the electronic health record, and possibly the kind of information the provider is wanting to access on a particular occasion).

Box 3.2: The value of health care information

Health care information only has value in the context of its contribution to a beneficial outcome on consumer care. Five criteria characterise information for timely and economical delivery of quality health services:

Quality — complete and accurate information must be available.

Utility — information must be presented in a form suitable to the user.

Proximity — information must be available at the time and point of decision.

Accessibility — information must be seamlessly available across the boundaries of health care profession, speciality, discipline, location, or care delivery environment.

Confidentiality — access to individually identifiable information must be limited to only those authorised parties having consumer consent.

Source: Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.122).

Information held in electronic form can be easily presented in a variety of ways. For example, data can be displayed in ways that a particular health care provider or consumer finds helpful or insightful and, indeed, changed to a different format (or to display different data) at the press of a key. Also, presenting time-sequenced data in graphical form can be easier to assimilate than being presented with the observations themselves. The information held in electronic health records can also be interrogated by many applications, for example to automatically generate medical alerts and reminders[15] (see Box 3.3) or to input into applications supporting clinical decision-making.

In order to construct (or add to) an individual's electronic health record, automatic prompts can be included as part of the system both to promote the capture of more complete information and to make data entry easier because it is more structured.

The ultimate test for a system of electronic health records in Australia will be the degree to which it achieves measurable benefits in terms of improved health, quality and safety of care and privacy protection for those choosing to participate compared to the costs of building and operating the system.

[15] Alerts and reminders are particularly useful in ambulatory care, where they can increase compliance and aid prevention. There is now evidence for such success and for the beneficial effects on provider behaviour as well (see McDonald CJ (1997), 'The barriers to electronic medical record systems and how to overcome them,' J. Amer Med Inform Assoc, Vol 4, No. 3, pp.213-20.

Deleted: physician

Box 3.3: Leveraging the electronic health record: reminders

Automatically generated reminders operating in conjunction with electronic health record systems can help both health care consumers and providers. Thus consumers can be reminded about advised follow-up consultations with general practitioners or to take recommended preventive action (eg participate in cancer screening programs). Indeed, studies have shown that such systems are effective in encouraging consumers to check back for key monitoring activities such as blood pressure checks, cervical screening, and mammography (Banks and Paliney 1990).[16]

In the case of providers, reminders/alerts can be generated on the basis of systematic analysis of both group and individual data (eg from what seems to work for what kind of consumers under what kinds of circumstances to possible adverse drug interactions or suggested treatment modifications given the medical history of the individual concerned).

Computer-generated reminders assist the care process by using the information available in the electronic health record to either jog consumers into action in the interests of their health or alert providers to possible problems with contemplated courses of action.

We know that the benefits will likely easily exceed the costs because achieving desired health outcomes depends on having the right information available when and where it is needed. This means that health information needs to cross what have become artificial boundaries to do with one's professional/discipline/speciality — something a truly integrated electronic health record system would achieve. When consumers see multiple providers in different settings, none of whom have access to complete information, consumer safety is more likely to be put at risk than where care is better co-ordinated (eg via electronic health records). Unsafe care is one of the prices we pay for not having organised systems of personal health information (which can mitigate a major source of medical misadventure).[17]

Possible roles for a system of electronic health records

The electronic health record and supporting infrastructure will be important tools in supporting the delivery of high-quality care via informed decision-making on the part of both providers and consumers. Just as there can be expected to be many different health care settings in which the electronic health record is accessed (ranging from hospital to home), an electronic health record system will play many roles in the provision of care both at the individual and community level. Following is a list of possible roles, which could be fulfilled by a system of health records made available electronically:

---

16 Banks NJ and Paliney RH (1990), 'Clinical Reminders in Ambulatory Care,' HMO Practice, Vol 4, No. 4, pp.131-6.

17 Emphasising systemic rather that individual error is a theme taken up in Kohn LT, Corrigan JM, Donaldson MS (1999), eds. *To err is human, Building a safer health system*, National Academy Press, Washington DC.

- form the basis of an historical account;
- record preventive measures (as well as curative and palliative interventions);
- support communication (eg consumer-provider and provider-provider);
- remind providers about anticipated health problems and planned actions (eg via care plan);
- identify deviations from expected trends;
- provide a legal account;
- support clinical and health system research;
- increase productivity of health care providers (allowing more time for the actual care process);
- support provider education;
- provide decision support (via particular applications — such as potential adverse drug interactions);
- access medical 'knowledgebases';
- assist with audit; and
- accommodate future developments.

3.2 Electronic health records in Australia

Primary care

Australian general practice is rapidly embracing computerisation — encouraged by the introduction of financial incentives. The General Practice Financial Group (GPFG) was established to progress general practice financing recommendations emanating from the 1998 Report of the General Practice Strategy Review Group, including the continued development, monitoring and implementation of the Practice Incentive Program (PIP). The GPFG comprises members from the key general practice representative organisations including the Royal Australian College of General Practitioners (RACGP), Australian Divisions of General Practice, Rural Doctors Association of Australia and representatives from the Commonwealth Department of Health and Aged Care.

The General Practice Computing Group (GPCG) was established as the peak national group for general practice computing. In 1998, it received Commonwealth funding to help support general practice computing and subsequently established the General Practice Information Management and Technology Strategic Framework. The Framework sets out a number of aims and identifies key outcomes and activities for general practice computing between June 1999 and July 2001. These activities focus on providing practical support programs to increase the effective integration of information management and technology systems at the point of clinical care and to develop the architecture and standards to create the

building blocks to enable the transition to electronic health records. Divisions of General Practice have also supported and promoted computerisation and are being encouraged to develop support networks and innovative approaches to information technology.

Supported by new capital through acquisition or interest from financiers, software suppliers are adding clinical records to their products, thus creating an electronic health record capability. As a result of these developments, a small (but increasing) proportion of primary care practices are taking steps towards a paperless office.

There are two commercial drug databases with interaction warnings in use. The development process of one has been accredited using International Standards Organisation (ISO) criteria and is reviewed externally. Two vocabularies are used, one proprietary and the other based on an extension of the International Classification of Primary Care. Results reporting with pathology companies is widely used, facilitated by simple text messages transmitted in Pathology Information Transfer (PIT) format — Health Level 7 (HL7) is used in very few sites. These enabling technologies, where they are not ISO compatible, are allowing the move to an electronic health record in a proprietary manner — which is not necessarily in the interests of providers or consumers, since systems of electronic health records have a 'public good' dimension (eg they can be of potentially great assistance in the field of public health), rather than being purely private goods. The very idea that an individual’s personal health information may (or could) be 'owned' by someone else (eg a company for private gain) has been a source of great concern to many Australians. The Taskforce believes that open standards should be adopted as a general rule (see further discussion about standards in Chapter 10).

Pharmacies have been computerised for some time, many are saddled with ageing software that provides limited functionality. Electronic prescribing trials are beginning and plans to electronically share the medication record between providers are being advanced. There is no standard medication identifier.

Communication links between hospitals and primary care are extremely limited nationally; both hospital and general practitice systems have been slow to implement HL7 — largely because of genuine risks in using the standard. All hospitals report their separation data in the International Classification of Diseases (ICD-10-AM), but this vocabulary is not sufficient to support full clinical systems.

Community health centres and community health professionals are dependant on State and Territory Governments to provide for their information technology needs and are some way behind general practice. A consortium of States behind the Community Health Information Management Enterprise (CHIME) project is aiming to address this and should see added facilities in this sector this year. The CHIME project has developed another vocabulary for its purposes which has implications regarding data collected in the future.

Secondary care

To date, electronic health record developments in Australian hospitals have been driven by the need to support management, audit, financial processes and planning functions. Thus, most hospitals have computer systems with applications that are geared towards administration rather than supporting clinical care. Implementation of electronic health records has been the exception rather than the rule.

There are a variety of systems operating in hospitals. Some hospitals have invested in whole-of-institution solutions provided by large international vendors, usually from the USA. A New Zealand company is also providing solutions. So called 'beacon sites' — such as the New Children's Hospital at Westmead (Sydney, NSW) — have an electronic health record 'federated system' providing access to clinical history, reporting, radiology (including images) and prescribing at the bedside.

Specialists are more likely to be using clinical software in private clinics than in public hospitals, and the systems in use are mostly based on general practice systems. Pathology providers have been computerised for many years and have led the way in providing results to medical practitioners. They continue to use the PIT format to enable this service.

Hospitals are keen to offer more efficient care and reach higher levels of consumer and professional satisfaction, and in a climate with limited funding the electronic health record is seen as one method of making progress. Also, large institutions benefit from being leaders in the introduction of technology — attracting motivated staff and gaining national profile.

Electronic prescribing

Electronic prescribing — and thus an ability to generate an individual's history of pharmaceutical consumption — would clearly be an important and integral part an electronic health record. The *Better Medication Management System for Australia* is being developed now following an announcement in the 2000-2001 Federal Budget.

Scheduled for implementation nationally from July 2001, this initiative will create a new electronic prescribing system and individual consumer medication records by linking prescriptions written for a particular individual by different providers or dispensed by different pharmacists. The early introduction of electronic patient medication records will be made possible by building on medication information already collected via the Pharmaceutical Benefits Scheme. The Medicare number will be used as the patient identifier to link medications to individuals — so that they can be brought together when consumers wish to grant access by their provider or pharmacist to their medication record.

The plans for this system, which will test many issues relevant to the development of the electronic health record, were proposed by an advisory group, set up by the federal Health Minister, to advise him on the best ways to use information

technology to improve prescribing and medication management. The group included a membership drawn from major organisations representing prescribers, dispensers and consumers, as well as representatives from the Department of Health and Aged Care and the Health Insurance Commission. The group's proposal took into account comments from a number of areas and a more detailed consultative process will underpin the further development and implementation of the initiative.

For consumers, the new system will provide much safer arrangements and better health outcomes. With the current fragmented approach to medication records, whereby individual providers or pharmacists only have records of their own prescribing and dispensing activity, there is always a possibility of adverse interactions between medications prescribed by different providers. This is because one provider will not be aware of what another has prescribed.

This system will mean that the prescription data only has to be entered once, removing a major potential source of error. In addition, pharmacists will not have to rely on being able to decipher the prescriber's handwriting.

For prescribers and pharmacists, an accurate and up-to-date knowledge of a consumer's medication history and the automatic triggering of drug alerts will result in a much improved and safer prescribing and dispensing environment.

The new system will be voluntary for consumers, providers and pharmacists (ie they will not be part of the system unless they choose to participate). Thus, consumers will have to give their consent before either their provider or pharmacist can look at their medication record.

Privacy and confidentiality issues will be addressed through a range of measures, including legislation and comprehensive security protection through the system. The protections which already apply to Medicare will be extended to cover all aspects of the electronic consumer medication record and the Office of the Privacy Commissioner has been consulted during the developmental process so far and will continue to be involved. It is intended to use public key technology and electronic digital signatures to maintain a highly secure environment for the entire system.

It is envisaged that the system will include an independent governance arrangement with representation of key stakeholders to oversight its operation and ensure appropriate rules for access to and use of data. There will also be a consumer feedback and complaints mechanism.

4 WHAT CAN WE LEARN FROM OTHERS?

If Australia puts in place a system of electronic health records it will not be the first to do so. Others have already implemented such systems (although usually not on a national basis). A relevant consideration is therefore what we can learn from the experience of others — both in Australia and overseas — before embarking on such an undertaking here. Experience is mixed, and there is much to learn from failure as well as from success.

4.1 Australian experience

Two state-level developments in Australia are beginning to enter the territory of electronic health record development: in New South Wales (NSW) and in South Australia (SA). Although quite different, they are both seeking to align with any national approach that may emerge as a result of this Taskforce's report to Health Ministers.[18]

New South Wales

NSW has a relatively well developed information technology health infrastructure by national standards. This is despite spending less than 1 per cent of the health budget on information technology. Access to 'knowledgebases' via the Internet (such as the Cochrane Databases and online journals) has been a great success and well received by all — especially rural practitioners.

In the recent review of health services, the NSW Health Council concluded that:[19]

> … there is substantial evidence internationally that information technology systems (particularly consumer information systems) can be powerful tools to support clinicians to provide care and to provide consumers with both access to more information and more control over their own health records.

There is a clear direction of a state-based approach to electronic health record development. The recommendation calls for the NSW Health Department to:

> ... cooperate closely with the Area Health Services and the Commonwealth Government to revise its [Information Management Technology and Telecommunications] strategy to set out a Statewide strategy to develop an electronic health record for every individual in NSW.

---

[18] Material in this section draws heavily on the paper by researchers at Flinders University on The benefits and risks of introducing a national approach to electronic health records in Australia (reproduced as Appendix B).

[19] Report of the NSW Health Council (2000), *A Better Health System for NSW*, NSW Government. Available at www.health.nsw.gov.au

Deleted: .

The approach entails initiatives to:

- describe what the “record will cover”;
- set out an agreement with the Commonwealth Government about timing, implementation and funding;
- detail how privacy and security issues will be resolved;
- determine how clinicians and consumers will be involved;
- introduce a patient identification number (PIN);
- link secondary and primary care; and to
- immediately mandate data and security standards, and develop a classification system.

Problems with the current systems are listed as:

- there is no single record of health care;
- there are no formal electronic links between primary care centres, between primary and secondary care, and between hospitals;
- there is no single consumer identifier;
- consumers have little or no access to their health records; and
- there is no way to determine the cost of care for an individual who utilises different services.

The report recommends utilising a consumer-held 'smart card' for personal health records and a staged approach with informed community debate. These efforts are to be investigated in a number of demonstration projects. The report acknowledges that “there is little point in having a unique identifier that is confined to state-administered services”. There is, however, no mention in the strategy for how this number would be propagated to primary care settings and the administration required for it to work.

The report emphasises certain changes, which may be summarised as:

- the ability to transfer clinical information from Emergency Departments to the wider hospital;
- electronic transfer of hospital discharge information to primary care; and
- electronic transfer of clinical information between hospitals.

South Australia

SA’s Department of Human Services examined several commercial clinical information systems and, since 1997, has run an intensive pilot study of the Open Architecture Clinical Information System (OACIS) (a proprietary product) in conjunction with the renal units of the four major Adelaide public hospitals.

OACIS is a consumer-centric information system, that can integrate a wide range of electronic data, including a patient master index (PMI), clinical notes, appointments, laboratory results (imaging included) and clinical orders. It does not provide integrated decision-support tools, except for a drug interaction module associated with pharmacy ordering. There is no intention to facilitate consumer access to personal data in the near future.

As at early 2000, it is planned to capitalise on the significant investment to date by extending OACIS to cover eight metropolitan hospitals, where it will be used by all clinical services. This is an initial phase only, the strategy being to eventually network this service state-wide, to country hospitals, smaller metropolitan clinical centres, general practitioner and specialist practices and private hospitals. Clinical data modules will be implemented during 2000 and 2001, with clinical ordering front-end functions to be developed and installed over the following 2 to 3 years (which will require the creation of interfaces to existing patient-service applications). The practicality of loading pre-existing consumer electronic data from major institutions is being examined.

The present-value development and roll-out cost is estimated at around $55 million, over 5 years. A cost-benefit analysis of tangible benefits implies that financial break-even will only be achieved after 7 years (but with recognition that there are additional less tangible benefits as well).

The decision to adopt OACIS state-wide has been based in part on a set of strategic principles:

- The system must be consumer-centred with the objective of establishing a full electronic medical record.
- OACIS should be accepted as much more than a simple substitution of electronic information for existing paper-based information.
- The initial roll-out will be to all clinical units of all major metropolitan hospitals to maximise the benefits in the short term. Further, within this phase, (1) clinical data management will be completed before clinical ordering will be attempted, and (2) any specific tailoring for individual specialities will be introduced last.
- The more general roll-out to smaller metropolitan centres, country centres and private providers will be a later phase(s).
- The capacity of existing information technology infrastructure must be reviewed critically in the light of predicted changes in data load and traffic; some of the necessary infrastructure has yet to be established.
- The pilot project highlighted that implementation management will be critical, especially of process change and ensuring an appropriate level of clinician ownership and involvement.

However, a set of significant issues (some very fundamental) have yet to be resolved and require policy and/or technical solutions. The major of these are:

- the desirability of adopting existing standards for the structure of the electronic health record and for data coding dictionaries;
- a suite of ethical, legal, confidentiality and security issues; and
- the necessity for (but difficulty of achieving) a reliable and functional unique patient identifier[20].

In essence, these replicate the important issues identified as generic elsewhere in this report, which highlights the very real risk of duplicating resource expenditure and of creating potentially incompatible solutions when independent regional developments do not benefit from a coordinated national approach. In recognition of this, there have been co-operative discussions with Commonwealth and State agencies, including NSW and SA.

Implications for a national approach

Regional approaches to systems of electronic health records in Australia are already diverging considerably. In spite of this, there is general awareness that adopting a national approach will reduce the risk (and therefore the cost) of building incompatible systems, and would shorten development times. Nevertheless, the benefits of a national approach will only be secured if reaching agreement on such an approach does not involve inordinate delays.

4.2 Overseas experience[21]

Other countries have considerably more experience with systems of electronic health records than does Australia, and so it is instructive to understand their experiences in order to learn any lessons for Australia.

United States of America

In 1991, an Institute of Medicine (IOM) study detailed and formalised the deficiencies of the extant manual system of medical record keeping, arguing for the creation of electronic health records residing in a system designed to support users by making available complete and accurate consumer data, generating practitioner

[20] There is acknowledgment of the value of a national approach to this but circumstances may dictate that a state-specific option be adopted for the initial metropolitan roll-out.

[21] Material in this section draws heavily on the paper by researchers at Flinders University on The benefits and risks of introducing a national approach to electronic health records in Australia (reproduced as Appendix B).

reminders and alerts, encompassing clinical support systems, and with links to collections of authoritative knowledge bases and other aids.[22]

This initial vision led to the establishment of the Computer-based Patient Record Institute (CPRI) which serves as a catalyst for continuing developments in the area. In 1997, CPRI spelled out a "means to describe the consumer-centred information needs within the health care delivery system, and all its components — whether in integrated delivery systems, individual settings, a community, or through teleapplications around the world."[23]

The objectives are to:

- improve individual health care and maintenance of health;
- facilitate timely, accurate, and comprehensive communication among caregivers;
- ensure confidentiality and integrity of health-related information about individuals;
- provide ready access to knowledgebases and decision-support systems;
- enhance the productivity and efficiency of the health care delivery system;
- encourage consumer participation in personal health care;
- support the improvement of the health status of the community;
- encourage and support clinical research and education; and
- support policy and public health responsibilities.

Canada

Canada's focus at the national level in establishing electronic health records reflects its national-provincial division of responsibility for health care. The federal government is primarily responsible for ensuring that the provisions in the Canada Health Act are consistently implemented across the country. The Provinces are responsible for managing and operating their respective health care systems. This division of responsibility and its influence on the human, technical and business dimensions of health care is a fundamental factor affecting the planning of information initiatives.

Over the last several years, the 'evolutionary' forces of this context have spawned several national initiatives, which have been focused on influencing and facilitating the establishment of electronic health records, rather than creating a single

[22] Dick RS and Steen EB (1993), eds, *The Computer-Based Patient Record*, Institute of Medicine, National Academy Press, Washington. A revised edition was released in 1997.

[23] Computer-based Patient Record Institute (CPRI 1996), Work Group on CPR Description, Framework for Definition and Modeling of the Computer-based Patient Record, Bethesda, MD, p.3.

prescriptive national plan. There are now a number of organisations, funding programs and initiatives which are working together to achieve this outcome.

The Office of Health and the Information Highway

The Office of Health and the Information Highway (OHIH) underscores the strong synergy the government sees between technology and health care delivery. OHIH initiatives include:

- The National Health Surveillance Infostructure — a network of networks with provincial partners and other stakeholders such as medical laboratories and poison control centres. These networks will enable data collection, integration and analysis from diverse sources for risk management — with the aim of saving lives, preventing disease and disability and thus reduce the cost of health services.
- The Canadian Health Network (CHN) — providing well organised, accessible and timely information on health promotion, disease prevention, treatment options and health system performance through multi-modal access, including WWW, 1-800 lines, interactive voice response and 'fax back'. The CHN aims to empower consumers through quality health information and overcome geographic and financial barriers, assisting all Canadians to more actively manage their health.
- The First Nations Health Information System — the system is designed to support case management, health planning and evaluation at the community level in Indigenous communities. The system will aim to ensure universal access to health information management and reduce risk through early detection of disease outbreaks, new diseases and antibiotic resistance. The system will also aim to offer a more comprehensive immunisation schedule management and communicable disease control.
- The Health Infostructure Support Program — established in March 1998 to support efforts to test and assess the use of new information technologies and applications in the health field through pilot projects in areas such as public health, health surveillance, 'pharmacare', First Nations health, 'homecare' and telehealth. It was open to non-profit, non-government groups and organisations in Canada. Thirty-six pilot projects were, or are currently being conducted by 33 non-profit, non-governmental groups and organisations in the health sector. The federal government will provide $8.7 million while private sector financial support in excess of $2.25 million has been committed to the applicants.

OHIH has now announced the Canada Health Infostructure Partnerships Program (CHIPP). CHIPP is a two-year, $80 million, shared-cost incentive program, aimed at supporting the implementation of innovative applications of information and communications technologies (ICTs) to bring better health and health services to Canadians. CHIPP will support projects in two strategic areas of ICT-based innovations in health care delivery, namely telehealth (telemedicine and telehomecare) and electronic health records.

This is the first national initiative that is directly focused on the creation of electronic health records. The rationale for the program is as follows:

> Electronic health records (EHRs) are the essential health information related to individuals and health care providers. They normally include the individuals' health information and unique identifier code; the identifier code for the health facility providing the service, the health care providers' code; and other relevant information. Having individual EPRs is important, but linking and sharing patient records across health care providers, that is building an EHR, will create a paradigm shift resulting in a consumer-centred integration of health care as well as more streamlined health administration and more informed policy making.

The Canadian Institute for Health Information (CIHI)

The Canadian Institute for Health Information (CIHI) plays a crucial role in the development of Canada's health information system. CIHI is a federally chartered but independent, not-for-profit organisation. It brings programs, functions and activities from the Hospital Medical Records Institute (HMRI), the MIS Group, Health Canada (Health Information Division) and Statistics Canada (Health Statistics Division) together under one roof. Its primary functions, which relate to the establishment of national electronic health records, include:

- identifying health information needs and priorities;
- collecting, processing and maintaining data for a comprehensive and growing number of health databases and registries, covering health human resources, health services and health expenditures; and
- setting national standards for financial, statistical and clinical data as well as standards for health informatics/telematics.

Specific initiatives that CIHI has initiated include:

- the Roadmap Initiative — a national vision and four-year action plan to modernise Canada's health information system. Led by CIHI, it is a collaborative effort with Statistics Canada, Health Canada and many other groups at the national, regional and local levels; and
- the National Data Model and Dictionary Project — the Conceptual Health Data Model (CHDM) is a reference tool for organising high-level health information and data. The CHDM provides a framework within which to view and define health information. The goal of this project is to further enhance the CHDM developed by the Partnership for Health Information Standards.

  Specific objectives include:

  - mapping the CHDM to an existing logical data model used by a significant number of stakeholders in Canada;
  - creating and publishing a standard data dictionary for CIHI entities and data elements; and
  - developing communication and education material to facilitate the use and acceptance of the CHDM.

Perceived benefits and risks

Although Canada has not had a specifically focused national plan for establishing electronic health records, the various projects and initiatives undertaken to date have essentially laid the groundwork for a national approach. The work done so far can be characterised as a national independent learning exercise. One could easily criticise it by saying that is has been too painful and inefficient. Nonetheless, it could also be seen as an essential step in creating a critical mass of awareness, understanding and commitment to establishing electronic health records.

Some of the lessons learned so far are:

- Generous funding has more often been a curse than a blessing while moving up the learning curve. There have been several multi-million dollar initiatives across the country that have yet to demonstrate the ability to assemble and share comprehensive health records. It seems that 'big bang' approaches have tended to bog down in the inertia created by the big politics, risk aversion and traditional command and control models which they attract.
- There is consensus among all the stakeholders that the time has come for fundamental innovation. One of the key insights of a joint working group formed by the Information Technology Association of Canada (ITAC) - Ontario Health Committee and the Ontario Health Providers Alliance (OHPA) is that, to quote Albert Einstein:

  > The significant problems we face cannot be solved at the same level of thinking we were at when we created them.[24]

- A promising development is the growing interest in the application of the 'open source' paradigm to the development of health care software and, in particular, to electronic health records and the development of community-based health information networks. An early adopter is the McMaster Primary Care Network (PCN), which has been established by the Department of Family Medicine, McMaster University in Hamilton Ontario, to participate in Ontario's Primary Care Reform initiative. The McMaster PCN is basing its strategy on MUFFIN, a primary care electronic patient record that has been available on an open source basis for nearly ten years. MUFFIN is unique in that it supports teaching, research, evaluation and delivery of care. One of the goals of the PCN is to modernise MUFFIN, create a self-sustaining, open source based strategy for its continued improvement and evolution, and to develop a truly systemic electronic health record solution for primary care.

In summary, the recently announced CHIPP program has the benefit of building on the experience gained in the various primary care, hospital, regional and provincial

[24] In other words the tools and processes we used to create the current impediments to establishing electronic health records will not likely provide the solutions we need. This is fuelling a growing desire and sense of urgency to innovate and collaborate at a local, national and global level to achieve what is essentially a globally shared vision.

initiatives that have been implemented independently across Canada. CHIPP has the potential of funnelling this experience into a manageable number of integrated national projects. A critical success factor for the CHIPP program is how well it can leverage the knowledge and experience gained in electronic health record initiatives across Canada and in other countries with similar health systems.

Implications for a national approach in Australia

On the basis of Canadian experience, a federal agency that has a mandate to develop the infrastructure and building blocks of the electronic health record would appear to be a useful strategy to speeding a coherent national response.

United Kingdom

The UK approach towards electronic health records is reflected in *Information for Health*, the information management and technology strategy for the National Health Service (NHS), published in 1999[25]. This charts a five-year evolution for hospital and primary care information systems, together with a number of other complementary health informatics projects. It now provides the blueprint for all new funded measures within the NHS Information Authority and the Policy Unit. The key measures within *Information for Health* relating to electronic health care record information are:

- a six-level progression towards electronic consumer records within hospitals;
- an electronic health record anchored in general practice;
- extensions to the NHS strategic messaging service;
- the use of NHSnet for many clinical and management communications between purchasers and providers;
- the launch of a national electronic library for health;
- the application of telemedicine services; and
- programmes for informatics education for health care professionals.

The NHS vision of the electronic health record is of a longitudinal patient record, anchored in general practice and possibly delivered through extensions to present general practice systems. There needs to be 24 hour clinician access to the electronic health record within the NHS. It must incorporate health and social care interfaces, supporting seamless care between general practitioners, hospitals, and the community. The implementation of electronic health record systems must conform to NHS technology standards, security and confidentiality policies. It must utilise the existing and planned NHS technical infrastructure: NHS wide network, the strategic messaging service (based on UN/EDIFACT), and NHS clinical terms

[25] National Health Service Executive (NHS Executive 1998), *Information for Health: An Information Strategy for the Modern NHS 1998 – 2005*, Dept of Health Publications, West Yorkshire, September 1998.

Formatted

(presently the Read codes, in future to be SNOMED-CT). Pilot electronic health record implementations will be demonstrated through 'beacon sites', which are being identified for accelerated implementation to illustrate and disseminate the practical means of realising electronic health records.

Implications for a national approach in Australia

In their report, the Flinders University researchers caution that problems that are affecting the UK's ability to put electronic health records in place exist to a far lesser degree there than in Australia — suggesting that the fact that they have arisen in a country where a great deal has been done at a national level demonstrates that there is a real need to consider carefully how to proceed in Australia.

New Zealand

It is worth dwelling at some length on the New Zealand (NZ) experience, given that government's initiatives in the health information area and the close parallels there may be for Australia.

Since the early 1990s, the NZ Government has been taking a national approach to health information and, since 1995, a co-ordinated view of the electronic health record. In 1996, it released its *Health information strategy for New Zealand.*[26] Initial developments involved solving the problem of identifying individuals, providers and consumers in different settings, and ensuring security, confidentiality and privacy of personal health information.

Two national health databases, the National Health Index (NHI) and the Medical Warning System (MWS) are at the centre of the infrastructure that ensures privacy and security — as well as access to health care professionals responsible for consumer care. The NHI is a register of all users of the health care system in NZ; everybody will be assigned a person identifier (currently between 93% and 95% of individuals have a person identifier) and their name, aliases, addresses and dates of birth are maintained on the register. This enables positive (unique) identification of an individual under strict legislative control of privacy via the NZ Privacy Act of 1993.

The justification for proceeding with a national plan for electronic health records can be summarised as:

- decreased time and therefore cost required for information management of health records;
- improved availability, transfer, retrieval, and 'shareability';
- linkage of health records for a particular consumer from different health record sources;

[26] New Zealand Health Information Service (NZHIS 1996), *Health Information Strategy for New Zealand: a joint venture between the Area Health Boards and the Department of Health*, www.health.govt.nz/HIS2000/indexhtm 1996

Formatted

Field Code Changed

- decreased cost of health record storage;
- multiple dynamic views of the electronic health record obtainable 'instantly';
- powerful abstraction and reporting capability by electronic health record systems for population health, audit, research and health service planning purposes;
- improved data quality and standards — via data entry validity checking, and direct data transfer from other sources, eliminating transcription errors; and
- underpinning for computer-assisted decision support.

The main requirements raised in the electronic health record report by the NZ Health Information Service (NZHIS) were:[27]

- gaining user confidence in computers, especially in respect of the availability, privacy and security of computer-stored data;
- adoption of a positive attitude towards computers in the workplace;
- careful strategic management of change, as well as champions for the new technology;
- the need for recognition and acceptance by those entering data that the usefulness of records extends beyond the care needs of the consumer;
- recognition that there are many legitimate (re-)uses of clinical information which are in the best interests of community, as well as of various other parts of the organisation (eg billing, research, statistics); and
- the need for users to become knowledgeable consumers of this technology (like a motorist) without needing to be experienced in its maintenance (like a mechanic) with adequate skills and proficiency in the use of the computer application.

This report concluded that:

> It could be argued that there is a strong business case for the development and implementation of computer-based medical records. All the necessary technology for implementation of full electronic medical records exists. Where electronic records are kept as an integral part of the care planning and delivery process, their data quality is normally high, and almost all the administrative requirements for data can be provided as a by-product of these records.

Progress on building blocks

NZ is well advanced on developing the necessary electronic health record building blocks.

The National Health Index (NHI) was first introduced in 1977 to assist public hospitals in managing consumer files and uniquely identifying consumers. The NHI

[27] New Zealand Health Information Service (NZHIS 1995), *Electronic Health Records*, 2nd edn (available at www.nzhis.gov.nz/publications/EMR.html).

Formatted

consists of a seven character unique identifier and a number of demographic data elements including name, address(s), date-of-birth, sex, ethnicity, and aliases.

The NHI is now used in both secondary and primary care and is used to access an increasing number of applications. General practitioners currently have at least 80 per cent (and up to 99 per cent) of their consumer registers indexed. All users of the NHI are bound by the NZ Privacy Act and the NZ Health Privacy Code. There is also a specific access agreement between the NZHIS and individual users.

The MWS is a national database, which serves the function of notifying health care providers of any information, or known risk factors that might be important in making decisions about consumer care. The MWS uses the NHI number for access and access rights are subject to similar conditions as for the NHI. The MWS has five distinct components:

- medical warnings (eg allergies, drug sensitivities);
- medical alerts (eg diabetic; renal failure requiring dialysis);
- health care event summaries (eg hospital admission date and principal diagnosis);
- contact details (eg next-of-kin); and
- donor information (eg kidney and heart donor).

The NZ Health National Health Data Dictionary contains, like its Australian equivalent, only high-level demographic and health items, reflecting its original purpose as a tool for health service administrators, planners, and policy makers. However, also like Australia, the NZHIS intends to expand the dictionary to include (more granular) clinical terms and concepts, which will greatly increase its utility for health informaticians, clinicians, and software developers.

HL7 is the official NZ standard for all clinical messaging. It is currently being used for:

- pathology orders and results;
- radiology and results;
- referrals, status, and discharge;
- NHI and MWS transactions; and
- claims and payments.

Electronic clinical messaging for pathology and radiology results in primary care is much more common in NZ than Australia — with an average of around 65 per cent participation nationally (and over 70 per cent in some areas). This will increase rapidly in the near future because the Government has introduced a requirement that all general practitioner billing claims must be submitted electronically by 1 July 2000. NZHIS established a national health Intranet in 1999. It is still in an early stage but will be used for information, messaging, and e-commerce across all sectors of health. The Intranet is expected to eventually replace the current

privately run X.25 network, which is used extensively for clinical messaging to general practitioners.

The Intranet architecture has 3 levels of security. Level one uses internet protocol (IP) on an NZHIS-managed Virtual Private Network (VPN). Level 2 creates security with X509 version 3 digital certificates with Public Key Infrastructure. Level 3 uses 128 bit encryption.

NZ has been a world leader in privacy of personal health information, enacting its Privacy Act in July 1993 and the Health Information Privacy Code in 1994. The latter formulates rules applicable to:

- collecting personal health information;
- storage and security;
- access and correction;
- use and disclosure;
- updating and disposal; and
- person identifiers.

Responsibility for privacy is unambiguous and rests with named individuals, as in the European Commission directive. There is no doubt that this approach has allowed some of the innovations described above to proceed.

The implementation paper from NZHIS raised the issue of change management.

> Change creates uncertainty; where there is uncertainty there is fear and rumour. The management of this requires investment of time and effort, and the use of appropriate ways to involve those who will be affected by it. Staff must be motivated by management to view the change as positive and beneficial and to become committed to it. They must embrace the goals of the change and be prepared to work towards their achievement. In addition, there will need to be serious investment in appropriate education and staff development activities.

In summary, the decision by the NZ Government in the early 1990s to invest in and promote key items of health information management infrastructure has positioned it as a world leader in the field, particularly in the primary care sector. This infrastructure includes the NHI, the MWS, a national clinical coding system for primary care (Read) as well as for hospitals (ICD), the early adoption of HL7 as the standard for health messaging, and more recently a national health Intranet and the attendant security apparatus in the form of Public Key Infrastructure (still in early development). National privacy legislation and a national Health Information Privacy Code have now been in place for over six years.

These initiatives have provided the essential building blocks for a national electronic health record implementation. Significant and pioneering work has already been done on a national electronic health record standard. This, together with the experience gained in the important items of infrastructure listed above, has enabled this small country to now play a major informed role in the development of international standards for the electronic health record and other areas of health

informatics. The NZ health software industry has also benefited greatly from this experience — with a disproportionate number (compared to Australia) being successful in the international market. These include Cardinal Health care, Orion Systems, Delphic, Houston, and Terra Nova.

NZ is clearly well ahead of Australia in its implementation and use of electronic health records in primary care. Despite this, the lack of an electronic health record standard to date has led to the same problems found in other countries, with little or no interoperability between different clinical systems except through simple messaging, although NZ has benefited from a single vendor implementation of HL7 messages.

The status of the electronic health record and other aspects of clinical computing in NZ hospitals is much the same as in Australia (and most of the rest of the world). There is generally only a Patient Master Index (containing demographic and minimal clinical information in the form of diagnostic coding) plus various departmental systems such as pathology and radiology with little or no interoperability. There is no integrated consumer-centred electronic health record. However, the NZ National Medical Warning System could be seen as the starting point for a national electronic health record 'regime' and the other items of information infrastructure discussed above will also help to provide a firm foundation.

The single level of government (and hence of health policy and funding) in NZ, together with the active involvement of the NZHIS and Ministry of Health in information management/information technology policy and implementation over a long period, have no doubt contributed significantly to the relative sophistication of health care computing, particularly in primary care. The small population and landmass have probably also played a positive role.

Implications for a national approach in Australia

The Flinders University researchers summed up what Australia could learn from New Zealand when it comes to electronic health records as follows:

> The building blocks for a national approach are clear from NZ experience. First, legislation that genuinely addresses consumer concern regarding privacy in a manner that balances the need for access to safeguard health has been in place for a number of years. Second, regulations, which ensure the security mechanisms necessary to achieve this balance, are also in place.
>
> New Zealand has a single organisation able to make decisions on a national approach to electronic health record implementation, unlike Australia. Recent initiatives to centralise decision making, such as the formation and funding of the National Health Information Management Advisory Council (NHIMAC), the General Practice Computing Group (GPCG) and the Electronic Health Record Task Force, are important and likely to encourage progress.
>
> There are more lessons to be learned from the New Zealand experience in the areas of building, implementing, and supporting the infrastructure necessary for an integrated

national health information management system. Principal among these are the need for a health identifier and a national coding system for primary care. All of these items are currently being considered in Australia. These processes will benefit from closer dialogue with our New Zealand colleagues so that we can gain from their experience.

Other countries

Europe has been a major centre of research and development of electronic health records and associated technologies. Use of computers in primary care is much higher in Europe than any other part of the world, including Canada and the USA — being particularly advanced in the Netherlands and Germany. Hospital information systems in Europe rarely contain consumer record data other than pathology reports, medication or diagnostic terms. Many are 'home grown' — commercial systems usually being sourced from the USA.

A number of publications describe the European efforts to introduce a framework to support electronic health record development (see Appendix B). The European Commission’s (EC's) directive to require consistent legislation in all countries is aimed at providing a safe environment for 'data subjects' while encouraging transfer of information between countries.

The drivers for uptake of computerisation of health care have been varied, but usually associated with government requirements or incentives. Germany, for instance, has implemented a health card — key information on a smart card. France requires physicians to submit their bills electronically. The Advanced Informatics in Medicine (AIM) program, funded by the EC, is the largest research and development effort in health informatics in the world. The program has been operational since 1989 and currently sponsors more than 100 major research projects; many are related to supporting electronic health record development.

One project in the AIM program is PROREC (PROmotion strategy for European electronic health care RECords), promoting and co-ordinating European-wide convergence towards comprehensive, communicable and secure electronic health records. This project has issued the 'Lisbon Declaration'.

Box 4.1: The 'Lisbon Declaration'

It is recommended that the Member States through the Commission promote a frame-work for action within Europe to further develop common aspects of the Electronic Health care Records [EHRs] based on the following:

- The EHR is the nucleus of the relationship between the consumer, the health care delivery system and its professionals. As such the EHR should be the core of the new generation of health information systems.
- The main objective of the use of any EHR must be to improve quality in care by having the record and its associated information always available for the health-care professionals when needed at the point of care.
- The use of EHRs should lead to direct benefits for the professionals by making their work more efficient. This will arise from supporting the diagnostic process, enhancing EHR accuracy and completeness, improving medical knowledge and disease management, and allowing better preventive care and consumer handling.
- Within health care systems, either at European, national, regional or local level, the use of appropriate EHRs will also contribute to adequate planning and resource management, facilitation of continuity of care, registration of health care interventions, improvement of epidemiological and morbidity information, and hence, a more cost-effective care process.
- The European citizen shall by means of any EHR have (1) a guaranteed right of access to the health care to which he is entitled, (2) right of access to his individual data and related services, (3) the effective protection of his right of free circulation with respect to the confidentiality of his individual data.
- Further actions and developments of EHRs should be based upon standards and consensus that ensure interoperability, and allow EHRs coming from different origins to be reliable, communicable, recognisable and comparable.
- The European health telematics industry is to tackle the need for the development of new products in a huge and growing market, offering enabling technology to fulfil user requirements. Multimedia, 3D images, interchange formats, message contents, linguistic barriers and suitable user interfaces are among the challenges to be overcome in a framework of confidentiality and security for consumer data.
- The effective cooperation between all interested parties including users, consumers, health professionals, authorities, industry, standardisation bodies and others at a European level and through a process of managed convergence towards European electronic health records, would benefit from the establishment of an appropriate structure based on existing organisations that could promote that mission.
- In order to achieve these goals and to encompass the future, Member States individually and through the Commission should encourage common efforts and policies through adequate resource allocation, focusing on the European EHR, and leading us to consumer-centred health care systems.

Source: PROREC Project AIF Lisbon Declaration available at www.sadiel.es/europa/prorec/Contenido.htm.

Features of successful electronic health record system implementation are summarised in Table 4.1.

Table 4.1: Features of successful electronic health record system implementations

Feature	*Description*
Long term projects	Electronic health record implementation over many years — the quickest was over 4 years (with a product developed over 20 years.) and may continue over many decades. “The single most important feature is that it is not finished!”
Involve ambulatory care	The needs of ambulatory (rather than inpatient) care appear easier to meet and developments can then be transferred to inpatient care.
Involve decision support	These systems depend on a significant amount of data to be successful and probably require clinicians to depend on the electronic health record system as the primary source of information.
EHR is not an end in itself	The electronic health record seen as a means to achieve improvements in health care quality, cost and access.
Sustained leadership by skilled clinicians	Commitment at the top to a (shared) vision and to bringing the value of information to health care. Average longevity of health managers is 2.5 years — average tenure in successful electronic health record sites is 8 years. All had clinicians as leaders.
Management of the health care facility	Poor processes are magnified by conversion to electronic form. “Attention to management factors is probably the most important step in implementing [E]PR systems”.
Sustained investment	The electronic health record is seen as an infrastructure issue — not just a capital investment with immediate returns.
Adaptation to local requirements	Not a single electronic health record system was an off-the-shelf solution — rather home grown or significantly modified commercial product. This suggests the need for high calibre IT staff.
Stable vendors	The development is likely to go on for many years — so a vendor who is likely to be in there for the long haul is required.
Focus on end user	All go well beyond the clinical representation on steering committees, help desks — and “reflect the real influence of users in the continued development of the project”. Even in multi-site roll-outs the implementation must be local.
Structured data	More highly structured data means more useful data which can be processed and provide decision support and other functions.
Data integrity	Autoloading data from other devices - biometric, ECG etc. and checks at the time of data entry, tracking compliance with documentation requirements etc.

Source: Appendix B.

5 BENEFITS OF ELECTRONIC HEALTH RECORDS

> The medical record has become the principal instrument for ensuring continuity of care. … Today, such records may contain lengthy notes from a multiplicity of primary care physicians, specialists, nurses and other health care providers, such as dieticians and social workers. These notes, together with the many results from laboratory tests and reports of different examinations (radiology, pathology, electrocardiography, and so forth), must be integrated into one common medical record.
>
> Barnett G O (1984)[28]

The principal benefit of any system of electronic health records is first and foremost to supporting consumer care and improve its quality: good information accessible when and where it is needed by both consumers and providers will greatly assist in tackling the causes of ill-health as well as treating it. Second, it should enhance the productivity of health care providers in the delivery of care. Third, it should prove invaluable in supporting clinical and health services research. Fourth, any such system should be designed to accommodate future developments in health care technology, policy, management, and finance in a flexible way. Fifth, and very importantly if electronic health records are to gain the acceptance and trust of both consumers and providers, individual privacy and the confidentiality of personal health information must be enhanced at the same time as these other desiderata are being met.

Implementing a system of electronic health records would revolutionise how we collect, store and use information in the health sector in Australia. It will also substantially shift the focus to consumers, by emphasising what is needed for self care and treatment by health care providers, rather than all the effort going on the kinds of information administrators need to run the health care system.

Expected benefits of electronic health records can be summarised as helping:

- consumers to become more involved in health care decisions by providing them with accurate information about their medical problems along with other information to assist them to stay fit and well;
- providers to deliver better care by providing both up-to-date details of the medical history of their consumers (including test results) and access to what constitutes 'best practice' and the latest research findings; and
- planners and administrators to leverage scarce health care resources to maximum effect in terms of the health and well-being of all Australians.[29]

---

[28] Barnett GO (1984), *The Application of Computer-based Medical Record System in Ambulatory Practice*, N Engl J Med, Vol 81.

[29] For example, group and area studies (based on de-identified electronic health records) will be able to reveal above-average sources of ill-health and inequalities of care — pointing to where

Deleted: ,
Deleted: '
Formatted
Deleted: ,'

Providers will be key players because the idea is to arm them with the information they need to provide the best of care for the people who consult them and to play their part in improving the public's health. The proposed national health information network (see Chapter 9), will make this possible by providing them with 24 hour secure access to the information important to the care of an individual, when and where it is required. This will, for example, immeasurably improve care in accident and emergency departments of hospitals, as well as ensuring that providers involved in the care of an individual are up to date with his or her treatment (provided that is the wish of the individual concerned).

5.1 Improving the quality of life and the quality of care

Electronic health records will play a key role in improving both the quality of life Australians lead, as well as improving the quality of the health care they experience from Australia's health care system.

Keeping fit and well is highly valued. But if you are unwell (eg suffer from a chronic condition or happen to be someone with complex health needs) then not having to have to recount your medical history at every turn (because your electronic health record can be instantly accessible when and where needed) will also be highly valued. That is why it can be expected that Australians who suffer from chronic conditions or have complex health needs will be among the first to want to participate in a national system of electronic health records — in order that providers that they nominate can have instant access to their personal health information. The result will be greater patient safety and better (because better informed) care. Thus, electronic health records have the potential to be of most benefit to those with the greatest stake in the system being able to produce health care of consistently high quality. This will boost Australia's already enviable record on healthy life expectancies.

Quality of life and life expectancies

On 4 June 2000, the World Health Organisation (WHO) released, for the first time, its new 'healthy life expectancy' rankings for babies born in 1999 based on an indicator developed by WHO scientists — the Disability Adjusted Life Expectancy (or DALE). DALE summarises the expected number of years to be lived in what might be termed the equivalent of 'full health.' To calculate DALE, the years of ill health are weighted according to 'severity' and subtracted from the expected overall life expectancy to give the equivalent years of healthy life.[30]

health care needs particular attention. (De-identified records are records stripped of all personal information that could identify the individual to whom the record relates.)

[30] World Health Organisation (WHO 2000), *The World Health Report 2000: Health systems: improving performance*, Geneva, 2000.

Formatted

Formatted

Box 5.1: Life expectancy: Quality counts

Measuring a country's health by the average life expectancy of its citizens is a bit like judging the performance of the London Underground merely by the number of passengers it carries: it takes no account of how people find the experience as they go along. That is why the World Health Organisation (WHO) has come up with a new measure of population health, called disability-adjusted life expectancy (DALE). Rather than estimating only how long a child can expect to live, Christopher Murray and his colleagues at the WHO have tried to calculate how much of the child's life will be spent in good health.

To do this, they have conducted random surveys around the world to see how disabling such conditions as blindness or chest pain are considered to be. These "severity weightings", which vary surprisingly little from country to country, are combined with standard epidemiological measures of years of ill health due to particular ailments and deducted from total life expectancy to yield the DALE. Worldwide, the average healthy life expectancy of babies born in 1999 is $7^{1}/_{2}$ years less than their total life expectancy.

Japan, Australia, France and Sweden all have DALEs of more than 73 years. Indeed, the Japanese are not only the world's longest-lived people, with an average life expectancy of 81 years, but, according to this new measure, they are the heartiest, with only $6^{1}/_{2}$ years of their projected lifespan spent in ill health. Low rates of heart disease are credited as one explanation of Japan's strong showing. But the WHO warns that this may change as a consequence of fattier diets in recent years and greater cigarette consumption since the second world war.

At the other extreme, the countries with the worst DALEs are in sub-Saharan Africa. The healthy life expectancy for babies in Sierra Leone, Niger and Malawi is under 30 years. AIDS, along with malaria, tuberculosis and other infectious diseases, is ensuring that life remains nasty, brutish and short.

Poverty is a powerful ally of illness; but greater wealth does not necessarily buy better health. America is famously the world's biggest spender on health care, but with a DALE of 70 years, it still falls behind Japan, which forks out far less.

Dr Murray admits that DALE is a rough-and-ready benchmark. Standard mortality statistics are hard to gather in some poor countries, let alone more sophisticated, culturally-sensitive assessments of illness severity. The WHO is busy working on both fronts to make DALE more reliable. If only the same could be said for the Underground.

Source: The Economist June 3rd 2000

Not surprisingly, the WHO rankings show that years lost to disability are substantially higher in poorer countries because some limitations — injury, blindness, paralysis and the debilitating effects of several tropical diseases such as malaria — strike children and young adults. Thus, people in the healthiest regions lose some 9 per cent of their lives to disability, versus 14 per cent in the worst-off countries.

Japanese have the longest healthy life expectancy of 74.5 years among 191 countries, versus less than 26 years for the lowest-ranking country of Sierra Leone.

Australia ranks second, with an estimated DALE of 73.2 years. The rest of the top 10 nations are France, 73.1 years; Sweden, 73.0; Spain, 72.8; Italy, 72.7; Greece, 72.5; Switzerland, 72.5; Monaco, 72.4; and Andorra, 72.3. Notably, The United States rated 24th under the DALE measures, or an average of 70.0 years of healthy life for babies born in 1999.

The accompanying WHO press release cited sharply reduced smoking rates, leading to lower lung cancer and heart problem rates as one of the reasons for Australia's high DALE ranking. The Economist newspaper report on the WHO rankings and the DALE concept is reproduced in Box 5.1.

Quality of care

Modern health care systems are unavoidably and increasingly complex — with many interdependent parts that must interact flawlessly to avoid mistakes being made and thus ensure patient safety. Achieving a consistent high quality of care is difficult in complex systems because even low probabilities of error associated with individual system components will translate into non-significant probabilities attaching to overall system failure.[31] Electronic health records can play a key role in patient safety by greatly reducing a major source of error — lack of information about an individual's previous health history. After all, eliminating reliance on memory and guesswork as much as possible is a basic to building safe systems — and encouraging a culture of safety more generally.[32] And when patients see multiple providers in different settings, none of whom have access to complete information, it is easier for something to go wrong than when care is better co-ordinated. Thus, substituting electronic for paper-based heath records is an important way of systematically designing safety into the processes of care — provided it is done in a way that mitigates the potential for error associated with the transition from pen, paper and post to the electronic world.

[31] For example, a patient in an intensive care unit is the recipient of an average of 178 different activities preformed per day that rely on the interaction of monitoring, treatment, and support systems (Leape 1994). The laws of probability tell us that even if each procedure works flawlessly 999 times out of a 1000, the probability that something will go wrong on any given day exceeds 0.16 (ie more often than 16 per cent of the time — since 0.999 raised to the 178th power equals 0.837).

[32] Millenson (1997) has noted, for example, that many medical errors can be attributed to the simple fact that the knowledge base to effectively and safely deliver health care exceeds the storage capacity of the human brain.

5.2 Commissioned study on the benefits of electronic health records

Cognisant of the need to examine whether the benefits of electronic health records are likely to exceed the costs, the Taskforce commissioned a study of the benefits and risks of introducing a national approach to electronic health records in Australia from researchers at Flinders University, led by Dr Sam Heard. Their report forms an integral part of the Taskforce's investigations and is included as Appendix B. Interested readers are urged to read that report since selected material only is reproduced here.

The researchers group evidence of benefits under the following headings, under each of which they also draw out implications for a national approach in Australia:[33]

- a greater consumer focus in health care;
- improved health outcomes;
- improved and appropriate access to health records for health providers;
- improved support to providers;
- improved quality and safety data;
- improved efficiency and quality of health care; and
- improved management and utilisation of health information.[34]

5.3 A greater consumer focus in health care

Increased access to education and dual incomes has meant that there is a generation of consumers who are ready, willing and able to take advantage of the new information age. They are also interested in health and willing to challenge health care providers and the basis for their advice.

The changing nature of health care is evident to all. Consumers increasingly come to the consultation with information about their health problems or the diagnoses they consider to be likely. Their ideas may be based on the results of a Medline

[33] For ease of reading, detailed references are not reproduced here; they can be found in Appendix B. Indeed, readers are referred to Appendix B if they are interested in the detailed material on which the investigators have drawn in arriving at the views summarised here.

[34] In introducing their material on benefits (see Part 4 of Appendix B) the researchers note the following caveats: that the body of scientific evidence demonstrating benefits is not overwhelming; that much of the evidence that is available comes from computerisation of different clinical processes in isolation (ie almost always without a true electronic health record), however, it is virtually certain that the clinical benefits that have been demonstrated will be substantially greater when these computerised processes work with a longitudinal electronic health record (likewise for economic benefits); and that almost all research has been done on systems that are not commercially available and hence there is no certainty that the same functionality can be delivered in a commercial environment.

search or from a Web site they have accessed through the Internet.[35] The nature of the consultation is also changing. The computer, present at the time of consultation, offers the possibility of accessing information very rapidly. It becomes the third party in a triad — the consumer, the provider and the computer — working to maximise the benefit to the consumer and the effectiveness and efficiency of the interaction.

Timely and appropriate access to and exchange of electronic health records can empower consumers and facilitate a greater consumer focus in health care, as stated in *Health Online*:

> Health consumers should be able to access their personal health information and it should be accessible across national and international borders in the interests on their own health care.

Consumers, therefore, need to be in a position to control and monitor the access and contents of their electronic health records — including control of disclosure of data appropriate to the type of care received.

Consumers need to be directly involved with creating their health records — for a number of reasons. First, to measure outcomes subsequently, the consumer's perceptions must be captured in the record. Second, consumer information needs to be reviewed for accuracy and completeness.[36] Finally, direct involvement in their records may improve consumers' health.[37] Consumers can be productively involved in negotiating the outcomes sought from clinical interventions and can tailor computerised decision support to their situation and need.

Other findings from the literature were:

- there is increasing evidence that electronic health records are accepted by consumers;
- when given the ability to access their own health records online almost all consumers take up the opportunity; and
- to overcome the language problem of the use of technical terms in the electronic health record which the consumer may not understand (eg anterio-inferior myocardial infarction), software tools are being developed to 'translate' such terms into the kind of language that consumers can understand (eg heart attack).

Consumers like receiving written health information (eg consumer information leaflets), and electronic health records will enable such information to be tailored to

---

[35] It is estimated that at least 100,000 Web sites have health-related content. Furthermore, the Internet makes it easy for consumers to access information from other countries as well as their own, so that for the first time in the history of medicine consumers have equal access to the knowledgebases of medicine.

[36] For example, paediatric records have been shown to be more accurate and complete when parents were given access to enter information directly into the record.

[37] Liaw's study of computer-generated patient-held health records (see Appendix B) concluded that the patient-held record is "an important determinant of patient participation in information and responsibility sharing, health promotion, and disease management."

Deleted: o

their personal circumstances — making the information potentially far more valuable to the person receiving it.[38] For example, information about the illness a person is suffering from can be printed out for the consumer to take home and refer to later.

Electronic health records enable consumers to become better informed about their health care, particularly since the information and communication benefits of the Internet make it easier for consumers to find out how to better care for themselves, develop a better understanding of their diagnoses and make better decisions among treatment options.

There is some evidence that electronic health records can improve the health of under-served populations (eg Aboriginal and Torres Strait Islander peoples and the homeless). Use of modern information and communication technologies also makes the delivery of health information in languages other than English cheaper and easier. Access to an individual's electronic health record will also assist the delivery of telehealth services, of particular benefit to both providers and consumers of health care services in regional Australia. They also facilitate the development of telehomecare, enabling consumers to remain in their own homes with monitoring and support systems that exchange data with their health record.

From a consumer perspective, electronic health records can facilitate a consistent approach to the monitoring and reporting of the outcomes of care by provider organisations and avoid problems relating to the legibility of hand writing in paper-based records. Moreover, studies indicate that when consumers are given access to their medical records the quality of record keeping improves.

With right of access to their health records consumers can:

- check the accuracy of their records;
- supplement the information contained in their records;
- make informed decisions about whether to give or withhold consent concerning the use of their records;
- review the 'log' of who has gained access to their record; and
- make informed decisions regarding complaints they may want to make concerning their health care.

Implications for a national approach in Australia

The drivers for consumer access to the electronic health record are:

- provision of individually tailored information for the consumer;
- correcting and adding to the content of the electronic health record;
- gaining an understanding of their health in historical terms;

[38] A 1996 US study found that consumers ranked "information from my own doctor's office" as the type of online health information that they desired most.

- assisting in informed decision making and reviewing current management;
- enabling improved and evidence-based self-care; and
- through access to information, the development of greater trust between the consumer and providers.

With access, electronic health records are widely accepted by consumers as a valuable resource in achieving and maintaining health. Consumers are far more likely to access them online if this is possible, rather than at the time of consultation. Interaction in a clinical setting may be more acceptable with small hand-held devices which are more private and less intimidating.

Clinical terminology used at present is not straightforward from a consumer perspective and efforts are required to ensure there is a consumer dimension to terminologies used in clinical care.

If consumers are to use the record then they must have some say in the design of tools for that purpose. A set of guidelines for involving consumers in electronic health record development and utilisation is required, along with research and development of tools to aid consumer access to and utilisation of their personal health information.

Accreditation of providers of health information online will assist consumers in their choice and handling of the material offered. Institutions such as the Health Issues Centre are developing Web sites for this purpose. Seamless integration of access to such online material should be a feature that is allowed for in Australian developments.

To support consumer access to personal health information, the Health Insurance Commission is exploring a product, called Medicare Online, which will give consumers access to their personal Medicare records. Potentially, this could be expanded to allow consumers assess to a much broader range of information, such as the location of hospitals or general practitioners.

Monitoring of service in different contexts is important to ensure equity of access to electronic health record services across the Australian health care system.

Consumer access to and control of electronic health records is critical to good functioning of those records and trust between consumers and providers.

5.4 Improved health outcomes

Consumers must benefit from the introduction of electronic health records. Ideally, the main benefit should be better health (not just the provision of more efficiently delivered health care — see Box 5.2). There is some evidence that this is happening:

- in an early randomised controlled trial, computerised feedback on hypertensive care by general practitioners led to a reduction of 5mm Hg of diastolic blood pressure and 4 fewer visits per year in the intervention group;
- computerisation of diabetic care was found to have been beneficial in 12 out of 15 of the more rigorous trials (the outcomes achieved were better control of blood sugar and also lower frequency of dangerously low blood sugar levels);
- adverse drug events are the most common type of iatrogenic injury and probably occur in a serious manner at a rate of approximately 3 per cent of hospital admissions (see also Chapter 13). Three consumers per 1000 admitted to hospital will die and one will suffer long-term disability due to adverse drug events — and it is thought that as many as 70 per cent of these may be prevented by improved information systems; and
- consumers are benefiting from shorter length of stays in hospitals as a result of automated clinical-support systems.

Implications for a national approach in Australia

Meaningful and valid evaluation of electronic health record implementations is required to monitor the net benefits to consumers' health.

The expertise and capacity to carry out this work needs to be developed and maintained in a form that is likely to serve the interests of consumers.

Studies that measure consumer outcomes need to have sufficient (statistical) power — an issue that may have funding implications and need to be brought to the attention of the National Health Medical Research Council.

5.5 Improved and appropriate access to health records for health providers

Electronic health records make possible simultaneous access by different health professionals at multiple sites, an important benefit as health care services increasingly become highly specialised and providers often work closely in multi-disciplinary settings (hence the concept of a health care 'team').

Electronic records are accessible from any location, even internationally, across a communication link or network. This is an obvious benefit to Australian people, many of whom are increasingly mobile, travelling away from home for work and leisure purposes. In particular, the ability to provide quality emergency care is

improved by the rapid transfer of health information that the electronic health record makes possible.

Box 5.2: Contrasting scenarios

Scenario: A construction worker falls from scaffolding on a building site and is rushed to hospital by ambulance unconscious. On site, incident forms start to be filled out for both administrative and medical purposes (eg worker's compensation). Meanwhile, the ambulance team passes their findings to the Accident and Emergency Department team on arrival. Starting with just this intelligence, the emergency team swing into action (including ordering a battery of tests). They effectively start a medical record from scratch, knowing nothing about their consumer's previous medical history — maybe they cannot even put a name to their consumer until he regains consciousness. They do their best under difficult circumstances but it is touch and go, particularly before vital test results become available. Along the way they make avoidable mistakes (it turns out that the consumer suffers an adverse drug interaction). Eventually the consumer is stabilised and admitted to hospital, where his stay generates numerous additions to his hospital record. On discharge, he goes to his general practitioner who has to question his patient closely about what transpired from the accident onward because she cannot offer the most appropriate care until she feels that she is sufficiently informed of relevant facts. Subsequently, a hospital discharge summary arrives, filling in significant details that her patient could not. Although the worker eventually recovers sufficiently to return to work, it is on permanently reduced duties (and pay), and the whole episode could have been much better handled if the various providers had been better informed (but simply did not have access to necessary information where and when it was needed).

Contrast the above with the following **scenario**. The accident happens as described, but during the ambulance ride one of the team recovers the man's health identifier and phones ahead so that, on arrival, the consumer's electronic health record is already available and has been scanned by Accident and Emergency Department team staff. The team springs into action and are able to avoid the adverse drug interaction because they have access to the individual's medication record. They, and the hospital staff more generally are more confident in their health care decisions and delivery because they have access to the consumer's electronic health record. Also, immediately on discharge, the (now updated) health record is sent electronically to the man's general practitioner who, in turn, can provide care that is fully informed. As a result, it never becomes 'touch and go', and the man is able to return to his employment far earlier than under the above scenario, fully fit. Linkage of health records for a particular consumer from different health record sources is possible with electronic health records in a way that is not available to paper records. With the consumer's consent, records kept at different sites, or within a health care facility, can be linked, merged and shared to create a single 'virtual' health record.

Both health care managers and administrators (72%) and health care providers (73%) rated the ability to share consumer data as the highest priority

implementation issue in the Medical Records Institute's ongoing electronic health record survey. This is because it is most likely to remove frustration and lead to real efficiency savings. Consumers are also likely to benefit from fewer delays, fewer repeats of tests and more appropriate care when providers have access to their electronic health records.

Pre-requisites for successfully being able to assemble a 'virtual' electronic health record which can draw information from many sites to present a particular 'view' accessible via, say, a Web browser include:

- an agreed record structure;
- shared concepts of professional process;
- a system of unambiguous person identification;
- an effective method of obtaining the individual's informed consent;
- a core set of information about consumers;
- protocols to maintain confidentiality;
- common terminology and coding;
- agreed interfaces between agencies;
- an appropriate information technology infrastructure;
- acceptance by consumers; and
- acceptance by providers.

Sharing information (eg via electronic health records) is now a priority in primary care, promising a "shared clinical perception of a consumers problems and needs" and the real prospect of 'seamless' care via 'seamless' information. Realising these objectives underscores the imperative to involve all types of care providers in electronic health record development.

A properly designed and implemented electronic health record can be accessed quickly and securely by any consumer or health professional around the world if the site of care and the electronic health record source are connected via the Internet. This access can extend to 24 hours per day if desired and even via a mobile phone or satellite.

Electronic health record systems inherently offer increased access to consumer data through their ability to search through an electronic record for specific information. Access to information may be particularly important in specific domains, such as in mental health care.

Timely and appropriate access to and exchange of electronic health records will benefit consumers, health professionals and managers but potentially poses a threat to consumers — through loss of privacy — and some threat to health providers (who may feel uncomfortable with their records being available to whomever the consumer provides consent).

Implications for a national approach in Australia

The sharing of health records has always been limited and remains the major frustration in electronic health record development to date. Investigating 'federating' legacy systems through Web-based technology remains attractive where there is a good deal of commonality.

There are a number of initiatives that aim to overcome this barrier in diverse but complementary ways. The first is simple messaging between systems — HL7 is the leader in this field. The HL7 Patient Record Architecture initiative takes this approach to enable sharing of documents in a machine readable manner and is converging with CEN efforts. CORBAMed is a technical group which aims to allow this sharing to be at a system level without the need for text-based messages and has developed the application interfaces to allow this. The Good Electronic (formerly European) Health Record (GEHR) offers a generic electronic health record information model that further standardises all these efforts by providing a standard architecture for the electronic health record within the system.

Even though the lowest level mechanism for standards has been accepted — HL7 messages — it is not necessarily the simplest as the detailed structure of each message has to be agreed and the means of incorporation into each system has to be developed.

However, agreement on and design of a record architecture is also a lengthy process, and while it promises to relieve much of the implementation risks and does not dictate the format of the record, this approach is as yet unproven.

If consumers are to control access to electronic health records, there must be a secure method for this to take place with a trusted senior clinical 'controller' or 'data guardian' at each electronic health record site. Sources of electronic health records must be known and their controllers held responsible for making them available in a secure manner. Further, the mechanisms by which this access will be available must be consistent nationally. Further, computer systems must also be reliable and barriers to access must not be so great as to impede health care.

5.6 Improved support to providers

The information in the electronic health record is static, but can be displayed and processed dynamically and selectively. This allows multiple views of the electronic health record to be obtained virtually instantly depending on the needs of the provider (eg problem-oriented, health summary, medications, chronological etc) — something that also improves efficiency. Further, the information can be automatically processed to assist the health provider and consumer in making decisions.

To achieve maximum benefit from implementing an electronic health record, four conditions must be met:

- users must have confidence in the data;
- they must use the record actively in the clinical process, at the point of care;
- they must understand that the record is a resource beyond direct consumer care; and
- they must be proficient in the correct use of the system.

These conditions must be met before the electronic health record can be relied on to hold the information required to make safe clinical decisions and support automated processing.

Computerised decision-support systems are computer software systems that are designed to aid health professionals when making important decisions. A system usually takes the form of provision of assessments or prompts which are specific to the individual and are selected from a knowledgebase according to their characteristics. Decision support benefits the consumer as it provides 'just in time' notification of best practice or possible adverse effects. Health care providers benefit from the convenience of getting relevant information at the moment it is required. Managers benefit from the cost-savings potentially associated with evidence-based care and avoiding adverse reactions — savings which are likely to be considerable (see Chapter 13).

The electronic health record underpins the success of such systems by providing detailed information on which to base decisions. The electronic health record needs to be organised in a way that allows safe automatic processing for this purpose. Apart from supporting decision support, the electronic health record itself can contain prompts and alerts. The GEHR architecture, for example, describes specific information structures that convey key prompts to health professionals opening the record.

To date, the most experience with personalised decision support has been with prescribing. Health professionals are no longer in a position to retain information about all medication interactions. Wyatt (see Appendix B) has concluded that computerised prescribing improves accuracy, appropriateness, speed and prescribing costs. His analysis of UK studies suggests that a little over one minute of clinician's time is saved per consumer, phoned requests from consumers are reduced by up to 38 per cent and 5 per cent fewer inquiries are received from pharmacists. Cost savings of up to 30 per cent have been documented. Accurate records of prescribing increased from 42 per cent with manual systems to 95 per cent with computer assistance.

Decision support can improve adherence to drug formularies by simplifying stock control and clinician information needs. One positive outcome is a reduction in keeping track of adverse reactions, beyond the capacity of health professionals without decision support.

Most research has taken place in hospitals. The more specialised setting makes the design and implementation of decision-support systems more straightforward. In primary care Delaney and colleagues conclude that computerised decision-support systems have great potential for primary care but have not addressed the needs of clinicians adequately, which are far more than just prescribing and so leads to a lack of demonstrable benefit.

It is widely accepted that clinical decision-support systems will increasingly affect decision making in health care and maximising this benefit is largely dependent on standardisation.

The electronic health record can be viewed in many ways and can offer situation-specific data to clinicians making decisions. An example is a list of all prior treatments offered for a particular problem or trend graphs for certain key parameters. It will be much easier to make a decision on a consumer's hypertensive treatment when a graph of all blood pressures is offered with line graphs of previous treatments and doses.

The electronic health record also offers the potential to filter knowledgebases to provide specific information sought by health care professionals or consumers. This advice may be of relevance to the diagnostic process, the consumer's understanding of their disease, prognosis or treatment. The advice may be sought by the consumer during the interview, in which case it may be shared at the time, given to the consumer as a resource to take away with them or e-mailed to them for convenience. Health professionals may seek information and retain it as part of the record to inform the consumer, a colleague or student in the future or as 'evidence' for a decision.

Australia has some high quality independent information on prescribing in the form of the *Australian Medicines Handbook* and *The Therapeutic Guideline*s. Referring to this information is too time consuming for most practitioners — if they can find the books themselves at the moment they are required! Context sensitive information from these sources, including prescribing options, doses and cost are sought by many health professionals.

There is some evidence that health professionals do seek information more often when using electronic health record systems. Further, integrating electronic health record with Web and knowledgebase access can lead to efficiency gains as demonstrated by Tarczy-Hornoch at the University of Washington. Finally, complex tasks may be assisted with specific tools, such as assessing risk of cancer from family history interpretation.

While decision support has a demonstrated role in improving the health care of individuals, access to clinical guidance and care pathways promises to deliver more. Consumers stand to benefit from a consistent and evidence based approach to their care by a range of health professionals. Health professionals, on the contrary, may experience some frustration although careful evaluation should demonstrate the risks of not following the guidance.

Access to protocols and guidelines at the time of care was identified as a key potential benefit of electronic health records by the UK Audit Commission Report. There is some evidence that this will lead to improved quality of care and ability to manage chronic conditions. Electronic health record systems offer the opportunity to access guidance at the moment of decision making and to have the guidance adapted to that particular individual and linked information and references online.

Electronic health records can be viewed in different ways by different users and for different purposes. The electronic health record offers health professionals and students the opportunity to review their records within specific contexts or audit different aspects of care or workload — much as was possible with the early medical records — while still offering the benefit of unit records or problem oriented records. This is considered an important aspect of electronic health records, which will require advocacy to be accepted by consumers.

Implications for a national approach in Australia

Clinical decision support has been demonstrated to make a difference in many areas, most particularly in prescribing and prompting for preventive procedures.

The electronic health record requires generic decision support tools, that is to say, aids to decision-making that can be used in different settings and with different clinical applications. There are three (not necessarily exclusive) approaches to consider for general implementation of decision support:

- a database of information and an instruction set on how to implement this within each software environment;
- a standard method for expression of rules with all decision support written using these 'languages' and implemented locally; or
- generic decision support engines — offered as a standard component for implementation.

A standard electronic health record architecture potentially simplifies implementation issues — the alternative is for system developers to implement the system in their specific context. This may lead to fragmentation and safety issues that are difficult to assess.

The barriers to implementation of these support systems are great — authoring and maintenance of generic guidance requires sophisticated tools that are still being developed. Even with such tools available, authoring is expensive and may only be affordable with international cooperation.

Safety of decision support is presently unregulated and issues such as processing electronic health records with missing data must be addressed, as well as formal evaluation procedures. Research topics focussing on the performance of clinical decision support have included medication dosage, diagnosis, prevention and disease-specific systems (eg hypertension or diabetes). This research needs to

continue as there is great potential to assist health providers in offering safe, evidence-based care in a timely and acceptable way.

Electronic health records have to contain sufficient data to support the added functions possible with computer assistance.

Acceptance of electronic signatures (or other strong user authentication) for prescribing and other orders will further advance the uptake of computerisation by clinicians, and hence the utility of incorporating decision support into these applications.

Access to expert knowledge must be fast enough and these days the Internet is the only practical alternative. An example might be enabling clinicians to respond to a medication scare in the media that does not give sufficiently accurate information. An e-mail notification with sufficient information, as well as expert advice, on how to deal with the situation will benefit health consumers and providers.

For such access to be meaningful there is a need to foster direct Internet access by providers to rapid-response expert opinion, as well as timely access during consultation.

High-quality resources need to be available, under control of a trusted agency. The UK has done this through the National Institute for Clinical Excellence (NICE) as guidance and care pathways require expert authoring and maintenance — this is a major enterprise. Further, accessing guidance and care pathways are only possible at a system level if the resources are made available in a standard way.

Appropriate student access to electronic health records must be considered important by all consumers and providers, while consumers must have control over student access. This may require raising of public awareness of the importance of educating health professionals.

Strategic feedback to health care providers may be possible through third-party tools on, for example, prescribing rates or immunisation coverage.

5.7 Improved quality of safety data

The electronic health record is quite different from paper records in its ability to validate data at the time of entry and the multitude of storage mechanisms available.

When clinical data are added to the electronic health record and maintained by providers who are responsible for care, the accuracy and quality of data is high. Further, when entering data into an electronic health record, checks can be made to ensure the information is accurate and adequate. For example, accuracy may be enhanced by querying implausible entries or rejecting impossible ones. Results and reports can also be entered directly and automatically from other systems, eliminating the possibility of misfiling and of transcription errors. Users' details

can also be entered automatically and unambiguously. Data entry becomes a formal process and the system can prompt for missing information.

There is a necessary trade-off between the drive to improve data quality and the acceptability to health providers — they will have to have the final say but need to be educated in the importance of data beyond the particular consultation.

Consumers will benefit if electronic health records can be more secure and yet at the same time more available than paper records. The major risk to consumers in the health care system was unauthorised use of personal health information by authorised users. With paper records this is particularly difficult to control. Clerical staff typing letters usually have access to the entire record, as do staff moving records around a health care facility. Unlike paper-based systems, electronic health record systems can monitor access to records by authorised users (as well as preventing unauthorised access).

Implications for a national approach in Australia

Accreditation of health record systems may involve assessing validation functions to ensure data quality.

Point-of-care data entry is important, but will only be undertaken if users are convinced of the benefits of the electronic health record system.

To protect consumers, it will be necessary to ensure that users are authenticated in a stringent manner. This is an issue throughout the computer industry, and measures should not be developed which are specific to the health care environment. Possibilities that are now available, and may become increasingly economic, include 'smart cards' carried by the user and biometric measurement — such as a fingerprint or retinal scan.

The ability to back-up electronic health record data is an important benefit and must not be left to the whim of the electronic health record controller. National policies of back-up for electronic health record sources should be developed in discussion with controllers, providers, consumers and the software industry.

Accreditation for electronic health record sources should be considered in light of the need to ensure adequate monitoring of access to electronic health records and strong user authentication. Software accreditation will need to address these issues, as well as data quality. It is important that the convenience of using electronic health records should not be jeopardised.

Enabling development of electronic health record systems in Australia to a point where communication can occur without the need to resort to paper will add to savings and boost efficiencies.

5.8 Improved efficiency and quality of health care

Paper records are not performing well in the modern health care environment. The (US) Institute of Medicine has summarised in detail the shortcomings of paper records. The electronic health record can assist in overcoming some of the problems with content, format, access, availability, retrieval, linkages and integration.

Murphy and others describe the key insurmountable risks with paper records:[39]

- the record may not be available as it is being used by another practitioner;
- the record is necessarily fragmented as it can only be structured in one dimension — front to back; and
- the record is not useful for audit or research without considerable effort.

Electronic health record systems have not abolished the use of paper — although some primary care offices are virtually paperless. In the large and exemplary electronic health record systems in the USA — none have completely done away with paper. It may seem paradoxical that at Kaiser-Permanente in Ohio, the only system to do away with paper charts, there has been an increase in the use of paper because every contact involves printing out a set of computer generated encounter forms — which are then scanned into the electronic health record.

Estimates of the time spent maintaining paper records are all above 25 per cent in a hospital setting. Estimates in the USA have been 38 per cent for physicians and 50 per cent for nurses. And, between 35 and 39 per cent of total hospital operating costs have been associated with consumer and professional communication activities. In ambulatory care, costs have been estimated at US$3 per consumer. This is due to the large number of file-related activities per ‘event’.

Estimates show that 20-30 per cent of clinicians’ time is spent searching for or organising medical information. Legibility of the electronic health record is far superior. The ability of the electronic health record system to provide user dependent data layout, assisted search as well as more output methods (screen, paper, e-mail, fax etc) and tailored output all aid productivity.

Single entry of demographics and other information used repeatedly reduces transcription expense and reduces billing omissions. Clinical and administrative efficiency is increased by as much as 62 per cent, and not only in secondary care. The clinical efficiencies are especially evident in repeat prescribing. Further, there is some evidence of improved quality of service delivery.

Staff satisfaction is increased when tasks are easier. Computer generated discharge summaries have been shown to be less burdensome, faster to generate and preferred to dictation in a randomised controlled trial in Canada. Hunt and colleagues’

[39] Murphy, GF *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia.

systematic review of clinical decision support shows almost universal improvement of the health care professional's performance.

Clinicians have views on how electronic health record systems should be implemented. Taking these into consideration not only aids acceptance of the electronic health record system but also assists physician learning as a by-product of the implementation. General practitioners in the UK have changed their practice due to the use of computers. There is an increase in provider initiated tasks which leads to such changes as an increase in immunisations (rates improved from 8-18%) and other preventative tasks (up by 50%), improved record keeping and problem list generation. It is worth noting that the improvements do not appear to be sustained at the initial level.

Achieving benefit cannot be taken for granted. Benefit did not occur where none of the clinicians had an intimate knowledge of the system nor responsibility for decision making during implementation. Benefit is also dependent on having access to computer workstations, which are reliable and provide suitable response times.

It is important to acknowledge that some health professionals and consumers have particular difficulty using computers, which may involve a special kind of dyslexia — a finding confirmed by more general studies of computer users. Mechanisms for these users to gain skills and confidence need to be incorporated into implementation plans. Despite this, there appear to be definite efficiency gains and user satisfaction with some electronic health record systems, although data entry remains the greatest impediment to this.

Just as users seek efficiency from the electronic health record system, so too is the ability to link to other systems such as billing, referral to (other) specialists, pathology and radiology orders. Consumers may benefit from aspects such as automatic notification to immunisation registers if payments to the consumer are dependent on this information as is presently the case. The major benefits will probably be to clinicians and managers from streamlining work patterns. Anything that speeds processes of care will benefit everybody.

Dealing with referral letters electronically has been addressed in some detail. The potential time saving by administrative staff of using electronic records is estimated at 6 minutes per clinical letter sent or received. With a projected clinical letter rate of about 18 million clinical letters per year in Australia this will save $36 million per year at $10 per hour. Estimates in the UK predict savings from full electronic exchange of information to be approximately $10,000 per general practitioner. Delivery times improve from days or weeks to minutes or hours. Legibility is guaranteed (assuming systems are compatible).

Automatic generation of recall letters is a successful strategy in primary care, particularly for those who rarely visit a general practitioner.

Methods for determining the true cost efficiency of electronic health record systems are being developed and trialed. Overall, financial models support cost savings.

Financial models by the University of Texas MD Anderson Cancer Centre (USA) predicted a 10 year saving of US$129.5 million on an investment of US$54.5 million. Kaiser-Permanente estimated the financial gain of US $3.4 million to operations after implementing a clinical information system. Further, analyses predict that the real returns will come from improved clinical management — rather than the present savings on administrative efficiencies.

Storage capacity in digital format is far smaller than the paper format and will save space.

Access to knowledgebases and performance data should limit consumer exposure to unnecessary surgery and consequent litigation and compensation.

Sometimes very large scale and expensive implementations are required before cost savings are possible.

Implications for a national approach in Australia

The national approach should aim to avoid the 'paper paradox' — more technology leads to more paper — ensuring that people have the skills and equipment to write and use information in electronic form.

Improved efficiency and satisfaction is relatively easy to measure with electronic health record systems. It is an essential feature of successful electronic health record systems and must not be jeopardised by other requirements. Implications of all other requirements must be investigated in relation to efficiency and user satisfaction and be found to be acceptable.

Efficiency of electronic health record systems will, to a large extent, depend on their connectivity. If a national approach is to be taken then a threshold level of implementation must be met in order to achieve efficiency benefits.

Monitoring of specialist waiting times can be part of the evaluation of electronic health record systems.

When links go beyond isolated systems, communication links and message protocols need to be in place and standardised. The drivers to implement standard HL7 messages are limited in the first instance as shown by the disappointing uptake in Australia so far. There may be a need to drive this implementation to encourage the early adopters (who gain little from their pioneering efforts).

Cost savings can become the motivation for using electronic health records, which may lead to markedly increased profits without consideration for quality of care.

Lowering prescribing costs seems less likely when prescribing systems are supported by the pharmaceutical industry, which is currently the norm in primary care in Australia.

5.9 Improved management and utilisation of health information

Electronic health records allow powerful abstraction and reporting capabilities for population health, audit, research, and health service planning.

Data from electronic health record systems can be used to support development of evidence-based protocols, generate risk prediction from routine data, or analyse outcomes and costs of programs or interventions. Such information can then be utilised in the electronic health record system from which it was derived, thereby completing a positive feedback loop.

Consumers can benefit directly and indirectly from research utilising the information in their records. They can also gain access to the results of quality-of-care audits, ensuring that their decision making is as well informed as possible. This will allow consumers to play an enhanced role in policy development.

Linking clinical databases can provide information of great value to policy and planning.

Population-based approaches to health care undertaken in Dutch and British general practice are probably a strong driver for the acceptance of the electronic health record — as population-based care is very difficult without some sort of computer assistance.

Managers and policy makers have a genuine need to ensure that investing in electronic health records is rewarded in terms of outcomes. Electronic health records allow data collection during clinical use of the electronic health record — which is a great advantage over paper systems (which require duplicate input).

Consumers will benefit from accurate performance information, for example through institution and provider bench marking. Information on outcomes can also be used to fine tune clinical guidelines, adapting them to individual circumstances.

Policy makers and managers wish to accurately:

- anticipate future trends;
- determine cost-effectiveness;
- evaluate where most value for the health dollar lies; and
- assess the evidence base of interventions.

Governments also hope to ensure that large outlays of public money are producing the outcomes they hoped for, and therefore seek more complete and accurate information on the effectiveness and efficiency of health program expenditures. Further, evidence derived from electronic health records can directly support development of population-based health care policies which are more firmly grounded in evidence.

Implications for a national approach in Australia

Managers and organisations are the main beneficiaries when data required for other purposes are collected at the time of provision of clinical care. It is clear from the research evidence that efforts to overdo this or make it the focus of the system may well jeopardise implementation.

Van Bemmel in his review of electronic health record systems in Europe points out that information in European health information systems is "not crying out to be used for electronic data interchange, research or shared care". This is due largely to the problems that arise when the data are to be used for purposes other than direct consumer care — for example, the lack of common terminology or different context. He stresses the lessons learned from experience — particularly the need to develop structured consumer records based on a clear conceptual model. If the data in the electronic health records are not based on a conceptual model, and are not well structured, it will not be possible to use that data for different goals, nor will it be possible for such data to be exchanged between health care providers to support shared care.

He goes on to stress that care providers need to be cognisant of the requirements for data to be shared over the entire health care domain and to support clinical research, policy making, assessment of quality of care, management and planning.

The National Committee for Quality Assurance (UK) has developed a framework for monitoring quality of care in an electronic health record environment. Such an approach may be required in Australia.

Accreditation of clinical systems, as practised in UK general practice, may be required to ensure that electronic health record systems can support the functionality to enable improved quality of care.

5.10 Other potential benefits

Health is one of the world's largest industries, and one for which borders are largely irrelevant. That means that successful initiatives — such as implementing a national system of electronic health records — are exportable. Thus, if Australia can successfully implement this report's proposal for a national health information network it may well be able to generate export earnings by selling it overseas, in particular to countries in our region who look to Australia for innovation in health care.

6 MANAGING THE ASSOCIATED RISKS

… what if these systems [electronic health record systems] do not work?

Frisse 'Computers and productivity: is it time for a reality check?'

Challenges to the implementation of a system of electronic health records include organisational and cultural barriers, legal issues, market issues, leadership and vision of decision makers and user acceptance issues. For example, such a system can be expected to be opposed by organisations that regard their internal information systems as competitive advantages and accumulated consumer records as corporate assets. Also, medical practice is extraordinarily complex and changes rapidly. Systematising even the process of performing medical procedures, much less rationalising the language and scientific knowledge underlying those procedures, is therefore a formidable challenge.

As explained in Chapter 5 and further discussed in Chapter 13, cognisant of the need to examine whether the benefits of electronic health records are likely to exceed the costs, the Taskforce commissioned a study of the benefits and risks of introducing a national approach to electronic health records in Australia from researchers at Flinders University, led by Dr Sam Heard. Their report forms an integral part of the Taskforce's investigations and is included as Appendix B.

Electronic health record systems have proved to be very difficult to design and implement. Thus, there are a range of issues and risks that need to be addressed in detail before the introduction of a national approach to electronic health records. Shortliffe has identified four obvious ones:

- the need for standardised clinical terminology;
- concerns about data privacy, confidentiality, and security;
- challenges of data entry by health professionals; and
- risks of integration of electronic health records with other information resources in the health care setting.

While these issues may be the most pressing for the moment, there are also other issues that will demand attention. This part of the report examines moral, legal and ethical risks, problems of equity and access, implementation, technical and financial risks associated with the design and use of an electronic health record for Australians.

6.1 Moral, legal and ethical risks

There are major moral, legal and ethical issues in the development and implementation of electronic health records which are of major concern to consumers and their advocates.

Health records contain highly sensitive information about a person's health problems, family history, personal behaviour and habits. For example, they may contain information about mental health, sexuality, drug use, genetic test results and HIV/AIDS and hepatitis status. Although the public has a high level of trust in current practices designed to protect the privacy of their medical records, new technologies and associated media attention have heightened consumer concern about privacy in the information age.

Consumers are concerned that information and communication technologies will make their personal health information much more accessible not only to health practitioners and hospitals but also to a wide range of interested third parties — such as accreditation and standard setting agencies, government agencies, insurers, employers, laboratories, pharmaceutical companies, pharmaceutical benefit managers, pharmacies and researchers. Furthermore, they fear that their personal health information may be used to discriminate against them in employment, insurance or housing decisions and may lead to individuals becoming the focus of unwanted attention.

Consumers' concerns about privacy and confidentiality can only be addressed by the explicit determining of the extent of the individual's control over their own electronic health record in regard to such things as:

- controlling access to the record;
- controlling access to specific information held in the record;
- controlling processing of the record;
- controlling movement of the record;
- controlling amendment of the record; and
- the degree of automatic notification to the consumer of who has accessed, processed or moved the record.

There is not a uniform approach to privacy protection within Australia — different standards and individual rights apply in different situations. The Australian Capital Territory is the only state or territory which has legislation covering the handling of personal information in both the public and private sectors. New South Wales, the Northern Territory, South Australia and Victoria have developed, or are in the process of developing codes addressing the privacy of health information in the public sector. In addition, various professional groups are developing voluntary codes of practice on consumers' access to medical records (eg the Royal Australian College of General Practitioners' Code of Practice for the Management of Health Information in General Practice).

In 1998, the Commonwealth Government announced it would introduce legislation to support self-regulated privacy protection in the private sector underpinned by the *National Principles for the Fair Handling of Personal Information*. However, it has been argued by some commentators that specific legislation relating to health information needs to be developed and a body established to oversee protection of the privacy of health information.

Consumer advocates are concerned about the growing number of people seeking access to medical records for secondary purposes and they are also increasing concerned about record linkage. The Consumers' Health Forum of Australia has recommended that the following three principles form the basis of privacy legislation:

- use of informed consent must underlie the use and disclosure of consumers' personal health information;
- the Commonwealth Government must proceed with national privacy legislation that is capable of both protecting consumers' privacy and ensuring their right of access to their own personal health information; and
- the Commonwealth and State and Territory Governments must co-operate in the development and implementation of nationally consistent standards to govern the use, linkage and disclosure of consumers' personal health information.

The need for legislation is reinforced by international trends which indicate that there are increasing demands being made by people not directly involved in health care for access to identified health information. Moreover, it is important that Australian privacy standards conform to international standards. Lesser standards may be a barrier to the global exchange of health information. For example, it seems questionable that Australia's 'light touch' approach to privacy in the private sector would be seen by the European Union (EU) as consistent with its privacy directive on personal information, which is enforceable at law.

At present, Australian consumers do not have a uniform right of access to their medical records. They have right of access to records created and held in the public sector but they do not have the same right of access in the private sector (which includes the records of general practitioners and many hospitals). Australia lags behind other countries in this regard and consumers in the UK (*Access to Health Records Act 1990*), New Zealand (*Health Information Privacy Code 1993*) and Canada (common law) have a uniform legal right of access to their medical records.

Consumer support for right of access is estimated to be between 75 and 90 per cent, and consumer advocates draw attention to the importance of access if consumers are to make informed decisions regarding access to their medical records by others:

> Effective notification and truly informed consent require that individuals know and understand the contents of the record.

> Consumers cannot be expected to be confident about the possible consequences of allowing their personal information to be used for research purposes when they do not have access to the information themselves.

Only the ACT has legislation which gives consumers a right of access to private sector clinical records. The ACT *Health Records (Privacy and Access) Act 1997* covers all health records, in any media, held by any health service provider. The Act has led to some changes in procedures at ACT hospitals. It has also led to a small increase in consumer requests for access to their records and, consequently, to a slightly increased workload associated with photocopying records. However:

> Overall, the staff of the hospitals welcome the new legislation, which will enable the public to feel confident about the procedures in place to protect their information, and to enable access to their documentation.

A recent report by the NSW Health Council highlights consumer problems with access in NSW:

> Consumers have little or no access to records, either in hospital or through their general practitioners. Also, there is currently no mandatory requirement for a general practitioner to release a consumer's health record when the consumer exercises their right to change providers, or when the general practitioner moves on. This is particularly important in rural communities, when the turnover of General practitioners tends to be higher than in metropolitan communities.

Although it has been argued that access will lead to increased litigation, this is not supported by the *Interim Report of the Review of Professional Indemnity Arrangements for Health Care Professionals* (1994). The report states that there has been no increase in litigation in NSW and Victoria as a result of consumers gaining right of access to their private hospital records under Freedom of Information legislation. Moreover, the report suggests that access to medical records:

> … establishes more open and equal provider/consumer relationships, enhances informed consent, ensures continuity of care across various providers and gives consumers greater control over their own health.

Ownership of paper-based medical records resides with medical practitioners who have had the right to decide whether or not to show a record to a person when requested to. The *Breen v Williams* High Court case confirmed this position and ruled that, under common law, consumers have no right of access to their medical records. However, the ownership of electronic health records is a complex issue, since electronic data can be copied very simply and the copy is indistinguishable from the original. Consumers, health care providers, managers and third parties are all likely to experience difficulty when there is a dispute — particularly as ownership may vary from record to record. Such ambiguity is likely to lead to legal action which will not necessarily resolve the situation. While each party might see advantage in resolving this difficulty, it is unlikely that the outcome will be satisfactory to the others.

While copyright would normally reside with the originator of the electronic health record entry, a health care provider with a duty of care towards a particular consumer will need to be able to access a copy of the person's electronic health record (with the person's consent) without the explicit consent of the clinician who holds copyright.

There is a need to define the boundary of the electronic health record. This can be quite straightforward in an environment such as that proposed by Good Electronic Health Record (GEHR), but highly ambiguous in a hospital environment where there are many disparate systems and paper records to be considered.

The *Electronic Transactions Bill 1999 (Cth)*, has paved the way for health care to work in a paperless environment. The legal acceptability of health records in Australia is ambiguous but has been described from a health provider's perspective. Although electronic health record systems are established in some medial centres in Japan, health care organisations are required by law to keep paper records. Similarly, in the UK, paper records are required by law, although approximately 10 per cent of general practices have been paperless for many years. Computerised records in the UK are certainly admissible in court although the record is required to be maintained on proper hardware, the records must be contemporaneous and there should be a full audit trail of additions and deletions. However, implementation of true audit trails in electronic health record systems around the world are unusual and no certification process is usually involved.

While the electronic health record has the potential to increase the amount and quality of information available to researchers and other interested parties, and subsequently to improve health care for consumers, it is not possible to achieve both the highest level of confidentiality and the broadest access to the record (whether on computer or paper). As confidentiality is very important, security of the electronic health record must be given high priority, as *Health Online* acknowledges: [40]

> With increasing recognition of the individual and public benefit that can be gained through greater access to de-identified and aggregated clinical data for policy, planning and research purposes, has come acceptance that strict protocols and protective measures need to be in place to ensure that such activities can be agreed and undertaken in an environment of public trust. ....Electronic data transfer across the health sector also raises questions, not only about authorised access, but also about the certainty that such data is sent only to whom it is intended. Certification and registration for the purposes of electronic identification and authentication are crucial to this context.

[40] National Health Information Management Advisory Council (NHIMAC 1999), *Health Online: A Health Information Action Plan for Australia*, Commonwealth of Australia, Canberra. *Health Online* is available at www.health.gov.au/healthonline.

Automatic processing of personal health information poses risks to the data subject. The EU's Data Protection Directive, which took effect in October 1998, protects the transfer of information to any country that lacks adequate levels of protection, including the USA. The Directive prohibits data processing unless:

- the data subject has given explicit consent;
- the data subject is physically or legally unable to give consent but processing is required to protect his or her vital interests; and
- the data subject has made the data public.

Health data is a special case and the benefit of processing for the good of the individual or the public good is acknowledged. For this reason there is a specific clause in the Directive to allow "processing of the data when required for the purpose of preventative medicine, medical diagnosis, the provision of care or treatment or the management of health care services provided that those data are processed by a health professional subject, under national law or rules established by national competent bodies, to the obligation of secrecy".

Implications for a national approach in Australia

Legislation is required to ensure that personal health information does not get into anybody's hands without individual informed consent. *Health Online* implies that additional federal legislation will be necessary to further protect the privacy of personal health information:

> The Commonwealth is in the process of introducing legislation concerning the protection of personal information in the private sector...However additional legislative approaches will need to be considered as emerging technologies are used to communicate highly sensitive information across health and community settings to support integration and coordination of care and to make better policy and planning decisions.

Consumer access to the electronic health record is a definite requirement for electronic health record systems. Consumers need to understand the contents of their electronic health record — they need to ensure that it makes sense to them. For this reason they will need to be involved in designing a common interface or one that is tailored to their needs. The extent of consumer control over the processing of a record is also an issue that needs to be resolved.

A national approach to the ownership of electronic health records, accepting that the ownership is ambiguous, is probably worthwhile to prevent the waste of resources. Hand-held or consumer-controlled electronic health records, consisting of copies of encounters recorded by different health care providers, may also resolve this situation without the need for legislation.

Whatever the final position on ownership, it is clear that consumers must have control over access to their health information.

Where a 'federation' model of health records (a virtual health record) has been implemented, a clear process is required at each location to define what constitutes the electronic health record in that environment. This is not trivial.

A national approach to legal recognition is essential with clear guidelines and processes for implementing legally acceptable audit trails.

Balancing access and security is difficult. As confidentiality is of the greatest importance and all means of access are a threat to that confidentiality, privacy protection must be a fundamental component of all technologies that offer access to the electronic health record. Only methods that offer far greater access with a small trade off on confidentiality are likely to be acceptable to consumers.

Control over access to parts of the record, even specific information, is considered important by many. This has been investigated by Jones who has demonstrated that neither clinicians nor consumers behave consistently. Others have raised issues of safety (eg referral or emergency treatment) and even if it were possible (eg hiding HIV disease data) to work with a record which is only partly available. Implementation trials will probably be required to assess the full implications.

Consumers who wish to have control over automatic processing of their personal health information may range from not agreeing to automatic contacts for preventative procedures to allowing all research agencies access for research purposes. Some consumers may wish to control very specifically each individual process.

Particular groups of consumers may have their own requirements concerning the collection and processing of their personal health information. The NSW Aboriginal Health Information Guidelines, for example, state that consent should be obtained from Aboriginal communities or Aboriginal community controlled health services for the collection and use of health related community information if Aboriginality is a key determinant, if data collection is explicitly directed at Aboriginal peoples; if Aboriginal peoples, as a group are to be examined in the results; if the information has an impact on one or more Aboriginal communities; and lastly, if Aboriginal health funds are a source of funding.

Minimal standards of completeness and accuracy of electronic health record data must be established for safe automatic processing, including aggregation of data. For example, decision support when prescribing cannot be regarded as completely safe without all current medications and previous adverse reactions to therapy being recorded in the electronic health record.

6.2 Risks to access and equity

The Australian population is diverse and some people may experience risks to access and equity with the introduction and implementation of the electronic health record. Rural and remote communities, Indigenous Australians, the aged, people

from non-English speaking backgrounds, mentally ill and illiterate people are already in a position of disadvantage when it comes to health care and may face further difficulties when electronic health records are implemented.

Communications infrastructure in rural and remote areas may mean that access to electronic health records is more difficult for people living in these areas.

It is very likely that other groups who are at high risk for health problems, such as people who are unemployed, chronically ill or disabled, with a history of substance abuse, or recent immigrants may face difficulties in accessing their electronic health records.

The varied social and cultural backgrounds of Australian health consumers mean that they also seek information and help from a wide range of complementary health practitioners. In one year in Australia, almost half of a representative sample of consumers had used at least one non medical complementary remedy and at least one in five had attended a non medically trained complementary therapist. Moreover, a study by Pirotta *et al*. found that "Doctors underestimate their consumers' use of these therapies, which may contribute to compliance and medication interaction problems."

A uniform approach to the recording of personal health information in relation to complementary health care is necessary and at present the role of the electronic health record is uncertain in this context.

Implications for a national approach in Australia

The potential for electronic health records to improve health outcomes is greatest in the case of those who are most disadvantaged in Australian society (ie those who tend to suffer disproportionately from ill health). Accordingly, a national approach to electronic health records should pay particular attention to ensure the best possible implementation in populations known to be at relatively increased risk (eg Aboriginal and Torres Strait Islander peoples and those living in remote parts of Australia).

A national approach to electronic health records must be culturally inclusive and be of benefit to all Australians. People without personal access to the Internet (and thus access to their health records online) must have private and affordable access through public means.

Consumers who do not choose to take advantage of online access to their health information should not be disadvantaged. Possible approaches to address this potential difficulty include assistance to seek information in settings such as primary health care, alternative means of access such as phone-in advice to trusted parties (who do have access to their electronic health records), or providing written information based on the contents of their electronic health records.

It is important that health providers do not to rely solely on the computer as their communication and information tool; rather they need to be provided with multiple modes of accessing multiple sources of information.

6.3 Implementation risks

One major difficulty in the implementation of electronic health records is that the control and design of hospital information systems has been in the hands of the managers and financiers of health departments.

A great deal has been learned about implementation of clinical computing systems over the past three decades. Frohwerk has described in some detail the issues for operations staff when approaching the implementation of an electronic health record system. Although systems may not deliver all they promised because of technical difficulties, most implementation issues are human and can be avoided. Atkinson challenges this view, somewhat, with his metaphor of growing, not building, an electronic health record system. He suggests an evolutionary process is required leading to a symbiotic relationship between the information system and the rest of an organisation.

Further insight may be gained from a major Canadian project involving the implementation of an electronic health record system in 4 hospitals between the late 1980s and 1996. Although implemented in 2 stages over almost 10 years and costing US$50 million, it was withdrawn due to boycotts by medical and nursing staff. The project was initially sold as facilitating medical work, improving coordination between nursing and medical activities, improving quality of care, and cutting costs. It resulted in information overload and standardisation, task load increase, work organisation rigidification, and expert autonomy negation. A summary of intended and observed effects of the proposed process innovations are described in Table 6.1.

Hannan has described in some detail the risks of implementing a clinical system designed in the USA in an Australian setting — only some of the modules could be implemented and new modules had to be developed locally. The lessons from this major implementation were:

- implementation needs to be incremental;
- electronic health record systems significantly alter work practices;
- it is preferable to start with a sound system that has been evaluated in its development;
- it took almost 10 years to implement an effective system;
- involvement of users is essential;
- the team must have a leader who is clinically orientated, understands the domain, is available to users and be able to take tough decisions; and
- projects must have an ongoing evaluation component to justify costs.

Table 6.1: Summary of intended and observed effects of process innovations

PROCESS INNOVATION MECHANISMS	INTENDED EFFECTS	OBSERVED EFFECTS
Process automation (direct data entry by nurses and electronic transformation and communication)	• Decreased clerical work load • Elimination of time lag • decrease in costs linked to clerical work	• Increase in nursing clerical tasks • Higher formalisation of data collection • Less flexibility in work organisation
Analytical improvement	• Improved analytic abilities	• High formalisation and standardisation of nursing cognitive process • Nurse deskilling • Information overload • Less flexibility in work organisation
Process sequence	• Acceleration of completion of the collection of nursing data	• Elimination of existing parallel processes - care delivery and consumer assessment • Less flexibility in work organisation
Tracking capability	• Tracking in real time of information processes	• Automation of people control
De-localisation (Elimination of geographical boundaries)	• Consultation of consumer files at a distance	• Inoperative for nursing work • Less flexibility in work organisation because of localisation constraints - bedside terminals
Integrative capacity	• Horizontal care supervision and coordination across various functions and departments	• Inoperative
Information capability	• Staff planning and allocation	• Increased control of staff • Less flexibility in work organisation • Increase in nursing task
Intellectual capability	• Build knowledgebase	• Inoperative

Source: Sicotte.

The 'people problems' are recognised as more important than technical problems. Some investigators have concentrated on these aspects of implementation. For example, Adyin evaluated an implementation in ambulatory care and concluded:

- most physicians anticipate enough benefits to be willing to use the system;
- computers must be accessible, easy to log into, and provide for physician movement and interrupted sessions;
- many physicians are concerned about losing eye contact with consumers;
- it is unrealistic to expect even people with good keyboard skills to enter their own lengthy notes;
- staged implementation, with order entry introduced first, may help physicians adapt gradually; and
- training should include protected time for instructional sessions for physicians, simulated consumer encounters to help physicians adapt their practice patterns, and tutors available to answer questions in the clinical setting.

Although it is common in hospital settings in the US to use dictation and transcription, it is worth noting that in primary care settings it has been found that health providers prefer to enter data directly.

Legacy systems will always need to be catered for in any large-scale approach to electronic health records.

The use of different data-entry mechanisms by health providers (when offered the choice) is quite varied and difficult to predict. Generally, more sophisticated approaches have not yet met users' expectations. Voice recognition promises much in the future for free entries, but is of limited value currently due to its requirement to adapt to each user and the technical difficulty of natural-language processing.

The inherent complexity of health-related information has made the task of describing an electronic health record information model challenging, and hence retarded the implementation of standardised systems or components. This is borne out by experience on the GEHR project, the CEN electronic health record pre-standard work, and cost-benefit evidence published relating to the use of HL7 v2.x in Australia and in the USA. GALEN, a major European project to enable capture and classification of natural language in health care, has not delivered the hoped-for results. Electronic health record information is complex due to having a number of levels of abstraction, as follows:

- Data: all kinds of text, terms, multimedia, quantities, units, and more recently XML and interactive information. Systems of formalised terminology have in themselves been sources of major difficulty, although the successful use today of such systems points toward their ubiquitous use in some form in the future;
- Basic clinical structures: groupings of data into semantic structures corresponding to basic clinical concepts such as 'blood pressure', 'prescription' and so on;
- Derived and synthesised clinical views: higher-level grouping and linking to support 'headings' (as in a paper record) as well as concepts such as 'problem', 'episode', 'care plan', 'care pathway', 'current medication', 'adverse reactions' and so on; and
- Record management structures: arrangement of clinical structures into containers such as 'transaction' or 'record section', which would typically be the unit of storage, transmission, security etc.

The size of the clinical information space (roughly, the second level above) is enormous, as can be gauged by the size of some of the terms sets (eg SNOMED has more than 300,000 terms).

Not only is the complexity of clinical information greater than in many other domains, it changes all the time, as evidenced by the evolution both of care management precepts of 'problem', 'issue', and more recently 'care pathway', and development in clinical concepts (eg the LOINC code system). The problem is the

same as in other sectors: software built on today's ideas may be out of date tomorrow.

The needs of health care providers and consumers may vary greatly. Specialists often need to keep lengthy records. Some have highly specialised notations, drawings and other recordings. Highly specific systems have been built to cater for locations such as intensive care or even to support care of consumers with particular diseases.

To enable the simplest sharing of data (not just text) requires standards. These are required in a minimal way for viewing a record from another site but are essential for any processing of the record (such as for decision support). Different standards are required at the different levels described above:

- Data: standardised vocabularies such as SNOMED-CT (merger of SNOMED and Read), ICD-10-AM and ICPC, image standards such as DICOM 3, signal standards (ECG), multimedia standards etc.;
- Basic clinical structure: standardised terms to label content such as LOINC, how to communicate this information in messages such as HL7 or through communication technologies such as CORBAMed, groupings of content into meaningful clinical concepts such as blood pressure, a prescription or an audiograph as partly covered by LOINC and more comprehensively in the GEHR archetype system;
- Derived and synthesised clinical views: more complex structures that have been developed over time by clinicians, now labelled by CEN and dealt with in GEHR and HL7-PRA but probably remain in the clinicians' domain; and
- Record management structure: arrangement of clinical structures into sensible 'containers' (as proposed by GEHR and more recently by CEN and the HL7-PRA) to enable record management as required by clinicians and consumers.

An agreed system of consumer identification has been one of the principal technical impediments to sharing health records outside particular health care institutions. In most countries there are proposals for national schemes, but almost none of these are implemented.

Security, according to the Oxford dictionary, is "safety against attack, impregnable, reliable, certain not to fail, in safe keeping, and firmly fastened". All of these concepts are valid when considering the electronic health record. There is an evolving framework, both theoretical and legal, to ensure and maximise the security of information systems. Security of systems is generally classified as follows:

- confidentiality - ensuring people can only access authorised information;
- integrity - ensuring systems do what is expected of them; and
- availability - ensuring that systems are available when required.

Security is not just a technical issue, but includes physical security, procedural security and staffing security. Security is a major concern for all involved in the implementation of information and communication technologies particularly those in banking and health care.

Theft of hardware is a threat, particularly in primary care. So is unauthorised access when systems need to be repaired or upgraded. The duties of the controllers to maintain physical security of the system must be agreed. There is wide acceptance of such requirements and generally system providers are interested in meeting such standards. Consumer acceptance is unlikely without confidence that this is the case and governments are under pressure to take a national approach to protection of health information and to consult with consumers in devising it.

Transferring electronic health records requires a different approach from the paper record. Machinery to intercept transmission data can be bought for as little as $200. Issues are somewhat similar to faxing records. However, transfer of an electronic health record is different from a paper record. An identical copy of the record, indistinguishable from the original, can be created and sent. Also, the record may be sent to many sites simultaneously.

Legal risks arise if a controller can move the electronic health record to another health care facility without strict rules on validating error-free receipt, acknowledgment of the status of the record and agreement to hold the record in a suitable state for required lengths of time — particularly if regulations differ across state boundaries. The transfer of the electronic health record may be to a health care facility, which works to standards which are similar to that of the originator of the record, or to a health care facility which has differing standards. The latter poses a potential threat to the consumer and clinician. Such transfers may be described as non-conformant and are more likely with international movements. The EU has made specific provision in its Directive to protect consumers from such movements of electronic health records. Consumers may only be willing to seek medical care on the basis that there will be no flow of information between providers. For example, for whatever reason, they may not wish their general practitioner to know about all of their medical problems. The same applies to some information which the consumer may wish to communicate to the general practitioner, but not a referral specialist. To deny this right would be against the best interest of the consumer and the public.

De Meyer and colleagues have analysed requirements for electronic health record transfers which they consider must include:

- the originator of record (authenticity);
- evidence of the integrity of the record (complete, unchanged);
- the date and time submitted;
- the date and time delivered;
- the date and time receipted — within a non-repudiation framework; and

- validation of data subject.

Further, data must be secure during transmission and, as stated above, there must be a framework of non-repudiation — that is someone who receives the record cannot deny this in the future. The most promising approach to these problems are the Public Key Infrastructures being developed as a generic solution to this problem across all sectors of the IT industry.

The use of the Internet to transmit electronic health records raises extra security concerns for both providers and consumers. A recent report, *The Future of the Internet in Health Care* lists several of the key security issues:

- protecting servers and databases from unauthorised intrusion/modification;
- authenticating the identity of senders and recipients;
- protecting the integrity of the message itself;
- ensuring that senders cannot falsely deny they sent a given message;
- establishing audit trails; and
- ensuring the confidentiality of messages.

There is growing evidence of increasing acceptance by clinicians of information and communication technologies especially if consumer care is seen to benefit. Bolton and colleagues showed that the belief amongst Australian general practitioners that "prescription writing is easier using a computer" jumped from 35 per cent in 1994 to 52 per cent in 1996. Further, the percentage disagreeing with the statement fell from 30 per cent to 16 per cent in the same period. The same group, however, were more likely to agree with the statement "If I were to computerise my practice, in order to maintain my income, I will probably need to work more than I do now"; 49 per cent in 1994 and 62 per cent in 1996. There is no doubt that a major barrier to uptake of electronic health record technologies is the preparedness of health care providers to take on the role of computer operator. Reed Gardner, who has overseen the Salt Lake City implementation at the Latter Day Saints Hospital states that success is 80 per cent dependent on people and only 20 per cent on technology. Research needs to describe best practice methods and cite clear evidence. An increase in the time spent with consumers seems likely — although this may be due to providing more complete care. A systematic review of consultations in general practice reveal that the consultation is approximately 48-54 seconds longer when a computer is used — this seemed to get longer with time. Most of this added time was due to computer tasks. Provider initiated and 'medical' content of the consultations increased at the expense of a reduction in consumer initiated and 'social' content. Clinicians' views have been surveyed and they say that they are not motivated to collect data that they consider to be non-essential. However, the application user interface design is important and can assist in achieving acceptable compromises.

Clinicians are increasingly aware that getting involved in the design and implementation of electronic health record systems is essential. Lack of input by clinicians into the design of health information systems has been cited as a major

factor in the failure of information and communication technologies in health services and has prompted many clinicians to become involved in such endeavours.

It must be stressed that education and training is essential — for all users of electronic health record systems, including consumers. For example, data quality has been shown to be dependent on training.

Implications for a national approach in Australia

Best practice for implementing electronic health record systems will need to be developed and be supported and documented. Clinicians will need to be intimately involved in that process, with planners and managers. The consumer must be there too!

Innovators will spend more money developing solutions and will carry greater risk of their approach 'becoming an island' through technological developments in new directions. A national approach needs to ensure fair exposure to risk in the development and implementation of electronic health record systems.

Legacy systems will continue to exist. Institutions will have systems that are not provided as total solutions that need to interact with other parts of these systems. Total solutions will need to communicate with systems at other sites. Proposals for future developments need to accept these two realities.

There is a limited understanding of the complexity of the information in clinical systems. Recent key work in HL7, CORBAMed, the Synex Project’s federated record system and GEHR confirms this. A national approach needs to embrace these aspects of electronic health record development.

Specialised recording will need to be catered for in any national approach. Until the formal meaning of notations are available for automatic processing, it may not be safe to include these in the electronic health record (as key clinical information may not be accessible).

The choice of standards is huge with more than 150 vocabularies in use today around the world, with merging of key players such as SNOMED and the UK Clinical Terms (Read). Alignment of HL7, CORBAMed and GEHR is beginning with a shared understanding of the move to more complex information models in clinical computing. A national approach will need to be cognisant of these developments.

A safe, unequivocal way of identifying individuals will simplify systems issues to a great extent, but will lead to a national overhead in maintaining this system and preventing duplications. It will also necessitate specific legislative privacy protections. Travellers, and others who do not give identification details consistently, will continue to confound efforts to build a national database. Linking the number to billing seems a useful way to minimise the administrative overhead but may not be acceptable to the Australian population.

A national and robust Public Key Infrastructure as outlined in *Health Online* is required to enable secure transfer of electronic health records.

Security measures designed to protect financial transactions over the Internet are likely to be adequate to protect personal health information during transfer of electronic health records. Given this situation, the main issue from a health perspective becomes the appropriateness of the electronic health record transfer.

The assurance of integrity of the electronic health record on transfer is extremely important, since subtle errors could creep in depending on the kinds of processing carried out at the receiver's end at each transfer.

Consumers and providers must be involved in design and development of electronic health record systems. A number of consumers and providers require a working knowledge of evaluation issues in order that they can assess the strengths and weakness of evaluation studies.

Consumers and providers require meaningful opportunities to 'test drive' and appraise fully functional systems - as well as effective training in maximising the benefit from their computer system and information management.

The ISO group, led by Australia and with input from Europe, Asia and the Americas, are determining a common set of requirements which can be used as the repository of agreed features of electronic health records. This will allow development of a requirements methodology for use in developing user interfaces, applications and systems, of which hospitals and other software development organisations can take advantage.

Consideration of the GEHR archetype approach is warranted — an electronic health record architecture which has the feature of allowing clinical models to be added and amended *post hoc*.

Undergraduate and ongoing post-graduate training and skill development in health informatics is important for the future success of design, implementation and evaluation of electronic health record systems.

Accreditation procedures may be required for clinical support in electronic health record systems.

6.4 Technical risks

The technical risks of installing and upgrading an electronic health record system can be overwhelming and account for a significant proportion of implementation risks.

Multi-site, 'federated', Web-based electronic health records have to overcome many of these risks but usually do so when there is a single controlling agency.

Computing power generally doubles in performance and halves in cost about every 18 months, but even with these major advances the true electronic health record has been difficult to achieve.

Technical risks with aiding health care providers to enter data remain, despite more user-friendly interfaces.

Entry of data into electronic consumer records is a critical function that is fraught with challenges, mainly because it involves translation not only of facts, but also of knowledge and intuition from the mind of a trained provider into a machine. Reading medical records is a highly complex task and many features of the layout can aid or hinder the reader. The ability to restructure such elements as the summary chart, depending on the requirements of the user, will aid searching and decision making.

The difficulty of the balance between free text (to aid comprehensive description of the consumer) and structured vocabulary (to aid automatic processing for, say, decision support) is still debated. Providers will need to be consulted extensively on this issue.

Clinical terminologies and vocabularies are evolving rapidly from simple lists of codes and texts to neural networks of concepts and thesauruses. Major developments are the merging of SNOMED-RT and the NHS Clinical Terms (Read codes version 3.1) to form SNOMED-CT, and the complex structures enabling natural language processing in GALEN and the UMLS. Decision support is best accepted by health care providers when integrated with prescribing and other order entry systems. However, although there are a huge array of guidelines and care pathways that have been published, few have been implemented in computer systems.

The benefits of digital information are considerable — enabling transfer, copying and access at a distance. Encoding information such as sounds and images requires a very large amount of digital data compared to text. The increasing digital storage requirements for encoded images and other complex data (see below) stretch the capability of modern hardware with a typical US medical centre generating 3.5 terabytes of data a year.

Table 6.2: Digital storage requirements for encoded images and other complex data

Electronic health record component	*Size*
One page of single spaced text	4KB
640 x 480 pixel 24 bit colour image (eg a high-resolution microscopic image	1MB
Digital AP chest X-ray (2048 x 2048 pixel)	8MB
'Typical' head MRI	20MB
'Typical' chest CT Scan	50MB

Source: Lowe (for multimedia components).

Implications for a national approach in Australia

The technical risks facing electronic health record development are considerable and much work is progressing on many fronts. These risks will not be resolved in the short term and others are likely to arise. A national approach must determine which are the highest priority and may be overcome or substantially reduced with a national effort, specifically:

- issues with Web-based 'federated' systems that straddle multiple sites;
- specialised query languages and databases for health records;
- experiments with electronic health record transfer using GEHR and HL7 and subsequent integrity analysis; and
- trials of data entry solutions in clinical settings.

Cooperation with international efforts to achieve natural language processing in health care needs to be fostered.

6.5 Financial risks

Australia has a complex funding model for financing health care and multiple agencies determining policy. Any approach undertaken will need to be acceptable to the private sector as well as the States and Territories, if it is to be embraced. Costs will almost certainly outweigh benefits in the first year, and may be hard to justify initially.

True costs of medium sized hospital Computer–based Patient Record (CPR) system was estimated in 1991 at between US$2 million and US$6 million in the Institute of Medicine report. Others estimate it to be as high as US$40 million depending on the size, systems already in place and other considerations. No one has made a similar estimate since. Efforts to find large scale solutions in Australia have been expensive — in the range of A$20-60 million. Accurate costings remain problematic not just in health care but in many industries. Service industries stand to gain the most in productivity from use of information and communication technologies but implementations in these industries are sometimes the least cost effective. Implementation is often ceased for financial reasons, for instance data entry costs reaching 17 per cent of billing.

Further, financial gain alone may become the focus of electronic health record implementations, but as two comparative studies in Australia have concluded, cost of systems has been a high priority barrier to the uptake of computerisation by health providers in primary care. This appears to have been overcome by the recent introduction of incentives through the Practice Incentives Program (PIP).

Financial risks may be associated with lack of involvement of clinicians at the time of implementation. An example is the University of Virginia Medical Center system, which was strongly opposed by physicians because it lacked sponsorship by clinicians, altered traditional working arrangements, changed professional relationships and constrained the medical education program. The system was eventually installed 3 years behind schedule at a cost which was three times that estimated. Following such experiences, health providers resent the opportunity cost of electronic health record systems with some justification.

There is obviously a need to limit the cost of electronic health record development. Countries like South Africa have a total health care budget that is roughly equal to the funding for the Harvard Medical School and Massachusetts General Hospital. Open source system development such as the LittleFish project is probably the only option for such situations.

Implications for a national approach in Australia

Any national approach will need to take into account the structure of the Australian health system and its funding. 'Open source' developments — a cooperative software development model — warrant investigation as part of a national approach.

7 NEED FOR A NATIONALLY CO-ORDINATED APPROACH

For a national approach to be effective there will need to be a shared vision to enable the development of a national strategic framework. Ensuring compatibility requires the development and implementation of agreed national standards for the capture, classification, storage, communication and security of information.[41]

7.1 Potential benefits of introducing a national approach

When contemplating a national approach to the electronic health record it is important to consider the 'drivers' within the health care system. Hospitals are being built with large and powerful communications infrastructures and without paper record storage areas. The driving forces for this change are many and varied and involve staff within the state and territory health departments, hospital executives, information technology providers in general, primary and secondary health providers who are leaders within their health care institutions, software providers to the health sector and more recently the federal government. Also, a number of companies with venture capital behind them are seeking to acquire or take a stake in software companies, general practices, pathology providers and other health resources. This "battle for the doctor's desktop" is taking place largely within the sphere of the electronic health record — the information technology provides access to the providers, who are seen as the brokers of this economic sector.

Consumers are also seen by some players as drivers for the move to an electronic health record. Companies are providing electronic health records on the Internet for consumers and hoping to 'conscript' health providers to use their record as the default standard through consumer pressure.

There is a trend to move from the support of health care management to supporting consumer care. Consumer information is more likely to be complete and accurate if it is coherent and developed over a period of time by providers and consumers in cooperation. Complete and accurate information is essential for aiding clinical decision making — the single greatest promised benefit of the electronic health record. It is also important for meaningful assessment of quality of care, consumer outcomes, management planning, policy development, research and education.

---

41 Mount CD, Kelman CW, Smith LR, Douglas RM. (2000) An integrated electronic health record and information system for Australia? MJA;172:25-7.

Deleted: 2000

Health Online states:

> The way ahead must acknowledge the importance of national collaboration. The benefits of adopting a national approach are considerable. The cost of information technology systems is high and a relatively small country like Australia needs to be able to maximise such investment through ensuring open architectures with high connectivity and integration are the basis for such investment in both the public and private sectors.

The potential benefits of adopting a national approach may well be considerable, but barriers remain. Further, it is important to consider the role of government in taking this approach. As *Health Online* points out:

> The Commonwealth's role is to create the enabling environment, whereby the information framework is sufficiently robust and flexible to accommodate the needs for security, protection of data and intellectual property, professional autonomy and organisational dynamics — and to adopt a leadership and co-ordination role where a national approach is necessary.

It is not easy to get it right.

Ensuring consumer benefits

Consumers will need to be involved in the design and implementation of electronic health records to maximise benefit and adaptation to their needs. Studies indicate that they are far more likely to access their records if they are available on line or via touch screen or hand-held devices. The expertise and capacity to meet consumer requirements need to be developed and maintained in a form that is likely to continue to serve the interests of consumers.

Heard *et al.* (Appendix B) see the following aspects of a national approach being required to assure consumer benefits:

- The new paradigm demands an explicit legal framework for the electronic health record including:
  - a requirement for each site to publish clear information policies and procedures to ensure appropriate work practices;
  - a national electronic health record security and privacy framework with uniform legislation; and
  - a national approach to training health providers who access electronic health records in the understanding of the duty of confidentiality and the legal sanctions for not observing it.
- The needs of consumers and health providers will have to be reconciled through involvement of consumers in electronic health record system design so that the aims of both parties can be achieved.
- Data entry tools for consumers and a consumer 'view' of clinical (coded) information need to be developed and the electronic health record architecture needs to evolve to support this.

- A suitable registration and certification scheme needs to be implemented for health professionals who make themselves available online (controls may be required).
- Monitoring of electronic health record services needs to be established in various contexts to ensure equity of access for all consumers.

Ensuring provider benefits

Health providers are increasingly unable to cope with the sheer volume of information it would be desirable to have at their fingertips to do their jobs well. Many recent technological advances in medicine add considerably to the amount and types of information collected. In addition to keeping a historical record of care, clinicians are expected at times to provide consumers with hand-held records, complete complex forms for different bureaucracies and record enough information to defend against unwarranted litigation. Elaborate care plans or medication charts require complete rewriting when the paper form is full, time expired or just worn out. Information is required to be entered many times to fulfil the requirements of recording care (eg the reason for the investigation, a flow chart to monitor chronic disease, referrals to other clinicians). In modern health care settings, the manual (or paper) record has many shortcomings and the electronic health record offers a leap in functionality and return for the effort expended in recording consumer data.

However, health providers generally understand current work practices and, although possibly complex and inefficient, the shortcomings are well known. Changes to work practices can be threatening and demand learning and commitment. In addition, health professionals may find data entry slower, more limited and a perceived interference in the provider-consumer interaction and relationship.

There is now sufficient experience to be reasonably sure that introducing the electronic health record needs to be an 'organic' process, led by knowledgeable clinicians, with health care providers involved in the selection and implementation of the system. Furthermore, systems introduced into hospitals with no real ownership by medical staff often fail.

A further key challenge to a national approach is therefore acceptance by health providers. After a period of major change in health care, introducing an electronic health record nationally will demand yet further adaptation. Health providers will need to understand the basis for change and, if that change is fundamental, the case for that change will have to be clearly made.

Achieving structured information such as the contents of the electronic health record demands standardisation of some sort across the domain where communication is to take place — ideally involving a national (or even international) approach. The standards must include:

- an approach to entry of data from defined vocabulary sets and a national approach to ensuring that these terms can be processed automatically when the electronic health record moves with the consumer to different points of care;
- a way of identifying medications, therapies and interventions that ensures safe processing for decision support;
- an approach to messaging from system to system that can be incorporated into the electronic health record in a consistent manner; and
- an approach to the 'structure' or 'architecture' of the health record which enables transfer of the electronic health record between systems.

Formulating an approach to terminology is not simple — a whole of health care solution is proving elusive. There are more than 150 niche terminologies in medicine — a situation that is almost certain to continue. But, SNOMED and the UK Clinical terms (Read) are to merge to produce SNOMED-CT which, although proprietary, may prove attractive as a whole of health care solution. The UMLS remains the only effort to pull terminologies together and provide some coherence.

Whatever the outcomes, everyone will need to ensure that health providers and consumers benefit, or systems will not be used. Change needs to be evolutionary, transparent and led by clinicians.

Heard *et al.* (Appendix B) see the following aspects of a national approach being required to assure provider benefits:

- Health providers must accept electronic health record systems. To do this they:
  - must be involved in and feel committed to the introduction of an electronic health record system; and
  - should lead the introduction of the system.
- Introducing electronic health record systems must take place in a transparent and evolutionary framework with best practice guidelines and careful change management.
- Electronic health record systems must support clinical decision making and information access at the point of care through:
  - a standard terminology and medication identifiers,
  - standard messaging, and
  - a fast communications network available to the clinician at the point of care.
- Electronic health record systems should support electronic health record transfer, access to audit tools, and future proofing of electronic health records through a standard health record architecture.
- Consumer understanding of the need for student health professionals to undertake supervised access to electronic health records must be assured.

Ensuring benefits for other users

Health administrators, researchers, health statisticians and policy advisers are also interested in the information that could be 'mined', with the consent of consumers, from a system of electronic health records. Most of these uses of health information would not identify the individual to whom the data relates because that aspect is irrelevant to the proposed purpose (eg to calculate immunisation rates). For such applications, only de-identified data are needed (ie information drawn from the electronic health record that has been stripped of any data that would allow it to be associated with a particular individual).

Researchers studying particular diseases are likely to be one of the few groups wanting access to identified data. Procedures will need to be developed to handle such requests and provide appropriate safeguards. Consumers will need to be reassured that the procedures and protocols will be in place to provide an adequate level of assurance.

A national approach makes it more likely that implementing electronic health record systems will lead to cost savings and productivity improvements as the greater the level of electronic exchange, the more commitment to the electronic health record as the primary data store, the more complete the record, the more reliable the processing and the greater the benefits. Institutions will have a firm basis to proceed with accreditation and other requirements through standardised reporting. Demonstrated cost savings will, however, be required before some institutions will be willing to embark on the process.

Managers want to protect their data for future use. A published standard for electronic health record information architecture and approach to terminology and classification will assist in the development of an open software market for electronic health record solutions, ensuring interoperability and preventing the 'vendor lock-in' syndrome. HL7, despite its shortcomings, is an example of a published interoperability standard that has enabled data exchange within and between some health institutions. In Australia, fear of vendor lock-in has probably been one of the impediments to centres computerising earlier. Actual vendor lock-in is probably an impediment to the quality and, particularly, the comprehensiveness of clinical information captured in primary care.

With a national electronic health record system in place, the costs of hospital in-house development of basic electronic health record systems could be expected to drop. This is because the costs of requirements investigation, information architecture design, terminology standardisation, and interoperability approach are substantially replaced by work carried out and published at the national level. Some of the actual costs of implementation of electronic health record applications and systems borne by hospitals would be replaced by externally purchased components and applications, which are known to comply to relevant national standards and architectures. In-house information technology departments would be able to

concentrate on value-added systems and applications, improving the level of information support at each particular facility.

Managers and policy makers are interested in the care of individuals across the system. With electronic data interchange the recognition of an individual is assured as long as the consumer identifier is known within each domain. The key advantage of a health identifier is the unambiguous recognition of an individual across the health care system. A national health identifier has been instituted in the UK although consumers usually attend the same centre for care. It has also been implemented in New Zealand and Canada and is mooted in Australia (eg South Australia and New South Wales).

In the new health environment with electronic health records, managers will be responsible for ensuring security and confidentiality. To do this they will need resources and a clear legal framework in which to act and deliver sanctions. Security requirements must be explicit, as must provisions for the backing-up of data.

Heard *et al.* (Appendix B) see the following aspects of a national approach being required to assure manager benefits:

- A legal framework and best practice guidelines need to be established for:
  - security of health data;
  - managing the introduction the electronic health record;
  - the balance of access and security appropriate in different settings;
  - system performance and useability; and
  - collecting management data as a by-product of recording care.
- The introduction of a health identifier needs to be carefully considered to aid local management.
- The vision of the health system of the future needs to have a ‘step wise’ implementation that is coherent and safe and reasonably inclusive.
- Health care professionals and consumers need to be aware that the importance of the electronic health record will often extend beyond the immediate consultation and for that reason will need to be structured and carefully maintained.
- Transparent methods of requesting and recording of consent for use of personal health data for management purposes should be incorporated into electronic health record development.
- A mechanism to bring about standardisation of electronic health record systems needs to be instituted, providing added resources for those who fully implement standards, some of which must be passed on to system developers.

National approaches can work to the advantage of the commercial health software industry. Developers can use nationally agreed standards and guidelines for core

requirements, information models, and interoperability, enabling them to reduce the costs of developing their own versions of this core work. Commercial vendors can also reduce the costs of implementing basic electronic health record facilities, by sourcing standard components, such as prescribing modules or terminology services, built to national specifications. They will then be able to focus their resources on value-added development, particularly on higher quality graphical user interface applications, specialist systems, and integration with billing and accounting systems.

The large majority of software vendors benefit from the certainty and stability which standards bring, provided these standards are implementable at reasonable cost and have strong support from relevant standards endorsement bodies. The only vendors who resist standards are those with a monopoly market position based on a non-standard, proprietary technology or product.

Heard *et al.* (Appendix B) see the following aspects of a national approach being required to assure manager benefits:

- A balanced approach to the introduction of standards:
  - which are easy to implement;
  - have a limited number of specific implementations (i.e. a generic solution);
  - are supported by rapid expert decision making;
  - are internationally compatible where possible; and
  - are kept up to date.
- A commitment to ensure benefit from the introduction of standards through:
  - seeking acceptance by the appropriate industry body that the standard is suitable;
  - proposing reasonable time lines for implementation of standards; and
  - ensuring financial reward or at least no financial disincentive for implementing these standards.

Ensuring societal benefits

The electronic health record is only one aspect of the information age and is evolving as a desirable achievement in a world that is transformed by the new information and communication technologies.

Population data collection is potentially useful to society through research and analysis. The costs of interfacing the various health departments' computers with provider systems and processing provider data should drop if a national approach to electronic health record systems and standards were adopted. Much of this cost will be saved by the providers, since they are normally responsible for establishing data fields according to government specifications. Health departments should realise a rise in quality of data extracted, since they can make assumptions about what

information is available, based on provider support for agreed national information models. The potential benefits to society of such uses of electronic health record systems have been listed by Mount *et al.*:

- better informed policy development;
- improved resource allocation and management;
- outcomes and cost-benefit analysis of interventions;
- identification of causes and risk factors of disease;
- more accurate and efficient collection of demographic data for management and epidemiology purposes;
- monitoring of disease outbreaks and adverse reactions;
- establishment of registers for diseases, devices and treatments; and
- post-marketing evaluation of drugs, devices and procedures.

These functions depend on record linkage. Where accuracy is greatly improved by consumer identification numbers. Such linkage, where it involves identified data, should occur in a context which respects individual privacy. Large scale data linkage may require separate legislative approval.

Finally, a national approach will align activities which will have to be repeated around the country. Some activities should be centralised so as to minimise duplication of effort. These core activities should be carried out with adequate resources and the ability to consult widely and rapidly with key stakeholders ensuring that the process is inclusive of special situations such as rural and remote populations, Aboriginal health, migrant health, the elderly and people with disabilities.

Heard *et al.* (Appendix B) see the following aspects of a national approach being required to assure societal benefits:

- The roles of the electronic health record are determined within the health model operating in that State or Territory.
- Open standards underpinning the electronic health record which prevent ‘lock in’ to proprietary solutions and maintain interoperability and communication.
- Introduction of a national health identifier to allow record linkage and thus quality information for research and policy development.
- Establishing an agency to monitor and advocate for implementation of the electronic health record, particularly for consumers and health professionals.
- Explicit accreditation of electronic health record systems through a transparent process and undertaken by a body with a consumer focus and mandate.
- Nominated national organisations to undertake and advocate for the ongoing development of the ‘building blocks’ of the electronic health record and guide its use nationally.

7.2 Implications of doing nothing

With so much happening in the area of health information (broadly defined) on the one hand, and so much uncertainty surrounding electronic health records in particular on the other, it may be tempting for governments in Australia to adopt a 'hands-off' approach. Given the interest of vendors in this general area, including electronic health records — why not let the market sort it out?

This is arguably unwise counsel for at least a couple of reasons. First, the market has not sorted it out (and is not likely to anytime soon) because of the risks involved (eg because most of the critical 'building blocks' — see Chapter 10 — are not in place); but also because it is unlikely that any one supplier can impose a solution by virtue of sheer dominance of the market for health information.

Second, given that the health sector is such a large component of the Australian economy (accounting for 8.5 percent of GDP and thus 1 in 12 dollars of all spending) plus the fact that 2 out of 3 health dollars are government financed, government can hardly afford to be a passive player when it comes to embarking on projects with the potential to truly revolutionise health care in this country. The fact is that Australian governments have a huge incentive to at least give their imprimatur to a coherent framework for the deployment of information and communication technologies in the health sector by determining appropriate compromises between the various interests and supporting a suitable infrastructure to ensure reasonable outcomes (and so avoid the kinds of development that led to the rail gauge fiasco of earlier times). The States and Territories are already moving (South Australia and New South Wales in particular) and the success of these first steps are dependant on realising a national approach to the electronic health record.

Continued use of paper-based records within Australia’s health care system is inefficient, and arguably detrimental to the delivery of consistent, high-quality health care to both individuals and the community as a whole (given the patent limitations of such methods). Also, in an 'information age' it no longer makes sense for anyone to have to endure lower-quality care because of lack of access to health information that has been previously recorded and stored.

7.3 Summary

A national approach to electronic health records should have clear and carefully considered aims and objectives. The evolutionary creation of such a system needs to resist being stampeded into precipitate action by unrealistic expectations about how quickly real progress can be made. Equally, the development of such a system needs to set realistic milestones and concentrate in the early stages on automating existing paper records which users find most valuable. Only in this way can such an undertaking demonstrate value for money early and consistently throughout its evolution.

The benefits of a national approach to the electronic health record can be summarised as maintaining consumer trust, maximising the efficiency of combined effort, and enabling the transfer of information. With concerted national endeavour involving consumers, providers, managers and the software industry, Australia is well placed to take part in international efforts to achieve a truly beneficial electronic health record and, at times, lead this venture. However, it is a long road. The current 'system' in Australia is mostly paper-based - with a patchwork of incompatible electronic functions. If electronic health record development is strategic, sensitively involves the stakeholders and is facilitated by national guidelines, it is likely that costs and risks will be manageable and earliest achievement of lasting benefits will result.

There must be a fair exposure to risk in this endeavour — such that activities that are of benefit to society rather than the provider, the consumer or software provider should be publicly funded.

Having agreed what the common components will be, a national approach needs to provide no additional constraints on the imagination of systems developers to provide what consumers, providers, and managers need. There is ample opportunity for commercial activity and profit in the implementation of electronic health records — installation, adaptation, clinical applications, message incorporation, and third party tools for audit and quality assessment.

The best electronic health record will be produced through cooperation of all parties, collective commitment to the approaches that show the most promise, and open non-proprietary solutions.

Some things seem reasonably certain. A national approach in Australia will do best if it takes an evolutionary approach, particularly in hospitals. Experience from other settings demonstrates that the best hospital systems are complex and require considerable in-house adaptation or development to be acceptable to users.

Software development cycles in health are about three years in length and fundamental changes in requirements set nationally need to take account of this. A national approach needs to be heralded over a period of time that lets developers take account of it in their normal evolution. Rightly, they will be responsive to their users needs — so it will help if the national initiatives are expressed through users rather than centrally. This can be in the form of requirements for accreditation, as in the UK, with certain funding being dependent on following this national approach. The software industry should ideally be a major player in determining these requirements and the accreditation process.

Finally, it must be acknowledged that some key commentators may not yet be willing to decide on how to move forward and may call for more research or training. They should be listened to in proportion to their knowledge and experience and their uncertainties addressed in the national approach.

A part of any national approach must be the education of the stakeholders — consumers, providers, managers and policy makers — in the important issues and risks that need to be addressed.

The electronic health record is not an end in itself, rather a means to improve the quality and cost-effectiveness of health care offered to Australians in a secure environment. The data collected should enable providers, managers and consumers to be reasonably sure that these outcomes are being achieved.

The UK ScopeEPR project raises issues that should be taken into account when initiating a national approach:

- learning from wider experience;
- avoiding unnecessary reinvention;
- enabling communication and integration—only possible with a national approach;
- accessing and investing in shared knowledge resources — via the Internet;
- working with global markets — there are opportunities for Australia;
- putting effort into solutions that may be shared; and
- monitoring international legislation — being compatible will benefit consumers.

Recommendation:

That Health Ministers agree:

1. to affirm the need for a national approach to electronic health records in Australia, and to the secure networking of health information more generally.

PART B

A HEALTH INFORMATION NETWORK FOR AUSTRALIA: WHAT IS BEING PROPOSED AND WHY?

8 POSSIBLE APPROACHES TO ELECTRONIC HEALTH RECORDS FOR AUSTRALIA

Investigating possible national approaches to electronic health records has involved the Taskforce in a number of activities. One was to consider what lessons should be learnt from past and existing initiatives to build such systems — both in Australia and overseas. Lessons learnt, which have informed the Taskforce's thinking, are summarised in Chapter 4.

The Taskforce also commissioned a number of papers (Appendices B and G) and members themselves prepared background papers on key issues (Appendices D, E, F and H).[42] Following consideration of these papers by the Taskforce, an Issues Paper was prepared which sought to identify the key challenges that would need to be addressed in formulating an approach to electronic health records in an Australian context (see Appendix C).

This Issues Paper was used as the basis for consultations and included a call for written submissions. Written submissions were also sought via advertisement in national newspapers, as well as through a targeted distribution of the Issues Paper to approximately 150 key stakeholder organisations. Information and feedback sessions, based on the Issues Paper, were held in all States and Territories (except Tasmania and the Northern Territory).

A summary of the points made and issues raised by the public consultations process appears in the following sections. These have shaped the Taskforce's thinking in developing its proposal for a national approach to electronic health records as described in Chapter 9.

8.1 Summary of information exchange and feedback sessions

The Issues Paper did not propose a particular solution to the question of electronic health records. Rather, it discussed key components of electronic health record schemes, based on the literature and knowledge of activity in Australia and other parts of the world. Thus the Paper provided background information and invited discussion on such issues as the definition of electronic health records, their objectives, purposes, uses, and possible record and network architectures.

It also introduced the concept of building blocks — those underpinning infrastructure issues that will be necessary components of any system, regardless of

[42] The most significant paper commissioned was one written by researchers from Flinders University, Adelaide (led by Dr Sam Heard) titled 'The benefits and difficulties of introducing a national approach to electronic health records in Australia.' This paper is reproduced as Appendix B.

the kind of national electronic health record scheme that is put in place. The building blocks include privacy protection, secure transmission of information, conforming to agreed standards and support for computerisation by health care providers (see Chapter 10).

The information and feedback sessions have provided valuable information and appreciation of people's thinking to assist the Taskforce refine its views on an appropriate way forward for supporting a system of electronic health records in Australia.

The following is a summary of what came out of the public consultation process, under the headings used in the Issues Paper.

Definitions

- There was general agreement about the definition proposed in the Issues Paper, namely:

  > an electronic health record is an electronic longitudinal collection of personal health information, usually based on the individual or family, entered or accepted by health care professionals, which can be distributed over a number of sites or aggregated at a particular source, including a hand-held device. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of a known party.

- However, a number of participants sought to clarify the intent of the Taskforce's work – ie is it investigating the introduction of a national approach to electronic health records or a national electronic health record?
- There was some doubt expressed over the use of the family as the base unit for electronic health records. It was suggested that family units are very changeable, and there may also be a risk of inappropriate disclosure of information. Using the individual as the basic unit but allowing aggregation of family records where consent existed could solve these problems.
- There was some concern about the statement 'the record is under the control of a known party'. Comments were made about the use of the word 'control' and what that means and the suggestion was made that 'custodianship' may be more appropriate. There was also concern expressed at the words 'known party' because it is not clear what is meant by the term.
- There was discussion about the need to define 'longitudinal' — when does an electronic health record commence and when would it end.
- A suggestion was made that the notion of ensuring that personal health information is kept private should be incorporated into the definition statement.
- A suggestion was made that the Taskforce needs to define the scope/parameters of the system it recommends. For example, who would the Taskforce define as being a health care provider — would it include for example, dieticians, weight loss consultants, alternative medicine practitioners?

Objectives

- While a range of suggestions was made to clarify and refine the objectives, there was general agreement with the objectives proposed. An overall view expressed was that the Taskforce needs to be clear about a core set of objectives, rather than fall into the trap of other electronic health record projects and aim for the world.
- It was suggested that there was a need to define what's not included – for example, is cost cutting an objective? Also the Taskforce was urged not to overlook the importance of administrative gains that can be made by providers.
- Another group suggested that objectives be stated in such a way that will enable performance to be measured at a later date.

Purposes

- Participants in feedback sessions argued for the inclusion of a section called 'supports clinical governance' because, as indicated above, there are substantial management and administrative advantages in the introduction of electronic health records.
- A number of participants made specific comments on the words used in the list of purposes and suggested alternatives. For example, the word 'medical' and 'clinical' should be changed to 'health'.
- 'Supports Clinical Care' was considered by some to be limited and to not effectively cover the notion of supporting clinicians and enabling decision support.
- Another group nominated the inclusion of 'supports clinicians' as a balance to the focus on consumers.

Uses

- Some contributors suggested additional uses – such as consumer safety, funding and reimbursement, and fraud detection.
- At a more general level, however, a view emerged that suggested uses should be infinitely flexible – ie. that uses themselves should not limit the design of electronic health records arrangements – that properly designed, a scheme of electronic records would provide the baseline data that could then be tapped for many uses.

Structure

- Participants were emphatic about the need to take account of what is already in place – ie general practitioners are increasingly receptive to simple health summaries and are using proprietary solutions. The RACGP is also an advocate of simple health summaries as a way of informing consumers.

- Care plans on the other hand were thought to be too large for electronic health records. Event summaries were said to be more practical than the whole plan.
- Some sessions reported the importance of commencing with a focus on a specific need group such as the chronically ill (diabetes?) – and build on this to successfully demonstrate the advantages of electronic health records.
- Others suggested that the key to electronic health records was getting the standard record architecture right at the start and extending the range of applications over time.
- Discussions concerning a possible electronic health record network focussed on the issue of distributed versus centralised data storage, with strong views expressed in favour of a distributed system.
- Other groups argued that the network architecture is a 'red herring' saying that business needs will determine how components of the electronic health record need to be supported.
- There was general support for the need for a standard record architecture. It was pointed out that having a standard record architecture did not mean that all aspects of an electronic health record would need to be implemented immediately, they could be developed over time. Several participants pointed out that the two architectures discussed in the Issues Paper, GEHR and HL7, were in fact complementary and not competitors.

Building Blocks

- The need for a unique health identifier was identified as an important pre-requisite for a national approach.
- It was suggested that managing the change and achieving cooperation between stakeholders would involve considerable effort. Failure to achieve cooperation and to manage the change will result in the failure of the proposal.
- The method of governance of any proposed scheme was seen to be crucial for the success of the project.
- The lack of data standards was thought to be a major obstacle to a national approach to electronic health records. The comment was made that there needs to be an incentive provided or a mechanism put in place to facilitate the adoption of agreed standards.
- Third party accountability and authentication was raised as an issue that needs to be considered and addressed. For an electronic health record system to operate, proper authentication of providers and third parties accessing data is required.
- There was considerable comment made on issues concerning consent and the difficulties that will arise from having a voluntary approach to participation. There was also discussion about gaining consumer consent and the mechanisms that could be adopted to facilitate this. There was concern raised about

situations where a consumer may not be able to give consent (eg if a consumer is in an emergency situation or is unconscious).

- Consumer accountability was also discussed. The point was made that consumers may have the ability to limit information available electronically, which may then impact on a health provider's ability to assess the health status of the consumer. In these circumstances, would consumers be held accountable and is there a duty of care required by consumers?
- There was considerable discussion about the need to have common coding and language standards. The comment was made that the current coding systems are flawed and the clinical component of the systems are poor.

Other considerations

- Contributors in several groups commented on the need to take account of cultural differences when making recommendations for a national approach to electronic health records. For example, Aboriginal communities may have considerably different needs from an electronic health record and the approach adopted for this group in the community may vary from that adopted for others. Similarly, people of non-English speaking backgrounds may have different concerns and varying needs that should be taken into account in the development and implementation of electronic health records.
- Funding issues need to be covered — where will the dollars come from? — Kaiser-Permanente, for example, estimates that transmission costs 25c/unit and set-up costs are likely to be in the order of $100 million.
- Need a proactive communications/education strategy.

8.2 Summary of written submissions

In addition to the information and feedback sessions, a total of 94 written submissions were received in time for their content to be taken into account for this report. The submissions came from a wide variety of stakeholder groups. Forty per cent of the responses came from providers or provider organisations. Most of these were from general practice related groups. Information technology industry and informatics groups provided over a quarter of all submissions while 15 per cent of submissions were from government agencies. It was notable that only 8 per cent of submissions came from consumer groups, with the remaining 11 per cent of submissions came from academics, manager/funders and others.

The summary of the written submissions is broken into two major sections. The first section covers key issues raised. Quotes from submissions are provided to give examples of the views of the respondents. The second section reports on more detailed issues that have been grouped under the headings used in the Issues Paper.

Points chosen for inclusion were either raised frequently or raise key issues.

Key Issues

Overwhelmingly the submissions indicated a generally positive response to the proposal for a national approach to electronic health records. At the same time, there was considerable variation on what respondents thought that approach should be. Following are a series of quotes which reflect the spread of opinion in submissions.

> The development of a national framework for the use of electronic health records could potentially be of great benefit to consumers, health care providers and the general community. (Consumer)
>
> Broadly speaking I would support the concept of a national approach to electronic health records for Australia … . (Provider)
>
> Yes act soon! … The government must take control of the development of electronic health information in Australia if it is to work well. (Provider)
>
> We commend the national approach to the development of strategies for the improvement of the collection, analysis and use of health information for the purpose of improving the health status of Australians." (Health informatics group)
>
> [The Department] strongly supports a national approach to this important issue and is keen to see progress. (Government)

Major concerns or qualifications were also raised in a number of submissions. These are discussed in the following sections with some example quotes taken from the submissions.

Protection of privacy

The protection of the privacy of the consumer should be the highest priority. Consumers should be given the choice of appearing on the 'database' or not. Further, consumers should always have the right to view the contents of their file on the 'database'.

> At a minimum, the right to individual consent must be honoured. (Consumer)
>
> Improved consumer access to health care records forms a basis for the consumer to engage in a health care partnership with providers. (Government)
>
> For consumers to participate as equal partners in decisions about their own health care they must have full access to information on their records. (Consumer)
>
> Consumer control over his/her own data is essential for privacy and to ensure data quality. (Provider)
>
> The effective protection of consumers' privacy will be crucial to the success of any electronic records system. (Consumer)
>
> The overwhelming difficulty with the concept is of course the risk of loss of privacy. (Provider)
>
> Privacy of medical information is of great concern to the public. Many still have memory of the Australia Card. (Provider)

The difference between a national electronic health record and a national approach to electronic health records

The Taskforce must recognise the difference between a national electronic health record and a national approach to electronic health records. Provider institutions will move towards the use of electronic health records regardless of whether there is a national electronic health record or not.

> … the NHS draws a distinction between the 'Electronic Health Record'(EHR) which is the shared record of an individual's care between all agencies, and the 'Electronic Patient Record'(EPR) which is the record of an individual's care within a particular agency. (Provider)

> I do not believe that … a totally online clinical record could justify its introduction in the foreseeable future. … At a hospital or clinical practice level, however, online records are both feasible and desirable. (Provider)

> Consumer records are developed in particular settings in order to meet particular needs … different data items will be of use in different settings, implying a system of controlled messaging between a network of systems rather than a central repository of data. (Provider)

> A distinction needs to be made between an Electronic Health Record (EHR), Electronic Medical Record (EMR) and Electronic Clinical Record (ECR). The kernel of any health record should be the ECR from registered health professionals. (IT Industry)

The work involved will be enormous

There was a clear message that the work involved in implementing a national approach to electronic health records will be enormous. Staying within the realistic boundaries will be important.

> … the objectives presented in the Issues Paper appear ambitious and should be defined in terms of realistic outcomes which relate specifically to the electronic health record and can be achieved within a pre-determined time frame. (IT Industry)

> To implement such a system will not occur in my working life. (Provider)

> Given previous experience with the implementation of products at a State level, the enormity of this project should not be underestimated. (Government)

> There are currently very high expectations regarding the likely benefits of such a system and the ease with which it might be implemented. Tempering these expectations may help to facilitate an environment that is more conducive to measured implementation. (Provider)

Primary objective should be 'consumer-centric'

There was general consensus that objectives and uses that are 'consumer-centred' should be given higher priority than those that are of benefit to planners, researchers and others.

> Overall, it is crucial for the maintenance of consumer confidence that the broad objective of any electronic records system is, and is strongly seen to be, improved health outcomes (as opposed to cost savings or administrative efficiency). (Consumer)

> [The Department] supports an electronic health records system that has a primary purpose of supporting consumer care … (Government)

> It is the delivery of the information required for safe, effective care that is the central purpose of the electronic record initiative, it is not just 'feedback'! (Provider)

> The first three listed objectives relate to the care of the individual health consumers and while supporting the validity of all six, it is these three which we consider to be of the highest priority. (Health informatics group)

Storage structures

There was some debate on the issue of standardisation of storage structures. Most of the contributions were in favour of a standard structure, there were some that considered it unnecessary and there were others who believed there was insufficient evidence to make a decision on this issue.

> To be of national use I think the structure should have a core generic architecture. (Provider)

> [My company] strongly believes that a standard architecture, such as GEHR, should be adopted. (IT Industry)

> Standardisation at the EHR architecture level is the only practical way to achieve the purposes given in the Issues Paper for the EHR. (IT Industry)

> A standard electronic health record architecture should be adopted for Australia … (Health informatics group)

> A standardised approach to the internal construction of electronic health records is not required. (IT Industry)

> The development of a standard architecture will impose a burden that ultimately detracts from further development of information systems for the health care sector whilst resources are directed to this re-engineering work. A better approach would be to adopt the XML schema approach. (IT Industry)

> No standard architectures have yet been implemented broadly enough to enable a firm recommendation based on evidence to be made yet. At this stage all options should be kept open. (Provider)

Ongoing dialogue

The need for ongoing dialogue with the key stakeholders to ensure the successful implementation of a national approach to electronic health records was identified as an important element of any implementation strategy. There was a high level of interest among the respondents in being involved in further consultations.

> As there has been little debate in the broader community about the implications of electronic health records I recommend that information, education and broad community awareness strategies be resourced and embarked upon forthwith. (Consumer)

> The Taskforce report should raise the fact that fuller consultation with all those who would be using it should take place if the system is to be workable. (Provider)

> I support and would like to be involved in a carefully considered investigation of the issues relating to electronic health records and in the development of a national electronic health record. (Provider)

> It is our belief that this work is being undertaken via a very sound approach, involving broad consultation which is likely to result in greater cooperation and coordination among the great number of organisations and individuals affected by it, and consistency across boundaries of state, sector and setting. (Health informatics group)

Objectives

There were a number of suggestions for more objectives to be added to the list proposed in the Issues Paper. These included:

- reduced iatrogenic disease, hospitalisations through reduced health provider related adverse events;
- efficiency gains to government and thus taxpayers through time saved retrieving information and reduced duplication of medical tests;
- minimisation of the opportunity for misadventure in treatment selection;
- improvement in medication safety – reduced opportunity for prescriptions to be misread; and
- prospect of incorporation of decision-support strategies to enhance decision making at the point of care.

While there were no suggestions made to delete any of the proposed objectives there was concern that the objectives were too ambitious.

There was considerable discussion about the priority that should be given to the objectives. The principle that consumer care was the most important and that other objectives were less important was widely supported.

Purposes

There was little discussion of the purposes beyond general support for those proposed in the Issues Paper.

Uses

A variety of additional uses were proposed including:

- a clinician or care giver being notified at point of contact with a consumer when the 'file' is 'opened' that a particular intervention was due — opportunistic prompting (mammogram, immunisation etc);
- access for pharmacists to the records to confirm the medications, strength and dose of medications that a person has been taking;
- pharmacists checking for previous adverse reactions to medications taken by the person;
- pharmacists checking for drug interactions if a new medication were prescribed for that person;
- a consumer being able to search custom educational links on his or her home page based on the person's health profile;
- a general practitioner receiving a reminder to check a patient's blood pressure and to schedule follow-up consultations for ongoing dietary counselling;
- a respiratory specialist reviewing the 12-month care plan formulated by a general practitioner for a patient with chronic obstructive pulmonary disease;
- a consumer providing a pharmacist with access to the diagnosis from a recent general practitioner visit so the appropriate drug is dispensed;
- use of spatial data for environmental and epidemiological analysis on the incidence of disease; and
- follow-up for screening programs and monitoring of immunisation and other public health programs.

Respondents suggested that, as with the objectives, priorities should be assigned to uses of electronic health records. The most important uses were said to be those that relate to the immediate health of a person and will assist with clinical decisions to maximise health outcomes for consumers. Following this were uses such as the monitoring of health care usage by medical practitioners to enable some evaluation of these services as to their effectiveness. Finally, uses were nominated which lead to policy initiatives that maximise the health outcomes received for the amount spent by governments.

Structure

The strongest message on structure was that a standard format for the data should be adopted although, as discussed previously, this was not unanimous. There was no consensus on which standard should be adopted. If anything there was support for the Good Electronic Health Record (GEHR) architecture as it is the most advanced. This may reflect the large number of general practice organisations that responded - and the trial of the GEHR architecture that the General Practice Computing Group is sponsoring.

There was a definite preference for online storage of data subject to satisfying security requirements. There was also broad support for storing the data as close to the point of use as possible.

Other points raised were:

- a distributed system would engender a sense of 'ownership' at the regional level;
- the security of data across the network is seen to be a major factor in the evaluation of any suitable networking technology;
- consumer held storage devices may have a place but capacity, replacement and security concerns were raised;
- the NSW Medical Practice Act includes detailed regulations concerning the data that should be captured in medical records;
- current information should be given priority (ie a condition treated some years ago may no longer be relevant and many respondents question the relevance of including such information); and
- general practitioners voiced concern regarding the extra time that will be needed to enter information into such an electronic 'database', and the time taken to determine appropriate information for inclusion.

Building Blocks

Points raised include:

- the building blocks omit workflow models (business process models) that might represent care plans, or care process protocols and guidelines in an active format;
- the main thing is to maintain an open debate on the system that is to be developed and the safeguards that will be included to protect people's privacy and security of data; and
- the need for training of end-users.

Other Matters

A number of additional questions were identified that respondents thought the Taskforce ought to address. They are:

- What are the incentives for consumers and health professionals to participate in this system?
- How will records be established for consumers who are intellectually disabled or who are not capable of deciding to participate in the system?
- How will diagnoses that are not current dealt with in the consumer records?
- What are the costs involved for this system and who will pay?

- How do we deal with a conflict in diagnoses, if a consumer attends two different practitioners?

8.3 A way forward

What was learnt from the information and feedback sessions and the public submissions process has had an important impact on the deliberations of the Taskforce. The most significant change of emphasis has been for the Taskforce to adopt an approach that favours the development of a framework for health information exchange, rather than a structure just designed to support a system of electronic health records – as explained in more detail in Chapter 9.

The information gathered through the consultation process has also convinced the Taskforce that a framework for sharing health information needs to be:

- able to build on current initiatives;
- built progressively over time, with early stages able to deliver demonstrable benefits cost effectively;
- of benefit to both health care consumers and providers;
- simple, and to reinforce consumer-provider relationships and operate in a decentralised (distributed network) environment; and
- a national system, based on a partnership with the private sector, and not one which is seen to be imposed by government.

Chapter 9 describes such a framework for health information exchange in Australia. It is the Taskforce's proposal to Health Ministers, based on the learning available in Australia and overseas. If the approach advocated were to be adopted and developed over time, the Taskforce believes it would meet the burgeoning information needs of the health sector in a flexible way, while at the same time allowing for necessary expansion, new adaptations and new applications into the future.

9 PROPOSAL FOR A NATIONAL HEALTH INFORMATION NETWORK

This chapter sets out the Taskforce's proposal for a national health information network. The first section describes how the proposal was shaped. The remainder of the chapter elaborates the proposal itself. The discussion continues in Chapter 10 with a description of the building blocks that need to be in place for the network to function effectively. Chapter 11 then sets out a proposed governance structure that the Taskforce believes will be required to oversee the work involved in the creation and operation of the network.

9.1 Shaping the proposal

The Taskforce has attempted to establish an agreed set of objectives as a starting point in formulating a proposal for electronic health records in Australia. The public Issues Paper (see Appendix C) proposed a set of objectives that have been refined in the light of comments received during consultations and in the written submissions.

The Taskforce advances the following statement as a basic set of objectives for a national approach to electronic health records in Australia. The statement consists of three key parts. The first part describes the overarching objective, which focuses on securing better health outcomes for Australians while enhancing their personal privacy. The second part highlights key areas in which a national health information network can contribute to efforts to realise the overall objective. The final part describes the mechanism through which these contributions will be achieved — emphasising the need for a national approach.

Objectives Statement

"Improved delivery of health care and better quality of care, consumer safety and health outcomes for all Australians while enhancing the privacy and respecting the dignity of health consumers by:

- empowering consumers to be able to take a greater responsibility for their own health care and be better informed about the choices available to them in respect of their health care;
- ensuring better decision-making which is shared by both consumers and health providers at the point of care;
- providing a flexible, seamless and integrated process of care through the improved delivery of health care and better quality of care, consumer safety and sharing and better exchange of information;
- providing better access to health care, particularly in rural and remote areas;

- building a best-practice, evidence based health system;
- encouraging better, more targeted health initiatives; and
- informing research, learning and training;

through developing a nationally coordinated and distributed system of electronic health records, which is based on the greater use of online technologies."

9.2 Options for electronic health records

The Taskforce identified four possible national approaches to electronic health records that could satisfy these objectives. These were to:

1. establish key 'building blocks' only;
2. encourage the development of institution-based electronic health records and electronic provider communications;
3. implement a single comprehensive national electronic health record system; and
4. create a national health information network.

The first option consists of developing and implementing the necessary standards and other infrastructure components that would allow the development of information tools and products that could usefully interact in a highly *laissez faire* environment. The building blocks would include a privacy and security framework, standards and telecommunications infrastructure.

An extension of the first option is to implement a coherent approach to the development of institution-based electronic health records that supports the effective exchange of information between providers. This represents the automation of existing arrangements. Significant improvements in messaging efficiency would be realised through implementation of this option.

The third option is to implement a single national electronic health record system that would be used in all health care institutions. This approach would achieve the standardisation required for seamless communication of information across the country - although the cost would be a lack of flexibility for contributors and users of the record.

A fourth option is to build a national health information network. A simple information exchange system (based, for example, on secure e-mail) would certainly assist with clinical decision-making (and health care decision making more generally) in situations in which the members of an individual's care team were known. It would also be able to assist in automatic reporting for management and statistical purposes, where those needs were readily defined in advance.

However, in order to build something of enduring value — something which can be built on into the future — it would be necessary to plan for a network of health information exchange built on open architecture principles that provides for the

storage of data in standard-format repositories (so that the data can be called up, as required and when authorised, and be manipulable by applications that may not yet exist, or even been contemplated). This would be the fully developed form of option four.

The Taskforce considered these four options and concluded that options one and two were necessary stepping stones but insufficient in themselves to meet the desired objectives. There is a risk that data would remain fragmented even if in electronic (and thus easily transportable) form. There is also a concern that scarce resources could be wasted through duplication of effort.

Option three represents a highly centralised and rigid approach. Stakeholders expressed concern about the possibility of a comprehensive, single electronic record – from the point of view of its practicality, as well as its privacy implications.

Option four can meet the objectives. It is a major undertaking in itself, but the Taskforce considers that it is achievable and would be of considerable benefit to the nation's health (at both the individual and societal levels). It is also consistent with stakeholder feedback in that it provides an approach that is flexible, can be added to over time and can be useful to all key groups (consumers, providers and planners). It is important to emphasise that the Taskforce is convinced that a simple information exchange network, based essentially on the exchange of health information between two points, would fail to achieve the objectives sought for a system of electronic health records for Australia. The inclusion of data storage as part of the network proposal is therefore essential to the utility of the scheme. At the same time the proposal is consistent with stakeholder concerns about the privacy impact of centralised storage – and an expressed preference for a distributed network arrangement to enable stakeholders to maintain control and autonomy over the information.

The following section describes the proposal for a national health information network.

9.3 Proposal to establish Health Information Network Australia (HINA)

As indicated in Chapter 8 and explained further above, the Taskforce has adopted the view that the best way to address its objectives for electronic health records is to develop a general approach to health information exchange, rather than a build a structure designed just to support a system of electronic health records. The proposal described below is for the development of such an approach — and a suggested working title is Health Information Network Australia (HINA).

The Taskforce has used the above objectives statement to guide its thinking about electronic health records. It has also taken into account the insights gained from the

consultations and the public submissions (summarised in Chapter 8). In particular, the Taskforce has formulated a proposal for a health information network (HINA) that can be used flexibly and is able to adapt to the evolving needs of users.

HINA would provide for the systematic collection of health-related and demographic information for an individual at the point of care. This information would take the form of event summaries (which themselves will require definition and agreement about standard format and content) — rather than attempt to capture all of the information that providers may collect in respect of each episode of care. Event summaries would include such things as: basic information about the outcome of health interventions; a hospital discharge report or referral; a summary of pathology investigations; and other summaries that health care providers generate now (albeit usually in paper form).

Information would be collected only for those consumers and providers who agreed to participate.[43] Furthermore, the data collected in event summaries would need to be agreed with the potential users of HINA — that is, consumers, providers and health care administrators and planners. As indicated by the proposed working title, these event summaries would be agreed national documents.

HINA would also provide for the storage of these event summaries in a standard format — so that they can be retrieved at any time and also so that the information they contain can be assembled in different ways (to suit the requirements of the authorised users).

The nature and location of storage facilities proposed as key components of HINA is such as to allow storage to be as close as practicable to the point of care that generated the event summary in the first place. Ideally, in the case of a hospital, for example, the hospital discharge summary or referral could be expected to be stored at the hospital itself. This would also almost certainly be the case for pathology records. In the case of general practice, providers are likely to choose to store information in a secure host facility at a regional level. The HIC or the private sector or Divisions of General Practice could be involved in establishing and maintaining such facilities (provided they can meet the stringent requirements).

The final decision on storage arrangements would be left to participating providers and would be influenced by such issues as cost and the ability of individual providers to meet the standard storage format requirements, mandated security

[43] The threshold 'consent' issue is addressed in detail in section 10.3. The ability to co-opt providers into contributing health summaries on individuals who want their personal health information to be made available to other providers via the network will depend on how a number of issues are resolved including: the potential for consumers to seek out providers who are willing to contribute health summaries to the network; the perceived benefits to providers in being able to access information about individuals and about the population (and sub-populations) more generally (thereby providing a basis for better decision-making); and the ability to design event summary recording arrangements that are minimally intrusive or disruptive of normal work practices (and thereby become an integral part of consumer/provider interactions).

standards and functional specifications, such as provider speed of access to information.

Finally, the proposal includes provision for accessing the information held in the standard format repositories — along with other information (such as best-practice guidelines and access to the latest research) which, combined with personal health information contained in the electronic health record, can assist in decision making at the point of care. This is where the real value of the network will be realised — as users of the Network (consumers, providers and planners) will be able to assemble different 'views' of the information according to their needs, provided consumers consent to the proposed uses.

Consumers will be able to request a summary of all health care interventions on the part of various providers (and may choose to maintain a separate record, electronic or paper-based, of their health history). Thus, subject to their consumers' consent, providers will be able to gain access to standard referral information from the hospital where a consumer has been cared for, or will be able to assemble information from more that one provider in order to develop a clinical history to assist, for example, in current decision making at the point of care.

Planners will be able to assemble a population (or sub-population) view of health based on the health information of individuals (in de-identified form).[44] In addition, statisticians will be able to describe the health of the population and their use of health services by assembling information from de-identified records. Researchers would also have access to de-identified personal health information. Access by researchers and statisticians would have to be limited to special circumstances and be subject to strict controls.

As the overall process is consent driven, it would be expected that generally consumers would express their consent at commencement of their participation in the Network. Others, however, may not express their views at the point of entry. In these circumstances, the appropriate process would be to seek consent before using this information for research or statistical purposes. Notwithstanding this approach, circumstances may arise where obtaining consent may not be practicable. Such circumstances, would need to be closely scrutinised by the HINA access control authority (Chapter 11) and would need to fulfil the criteria for such circumstances as provided for under section 95A of the *Commonwealth Privacy Act* and the *Privacy Amendment (Private Sector) Bill 2000*.[45]

The ability to access the network and to create tailored views of the information stored on the network will depend on appropriate links being established between

---

44 That is, personal health information stripped of any data that would permit identification of the individual.

45 Section 95 of the *Privacy Act 1988* (Cth) provides for a tightly defined set of circumstances under which identified data could be made available. Similarly the *Privacy Amendment (Private Sector) Bill 2000* tabled in Federal Parliament in April seeks to establish strict protocols for access to identified health information in the private sector.

the standard format repositories. The HINA proposal therefore includes provision for Internet-based connections between sites, with mandated security and encryption arrangements in place (see discussion in relevant section of Chapter 10 and Appendix E).

Thus, HINA will comprise a secure network as a basis for exchanging health information — including personal and other health information — principally to assist consumers establish a record of their health care interactions and for providers of health care (in partnership with consumers) to make better-informed decisions at the point of care. Participation both on the part of consumers and providers would be voluntary — with consumers agreeing to make their personal health information (in whole or in part available) to nominated providers for specified purposes. Such purposes would be expected to include for statistical and research purposes (with most such purposes being able to be satisfied by access to de-identified data).

9.4 Components of HINA

The major components of the proposed national health information network (illustrated in Figure 9.1 two pages away) are:

1 the source systems;

2 event summaries;

3 online storage nodes;

4 central services;

5 applications; and

6 access points.

The source systems are information systems used by the participating providers for their own purposes. These systems will be capable of preparing and issuing event summaries in accordance with the agreed standards for their structure and content. Providers will also use these systems for sending secure messages to consumers, other providers and approved organisations.

Event summaries will be reports that contain key information describing the relevant health event or encounter. These will usually be produced automatically from information collected by providers for their own purposes. They may occasionally be developed as a standard form mostly populated from existing information with prompts to provide additional information relevant to the particular report.

The online storage nodes will simply be computers that store the event summaries in a fashion that enables ready access to and use of the data they contain. To satisfy this requirement they will need to conform to an agreed structure (see Chapter 10).

A number of central services will be required for the efficient operation of the network. Foremost among these will be an index listing the location of all the event summaries.[46] This index will allow for the rapid location of any desired information when preparing reports for users. Other services could include, communications and offline analytical capability.

Applications will be computer programs that will allow users of the network to view the information in ways that meet their particular needs. Examples would include health summaries tailored to the particular needs of the user, medication lists, pathology results, and decision-support tools that may draw on other kinds of health information (eg lists of drugs which, if taken together, could lead to adverse reactions and reminders to providers to follow-up the outcomes of previous interventions).

Access will be provided by secure Internet connections. For consumers this could be from home or public access points. Consumers may at some point also elect to construct their own health histories and store them on personalised Web pages. However, where people choose not to directly access their own health information, ready access to paper copies will be required (eg at medical practitioners' offices). For other users, access would be provided by desktop Internet connections that form part of the network.

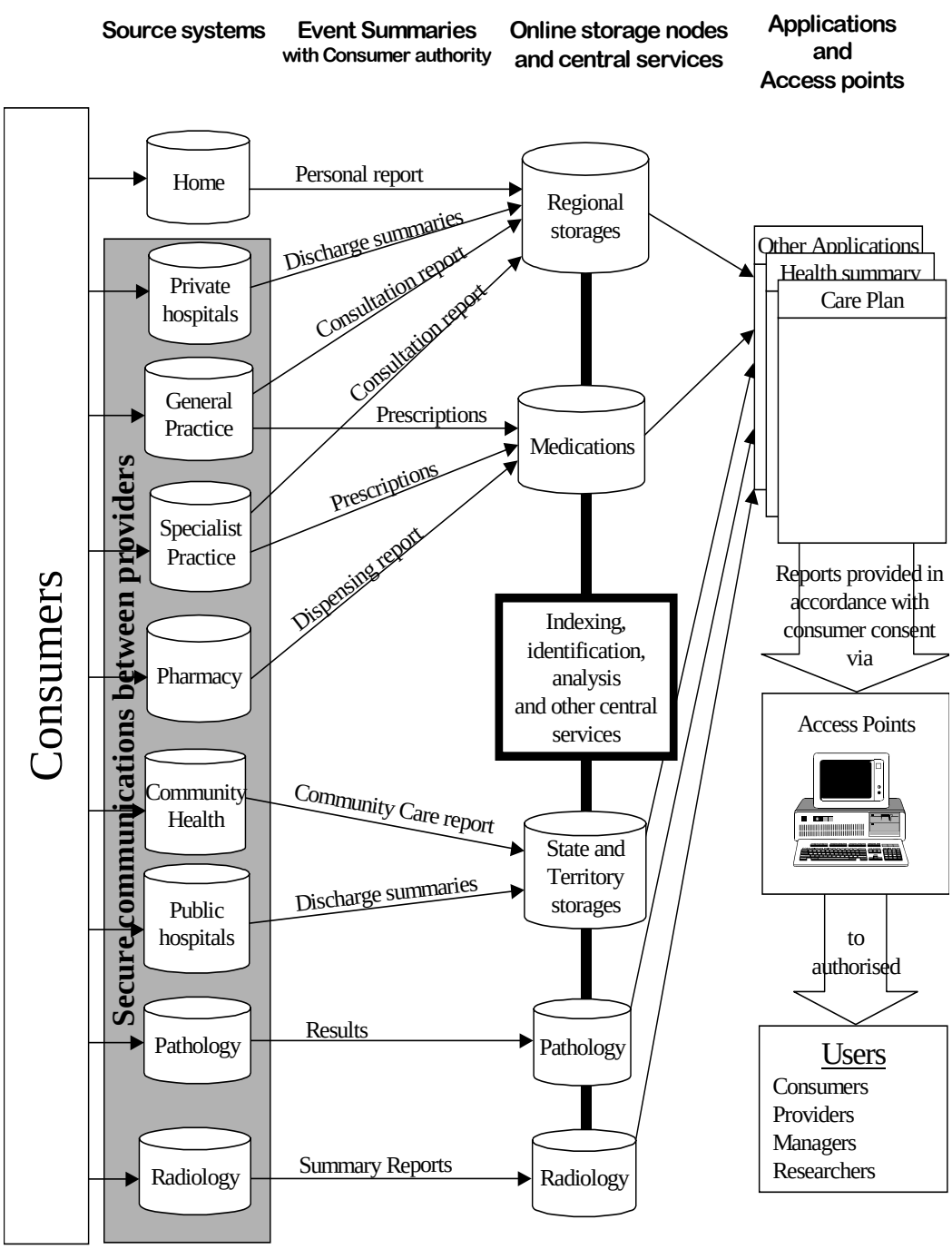
The flow of data through the network is also shown in Figure 9.1. The starting point in understanding the data flow is that all health information originates with the consumer. Information is supplied by the consumer or is generated as a result of an episode of care or medical consultation. The initial collection of information therefore occurs during the interaction between a consumer and a health provider. The provider will record information required for his or her immediate purposes and would also include data necessary to meet payment, administration and legal requirements as well as clinical needs.

When requested by a consumer an event summary would be automatically generated by the provider's information system from the data already collected and sent to the appropriate online storage node. The event summaries would be supplied to the network with the necessary licenses or authorisations to allow for their use without the separate authorisation of the supplier, subject to the consumer's privacy requirements.

The event summaries would contain data identifying the individual, provider and institution etc, relevant time and date information plus data determined by the type of event being reported.

[46] Metadata are data about data (eg descriptions of what kinds of data are held where on the Network).

Figure 9.1: Health Information Network Australia



The collection of an individual's event summaries will form the basic building block for information supplied via HINA in response to requests by authorised users. The consumer would control access to that information through the application of agreed privacy and security procedures. For example, all personal health information would be automatically encrypted prior to transmission in order to protect the privacy of the individuals concerned. Illegal attempts to access information held on or transmitted across HINA would be automatically detected and precipitate immediate investigative action — with substantial penalties for breaches of privacy requirements. The public would need to be informed of their rights, and the process for initiating action if those rights were violated (see Chapter 12).

9.5 Uses of HINA

There is a multitude of possible uses for data proposed to be held on HINA and the design of the network is such that uses will not be restricted or static. As new uses or applications are conceived and implemented by network users, HINA's flexible standard storage system will be able to support new, approved uses. Having said this, it is important to nominate an initial set of agreed uses. It is also crucial to recognise that only those uses that the individual has expressly consented to would be possible under HINA.

Initial agreed uses will determine the kind of information collected in event summaries from the start and, although event summaries could be varied over time, it would be helpful early on to focus effort on information that will be immediately relevant to an initial set of valued uses. The other reason for identifying an initial set of uses is to focus on these uses early on (and to include them as part of the design of the scheme) and in doing so quickly demonstrate the value of HINA to potential users.

In a review of possible early uses of HINA, the Taskforce has examined the work of the ACT Department of Health and Community Care which has recently been looking at the possible applications for electronic data as part of its own Health Information Networking (HIN) project.[47] Its investigation identified over 200 possible uses from which just six were chosen for the project:

- secure e-mail;
- pathology ordering and results;
- medication data exchange;
- hospital discharge reports;
- hospital discharge planning; and

[47] ACT Government Business System Project Business Case: Health Information Networking (HIN) Phase 1.

- admissions management.

The Taskforce has identified one overarching use that the initial implementation of HINA should support. This is care planning. This would constitute a summary view of an individual's record, including a proposed health care plan — with the ability to delve more deeply into areas of particular interest engendered by the individual's encounters with the health care system. The front (or 'home page') view could, for example, display a number of elements, depending on the access entitlements granted by the consumer, including:

- basic demographics such as pertinent family medical history;
- known allergies and other alerts;
- a history of diagnoses;
- medications — both prescribed and dispensed;
- a recent event list — with links to relevant reports;
- links to recent pathology results;
- links to radiology reports (possibly with a further link to relevant images themselves); and, importantly
- the current care plan (including agreed clinical and personal outcome goals).

The actual view displayed could be tailored to the preferences and needs of the particular user at the time of access.

To support the care plan, data from a number of sources would need to be made available via HINA. These would most likely include: general practice and specialist consultation summary reports, prescriptions, hospital discharge summaries, pharmacy dispensing reports, pathology result reports, radiology reports, other specialists consultation reports and community health service reports.

The care plan summary is therefore a reasonably 'high-level' application, dependent on a number of other event summaries being collected, stored on and accessible over HINA. The Taskforce has also reviewed information on possible uses collected as part of the consultations on its Issues Paper (and from written submissions) and has assembled the following as suggested indicative initial uses for the exchange of information to achieve better health outcomes:

- secure communication between providers;
- medication management;
- pathology reporting;
- hospital/community communication; and
- immunisation reporting.

Categories of uses and consumer consent

While the uses described above can be added to and, depending on the information stored on the network, could be almost infinite in number, these uses will also need to fit within agreed categories. And consumers must have the ability to nominate the categories of use for which their information can be used.

It is suggested that the categories of use would be limited to:

- personal access by consumers;
- clinical decision making by approved providers when authorised; and
- research, planning and management purposes approved by the access control body as described in Chapter 11.

Consent principles are discussed in more detail in Chapter 10 and Appendix H, however, here the focus is on the processes that consumers would have at their disposal to nominate the categories of use for which they would allow their personal health information to be used. In particular, the process that is envisaged would involve consumers nominating the uses to which their information could be put at the time they register with the network. The process would also allow for subsequent revision of these initial preferences and would include regular prompts to providers to reaffirm or change the preferences of consumers regarding the uses to which their information could be put.

One possible mechanism would be for consumers to make use of access points in government shopfronts or provider institutions with assistance if desired. Alternatively, if they have the necessary security arrangements in place, people could access their record from home and make changes from home. It is likely that control of access at the point of care will be achieved through the use of a physical token and associated authentication techniques including the use of digital signatures (see further discussion in chapter 10). This would allow consumers to nominate on a case by case basis the categories of use for individual event summaries. At this point, consumers would also be able to nominate whether or not there are specific items of information they would want protected from wider exchange on the network. Essentially, this means that consumers would be able to explicitly nominate the information that can be shared between providers and that which cannot.

9.6 Convergence of clinical and administrative systems

HINA is intended to be a network to better manage clinical information. Its objectives have better clinical outcomes in mind. The uses outlined above are clinical uses.

A health-wide administrative/financial network is already developing in Australia. Routine simplified billing and electronic claiming processes are being extended into private hospitals and general practice surgeries, and the Health Insurance

Commission (HIC) already has a substantial network based on its own offices distributed across the country. Also, to assist in the administration of health programs, the HIC is using advances in information technology to provide better, more responsive services to all its clients. The HIC is developing a range of information and technical solutions in the health sector, for example, neural networks, implementation of public key technology and electronic lodgement systems for Medicare claims.

The question arises about the potential for convergence between clinical information, the focus of HINA, and the administrative/financial information, such as that managed by the HIC. The Taskforce's view on this matter is that the different information sets should remain distinct from one another — that is, information gathered for clinical purposes should not be used for administrative or financial purposes without consumer consent, or be linked routinely with information gathered for such purposes.

At the same time, the Taskforce argues that the two sets of information can be transmitted securely and separately via the Internet due to the data protection conferred by public key infrastructure. Thus, computing equipment being installed in health facilities will be able to be used for both administrative and clinical purposes. Identification procedures should be common, as should security, encryption, messaging and other arrangements. Information collected for both clinical and administrative purposes could be integral to a single action (such as an intake interview in a hospital). However, the different purposes for collecting and disclosing information and respective consumer consent arrangements would need to remain transparent. Appropriate safeguards must be put in place to prevent those needing to access administrative information from inappropriately accessing clinical information without consumer consent. At the same time, importantly, consumers may wish to combine their information from different sources, either directly or through linked applications — within the strict consumer consent and privacy conditions that will be fundamental to the operation of HINA.

9.7 Building for the future

HINA is designed to collect, store and share personal health information among users who are authorised by health consumers and providers to have access to all or parts of that information. Information will be collected at the point of care, and stored on HINA in local storage nodes.

For ease of implementation these points of collection will initially reflect existing health servicing arrangements. As the system matures, these points of information collection will evolve and adapt to changing arrangements. Even in the initial stages, the information generated for storage and access via the network will be able to be used — with appropriate consent — in any health care setting with a computer connected to the network, and will be particularly valuable in trials that

are testing new service-delivery arrangements — such as new approaches to co-ordinated care.

Having said this, the real test of HINA's usefulness and durability will be its ability to be adaptable to future changes in methods of delivering and funding health care services.

The Taskforce is of the view that the proposed HINA would serve as a sound initial investment, and be adaptable to all possible developments (whatever they may turn out to be). The reason for this confidence is that there are a number of fundamental characteristics of the proposed network that allows it to be modified over time to cater for changes to the health care system (both planned and unanticipated). They are:

- Information is gathered from basic health events: capturing health information as a result of encounters with the system (a series of events) allows the linking of the resulting information on the individual events on whatever basis is desired (for example provider, condition, service or care plan centric).
- New contributors can be added: more provider types will participate in the system once its functionality has been established so that, over time, it is reasonable to expect that others such as nurse practitioners, dentists, dietitians, physiotherapists, podiatrists, optometrists, blood banks and the like will become part of the network.
- New uses can be catered for: new 'views' on the data available through HINA would allow new applications to be supported (with new uses easily constructed from existing tools) provided the individual had specifically consented to this new use. Such new uses would require an open architecture and open access regime which HINA would be.
- Changes can be made to the data collected: changes in the agreed content of the event summaries would also allow for additional uses to be supported.

Essentially, the proposed HINA would allow 'modules' of information to be shared in a flexible and evolving way which is ultimately independent of the health system as we know it today, and sufficiently robust to adapt to the way health care will be delivered tomorrow — by establishing the business rules and standards by which these modules are able to interact. Importantly, it will allow the necessary re-engineering of health service delivery being undertaken within the whole online health agenda to broaden the present focus on disease and treatment to focus more on prevention and wellbeing.

Ultimately, all locations where health care takes place (including the home) could be linked into HINA.

Recommendation:

That Health Ministers agree:

2. to the establishment of a health information network for Australia (working title Health Information Network Australia, or HINA) as described in this chapter.

10 INFRASTRUCTURE TO SUPPORT THE NATIONAL HEALTH INFORMATION NETWORK — BUILDING BLOCKS

A number of important foundational components are necessary for the successful construction of the National Health Information Network (HINA). These are described as the building blocks and, to use an analogy from another network, they are like the roads and road rules, the bridges and other infrastructure components of the transport network. Without a satisfactory information infrastructure HINA will not be able to operate. The key building blocks are described below in a way that addresses:

- why each component is needed;
- the current state of development of each component; and
- the Taskforce's view on what needs to be done to develop each component to the point necessary to support HINA.

The building blocks are:

- privacy, confidentiality and security;
- standards;
- telecommunications infrastructure; and
- encouraging uptake and use of information technology.

10.1 Privacy, confidentiality and security

People reveal highly sensitive information to health care providers. If this information were used inappropriately, it might lead to serious consequences for a consumer — such as being refused insurance, a job or a bank loan or personal embarrassment. Furthermore, in these circumstances, it may be difficult for the individual to recover from such disclosure or hold anyone accountable. Any new health data record-keeping system — such as a system of electronic health records — must therefore ensure that information is used appropriately or people will not use it.

Several issues are involved. First, personal health information needs to be kept *confidential* — it should be used only for approved purposes and shared only among authorised people (typically associated with the consumer by a special relationship, such as the provider-consumer relationship). Second, an appropriate level of *privacy* for the information must be established — to ensure that an individual's right to keep his or her personal health information confidential is maintained while also realising the benefits that can accrue to society if the

information is shared more broadly. Finally, electronic health records must be protected by adequate *security* — that is, administrative and technical measures must safeguard them against loss, modification, or inappropriate dissemination.

Privacy and confidentiality

The degree to which individual consumers' privacy is protected and is seen to be protected is critical to the success of initiatives aimed at greater sharing of personal health information by electronic means. Virtually unconditional trust placed by a consumer in his or her health care provider that information imparted to the professional will remain confidential, is fundamental to the consumer's relationship with the provider as well as the quality and appropriateness of the care received.

Consumers and the general community currently have a high level of trust in the way in which highly sensitive health information is handled within the health sector. However, the capacity for emerging information and communications technologies to assemble, store and transfer information in unprecedented amounts has understandably generated concerns that consumers' health information privacy might be lessened in the electronic age. Providers likewise have expressed concerns that their privacy could be eroded as electronic information exchange increases across the health sector.

Before the development and implementation of electronic health records can proceed on a national scale, therefore, both consumers and providers need to have a strong sense of trust that personal health information will be adequately protected and that the boundaries are firmly in place to restrict information exchange to a 'need-to-know' basis only. While confidentiality and security are clearly important considerations, the concept of information privacy goes much broader in its scope, covering all aspects of the handling of personal information including: the right of individuals to be informed about why their information is being collected; having access to their information; and having a say in how their information is used and to whom it is disclosed.

In this context, there has been a growing realisation that Australia's approach to health information privacy and the ethical use of such information should be strengthened, to respond to current demands for data sharing and to plan for the increasingly complex issues that are emerging as advances in technology open up new possibilities for using information. These initiatives can only successfully proceed within an environment in which consumers can be confident that their privacy is protected and where they can understand and maintain a reasonable level of control over how their personal health information is handled.

Box 10.1: Current legal environment – Access to personal health information by consumers

Public sector: The Commonwealth, the States and the ACT, each have Freedom of Information legislation which grants to the public a general statutory right to obtain access to documents held by public agencies. This right is subject to limitations and exemptions based on a range of concepts, including the public interest. For example, in some circumstances, information communicated in confidence by or to an agency may be exempt from disclosure as may information about an individual which is reasonably likely to harm that person if disclosed to him or her.

Public hospitals and community health centres are public agencies for the purposes of Freedom of Information legislation. Accordingly, members of the public are generally entitled to access their health records relating to them which are in the possession of these bodies unless there is a statutory power to withhold the records or parts of them. The person concerned has a right of appeal against a decision refusing access.

The Privacy Act 1988 (Cth) presently extends only to Commonwealth and Australian Capital Territory Government agencies and certain businesses providing or reporting on consumer credit. The Commonwealth's limited involvement in delivery of health services means that most health service providers are not bound by that Act.

The only other Acts of Parliament which confer public rights of access to health information are the ACT Health Records (Privacy and Access) Act 1997 which came into force on 1 February 1998 and the NSW Privacy and Personal Information Protection Act 1998. The Health Records (Privacy and Access) Act applies to records kept by any health service in the ACT, in both the public and private sectors. It also applies to personal health information in documents kept by organisations other than health services. The NSW Act establishes privacy principles that must be observed by all NSW public sector agencies and entitles individuals to access information which relates to them.

Private sector: Only the ACT has legislated to provide members of the public with a general right of access to private sector records. New South Wales has given limited rights of access under regulations governing private hospitals, day-procedure centres and nursing homes.[48] Apart from these legislative provisions and the right to obtain court orders for the production of health records in some circumstances, there is currently no statutory right of access to records created in the private sector. The writer of the health record in the private sector is generally entitled to determine whether consumers can access that record, unless a Court orders otherwise.

The *Privacy Amendment (Private Sector) Bill 2000* will give consumers the right of access to those records that relate to them, and are held by private providers and private organisations. Specifically, the proposed Bill states that individuals must be given access to health information held by those individuals and organisations to which it applies unless, amongst other things, providing access would pose a serious threat to life or health of any person.

Source: Appendix F.

[48] Private Hospitals Regulations 1996 (NSW), Day Procedures Centres Regulations 1996(NSW) and Nursing Homes Regulation 1996 (NSW).

To this end, the Commonwealth has been working on private sector data protection legislation and, as a result of this work, the *Privacy Amendment (Private Sector) Bill 2000* was introduced into Parliament in April 2000. The Bill gives statutory force to the *National Principles for the Fair Handling of Personal Information*; principles widely accepted as representing good practice for the handling of personal information.

Coupled with privacy is the related notion of confidentiality. Health service providers are bound by a duty of care to keep confidential information that is disclosed to them in the course of the professional relationship. As a general rule, confidential information cannot be disclosed by a health provider without the consent of the consumer. Consumer consent must be fully informed, including being informed of the benefits and risks inherent in the electronic exchange of health information. These matters are also covered under the proposed Commonwealth legislation.

Challenges in protecting privacy

Within this privacy/confidentiality framework, there are clearly a number of challenges that need to be acknowledged and addressed — namely: potential breaches to privacy and confidentiality; unauthorised access to health information; and widening of uses of health information over time ('function creep').

At a minimum, any approach to protecting privacy in the context of electronic health records must be based on the following premises:

- an appropriate legislative framework needs to be in place, that:
  - provides complaint mechanisms and rights of redress;
  - specifies the circumstances under which health information can be collected and used; and
  - makes individuals who misuse such information held liable for such actions.
- individuals' health information should be only used and disclosed for health sector purposes;
- consumers should have access to their own health information and control over who has access to their information and to whom it is disclosed;
- appropriate security measures must be in place wherever health information is collected, stored or transmitted; and
- any secondary uses of health consumers' information such as for research, policy or planning, must pass the test that they are in the public interest and that personal privacy is not compromised.

Opportunities for enhancing privacy protection

While there will be challenges that need to be addressed to ensure adequate privacy protection, the use of electronic health records also provides an opportunity for enhancing privacy over that currently achieved in a paper-based system. Paper records and charts do not track who has seen or accessed them. Records that are kept in public view such as the end of a hospital bed or on a fax machine on a reception desk are subject to security breaches. Clerical/administrative staff may be privy to sensitive information which they are not entitled to, nor need to know, to carry out their duties.

Electronic health records can build in features that: bar access to all or parts of the clinical information contained therein; track who has accessed the record (ie audit trails); and (as described in Section 9.5) allow consumer control over approved access to specific providers — in ways that are difficult to achieve in manual record keeping systems. It is as much about boundary setting as it is about information.

In light of these challenges and opportunities in the area of privacy and confidentiality, the Taskforce endorses the adoption of strict privacy arrangements and therefore considers the Commonwealth's private sector privacy legislation to be an important platform for the development of the network. In taking this view, the Taskforce also considers that further work is required in the privacy/confidentiality area. This will include the need to consider if specific safeguards and legislation are needed in respect of some aspects of the proposals, for example to specify how a health identifier would be protected, to specify additional protection for personal information used in data-matching activities or to specify the permitted uses of personal information held in the HINA.

The adoption of the private sector legislation will see three separate regimes - the Commonwealth Privacy Act, the private sector legislation and state based public sector legislation. The Taskforce considers that a nationally consistent privacy framework is important and therefore supports the enactment by States and Territories of consistent, complementary legislation that covers health information held by public sector agencies. The Taskforce also notes that the Attorney-General has foreshadowed a review of the proposed private sector legislation after the new provisions have been in operation for two years. The Taskforce therefore proposes that progress towards achieving a national framework also be reviewed at that time.

The Taskforce also considers there will be an added need to specify circumstances of consent to use personal health information that are in addition to existing circumstances for collecting such information, in an environment of electronic information exchange. The Taskforce is of the view that participation in the network as proposed in this report should be based on consumer’s informed consent. Health consumers should be informed about exactly what they are consenting to — both in terms of what information they agree to being transferred and to whom, and for what purposes. The Taskforce therefore proposes that legislation be developed that sets out the way consent should operate and specifies

the accompanying health service professional's responsibilities and obligations in respect of the network. This would be at the core of legislation that may be required to establish the HINA and its governance arrangements.

Recommendation:

That Health Ministers agree:

3. to the establishment of a uniform data protection regime across Australia to apply to personal health information — a regime which enhances the privacy and respects the dignity of individuals.
4. to having individual participation based on informed consent. That is, that a framework of uses or use categories as described in Section 9.5 for the information contained within the network should be developed and communicated to consumers of health services so that they are informed about exactly what they are consenting to – in terms of what information they agree to being transferred (via HINA), to whom, and for what purposes. Only those uses that are specifically consented to should be permitted without seeking further consent. This will require that legislation be developed that sets out the way consumer consent should operate and also specifies the responsibilities and obligations of providers in respect of network operation. This would be at the core of legislation that may be required to establish HINA and its governance arrangements.

Security and authentication

Security safeguards are related to the concepts of privacy and confidentiality in that breaches of security can have the same serious consequences for health consumers. When institutional security standards governing the handling of paper-based consumer records are inadequate, the records can easily be lost or viewed and copied without leaving any trace of the action. Still, while the confidentiality of paper-based records is easily compromised by authorised people who misuse their access to consumer information, the sheer bulk of paper records helps keep them private: information is not easily abstracted from paper records. The fluidity of computer-based consumer records, however, makes securing their confidentiality more problematic. A sound security framework, which mandates minimum security standards for the health sector, must therefore be in place to prevent unauthorised access and misuse of the health information contained in the proposed network.

Box 10.2: Security technologies

Appropriate use of health information can only be ensured if those trusted to use the information merit that trust. However, there are technological approaches to ensuring that the data cannot be inadvertently lost, damaged, or erased, and that they are only available to a defined community of users.

If a computerised consumer record system is to operate without a paper backup system, it must function reliably all of the time. To ensure data integrity, computer systems often store critical data on redundant arrays of independent disks (RAIDs). These arrays write data onto two or more hard disks simultaneously, In addition to providing a backup copy of the data, RAIDs also speed up the system, making data accessible from the disk that can retrieve them the quickest. One of the disks is taken offline for a few minutes once each day, and a copy of its contents can be transferred to a backup tape while the other disk continues to function, after the backup is completed, the disks are desynchronised. The data on the tapes are often transferred to magneto-optical or CD-ROM disks for longer term storage. Multiple copies may be made, with one copy remaining offsite. Redundancy is also used for the central processing units and other hardware components of *fault-tolerant computer systems so* that faulty components can often be identified and replaced without turning off the computers. Using these techniques, consumer record systems have been designed that are available for use 99.5 per cent of the time.

To restrict access to records to authorised personnel only, clinical personnel must enter their name and a personal password before accessing computer files. This restriction only works if the password cannot be overheard or easily guessed. Some systems either assign complex passwords or require that they are periodically changed, but this raises the possibility that the passwords will be forgotten or mislaid because they are more difficult to remember. More robust techniques require that authorised users possess some physical device in addition to a password. One such device is a handheld *authenticator,* which encrypts a user's password using a short string of text issued as a challenge by the host computer. The challenge text, and hence the expected response, can change with each attempted access to the computer. Alternatively, security systems might require that a device such as a *smart card* be inserted in the computer while files are being accessed. Finally, biometric identifiers such as a retinal scans or fingerprints can identify authorised computer users, although these techniques are rarely employed in health care institutions because they require expensive equipment.

Maintaining a usage log of all documents accessed and changed helps discourage improper use of records by unauthorised (or even authorised) personnel, The log can be scanned manually or automatically to detect attempts to log onto the system or change files, and its presence discourages such attempts. The integrity of a document and responsibility for its contents might be additionally certified by the use of *digital signatures.*

In principle, a hospital might choose to protect its consumer records by using encryption techniques as well, making the information uninterpretable. It could encrypt data using *symmetric encryption,* where all users of the data would need to know a particular decoding password, or it might use *asymmetric encryption,* where the documents for a particular user are encoded with a well-known public key and decoded using a private key known only to the intended user. In practice, clinical documents and messages are intended for rapid access by multiple users; they are

rarely encrypted because it slows down the processing and because an adequate Public Key Infrastructure has not been established.

Health care institutions often connect their computers to broader networks of computers so their members can communicate via e-mail and have access to remote databases and Internet resources. Separate computer networks are sometimes maintained to isolate consumer records from these communications needs. Alternatively, *firewalls* may be put in place that stand between computer networks internal and external to the health care institution; firewalls are systems of computers and switches that restrict to approved locations the destination or source of data packets entering or leaving the hospital's network.

Source: Office of Technology Assessment (OTA 1995). Adapted in part from U S Congress, Office of Technology Assessment (1994), *Information Security and Privacy in Network Environment*, OTA-TCT-606, Washington, DC: U.S. Government Printing Office, September.

In Australia, the Commonwealth Government's Gatekeeper project is being implemented and will establish a security environment for electronic communication between the health sector and Commonwealth agencies, such as the Health Insurance Commission (HIC) and the Department of Health and Aged Care. The results of this work will inform health sector security requirements for certification, encryption and registration of providers and organisations.

In addition, the Public Key Infrastructure (PKI) technology has been endorsed by the Commonwealth Government as the way by which information can be transferred securely. The PKI technology establishes a secure method of point to point transmission by creating a public key and a private key for individual users. The public key encodes information in a way that can only be 'opened' by using the private key at the point of delivery. The HIC is progressing work in developing the use of PKI technology for the transmission of administrative health data. This work is at an advanced stage of development but requires further work before it can be released.

In addition to the development of secure transmission of health information, information and communication technologies implementation standards, which include business/user requirements for security at a national level, are needed. Currently, a working group of Standards Australia's Health Informatics Committee (IT/14/4) is working toward the development of a national health sector security standards framework as a means of setting directions and priorities for standards development in this area.

For health information to be transmitted securely, there is also a need to have a high level of confidence in correctly identifying the individual about whom information has been recorded — that is, a method of authentication or verification. Such a process of verification of the identity of the consumer consenting to the storage, transmission or access to information is critical from a safety and quality point of view but, at present, individual health consumers are identified by name, address and date of birth when their health records are forwarded to another health provider. There is therefore a potential for serious misadventure and adverse

consumer outcomes if transfer of clinical information such as prescription data or medical history is not accompanied by a foolproof system of consumer identification. Because of these concerns, work is proceeding within the Commonwealth on the potential of a health identifier that would provide a number for the life of each health consumer and for it to be used under strict privacy protocols in the health sector only. The Taskforce endorses the need for a national health identifier and proposes that an approach be agreed by Health Ministers so that implementation can occur concurrent with the development of HINA. Options are canvassed in Appendix H.

Providers also need to be able to be uniquely identified:

- to ensure that the information is only accessed by the provider (at a particular location) authorised by the consumer;
- to ensure that a provider is a bona fide health professional (via links to professional registration bodies or other appropriate sources);
- for professional accountability purposes (such as to establish duty of care); and
- to facilitate the efficient payment of any relevant professional fees or rebates.

Provider authentication will ensure that information is sent to the appropriate person at the correct destination. In addition, however, a provider may supply professional services from a variety of locations. A system of electronic health records also needs to be able to provide access to information from the location at which it is stored, and transmit information to the location at which the information is required — that is, a location or facility identifier. In this context, a facility may be defined in a number of ways, including:

- the location at which services are actually provided;
- the location at which health records are electronically stored; or
- a combination or linkage of these locations.

A facility identifier could also be used to administer health programs that need to differentiate between locations at which a service is rendered by a particular provider, as well as distinguishing between providers rendering services at a specific location.

Finally, particularly for some highly sophisticated medical technologies, the actual piece of equipment used may need to be identified to allow a clinical decision to be made (for example the reliance to be placed on a result depending on the resolution of imaging equipment), or an administrative process to occur (such as the differential payment of a rebate).

The Taskforce's view on these matters of security is that their early development is a non-negotiable component of the building blocks needed to support HINA. The Taskforce therefore proposes:

- development of a national health sector security standards framework[49];
- continued development of the PKI project (as the principle security framework) to enable secure communication within the health sector. The framework should be developed as a minimum standard and be based on a set of agreed principles, addressing administrative, physical safeguards and technical capabilities;
- identification of the requirements, roles and responsibilities of an organisation that may fulfil the role of a certification or registration authority and the establishment of such registration and certification authorities;
- introduction of a health-wide identifier;
- development of identification systems for providers and facilities; and
- investigation of the use of digital signatures for authenticating medical and other providers authorised to provide Medicare, pharmaceutical or immunisation services — or, alternatively, investigation of the potential of State/Territory health professional registration authorities, professional associations or other relevant institutions such as area health services to develop a comparable system of provider authentication.

Recommendation:

That Health Ministers agree:

5. to the establishment of a sound security framework (including public key infrastructure technology), which mandates minimum security standards for the health sector, to ensure the confidentiality of personal health information and to prevent unauthorised access to, and misuse of, the health information stored in the form of electronic health records on the network.
6. to the establishment of a national health identifier to be used only in the health sector under strict privacy protocols and which is implemented concurrently with HINA. Similarly, providers and facilities/locations need to be reliably identified to eliminate any uncertainty about who was involved in an episode of care and where that care was provided.

[49] The Commonwealth Department of Health and Aged Care and Standards Australia's Health Informatics Committee (IT/14) have developed a draft *National Health Information Standards Plan for Australia* on behalf of the National Health Information Management Advisory Council. Further detail on the aim of this Plan is discussed later in this chapter.

Formatted

10.2 Standards

Lack of widely agreed and implemented standards for health information is a factor that has hindered implementation of health records in electronic form. Until health care providers collect data in a standard format according to widely accepted definitions, it is virtually impossible to link data generated in various parts of the health care system in any meaningful way. This is a challenging task, if only because the health care system has highly heterogenous data and information needs.[50]

Increasing interest in electronic health records has underscored the important role that standards play in the whole electronic health record endeavour to ensure compatibility and transferability of consumer records from one setting to another.[51] For example, in its 1991 study, *The Computer-based Patient Record: An Essential Technology for Health care*, the U.S. Institute of Medicine (IOM) noted that:

> A variety of standards must be developed, tested, and implemented before the computer-based patient record can realise its full potential.

The Commonwealth Department of Health and Aged Care and Standards Australia's Health Informatics Committee (IT/14) have developed a draft *National Health Information Standards Plan for Australia* on behalf of the National Health Information Management Advisory Council. The draft plan intends to provide the basis for a national strategic approach to the development of health information standards that will address the ongoing demand for a standards-based framework to permit communication between different information systems throughout the health sector so that health information can be interpreted regardless of its origin. The Taskforce endorses the development of the plan and proposes that the future work relating to standards development required for operationalising electronic health records be incorporated into the plan.

In addition to security and authentication standards discussed in section 10.1, standards are also required in the following areas to allow the Network to operate:

- data standards;
- classification and coding standards;
- messaging standards; and
- information storage standards.

---

[50] Thus, typically, a hospital might have separate systems for admission, discharge and transfer; clinical laboratories; radiology; pharmacy; and financial accounts. In addition, those proposing replacement systems must support what will become *legacy* systems — so that incrementalism becomes the order of the day, rather than implementing revolutionary systems.

[51] Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.xiv).

Data standards

Throughout the health sector, information technology is becoming more readily available, more easily used and more readily accepted and is able to generate and process increasing amounts of information. However, because of the enormous array of information systems and data collections in Australia, bringing data together from existing systems is neither easy, nor cost effective. This has arisen through the use of disparate processes in the development of many information systems and data collections.

The National Health Information Agreement infrastructure provides an established, effective and operating infrastructure for data standards. Under the Agreement, the National Health Data Dictionary (NHDD) is developed as the authoritative source of health data definitions where national consistency is required. The NHDD provides a core set of standard, nationally agreed classifications to describe the full range of health services and population parameters, including health status and determinants. It aims to promote uniformity, validity and consistency in data, and aligns with nationally and internationally agreed protocols and standards wherever possible. It is available electronically through the National Health Information Knowledgebase, which is a repository for health information standards and classification systems. The NHDD has in the past included only data elements required for statistical purposes, but will be expanded to include a broader range of clinically useful elements.

The National Health Information Model provides the conceptual basis for the NHDD. The model provides the framework and the Dictionary provides the detailed definitions. It has broader potential for use in standardising the fundamental structural elements of health and welfare information in Australia, providing a framework for organising information, developing data and designing new information systems, and providing a framework for the stable and consistent storage and expression of data.

The Australian General Practitioners Data Model and Core Data Set Specification project was established by the Commonwealth Department of Health and Aged Care to develop a complete data model and data set that will describe and document clinical activities in general practice, facilitate the exchange of information between general practice and the broader health system, underpin decision support systems, as well as provide a sound basis for the development of general practice computing applications. The data model will be consistent with the National Health Information Model. A core general practice data set will be defined which identifies the information general practitioners are likely to use, as well as key data that other health care sector users would require from general practice. Wherever possible, the general practice core data set will use existing fields and definitions from the NHDD.

The Taskforce proposes that the NHDD form the basis for an expanded set of data definitions needed for the development of HINA, incorporating the outcomes from

the General Practice Data Model and Core Data Set Specification project and which can complement the arrangements that already exist for community services definitions.

Recommendation:

That Health Ministers agree:

7. that the National Health Data Dictionary form the basis for an expanded set of data definitions needed for the development of the network.

Classification and coding standards

High quality information is a prerequisite for clinical, planning and resource allocation decision making. There is an increasing expectation that decisions will be made on a holistic basis, taking into account the different forms of care and treatment that the consumer receives in all settings. For this to occur, information needs to be shared between all decision makers, whether for clinical or service management and planning purposes. To be effective it is critical that common definitions and classifications are adopted across different types of health (and welfare) services. At present, different classifications are used between settings, and there are also cases where multiple classifications are used within a single setting (eg mental health).

Internationally, the World Health Organisation (WHO) takes the lead in the development and implementation of health classifications. The best known classification is the International Classification of diseases, which has existed for over 100 years and is now in its tenth revision (ICD-10). The second core WHO classification is the international Classification of Impairments, Disability and Handicaps.

The WHO has a network of Collaborating Centres across the world to assist it in its health classification work. The Australian Institute of Health and Welfare is the Australian Collaborating Centre, with the National Centre for Classification in Health (NCCH) playing a key role in the centre. There is an active work program across both classifications, and Australia is playing key roles in ICD updating (NCCH), ICIDH redevelopment (AIHW) and developing linkages between health classifications (AIHW).

In Australia, the classification of cause of death and diagnosis and interventions for hospital inpatients, and the associated coding, is well developed. The Australian Bureau of Statistics (ABS) classifies causes of death, including underlying cause of death; NCCH provides expert advice and support to ABS in this work. Hospital classifications are developed and supported by NCCH, which produces the comprehensive classification ICD-10-AM for this purpose; implementation is the responsibility of clinical coders within each hospital. The classification is the basis

for 'casemix' arrangements in hospitals throughout Australia, showing the value of a well developed classification far beyond statistical and planning purposes.

In other fields, there is much less of a consensus on methods of classification, and this reflects the position internationally. A General Practice Coding Jury is now seeking consensus on a standard classification for use by general practitioners, and some work has been done to develop classifications or coding systems for areas such as community health and ambulatory care.

The issue of vocabularies and terminologies requires careful consideration. There are no agreed definitions on the distinction between reference terminologies, reporting terminologies and interface terminologies, although a consensus is emerging, informed by the international activity of ISO/TC215 on health concept representation. The key concepts from an electronic health record perspective are:

- a reference terminology which provides an anchor point to facilitate the interoperability of classifications used in different settings;
- a classification system that codes and represents groups of like clinical terms;
- an interface terminology which is used to map colloquial terms and synonyms to a particular classification.

A National Audit of Health Classifications has been undertaken to identify the current status of classification development and gaps in existing classifications. The scope of the audit includes all classifications, controlled vocabulary, nomenclature and thesauri used in health.

The Taskforce acknowledges the importance of work in this area, notwithstanding its fragmented nature and lack of an immediate ‘turn key’ coding and classification strategy.

Recommendation:

That Health Ministers agree:

8. to the establishment of an expert group (which includes key players in health classification in Australia, health consumers and expert representatives of users for clinical, planning, statistical and research purposes) under the auspice of the National Health Information Management Group to be tasked to:

- establish (by June 2001) a sustainable process for the national maintenance of classifications and terminologies, and mechanisms to facilitate interoperability through the use of an appropriate national reference terminology;
- agree (by June 2002) upon national classification systems for all sectors identified within the framework (taking the WHO Family of Health Classifications work as a starting point); and
- establish (by June 2002), a national mechanism for the assessment and accreditation of interface terminologies in use in all health care settings.

Messaging standards

Information related to consumer health care is held in a variety of data formats and information structures, using a range of computer applications and paper based systems. The adoption of common messaging standards will enable communication and sharing consumer health care information between disparate systems.

One of the most widely used messaging standards is the HL7 standard for electronic interchange of health data (see Box 10.3). HL7 was originally a standard for communicating laboratory data and other clinical observation data between software applications, but it now includes structures for communicating clinical orders, billing information, and patient admission, discharge, transfer, and registration information within single institutions. This suite of standards has brought a level of order to the varied approaches to sending messages within and among health care institutions.

HL7 and UN/EDIFACT allow computers to convey data in an organised manner. Where computers need to interact, messaging standards are appropriate. XML allows humans to store, display and print information. Where humans need to read information, then XML will be used. XML is not concerned with the senders or receivers of the information. These are complementary processes. The development of HL7 Version 3 is principally concerned with organising the XML transfer.

Box 10.3: Health Level 7 messaging standard

Standards for interchanging health data and assigning codes to medical concepts underlie all efforts to make patient records electronically accessible.

Messaging standards specify the *syntax* of an electronic message and coding standards specify its *semantics*. A similar distinction exists for more familiar messages, such as postcards. The syntax of a postcard corresponds to the arrangement of its elements: the addressee's name appears in a standard position, the city in another, the message is placed in a box on the left half and the stamp in the upper right, and so on. The arrangement is set by international postal conventions.

The meaning of the letters appearing within a given element (its semantics) is determined by an entirely different set of conventions, namely the language employed by the correspondent. Similarly, HL7 and other messaging standards specify the order of the many discrete elements that make up a message and indicate which elements are required and which are optional. ICD-10-AM and other coding systems assign meaning to the characters in the message.

Electronic Messages

HL7 messages are streams of text that are relatively simple to interpret, As an example, the portion of the message that carries the patient's address might be represented as "...1432 Hosteler Street 'Apt 232^Chlcago^IL^60603^USA... " In addition to demographic information identifying the patient, an HL7 message delivering the results of a laboratory test might include hundreds of other data elements containing numerical values for the measured parameters, the measurement units,

and portions of the message that bore the initial request so that the request and response can be matched and reconciled.

The data elements contain internal indications of the coding standards to be used. For instance, one small portion of the standard message defined by HL7 contains the patient's diagnosis. This slot might be filled with the characters "410.1^I9C. " The software application receiving this message knows from the position of the characters within the message that this is a diagnosis, and it simply has to assign meaning to the character by looking up diagnosis number 410,1 in the set of codes published by the ICD-9-CM Committee. The table would indicate that the diagnosis is '(anterior myocardial infarction. " Alternatively, the same diagnosis could be conveyed in a different coding scheme employing an entirely different code set, but still using the same HL7-defined structure. This allows the software application sending a message to choose whatever coding scheme is most appropriate for the data it processes. Libraries of disease and procedure descriptions can evolve without necessitating any changes in the software governing how messages are sent.

Source: Adapted from OTA 1995.

Recommendation:

That Health Ministers agree:

9. that further work proceed in the area of messaging standards and, in particular, that:

- HL7 and UN/EDIFACT be promoted in international standards forums;
- HL7 be endorsed as the messaging standard in Australia for the transfer of information within the health environment;
- XML be investigated as the preferred technology medium to exchange health information; and
- a message usage model to defined whereby HL7 and UN/EDIFACT can be used in a complementary way in Australia.

Information storage standards

A crucial component of HINA is the use of standards to define the structure of the storage facilities wherever they are located. Unless a standard format is used for storage the value of the network will be seriously compromised — information will not be able to be shared, and the various network applications will not function.

The search for a practical, workable solution to this requirement occupies health informaticians around the world. To date the possible candidates include the use of structured messaging typified by HL7, system interoperability typified by CORBAMed and record architecture proposals such as the Good Electronic Health Record (GEHR).

The Taskforce holds the view that given the state of the art there is insufficient evidence to recommend a single solution. The GEHR appears to have the best prospects and is the subject of a trial within Australian general practices through the General Practice Computing Group (GPCG) at present.

The Taskforce therefore proposes that further work proceed in this area, building on developments to date.

There are several issues with respect to information storage that relates to general principles of records management. Some examples of the types of matters that need to be addressed include:

- What volume of data should be captured and stored for each health encounter?
- How long will the data retain currency and validity?
- When should the data be moved to 'near online' or even 'off line' storage and archived?
- For a lifetime record, how will the associated classification and coding systems and record formats be maintained in association with the source data to allow meaningful retrieval?

The Task Force proposes that further work proceed to develop comprehensive policies and standards for records management. This should take into account current industry initiatives in the fields of records management and e-commerce and involve wide consultation with providers and consumers.

Recommendation:

That Health Ministers agree:

10. that further work proceed in the area of information storage standards and, depending on evidence coming from the General Practice Computing Group (GPCG) trial, that the Good Electronic Health Record (GEHR) architecture be further tested in formative work associated with HINA.
11. that further work be undertaken to develop comprehensive policies and standards for records management.

10.3 Telecommunications infrastructure

A system of electronic health records will require appropriate infrastructure on which to run. Networks provide a physical channel for exchange of data between computers and have become commonplace in most settings heavily dependent on computer-aided assistance (now most sectors of the economy).

Use of Internet, Intranet and network technologies has driven a rapidly increasing demand for telecommunications. As in Australia, the dominant telecommunications trend internationally is towards deregulation. The de-regulated telecommunications

market and the advancement of telecommunications technologies also presents opportunities for reducing cost and improving service not previously available.

Health services expenditure in Australia was estimated to be $47.3 billion in 1997-98. In terms of industry sector this would place health care as one of the largest enterprises within Australia. The size and potential of this enterprise increases the possibility of overseas competition entering the market.

The use of telecommunications in health care continues to expand rapidly as a means of supporting integrated health care. The use of information, information technology and telecommunications in health, requires focused investment and the provision of the right tools to achieve a sustainable health industry future across all providers. With the merging of the medical and social model of health, a person centred model should evolve that draws upon population based knowledge for diagnosis and/or service delivery. No matter what form of communication is used, the more effective it is, the greater the outcome.

In this context the Taskforce proposes that work be undertaken to develop a strategic framework for telecommunications infrastructure development.

Recommendation:

That Health Ministers agree:

12. to work proceeding under the auspices of the agreed governance structure for HINA to:

- identify an affordable and cost-effective strategic direction for health telecommunications over the next 3 to 5 years, identifying and describing service requirements, infrastructure requirements, key projects, management and organisational arrangements (including staffing and training); and
- assist the development of communications infrastructure options with a standard approach to enable health care providers to link to each other to form regional, Statewide and eventually a national information network.

10.4 Encouraging uptake and use of information technology

The greater uptake of information management and information technology applications by health providers, coupled with increased opportunities for training and support of health care workers on the use of such applications, will help to achieve significant improvements in the quality of care delivered for consumers. The effective use of information technology is also one of the central factors for ensuring continuous improvement and increased efficiency in the health sector.

The Commonwealth commissioned research in 1998 to look at the barriers for the wider uptake of computers for clinical practice. Some of the key barriers identified include concerns regarding: costs (including financial, time and effort); lack of

computer skills and literacy; privacy and confidentiality; actual direct benefits to general practitioners; reliability and potential obsolescence of software and hardware; and lack of appropriate software applications.

The Department of Health and Aged Care is already working in partnership with the GPCG to develop and implement strategies to enable the progressive adoption of appropriate information management and information technology systems in general practice. One of the key strategies implemented by the Commonwealth has been the Practice Incentive Program (PIP), which provided funding for general practitioners to encourage them towards computerisation in the consulting room.

Much of the focus to date, however, has been limited to general practitioners. The Taskforce proposes that future work should include identifying the key infrastructure and standards barriers that exist for other providers in the health sector and developing workable incentives to increase their uptake of information technology. This, together with the plans for general practitioners, could form the basis for a sector-wide strategy for take-up.

Education and training are also important issues to be addressed as part of the overall uptake of information technology. Already, States and Territories have recognised the importance of equipping students with information technology skills so that they can participate in the broader information economy and this will be critical in bringing about generational change.

However, one of the major impediments to accelerating the uptake of information and communication technologies in the health sector is a lack of support and training on the practical application of computer hardware and software applications. The information technology skill base amongst many health care workers is low, and opportunities to enhance their knowledge in this area, particularly in respect to medical software and data transfer capabilities, has been impeded by a lack of any ready support in day-to-day situations, as well as the lack of any relevant training opportunities.

There are, however, many industry specific organisations, such as Divisions of General Practice, already coordinating information technology support and education for providers at a local level. The Taskforce proposes that this work be continued with general practice organisations (particularly Divisions of General Practice and their state-based organisations) to identify mechanisms for improving the provision of locally accessible information and training for general practitioners, particularly for those practitioners in rural and remote areas. In addition, the Taskforce proposes that support be given to the development of education and training models, which increase the use and uptake of information technology among workers in all health sectors.

Recommendation:

That Health Ministers agree:

13. that the education and training of health care providers will be vital to the success of HINA, as will be gaining the acceptance and trust of health care consumers. These will be major tasks that will take time and require appropriate resourcing. The body tasked with operating the network should be charged with these education, training and consumer acceptance responsibilities.

11 GOVERNANCE OF THE NATIONAL HEALTH INFORMATION NETWORK

The creation of Health Information Network Australia (HINA) will be a major undertaking over a number of years. The task will require cooperation between the Commonwealth and State/Territory Governments and the involvement of all major stakeholders. Costs will be considerable (see Chapter 13). Governance of the development and operation of HINA will be a substantial undertaking in its own right and will have to encompass the interests of a diverse group of stakeholders. The arrangements will need to gain the trust of the general public. They will need to ensure that the considerable amount of work occurring in the field on health information systems is encouraged and not stifled.

A large amount of public and private money will be expended during the development and operation of HINA. Capturing the benefits of market forces will involve interaction with commercial product and service suppliers.

11.1 Governance roles

The Taskforce considers that there are three broadly defined areas of activity involved in setting up the network. The first concerns defining the detailed operational policy, setting the business rules and managing the process. The second concerns the actual implementation of the network – from gaining agreement to the content of event summaries to setting in place storage facilities that conform to the agreed structure standards — and developing the underpinning building blocks. The third involves access — determining access rules, how consent will operate, appropriate uses etc, and regulating access.

One approach to governance for the first two activities would be to set up a body responsible for the operational policy and setting the rules, and encourage others to take the running and resource the implementation of the network.

Another approach would be to require the governance body to be wholly responsible for setting the rules and implementing the network. This approach would not, of course, preclude the contracting out of services as the network is rolled-out.

The Taskforce's view favours the former approach — if the governance body were given the responsibility, staffing and resources to plan and oversee the development of the network. Actual implementation could then be contracted to others or, where possible, should be taken up by private sector interests. The Taskforce also advocates an ongoing role for the governance body, for the foreseeable future — to regulate the operation of the network.

In terms of the third function identified above, namely access control, the Taskforce favours a separate entity that would be independent of network planning and implementation — ie a body that could act independently and be seen to represent the interests of all user groups (consumers, providers and planners).

11.2 Governance options for HINA

There are a number of options available for the governance of HINA. They include:

- a separate unit within the Department of Health and Aged Care;
- a statutory authority within the Commonwealth Health portfolio;
- a separate organisation/business enterprise accountable to Australian Health Ministers; and
- a private sector organisation.

The first of these options could operate in much the same way that the Office of Hearing Services currently operates. Under this model, the governance body would be accountable to the Secretary of the Commonwealth Department of Health and Aged Care. However, the major disadvantage of this model is that it would be seen as a Commonwealth body and therefore not necessarily representing State and Territory jurisdictions and the private sector.

An example of the second option would be the Australian Institute of Health and Welfare or the Health Insurance Commission which sit within the Commonwealth health portfolio and report directly to the Federal Health Minister. However, this option, as with the first, runs the risk of not being sufficiently representative of other jurisdictions' interests..

The third option includes three possible sub-models for establishing the governance body:

- a committee/council established by, and reporting to Health Ministers as is the case with the National Health Information Management Advisory Council;
- an independent, for-profit company with shares being held by stakeholders — in this case Commonwealth, State and Territory governments and other stakeholders; and
- a non-profit company limited by guarantee in which the Commonwealth, States and Territories and other stakeholders would be represented in proportion to their contribution. The National Prescribing Service, set up with the aim of improving prescribing practices, is an example of such a body.

The first of these sub-models would build on existing structures — hence NHIMAC (through a continuation of the Taskforce) could take on a role in overseeing the development of HINA. The work (policy, planning, overall management, service level agreements with delivery agencies, monitoring progress

etc) would be undertaken in an existing agency, possibly the Commonwealth Department of Health and Aged Care (as is currently the case).

The second of the sub-models would be less attractive as it would be distrusted by many stakeholders because a profit motive would be seen to be incompatible with the provision of an equitable service to a wide range of users. Profit would be generated by selling information and this may exclude or burden some users, particularly consumers who would be the source of information in the first place.

The third of the sub-models, the model of a non-profit company, would provide the independence from any one jurisdiction, allow representation from all sectors and could have a sufficiently robust constitution to allow it to function with a reasonable level of autonomy. At the same time, stakeholder participation through guarantor arrangements would allow stakeholder groups to have ownership and actual buy-in to the whole developmental process. The Department of Health and Aged Care and the HIC, along with State and Territory health agencies, would have a powerful influence in the management of the company but their influence would, presumably, be balanced by provider and consumer interests.

The fourth option listed above, that of an entirely private sector organisation, would run the risk of not adequately representing government and public sector interests — the same issues raised under the for-profit sub-model above. Clearly, the public sector which is currently responsible for funding two-thirds of the total annual recurrent expenditure on health services needs to have a key role in ensuring that the governance arrangements adequately protect public interests.

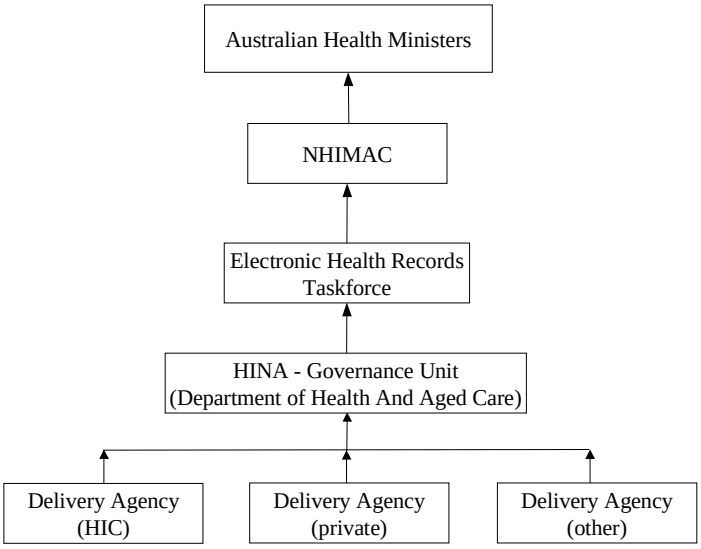
In summary, the Taskforce's view is that there are two realistic options for governance — the existing structures model based on NHIMAC and a governance unit in the Department of Health and Aged Care, and a model that is based on a non-profit organisation with limited liability and with stakeholders participating under guarantor arrangements — with majority ownership in the public sector.

Under each of these models, the role would be to manage the design and oversee development of the network, and have an ongoing monitoring and regulatory role, the actual implementation could be handled by a number of players. The HIC would be expected to have a significant delivery role in areas like security and the health identifier. It may also have a role in establishing and maintaining information storage facilities. However, private sector organisations could also have a role in hosting information services for health providers, as long as they met certain standards and they entered into contract arrangements for the free flow of information across the network.

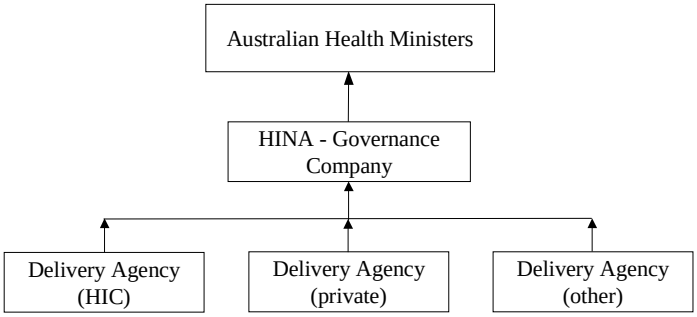
The two HINA governance models are summarised in the diagram below.

Figure 11.1 Health Information Network Governance Models

Model 1. Governance based on existing structures



Model 2. Governance based on not-for-profit company reporting to Health Ministers



The main advantage of the first of the models is that it builds on existing structures. It would not require enabling legislation, nor would it require a separate infrastructure. It would avoid 'another layer' of administration and would avoid

any conflict of role and responsibility with NHIMAC (see below). However, it does have the disadvantage of building on a model (NHIMAC) that doesn't represent all the jurisdictions — although this could be managed by changing NHIMAC to make it fully representative, or by making sure that all jurisdictions are represented on the Taskforce which would act in a more direct role (for NHIMAC) with the governance unit in the Department of Health and Aged Care. The unit itself could be staffed by the jurisdictions and the Commonwealth.

The other difficulty with this model is that NHIMAC would have no real authority to act or give directions. Nor would it have any responsibility for actions taken by the governance unit. The real authority (and responsibility) would devolve to the unit in Health and Aged Care, although it would be answerable to Health Ministers.

The second model has the advantage that it would be at 'arms length' from government while, at the same time, being answerable to Health Ministers. The Commonwealth and the States and Territories would have a substantial, though not exclusive, interest in its management — depending on the resources each jurisdiction were to bring to the table and with the proviso that the company remained in majority public ownership. The HINA governing body would therefore be accountable to participating Health Ministers. Health Ministers would be able to shape the direction of the network and would be able to close it down if they so decided.

Disadvantages of this model follow from it being additional to existing structures. It would be a new agency, requiring legislation, resourcing and accommodation within existing structures. The engagement of the private sector could also bring with it challenges of neutrality.

In the end, the Taskforce has remained non-committal about the two models. Each would work. Neither is perfect. The Taskforce believes that, ultimately, Health Ministers will have a preference and believes that a final view should be left to such judgement.

11.3 Governance of the access control function

As indicated under section 11.1, the Taskforce is of the view that the access control function should be the responsibility of a separate body. This function goes to the heart of what will be legitimate consumer and provider concerns about privacy and confidentiality, and the Taskforce views this to be a matter that should not be compromised if consumer and provider confidence is to be fostered.

The access control body would set the rules about access, how consent will operate and how users can be authorised. The actual licensing of users would, presumably, be handled by one of the delivery agencies described under section 11.2. The exception to this might be higher level users of information — that is researchers and planners. It might be appropriate for applications to use information collected

on the network to be processed by the access control body to ensure the highest level of security.

The access control body could also be expected to monitor access arrangements, investigate complaints and take action against individuals or organisations found to be in breach of access rules. Supporting legislation with penalties for access breaches will be necessary. The role of the access control body in investigating complaints of breaches of access rules will need to be considered carefully in its development to ensure that there is no overlap with other avenues of complaint such as the Office of the Federal Privacy Commissioner.

With these functions in mind and an already stated preference for a separate access control body, the Taskforce is of the view that the access control body needs to be established along the lines of the Office of the Federal Privacy Commissioner, with a high profile, trusted individual becoming a focus for the body. The Office could be established in the Federal Health portfolio but, as in the case of the Federal Privacy Commissioner, a level of independence would need to be institutionalised for the principal office holder.

Recommendation:

That Health Ministers agree:

14. that governance for HINA be based either on existing structures (NHIMAC and a governance unit in the Department of Health and Aged Care) or through the establishment of a not-for-profit company. Delivery of HINA be contracted out by the governance body; and

15. that a HINA access control authority be established within the Federal Health portfolio with similar independence to that of the Office of the Federal Privacy Commissioner.

PART C

HOW DO WE GET THERE?

12 IMPLEMENTING THE NATIONAL HEALTH INFORMATION NETWORK

All that is involved in getting Health Information Network Australia (HINA) up and running will not happen overnight. It will entail a lot of work. Success will depend on the commitment of those who are dedicated to transforming Australia's health care system into one that can deliver better health outcomes more effectively by leveraging health information. As a result, a lot of people will have to change the way they work, and the change-management processes involved will require a commensurately large effort in terms of education and training and, indeed, cultural change. There will be a need for leadership and commitment. Equally, HINA has a great deal to offer in terms of improving both health and health care in Australia, to the advantage of patients, providers and the public.

Chapters 9-11 describe the proposed Health Information Network Australia (HINA), the underpinning building blocks and a proposed governance structure to enable HINA to be established and operate successfully. Implementing HINA is clearly not a simple task. The building blocks alone are complex. Much of the work in this area is relatively undeveloped. Some elements, including for example the standard-format data-storage arrangements, are untried in a large-scale operational environment. As such, in addition to the recommendations described in Chapters 9-11, the Taskforce proposes that a Health Information Network lead implementation site or 'test bed' (or series of test beds) be established to prove the concepts and technical feasibility of the Network and its underpinning building blocks in an experimental environment that can be closely monitored, managed and learnt from. The proposed testing of various components of the Network is discussed in more detail in section 12.2.

Apart from technical issues, the implementation of HINA in its fully developed form is a major undertaking and one that will require a substantial cultural change. The Taskforce therefore also proposes that a significant investment be made in educating consumers and providers and publicising the benefits for consumers and the wider community of participation in the Network (see section 12.5).

In recognising these complexities, the Taskforce proposes a three-stage approach to the full implementation of HINA, with the view to having it fully operational within five years. The three stages are:

Stage 1: Design and development, including lead implementation site(s) (years 1-2);

Stage 2: Construction and initial operationalisation (years 3-5); and

Stage 3: Growth and expansion (beyond year 5).

The implementation arrangements for key components of the proposal (the Network itself, the building blocks that underpin it, appropriate governance arrangements, proving aspects via 'test bed' implementations, and education and publicity) are discussed within this framework and are presented in timetable format at the end of the chapter.

12.1 Health Information Network Australia (HINA)

The establishment of HINA will take time. The component parts described in Chapter 9 include: standard event summaries (to be agreed among key stakeholders, including consumer representatives, medical practitioners, hospital administrators, representatives of the diagnostic testing industry, and other health service providers); standard storage facilities (comprising a distributed network of local storage nodes all conforming to the same content and data standards); and a capacity to draw on the information held on the Network to create various 'views' of consumer (and other) information according to need and depending on consumer consent.

In this context, the Taskforce proposes that Stage 1 of the implementation of HINA produce elements of the Network that are immediately useful (so that the investment involved should be leveraged to the maximum extent possible, especially in the early stages of the project). This would involve getting agreement from stakeholders to the data that the event summaries would comprise, and to their agreement to contribute this information to the Network (in the case of consumers wanting to participate). This stage will also require the development of a method of completing event summaries that becomes, as far as possible, an integral part of provider/consumer interactions (to minimise any additional burden on providers).

Even without the full Network in place, the development of standard event summaries would represent a significant advance on current practice. Summaries of contact with general practitioners, hospital discharge summaries etc will be able to be moved from point to point via secure e-mail and will provide useful information and a referral mechanism long before the commissioning of standards storage facilities — the precursor of higher-level applications of HINA.

The Taskforce also proposes that there be an early focus on the establishment of those applications that will create maximum impact at modest cost, namely:

- secure communication between providers;
- medication management;
- pathology reporting;
- hospital/community communication; and
- immunisation reporting.

An underlying principle is to ensure that positive network benefits will be realised in this early phase of developing the Network to ensure that industry players will want to be involved from the outset.

Beyond this initial stage, the Taskforce proposes that the focus of development in Stage 2 of HINA be on the construction of the online storage nodes and other major components of the Network, with the aim to have HINA fully operational within 5 years. Beyond that, Stage 3 would see HINA being expanded to include additional applications (eg supporting personal, clinical, management and research objectives), - with success being reflected in widespread consumer and provider participation in the Network.

Recommendation:

That Health Ministers agree:

16. to a staged implementation of the network in accordance with the Taskforce's proposed timetable, noting an early focus on those applications that will create maximum impact at modest cost, namely:

- secure communication between providers;
- medication management;
- pathology reporting;
- hospital/community communication; and
- immunisation reporting.

12.2 Creation of a 'lead implementation' site

As discussed, HINA can only be established progressively. Many of the issues that need to be addressed at the outset to enable electronic health records to operate are complex, and much of what is being proposed by the Taskforce has not been tested in a large-scale operational environment. There are, however, some projects currently underway which pilot certain components of an electronic health record and which can inform the full roll-out. These include, for example, the General Practice Computing Group's trialing of the Good Electronic Health Record as a standard information storage structure for general practice.

Notwithstanding the lessons that can be learnt from existing initiatives, the Taskforce believes that it will be necessary to establish one (or more) lead implementation site(s) to implement various aspect of HINA in microcosm (including, desirably, a mini version of the full Network). Such a site would prove the concepts and technical feasibility of the Network and its underpinning building

blocks in an experimental environment that can be closely monitored, managed and learnt from.

It is also proposed that the Network lead implementation site(s) be developed in Stage 1 so as to be operational within twelve to eighteen months following Health Ministers' endorsement of the Taskforce's recommendations. The early creation of the lead implementation site(s) will enable an analysis of the feasibility of, and confirm the likely costs associated with implementing the Network across Australia (so that recommendations can be made to Health Ministers on a strategy for a national roll-out). In the end, however, the effectiveness of lead implementation sites will depend on how well they are planned and implemented — and a key component of this will be the development of a well-considered evaluation strategy and its integration into the process from the beginning.

The site of the Network lead implementation site(s) is a further important consideration and, ideally, it/they should be established in an environment that is representative of the rest of Australia — so as to provide a high level of confidence in the ability to replicate the Network throughout the country. In addition, the Taskforce suggests that the following factors be considered in choosing a site (or sites):

- need for ready access to the site by those involved in implementation;
- level of infrastructure available;
- possibility of co-location with other projects that have a commonality of interests — such as Coordinated Care Trials;
- possibility of one test bed but multiple sites;
- involvement of both rural and urban communities;
- inclusion of key elements of the health sector — acute care, primary care and community care; and
- the level of interest and support from the local community.

One approach that could be adopted is to seek expressions of interest from regions across Australia to create an opportunity for all options to be considered. This would also strengthen the case for the notion of one test bed, but multiple sites. In addition, it would require a well-thought-out approach to the lead implementation site — whether certain aspects of HINA could be trialed in different parts of Australia and one location be reserved for a full test of the Network, or whether the full model would need to be set up in a number of locations. The Taskforce advocates the former approach — that is, satellite testing of individual Network components and a full test in one location — as being the more realistic and cost efficient. It would also create a truly national lead implementation site with (possibly) all states and territories contributing to the development of the full Network.

Recommendation:

That Health Ministers agree:

17. to the establishment of a 'lead implementation' site as a small-scale version of the full network, along with simultaneous trialing of particular network features in other settings — as a way of informing the full-scale implementation of HINA.

12.3 Building block priorities

The building blocks described in Chapter 10 include privacy and confidentiality, security, standards and physical network infrastructure. While these are all vitally important, the Taskforce has identified those areas that need to be dealt with in Stage 1 of implementing HINA. They are issues that are judged to be:

- strategically important to the establishment of HINA; or
- require additional resources and/or guidance (without which progress would be slowed or the likely outcome would end up offering something that would not be useful to HINA).

Issues that fall into the first category are privacy and security. Without a convincing demonstration that these matters can be dealt with satisfactorily, neither consumers nor providers will participate – and they cannot be dealt with satisfactorily unless wide consultation informs the process. Issues that fall into the second category include coding and record-management structures. Activity in the coding area is currently fragmented and is in danger of remaining undeveloped. The record management structures area is critical to the development of standardised information storage facilities for health information in the proposed HINA. Currently the GEHR is the most progressed option and is the subject of trialing under the auspices of the General Practice Computing Group. Further development of GEHR and investigation of alternatives will need to be a priority. Further trialing in a test site may also be necessary.

While not strategically important, it also should be emphasised that work in other areas, such as messaging standards using HL7, will need to continue concurrently. Concentration on putting some building blocks in place should not be at the expense of progress with others.

12.4 Governance arrangements — timing and transition

The Taskforce's proposals concerning governance are described in Chapter 11. The issue here is the one of timing and transition. The Taskforce's view is that, if Ministers agree to establish HINA, then governance arrangements are critical to its implementation — by providing for broad Commonwealth, State and Territory

support and the momentum and resources to make an immediate difference. The Taskforce proposes that the governance arrangements as set out in Chapter 11 are introduced in Stage 1 of the implementation process.

If Health Ministers prefer the not-for-profit company model of governance (Section 11.2) this will not require a legislative framework. However, Australian governments will need to support the development of HINA through specific budgetary measures — and the earliest opportunity for support at this level will come in the 2001-2002 budget cycle.

The Taskforce's view is that work should proceed in advance of the budget cycle. This clearly cannot anticipate the outcome of government deliberations, but the Taskforce feels that preparatory work can be done that would not be wasted even if HINA were not to proceed as proposed. The development of national consultation summaries, national hospital discharge referrals, a national health identifier and other building blocks addressing security, messaging, etc would all be important work that would have value in health information applications regardless of whether HINA proceeds.

The Taskforce therefore suggests that, as a transitional arrangement, a HINA Unit be created in the Department of Health and Aged Care and that the Unit be jointly resourced and staffed by the Commonwealth, States and Territories. The role of the Unit would be to commence work on HINA fundamentals as described above, without committing resources on a scale that will properly require parliamentary approval.

In this context, the Taskforce also suggests that the Taskforce have a transitional role — that is it continues to act as a reference group for the early development work of the HINA Unit. In proposing this role, it may also be appropriate to suggest a review of the membership of the Taskforce to ensure that, as the implementation phase is entered, key interests are adequately represented.

This transition proposal is very much like the governance model based on existing structures (Section 11.2). This has some advantage in starting down a track that may be chosen by Health Ministers for more permanent governance arrangements. However, it is also adaptable to the not-for-profit model (or indeed other approaches) that Health Ministers may prefer.

Recommendation:

That Health Ministers agree:

18. that interim HINA governance arrangements be based on continuation of the Taskforce and the establishment of a special HINA Unit in the Commonwealth Department of Health and Aged Care, and that the Unit be jointly staffed and resourced by the Commonwealth and State/Territory jurisdictions.

12.5 Education and publicity

The proposals contained in this report are significant. While the concept of HINA is simple enough, when implemented in full, it will affect all health consumers and providers in Australia. In some respects, however, it is merely aimed at bringing the health sector into line with other sectors of the economy - such as retailing or banking - where electronic transactions are now accepted as a normal part of everyday life. Having said this, it is also true that health is different and people rightly will be anxious to know what advantages it will offer them and what guarantees can be provided that their personal health information will remain confidential and secure. Even beyond this, people will want to have control and will want to be confident that they will be presented with genuine choices — with the power to refuse to consent to actions that they believe not to be in their best interests. Recent focus-group testing undertaken by the Department of Health and Aged Care confirms that consumers hold firm views along those lines. When consumers understand the advantages (to themselves and to others) of adopting new ways of collecting and sharing personal health information, they will want to participate, providing they can be reassured that their privacy will be protected and their dignity respected. The same is true of providers, who may also be rightly concerned about exactly what information, gathered in face-to-face consultations, would be shared with others in the interests of the health of the individual and the community as a whole.

The key recommendations of this report have been developed in a way that aims to maintain a consumer and provider focus. HINA itself will deliver better health information to consumers and providers. The building blocks emphasise the importance of privacy and security. Governance arrangements make explicit the provision for consumer and provider participation in the management of HINA. The idea of the 'test bed' will provide a live test in a controlled environment to prove all the key components of HINA (including privacy and security) and that they work to the satisfaction of both consumers and providers prior to widespread implementation.

If, however, individual consumers or providers remain unconvinced, they need to know that the HINA proposal is one that they can elect not to participate in (and stick with the *status quo).*

The Taskforce believes these issues are fair and reasonable. The proposal endeavours to address the legitimate concerns people may have but nevertheless to preserve the option to remain outside the Network for those who so choose. However, it will be important to be able to effectively communicate this message —the benefits, safeguards, and the guarantee that people can elect not to participate if they choose. The Taskforce therefore urges Health Ministers to adopt a positive approach to publicity and education, to invest early in developing a strategy and products and be ready to commence a well-orchestrated approach to publicity and education at the time HINA is announced.

The Taskforce has not pursued publicity and education aspects of the proposal to the point of being able to recommend a detailed approach. However, publicity and marketing were raised by a number of participants at the consultations run by the Taskforce and in subsequent submissions (see Chapter 8). The views concerned are reflected in the issues spelt out above. Nevertheless, the Taskforce does have a general view about how education and publicity should be developed and delivered. The Taskforce is convinced that a networking approach will be most effective. It will be important to involve key groups from consumer organisations, professional bodies, research and other organisations. From the discussions Taskforce members have had with individuals from these groups, there would appear to be considerable goodwill towards a national scheme being developed in sympathy with consumer and provider interests. If this can be developed further and organisations can be encouraged to explain and publicise the network with their members, the word will be carried widely in the community. This approach is recommended over a centralised 'government' campaign. A networking approach will, of course, still require resources, although resources will be expended by key groups rather than a single advertising agency (see publicity/education costs are included in costings presented in Chapter 13).

Furthermore, the Taskforce stresses the need to establish mechanisms to enable widespread consultation with consumers and providers. This process could take the form of information sessions and consultations with specific consumer and professional organisations. In addition, the Taskforce proposes that both consumers and providers be involved in the design, testing and implementation of HINA.

Recommendation:

That Health Ministers agree:

19. to a network marketing model being adopted for HINA education and publicity, and that publicity be given high priority in the lead up to (and beyond) any announcement by Health Ministers.
20. to the establishment of a mechanism (such as the establishment of a widely representative consumer group) to enable widespread consultation with consumer and provider organisations on announcement of HINA by Health Ministers and to the engagement of consumers and providers during the implementation of HINA.

12.6 Summary of stages for establishing HINA

The following provides a summary of what is to be achieved by the end of each of the three stages of implementation. This is represented diagrammatically in Figure 12.1.

Stage 1: Design and development — End of year 2

- Develop standard event summaries and mechanisms for operation.
- Construction of a lead implementation/test bed.
- Focus on strategic building blocks (privacy, security, standards).
- Governance structure established.
- Publicity and education activities commenced.
- Access-control arrangements put in place.
- Commence evaluation of lead implementation site(s).

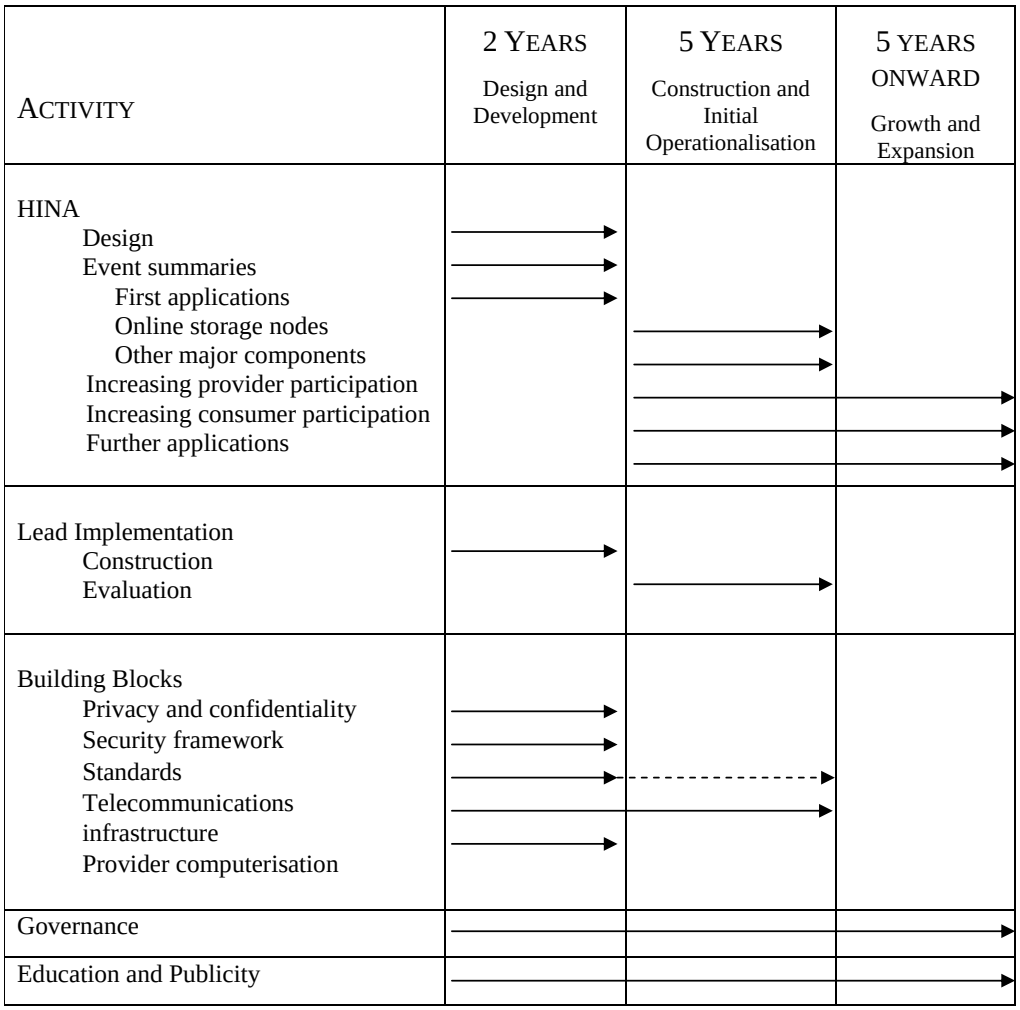
Stage 2: Construction and initial operationalisation — End of year 5

- Construction of major online storage nodes complete.
- Construction of other major components complete.
- Wide provider participation.
- Increasing consumer participation with an emphasis on groups standing to benefit most.

Stage 3: Growth and expansion — Beyond year 5

- Operational system nationwide.
- Widespread participation by consumers.
- An extensive array of applications supporting personal, clinical, management and research purposes approved and available for use.
- Applications supported (nationally and in development region).

Figure 12.1: Summary of stages in the development of the Health Information Network Australia



13 INVESTING IN THE NATIONAL HEALTH INFORMATION NETWORK

By providing systematic and comprehensive management of health information, the proposed national health information network (HINA) could prevent a large number of the adverse health care events that currently cause much avoidable pain and suffering, and claim over 10,000 lives each year. Quantifying benefits that HINA could bring is difficult; nevertheless likely savings of at least $1 billion each year from reductions in hospitalisations and duplication of tests can plausibly be argued, and at least as much again in terms of increased economic activity associated with unnecessary days absent from work. If one is prepared to put a value on human life, an annual benefit estimate of $33 billion could be advanced.

This chapter addresses the likely benefits and costs attributable to the Taskforce's proposal to build a national health information network (HINA), and thus whether the proposal is likely to represent a sound investment in the health of Australians. This is a difficult question to answer in quantitative terms. While it is challenging enough to estimate the likely costs, the benefits are much less amenable to quantification. This is especially so because there is no precedent available to the Taskforce - there is no national electronic health record system that can provide a basis of comparison for calculating potential net savings for the Network proposal for Australia. Nevertheless, this chapter attempts a broad-brush quantification of benefits, before turning to the likely magnitude of the investment necessary to make HINA a reality.

13.1 Benefits of HINA

Chapter 5 canvassed the expected benefits of HINA. In brief, the practical benefits of electronic health records to health care consumers and providers include:[52]

- Patient safety — provider access to a patient's previous and recent medical history plus what is considered best practice when it comes to treatment will mean greater safety for patients, because HINA will fill in the information gaps and take a lot of the guesswork out of heath care.
- Integration of care — online communication between general practitioners and hospitals will speed access to services and information such as electronic referrals, outpatient bookings, discharge information, and test results. The coordination of multi-professional and multi-agency care for elderly, frail and

[52] This list was adapted from National Health Service Executive (NHS 1998), *Information for Health: An Information Strategy for the Modern NHS 1998-2005*, HMSO, London pp.24-5.

Deleted: (NHS)

vulnerable patients will be substantially improved and seamless care become a reality rather than a goal.

- Improving outcomes — providers will be able to make better decisions with up-to-date guidance, complete and legible clinical histories and up-to-date test results at their fingertips, together with relevant alerts and reminders. Patients will benefit too. For example, repeating an X-ray because the result of a previous one has been lost or cannot be easily retrieved involves the patient in unnecessary exposure to radiation. General practitioners will have expert and easily accessible desktop guidance on medication options through online decision-support systems to improve the efficacy of primary care prescribing.
- Improved privacy and confidentiality of personal health information and increased individual consumer control over information — compared with the pen, paper and post world of health records now, electronic health records can greatly increase the security of personal health information by restricting access to authorised users (who must prove their identity) and ensuring that such information cannot be amended, lost or destroyed.
- Convenience and confidence — patients will be spared the ritual of repeating their name, address, previous and recent medical history to every health care provider they have to deal with. The confidence of patients is increased if they know that providers have access to relevant parts of their medical history. Confidence is also boosted when consumers have access to their own records.
- Using evidence — by integrating electronic health records with active clinical systems, general practitioners will have desktop access to referral guidelines and advice on first-line treatment agreed with local specialists. This will improve the quality and appropriateness of referrals to hospitals. Hospital staff, and especially junior doctors, will have online access to current best-practice guidelines and personal access to the latest research findings, treatment and medication options.
- Supporting analysis — analysing the data held within records will create the information needed to meet the requirements for clinical governance and inform policy and planning processes.
- Improving efficiency — the 1995 Audit Commission report *For Your Information* — a study of information management and systems in the acute hospitals — estimated that 25 per cent of doctors' and nurses' time was spent collecting data and using information. Electronic health records will reduce the amount of time spent on this activity, and free more time for direct patient care.

All these benefits will be highly valued by Network participants, albeit hard to quantify. All would be a direct result of some combination of: improved levels of communication between providers; improved data management; and the creation of a suitable infrastructure for implementing a systemic quality-assurance system to improve patient safety.

In order to attempt some quantification of likely benefits, adverse events in health care are examined. There have been a number of studies in recent years which provide quantitative estimates of the extent of this problem, both in Australia and overseas. The most significant study conducted in Australia was the Quality in Australian Health Care Study,[53] where 14,000 admissions in 28 hospitals were screened for adverse events. The study reported that 16.6 per cent of admissions were associated with adverse events, of which 51 per cent were considered preventable. It was suggested that the most effective approaches for preventing these events would be: quality assurance (56 per cent); education (32 per cent); system change (15 per cent); and improvement in communication (11 per cent).

Some of the potential benefits of the HINA are presented below. Each of these areas could result in significant improvements in the quality of care and, in addition, lead to large cost savings. The possible magnitude of some of these savings is explored in Table 13.1.

Some of the consequences of HINA where savings can be costed

- A reduction in deaths from adverse events.
- Reductions in the cost of care through reduction in hospitalisations arising from adverse events and unnecessary duplication of tests.
- Increased productivity through a reduction in days absent from work.
- Reduced expenditure on supporting patients disabled as a result of adverse events.
- The automatic creation of a product registry for the recall of defective medical devices.

(Estimated savings are presented in Table 13.1. However, as a conservative estimate of potential benefits resulting from HINA, only one-tenth of total potential savings are assumed to be attributable to implementing HINA).

Reduced deaths

The 1992 Quality in Australian Health Care Study estimated that 18,000 people died in that year as a result of the care they received. Seventy per cent of these deaths were considered to be preventable. Similar rates of adverse events were reported in the USA in 1999.[54]

If, as a result of HINA coming into operation to provide vital information whenever and wherever needed, preventable deaths could be avoided to the extent of just 10 per cent, this would result in the saving of 1,260 lives every year.

---

[53] Wilson RM Runciman WB Gibberd RW Harrison BT Newby L Hamilton JD (1995), 'The Quality in Australian Health Care Study,'. Med J Aust, 163(9):458-71.

[54] Kohn LT, Corrigan JM, Donaldson MS (1999), eds. *To err is human, Building a safer health system*, National Academy Press, Washington DC.

Reduced hospitalisations and unnecessary duplication of tests

The 1992 Quality in Australian Health Care Study found that adverse events resulted in an average of 7.1 extra days of hospitalisation. There were 5.57 million separations from public and private hospitals in 1997-98. (Again, if a 10 per cent reduction in extra days in hospital were to result from the introduction of the HINA, and it is assumed that a day in hospital costs $320, then the annual saving would be $110 million).

A commonly reported (but usually undocumented) problem is the unnecessary duplication of tests that occurs when patients are admitted to hospital and previous test results are not available. It is likely that the HINA could virtually eliminate this duplication thereby saving around $56 million per annum.

Increased productivity

Additional days in hospital resulting from adverse events have been mentioned and costed. However, a further cost to the community is also created whenever an employed person cannot work. Many patients who require health care are elderly and thus would be retired, however, the cost presented in Table 13.1 is a very conservative estimate of the actual loss of productivity attributable to adverse events. (Assuming an average income of $20,000 per annum and 12 weeks average loss of work, a 10 per cent improvement due to the HINA would save $180 million per annum).

Reduced disability

Thirteen per cent of adverse events in the Quality in Australian Health Care Study resulted in permanent disability. Of these more than half were considered to be preventable. For this estimate, a conservative cost of annual supportive care of $30,000 is used for severe disability and $5,000 for less significant impairment. (A 10 per cent improvement would save $65 million annually).

Product registries

The cost of performing a recall of a defective medical device is hard to estimate. At present many problems are encountered in undertaking this process. In this country, for example, there is no comprehensive list of all patients who have had a particular implant, and hospital records must be searched for this information. Locating patients who are potentially at risk is a further challenge, the Medicare database is current only if a patient has made a recent claim. HINA will provide a simple and efficient solution to this problem.

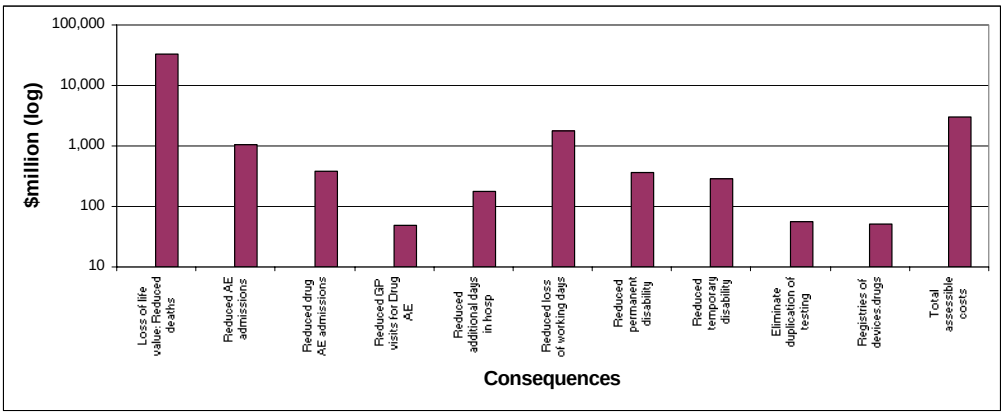
Methodology underlying calculations of cost savings

By assessing the cost of these various adverse events, an estimate of the financial magnitude of the problem can be calculated. This amount represents the scale of potential savings attainable if these events can, in future, be prevented.

As shown in Table 13.1, the estimated annual cost to the community of preventable adverse events is some $3 billion. This is calculated on the basis of 5.6 million admissions per annum, nationally. If a dollar value is put on a life lost[55] then a figure of $33 billion per annum can be calculated. A graphical comparison of costs is shown in Figure 13.1.

The Network can contribute to controlling these problems by providing a mechanism for quality assurance, education and communication. Although it is difficult to estimate the extent of this effect, it would seem reasonable to expect that a fully implemented health information network could prevent the majority of these types of medical errors. If there were an overall 10 per cent improvement in the rate of adverse events, it would save $300 million per annum.

Figure 13.1: Relative costs of adverse events (log scale)



55 Murphy K and Topel R (2000), *Exceptional Returns: The Economic Value of America's Investment in Medical Research*, University of Chicago Business School.

Table 13.1: Estimated costs of *preventable* events including adverse events and other occurrences resulting from inadequate available information

Consequences of Adverse Events (AE) and lack of appropriate information	Electronic Health Record Capable or Required*	Include in total sum	Present cost pa ($m)	Rationale#
Loss of life valued at $3m per life[1]	Required	No	33,000	0.2% death rate used: Australia, preventable death rate per admission: 0.57% [2] USA preventable death rate per admission: 0.2% [3]
Admissions resulting from AE	Required	Yes	1,100	49% of AE admissions caused by previous AE, 51% preventable, duration averaged 7 days[2] at $320 per day
Admissions resulting from drug AE	Capable	No	370	Drug AE cause 3% of admissions, average duration 7 days[2]
GP visits resulting from Drug AE	Capable	Yes	50	Drug AE cause 2% of doctor visits, [2] (costing for MBS items 23 and 36)
Additional days in hospital due to AE during admission	Required	No	170	8.3% preventable, 7 days extra for AEs[2] @ $320pd
Loss of working days resulting from AE	Required	Yes	1,800	77% of AE led to <12 months disability, 51% preventable, assume loss of work to be 12 weeks[2] @ av income of @20,000pa
Permanent disability resulting from AE	Required	No	360	2.2% of AE permanently disabled, 58% preventable[2], cost of care pa ~ $30,000pa
Temporary disability resulting from AE	Required	No	290	77% of AE led to <12 months disability, 51% preventable[2], cost of care ~ $800
Duplication of testing	Required	Yes	56	estimate 10% of admissions involve repeat of standard screening tests @ $100 per event
Registries of devices and drugs	Required	Yes	50	Estimate one major recall every 10 years, @ cost of $500m
Total assessable annual costs			3,000	Excludes life value, and other sub-categories noted that were already counted

Notes:
* An Electronic Health Record may be capable of detecting these events even without an associated health information network, alternatively, it may be required in combination with such a network.
# Estimates calculated using a national admission rate of 5.5m per annum (National Hospital Morbidity (Casemix) Database, AIHW Australian Hospital Statistics, 1997-98)
1 Murphy K. Topel R. (May 2000) *Exceptional Returns. The economic value of America's investment in Medical Research.* University of Chicago Business School. Their estimates of 'life value' range from $3-7m.
2 Wilson RM, Runciman WB, Gibberd RW, Harrison BT, Newby L, Hamilton JD. (1995) *The Quality in Australian Health Care Study*. Med J Aust;163(9):458-71.
3 American Hospital Association, (1999) Hospital Statistics, Chicago.

Formatted
Deleted: 1999
Formatted
Deleted: HIN
Formatted
Deleted: a HIN
Formatted
Formatted
Deleted: , May 2000
Deleted: 1995

Scenarios of adverse events that could be prevented by HINA

One way of making the above quantitative estimates more concrete is to relate them to everyday life, in the form of the following scenarios (see Box 13.1) on *communications*, *emergencies*, *surveillance* and *tracking*.

Box 13.1: Estimated costs using scenarios of adverse events

Communications (without HINA)

This situation may occur when a patient is referred by a general practitioner for admission via the Accident and Emergency (A&E) department of a public hospital. In this example, the treatment of a 70-year-old woman with fever and chest pain is described. She is not known to the (male) general practitioner as she is visiting her family from interstate.

She presents late in the afternoon to the general practitioner. He manages to arrange an extra appointment in his busy schedule. After examination, he decides that admission is appropriate, he orders preliminary pathology and radiology (for example, FBC, EUC and CXR) at the local laboratory. She is then sent to the local hospital for admission. (The investigation results are not at this stage available to the general practitioner).

She presents to the hospital an hour later. Documentation received from the referring general practitioner consists of a handwritten note, including a provisional diagnosis (pneumonia) and a request for admission. Past history is briefly outlined. She repeats her story and tries again to remember her entire medical history for the nursing staff and resident medical officer. This takes about 20 minutes.

Having examined her, the admitting doctor accepts the provisional diagnosis. He tries to call the general practitioner to discuss management but is only able to speak to the after hours locum doctor who knows nothing of the patient and is on a house-call (resident time spent, 15 minutes). He is thus unable to retrieve her record. The pathology laboratory has also closed for the night. The admitting doctor decides that in the circumstances he will have to repeat the investigations and orders the standard batch of FBC, EUC and CXR ($87 and 20 minutes nursing time). She is asked about allergies and remembers that she had a rash after taking some cold tablets several years ago, but cannot remember any further details. A search for previous hospital files is conducted but reveals no previous admissions (administrative staff time, 10 minutes).

She is prescribed intravenous penicillin and re-hydration. Treatment is commenced in the A&E department but produces a rapid deterioration. She becomes shocked and requires resuscitation. She is admitted to the intensive care unit. (Cost of two days in the ICU approximately $3,000 — see Table 13.2). Alternative antibiotics are prescribed, she recovers and is discharged home after seven days in hospital.

Some days later, she returns to the general practitioner for follow up and finds that he has not yet received her discharge summary. He calls the hospital to obtain her care plan (10 minutes) and finds that her record has been filed and is not immediately available. He asks the resident doctor to call him back later (resident time 15 minutes, general practitioner time 10 minutes) and suggests that the patient visit him the next morning (additional consult $26).

Alternative communications scenario (with HINA)

A new patient presents to the general practitioner complaining of fever and chest pain. She is a participant in HINA and gives her permission for him to access her personal health information via HINA. Her full medical history appears on the doctor's computer describing her general good health with a possible allergic episode to Amoxicillin some 15 years ago. The general practitioner refers her for pathology and radiology and sends an admission request to the admitting officer at the local hospital by secure e-mail. She then makes her way to the hospital. On her arrival, the admitting doctor reads the e-mail, examines her and checks the results of the pathology and radiology that have already been forwarded to the hospital. With her permission, he retrieves her medical history and notes the history of a possible allergic incident. He commences an alternative antibiotic and admits her to the ward. She returns home in three days.

Some days later she returns to the general practitioner for follow up. Again, the general practitioner accesses her record, examines her discharge summary and then discusses with her the need for continuation of her antibiotics for another week.

Table 13.2: Additional expenditures due to insufficient information on admission and the resulting adverse event ($)

Item	*Cost*
Additional tests[1]	87.00
ICU 2 days[2]	3,000.00
Medical ward additional five days[3]	1,600.00
Additional time for Resident doctor to retrieve information	20.00
Additional time for GP to retrieve information	20.00
Additional admin and nursing time	30.00
Additional consult with GP	26.00
Pain and suffering	Additional, uncosted
Total	4,783.00

Notes: 1 Benefit payable for standard investigations including pathology and Chest Xray (Medicare Benefits Schedule)

2 Estimate of cost for ICU bed and services, $1,500 per day

3 Estimated average cost of standard ward accommodation, $320 per day, (derived from private insurance claims data).

Although not all consumers are at risk of this type of adverse event, many admissions involve the repetition of a number of processes. Admission will usually require the process of recounting past medical history – a process that is far from accurate and is both trying for the patient and time consuming for the doctor.

Repetition of investigative procedures is also costly and not without risk to the patient.

A non-networked, consumer-held electronic health record (for example in the form of a 'smartcard') could assist in these type of situations, but would be inferior to one accessible via HINA in several ways. Storage capacity will always be a limitation, however, the principal shortcoming of such a record is that it will be unlikely to be current. The card must be physically available to the provider for updating information. Thus the real-time addition of reports from disparate sources (such as pathology, radiology and the hospital) is not possible. The need to provide a secure, current backup for each card could not be addressed without the introduction of a network with information storage capability.

Although clearly hard to quantify with much confidence, annual gains of the order of billions attributable to HINA are not implausible — providing more than sufficient justification to proceed with such an investment. As the headnote at the beginning of the Summary of this report puts it:

> Australia now has a unique opportunity to invest in the health of its people by building a national health information network to support a system of electronic health records for those who want to share potentially vital information with their various health care providers. Such an investment holds the promise of better health, higher-quality care and improved personal privacy because the information that providers need to know will be accessible when and where it is needed (in contrast to the existing situation with paper-based records). The aim is to ensure that information is used to help consumers receive the best possible care. Building such a network will be a challenging task, not just because of the complexity of modern health care practice but also because consumers will demand control over their personal health information, including that it is only made available to authorised people on a need-to-know basis and that their privacy and dignity is respected at all times.

Box 13.2: Scenarios illustrating where additional expenditures may result due to insufficient information on admission

Emergencies (with HINA)

A 23 year old male is brought to hospital by ambulance, having been found in an unconscious state after a motor vehicle accident. He is carrying his driving license but no other identification. The resident doctor accesses HINA using the patient's name combined with his sex and apparent age. The doctor must over-ride security to gain access to this record — a routine audit will be generated by the system to confirm the appropriateness of this action. On examining the patient's file, the doctor discovers that the patient is diabetic and has recently changed his medication regime. The patient is treated for hypoglycaemia at once. A large number of alternative provisional diagnoses are eliminated and the associated cost of (irrelevant) investigations avoided.

Surveillance and post-market evaluation

A patient presents to her general practitioner with joint pain. The general practitioner notes the symptoms in the patient's record and, suspecting rheumatoid arthritis, orders the appropriate tests.

At the Department of Health, a routine post-market investigation is being conducted to examine the effects of a new cardiovascular drug released one year previously. It is noted that a large number of patients who were commenced on this drug have been tested for rheumatoid arthritis. Further investigation is conducted by examining the records of all patients who have been prescribed the drug and it is found that all patients with the symptoms were also taking another well-established drug. Thus an unusual drug interaction is revealed that would not otherwise have been detected.

Tracking (with HINA)

When a problem is detected with a particular medical device, intervention or drug, it is currently exceptionally difficult to determine who has been exposed. Several examples of this situation have occurred in Australia, probably the best known is the case of the Bjork-Shiley CC heart valve which was used here and in the US in the 1980s. The Shiley Research Centre was established to track those patients who had received the problem valves as no systematic registry exists. Three years of detective work discovered only 85 per cent of the valves that were known to have been imported. Thirteen Australian patients died from catastrophic failure of the prosthesis.[56] A similar challenging and highly costly scenario occurred in Australia when an association was detected between the use of pituitary hormones in the 1970s and the later development of Creutzfeld Jacob Disease.[57]

With a HINA in place, the establishment and management of a national product registry for all medical devices would be automatic. It would also be possible rapidly and cheaply to determine who had used a particular drug, or had received a certain surgical treatment. The present fragmented system of medical records provides a less efficient mechanism for product recall than is available in the automobile industry.

Large savings can be made if problems with treatments are detected early. An example of how a registry system can work is provided by the Christiansen hip prosthesis case. The early failure of this device was noted through examination of the Swedish national hip registry. Over the border in Norway, the problem had not been detected by an incident reporting system similar to the one that exists in Australia.[58] Twenty seven million dollars had been spent on the actual prostheses — a much greater amount would be required to allow for their early replacement. A more recent example is the 3M Capital hip implant, which was discovered in the UK to have a failure rate at five years of four times the expected rate.[59] A Hazard Alert was issued by the Medical Devices Agency that required up to 5,000 Capital hip patients to be reviewed for replacement.[60]

---

[56] Callaway A(1997), *Post Implant Patient/Valve. Tracking. In: Section MD, editor. A Program for the Tracking of Implantable Medical Devices*, TGA, Canberra.

[57] Lazarus L (1985), *Suspension of the Australian human pituitary hormone programme* (editorial). Med J Aust, 143(2):57-9.

[58] Ohlin A (1990), *Failure of the Christiansen hip. Survival analysis of 265 cases*. Acta Orthop Scand, 61(1):7-11.

[59] Muirhead-Allwood SK (1998), 'Lessons of a hip failure,' (editorial; comment) (see comments). BMJ, 316(7132):644.

[60] Medical Devices Agency (1998), Hazard Report: 3M Capital Hip System, Report No.: HN9801, London.

Deleted: '
Formatted
Deleted: '
Deleted: '
Formatted
Deleted: '

13.2 Costing HINA

Independent consultants were commissioned by the Taskforce to cost the development of the HINA. They were asked to prepare an indicative costing and, accordingly, further refinement of the costing model and assumptions may be necessary.

The result of the costing work is described in Appendix G and summarised below. It covers the following components.

- Governance — this includes the creation of a unit within the Department of Health and Aged Care to coordinate and manage the development activity and oversee the operation of the network.
- Development costs — these include the creation of the key building blocks including privacy, security, standards, work on the test bed, community liaison, public key infrastructure and support for the uptake of information technology.
- Implementation costs — these include the purchase of the hardware, software and accommodation for the data centres as well as staff and communications costs to operate the centres.

Indications are that, for a relatively small investment of the order of $120 million over 10 years, much in the way of the governance and the building blocks can be developed. This would include: privacy, confidentiality, security and authentication, standards development, a telecommunications strategy, uptake of technology and community liaison — as well as the development of the lead implementation site(s) and communications strategy.

The establishment and operation of the information storage facilities, communications costs and investment in source systems would bring the Network into full operation (takeup rate estimated to be in the order of 80% by year 10), and by then the savings would be expected to be clearly evident. The all-up costs, currently estimated to be in the order of $430 million over 10 years, would be more than offset by measurable savings by that time (see previous section). Costs will also need to be apportioned because the costers have provided a full system cost. That is, costs will need to be attributed to the private sector and to the public sector on an agreed Commonwealth/State cost-shared basis.

Recommendation:

That Health Ministers agree:

21 to set in train further work, in co-operation with other jurisdictions, to further refine the likely costs of HINA, given the uncertainties that necessarily attach to the costing exercise that has been possible for this report (eg in terms of what infrastructure is already in place, or in prospect, which HINA can use).

13.3 Risk management

As indicated above, the costing prepared for the Taskforce is indicative. It is therefore important to consider where there are risks, particularly of an underestimate nature, but more generally of possible threats to the integrity of the estimates. As far as possible, the Taskforce has endeavoured to isolate possible threats or risks to the project costs. The main risks the Taskforce has identified are:

- Additional storage may be required due to an underestimation of the size of the event summaries (currently based on a standard 4 kilobytes for general practice consultation event summaries), or the number of summaries generated and supplied.
- Processing capacity may have been underestimated.
- People may join the system at a higher rate than expected — although this would only affect the steepness of the cost curve in the early years (the cost model assumes take-up will approximate 80 per cent by year 10).
- The staffing level assumptions may be inadequate.
- Owners of source systems may be unable or unwilling to participate without an injection of capital to upgrade their computer systems or incentives to encourage their contribution of information to the network.
- The network may require significant re-design work.
- There may in the end be insufficient benefits realised, possibly through a slower than expected take-up rate.

Having identified these risks, the Taskforce has also built into the Network design a mechanism for their management. Basically this rests on the staged implementation approach discussed in Chapter 12. Staged implementation allows for the review of costs and performance at key stages in the project. A staged approach will also allow for the opportunity to assess the political, financial and technical risks and make appropriate changes to the project, as the Network is built.

However, the key to cost risk management is the lead implementation site. The lead implementation project will establish all components of the Network in one location (or in a number of satellite sites) and in doing so will encounter all the issues raised above — without having to commit the major investment of the

Network. The lead implementation project will test whether the storage estimates are accurate, it will monitor take-up rates, it will assess source system capabilities etc. The lessons learnt in the lead implementation project will allow project costs to be revised, and adjustments to be made to the design itself. It is for this reason that the Taskforce believes that while in-principle agreement to establish the network should be recommended to Health Ministers, funding and commitment should only be to the first stage of development. Subsequent funding should be dependent on satisfactory completion of each stage as the project is implemented.

Recommendation:

That Health Ministers agree:

22 to commit resources (on an agreed Commonwealth, State and Territory cost-share basis) to the first stage of implementation, with a review of the network's value for money after two years.

GLOSSARY

Access Control	A process that determines who is given access to a local or remote computer system or network, as well as what and how much information someone can receive.
Asymmetric key	Also referred to as public key or two key encryption. A method of encryption in which different keys are used to encrypt and decrypt. The keys are mathematically related but it is not possible to infer one from the other. One key may be made public and the other kept private, allowing Smith to encrypt and send a message to Jones using Jones' public key and Jones to decrypt it using her private key. With RSA (see below) either key can be used to encrypt as long as the other is used to decrypt, but anyone with access to Jones' cyphertext can decrypt her messages because her public key is known.
Authentication	In computer security, the act of identifying or verifying the eligibility of a station, originator or individual to access specific categories of information. In data security, a measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station or originator. In data security, processes that ensure everything about a teleprocessing transaction is genuine and that the message has not been altered or corrupted in transmission. In computer security, the process that verifies the identity of an individual as established by an identification process. In data security and data communications, both the prevention of undetected alteration to data and peer entity (mutual verification of each other's identities by communicating parties) authentication. A process verifying that users are who they say they are. An example of authentication is requiring users to identify themselves with a password.
Authorisation	The process that grants access to a local or remote computer system, network or to online information.
Bandwidth	The amount of data that can pass through a given communications channel in a standard amount of time (usually per second). An indication of the capacity of the network’s 'pipes'.
Broadband	Term used to describe a network that can transmit a wide range of signals, including audio and video. Broadband networks are especially useful in the 'networked world', as they can carry many signals at once, resulting in faster data transmission.

Certificate	A set of information which, at least, identifies the certification authority issuing the information; unambiguously names or identifies the owner; contains the owner's public key; and is digitally signed by the certification authority issuing the certificate.
Certifying authority/Certificate Authority (CA)	An entity that verifies the identity of another entity, allocates a unique name to that entity and verifies the correctness of information concerning that entity by signing a public key certificate for that entity. The entity or service that distributes electronic keys for encrypting information and electronic certificates for authenticating user and server identities. Identifies VPN users by authentication or certification. The CA issues certificates (usually based on X.509 public key encryption) to other devices requesting them, similar to how a person's driver's licence is requested for ID when he or she uses a credit card.
Confidentiality	Confidentiality protects the privacy of information being exchanged between communicating parties.
Digital Certificates	A public-key directory entry that has been "signed" or validated by a certification authority. Digital certificates are used to verify digital signatures.
Digital Signature	A coded message added to a document or data that guarantees the identity of the sender.
Client	A computer or software that requests a service of another computer system or process (a "server"). For example, a workstation requesting the content of a file from a file server is a client of the file server.
Confidentiality	In computer security, a concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for such data about individuals as well as organisations.
Cryptography	The art or science that treats of the principles, means and methods for rendering plaintext unintelligible and for converting encrypted messages into intelligible form.
Decryption	The conversion of cyphertext into its plaintext equivalent by use of the appropriate key.
DES (Data Encryption Standard)	The Data Encryption Standard (DES) specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of computer data. It became mandatory for US Federal agencies in June 1977. The algorithm is public but the design principles remain classified. DES uses a 56-bit key and encodes text in 64-bit blocks. A standard encryption technique that translates data into an unbreakable code for public transmission. It uses a binary number as the encryption key. This key, preferably chosen randomly for each session, is used to create the encryption pattern.
Digital signature	A digital signature is a technique or procedure for the sender of a message to attach additional data to that message which forms a unique and unforgeable

	identifier of the sender and the message.
EDI (Electronic Data Interchange)	A set of standards for exchanging orders and other business transactions by electronic format. EDI is often supported by Value Added Networks (VANs).
e-mail (electronic mail)	The method by which computer users can exchange messages with each other over a network.
Encryption	Transformation of data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption). Process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The manipulation, or encoding, of information to prevent anyone other than the intended recipient from reading the information. There are many types of encryption, and they are the basis of network security.
Firewall (or proxy server)	Usually an enhanced router, this VPN device (*q.v.*) restricts access to and from the Internet similar to the way a RAS screens dial-in users (*q.v.*). A server or collection of components that supervises all traffic in and out of a network, permitting only traffic which is authorised by local security policy to pass.
Hacking	The act of gaining unauthorised access to a computer network by defeating the system's access controls. The act is often compounded by one or more offences relating to breaches of confidentiality, privacy, national security, altering or erasing data, intellectual property and commercial interests.
Hash Code	A unique, mathematical summary or "fingerprint" of a document that serves to identify the document and its exact contents. Any change in the hash code is an alert that the document's contents have been altered.
Health Care: Primary, Secondary, Tertiary, and Quaternary	Primary health care is the first point of contact between a patient and the health care system, usually with a general practitioner (GP). Secondary health care is specialist care, typically following referral from a primary health care provider. Tertiary care is provided by specialised hospitals equipped with diagnostic and treatment facilities not available at general hospitals or by doctors who are uniquely qualified to treat unusual disorders that do not respond to therapy that is available at secondary care centres. Acute care refers to medical and surgical treatment and care mainly provided in hospitals.
Health Care Data (and specialised sub-	At its most fundamental level, health care data includes basic medical and clinical patient records and the ancillary data linked to them, such as family history, laboratory, pathology, imaging, prescribing, pharmacy, interview,

sets of such data)	and therapy data. Almost all such data can be recorded in digital form and processed electronically. Health care administrative data (eg eligibility, admissions and discharge data; routine operational data; and insurance and financial transactional data). For such purposes as management, payment, and auditing, these are processed and stored in many institutions beyond clinical settings. Population-based public health data (birth, death, abortion, and other vital records; screening and disease- monitoring data; many health- services data; and registries concerning such matters as infectious diseases, cancer, birth defects, vaccination, implanted medical devices, and genomics). Primary research and technical regulatory data (basic research data; data collected in health services, outcomes, economics, and other studies; and clinical trial, drug safety surveillance, and other data generated to support product and service development and market authorisation). Research is, of course, performed on data collected specifically for the purpose, but research can also be performed on any health related data. Detailed patient- level cost data may, for example, be studied in economic analyses.
Identification of consumers, providers, locations/facilities and devices	A person identifier is a universal code that uniquely identifies each individual within the health system. Such an identifier can be simply assigned or based on some unique characteristic of the individual (called biometric identification). Similarly providers, facilities, individual devices and the location of the point of care may all have to be capable of unequivocal identification to guarantee the integrity of a system of electronic health records.
Information and communication technologies (ICTs)	Seen as the building blocks of the 'networked world', ICTs include telecommunications technologies (such as telephony, cable, satellite and radio) as well as digital technologies (such as computers, information networks and software).
Integrity	Integrity involves protection of data from corruption, destruction, or unauthorised changes. Similarly, the configurations and basic integrity of servers, applications, and other network components must also be protected.
Internet	The Internet is behind much of the explosive growth in data communications. Often characterised as a *network of networks*, the Internet is a set of protocols for enabling computers to connect and communicate with each other. Viewed in another way, it is like a communications platform that enables a range of other, Internet-specific programs to run. A major stimulus to much of this Internet growth in recent years has been the development of the hypertext transport protocol (HTTP) and the easy-to-use web browsers that emerged to exploit it. Indeed, so ubiquitous is web-browsing-based Internet usage that for many people the Internet and the World Wide Web are synonymous. Indeed, given the ability of web-browsers to emulate a wide range of more function-

	specific client programs (eg e-mail), many other Internet programs have, fact, been absorbed into browser-based functions.(Source: National Bandwidth Inquiry Report (1999), Australian Information Economy Advisory Council (T. Cutler, Chair), Commonwealth of Australia. Document available at http://www.dcita.gov.au (pp.10-11). The Internet was not originally designed with businesses in mind. It lacks the technology required for secure business communications and transactions. A worldwide system of computer networks. Networks connected through the Internet use a particular set of communication standards, known as TCP/IP, to communicate.
Intranet	A network which is internal to an organisation which uses Internet technology to communicate and share information.
Key	A key is a number, whose size is expressed as a number of bits in binary arithmetic (eg 56-bit).
Key Distribution	Public keys can be distributed freely through listing on a bulletin board or via a directory. Public key encryption depends on confidence the public keys are correct. Users need to be assured they have valid keys for other people and keys need to be provided/copied by dependable means.
Key Length	The size of a key and measure of its strength. In simplistic terms a 40/384-bit secret/public key system may be classified as weak, a 56/512-bit system as borderline: and an 80/1024-bit system as strong.
Network	In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub-networks.
Nodes	In a network, a node is a connection point, either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognise and process or forward transmissions to other nodes.
Non-repudiation	For a business transaction to be valid, neither party can later deny the existence or execution of that transaction. Use of digital signatures is growing in practice and in legal acceptance as a means of protecting transactions from later dispute.
Plain Text	Data or a message in ordinary language or format, which can be understood by a person or a computer
Private-Key Security	Also known as symmetric-key security, this method is based on both parties having the same encryption key, as in secret-key cryptography. The client and server share a key to encrypt and decrypt information on a network.
Public Key	A Public Key Authentication Framework would allow for the establishment

Authentification Framework (PKAF)	of a trusted public key system, allowing any entity to determine the trust and validity of a public key certificate claimed to be associated with another entity. The proposal was prepared by the PKAF Task Group, formed by Standards Australia from representatives of industry and government.
Public Key Infrastructure (PKI)	Public Key Infrastructure is a set of servers, software, protocols and application programs used to manage the Private Key's and Public Key's of a group of users. Users are generally able to create and update their own key pairs, and a Certificate Authority is used to sign new Public Key's. Some mechanism is made available by which users may conveniently and reliably retrieve and use their own Private Key's and other users' Public Key's.
Public-Key Security	Also known as asymmetric-key security or public-key encryption technology, this is a mechanism for securely distributing encryption keys that are used to "lock" and "unlock" data across an unsecured path. Public-key security is based on encryption key pairs, in contrast to methods based on having a single, shared key, as with private-key security.
Remote access server (RAS)	The VPN server for the remote access switch client. The RAS contains all the authentication (logon identification [ID] and password, for example), authorisation and accounting information about a remote user. The RAS always verifies this authentification, authorisation, and accounting (AAA) information from the remote access switch client before granting permission to access the public LAN.
Router	A computer that controls traffic on a network.
Server	A computer or software that provides resources, such as files or other information, to client software running on other computers.
Symmetric key	A method of encryption in which the same key is used to encrypt as to decrypt. Also referred to as secret key or single key encryption. This sort of encryption is used in telephone scramblers. The key length can be varied for different levels of protection. It is a much faster process than using asymmetric keys.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	The suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of world-wide internetworks. Today, millions of users are connected to the Internet via software which uses the TCP/IP Internetworking Protocol suite.
Trusted third party	An entity providing user services ranging from the provision of authentication services such as the verification of a client's public key, time stamping of documents, digital signatures and key retrieval services.
Tunnelling	Used to hide the true structure of the frame content, packet, or segment being

	transmitted.
Virtual private network (VPN)	A VPN is a data network that adds certain quality-of-service features — at least privacy and security — to the Internet. An Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. However, it includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system.
WWW (World-Wide Web, “the Web”)	A client/server system for finding and retrieving Internet information. To access the Web, you run a browser program, which can get documents from sources all over the world. Browsers usually can also search documents and databases. The documents the browsers display include hypertexts, which are documents that include highlighted cross-references (or links) to other documents. Select a link and the document to which it is pointed is displayed. The document can be text, graphics, sound, video or other multimedia formats.

REFERENCES

Australian Bureau of Statistics (ABS 1998), *Population Projections: 1997 to 2051*, Cat. no. 3222.0, Canberra.

Australian Institute of Health and Welfare (AIHW 1999), *Health Expenditure Bulletin No. 15: Australia's Health Services Expenditure to 1997-98*, AIHW Cat. no. HWE 13, Canberra.

Banks NJ and Paliney RH (1990), 'Clinical Reminders in Ambulatory Care,' HMO Practice, Vol 4, No. 4, pp.131-6.

Barnett GO (1984), 'The Application of Computer-based Medical Record System in Ambulatory Practice,' N Engl J Med, Vol 81.

Callaway A (1997), *Post Implant Patient/Valve. Tracking. In: Section MD, editor. A Program for the Tracking of Implantable Medical Devices*, TGA, Canberra.

Carter M (1998), 'Should patients have access to the medical records?', MJA (vol. 169) p.596.

Computer-based Patient Record Institute (CPRI 1996), Work Group on CPR Description, Framework for Definition and Modeling of the Computer-based Patient Record, Bethesda, MD.

Dick RS and Steen EB (1993), eds, *The Computer-Based Patient Record*, Institute of Medicine, National Academy Press, Washington. A revised edition was released in 1997.

Heard S *et al.* (2000), 'The benefits and difficulties of introducing a national approach to electronic health records in Australia', specially commissioned study (see Appendix B).

House of Representatives Standing Committee on Family and Community Affairs (1997), *Health on Line: A Report on Health Information Management and Telemedicine*, AGPS, Canberra.

Kohn LT, Corrigan JM, Donaldson MS (1999), eds. *To err is human, Building a safer health system*, National Academy Press, Washington DC.

Kelman CW (2000), *The Australian National Death Index*, Australian and New Zealand Journal of Public Health, 24-2 p91-2.

Lazarus L (1985), 'Suspension of the Australian human pituitary hormone programme,' (editorial). Med J Aust, 143(2):57-9.

Leape LL (1994), 'Error in medicine', JAMA 272:1851-57.

Lowrance Dr WW (OECD 1999), 'Scoping study for an OECD project on data protection in transborder flows of health research data,' DSTI/STP/BIO(99)3.

Medical Devices Agency (1998), Hazard Report: 3M Capital Hip System, Report No.: HN9801, London.

Millensen ML (1997), *Demanding Medical Excellence*, University of Chicago Press.

Mount CD, Kelman CW, Smith LR, Douglas RM (2000) An integrated electronic health record and information system for Australia? MJA 172:25-7.

Muirhead-Allwood SK (1998), 'Lessons of a hip failure,' (editorial; comment) (see comments). BMJ, 316(7132):644.

Murphy GF, Hanken MA and Waters KA (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia.

Murphy K and Topel R (2000), *Exceptional Returns: The Economic Value of America's Investment in Medical Research*, University of Chicago Business School.

National Bandwidth Inquiry(1999), Report of the Australian Information Economy Advisory Council, Commonwealth of Australia, AGPS.

National Health Information Management Advisory Council (NHIMAC 1999), *Health Online: A Health Information Action Plan for Australia*, Commonwealth of Australia, Canberra.

National Health Service (NHS) Executive (NHS 1998), *Information for Health: An Information Strategy for the Modern NHS 1998-2005*, HMSO, London.

National Standards Policy Advisory Committee (1978), *National Policy on Standards for the United States and a Recommended Implementation Plan*, Washington DC.

New Zealand Health Information Service (NZHIS 1995), Electronic Health Records, 2nd edn.

NSW Health (1999), Ethical Management of Health Information, discussion paper.

Ohlin A (1990), 'Failure of the Christiansen hip. Survival analysis of 265 cases, ' Acta Orthop Scand, 61(1):7-11.

Powsner, Wyatt and Wright (1998), 'Opportunities for and challenges of computerisation', The Lancet vol 352, 14 Nov, p.1617.

Report of the NSW Health Council (2000), *A Better Health System for NSW*, NSW Government.

Tang PC and Hammond WE (1997), 'A progress report on computer-based patient records in the United States', in *The Computer-based Patient Record: An Essential Technology for Health Care*, rev edn, National Academy Press, Washington DC.

US Department of Health and Human Services (1998) *Unique Health Identifier for Individuals: A White Paper*, Washington DC.

Wilson RM Runciman WB Gibberd RW Harrison BT Newby L Hamilton JD (1995), 'The Quality in Australian Health Care Study,'. Med J Aust, 163(9):458-71.

PART D

APPENDIXES

A CONDUCT OF THE INQUIRY

A1 Establishment of the Taskforce and its terms of reference

With the agreement of other Australian Health Ministers, Taskforce members were appointed as a sub-committee of the National Health Information Management Advisory Council (NHIMAC) by the federal Health Minister with the terms of reference set out on page iii of the report. Members of the National Electronic Health Record Taskforce met for the first time on 30 November 1999 and convened six times in all to finalise their report to Health Ministers via NHIMAC.

A2 Conduct of the inquiry

The Taskforce released an Issues Paper on 21 March 2000 and held public meetings to discuss issues raised by the terms of reference in all States and Territories except Tasmania and the Northern Territory. These meetings were held over the period 6-11 April 2000.

The Taskforce also called for written submissions, placing a notice in the Weekend Australian, the Sydney Morning Herald, the Canberra Times, the Age, the Brisbane Courier Mail, the Adelaide Advertiser, the West Australian, the Burnie Advocate, the Hobart Mercury and the Northern Territory News on 18 March 2000, with a deadline of 17 April 2000. As of 16 May 2000, 94 submissions had been received. Summaries of the mains points made in the meetings and in submissions appear in Chapter 8 of the report and the intention is to make written submissions available on the *Health Online* Website (www.health.gov.au/healthonline) as soon as practicable (with the agreement of those responsible for submissions).

A3 Public meetings and submissions received

Details of meetings and written submissions received are set out below.

LOCATION	DATE
Sydney	6 April 2000
Melbourne	10 April 2000
Brisbane	11 April 2000
Adelaide	6 April 2000
Perth	7 April 2000
Canberra	10 April 2000

NAME OF PERSON/ORGANISATION MAKING SUBMISSION	SUBMISSION NUMBER
Dr Gerard Flaherty, University of Tasmania	1
Women's Health Victoria (WHV)	2
Bayside Health Service District - Queensland Health	3
St John of God Health care, WA	4
General Practice Divisions of WA	5
Top End Division of General Practice	6
Intech	7
Peter MacCallum Cancer Institute	8
Dr Merelie Hall (personal submission)	9
Canterbury Division of General Practice Ltd	10
King Edward Memorial & Princess Margaret Hospitals, WA	11
Association of Professional Engineers, Scientists and Managers (APESMA) Australia, Pharmacists Branch	12
Associate Professor Jim Warren, University of South Australia	13
CRC for Distributed Systems & Technology and Centre for Online Health, University of Queensland	14
Caroline Chisholm Centre for Health Ethics Inc	15
United Medical Protection	16
Collaborative Health Informatics Centre	17
The Society of Hospital Pharmacists of Australia	18
Dr Milana Votrubec, The University of Sydney (personal submission)	19
Health Informatics Society of Australia (ACT)	20
Australian Red Cross Blood Service (SA)	21
The Royal Australian and New Zealand College of Obstetricians and Gynaecologists	22
Tasmanian General Practice Divisions Ltd	23
Medical Software Industry Association (MSIA)	24

NAME OF PERSON/ORGANISATION MAKING SUBMISSION	SUBMISSION NUMBER
Royal Australasian College of Surgeons	25
Pathology Consultative Committee	26
Resolutions (Qld) Pty Ltd	27
IBA Technologies Ltd	28
Health Communication Network	29
Hornsby Ku-ring-gai Ryde Division of General Practice Ltd	30
Docle Systems P/L	31
National Resource Centre for Consumer Participation in Health	32
General Practice Divisions Victoria	33
InfoCARE WA	34
Westgate Division of Family Medicine	35
QPSX Communications	36
National Centre for Classification in Health	37
Health Care Complaints Commission	38
South Burnett Health Service District	39
Dietitians Association of Australia	40
Brisbane North Division of General Practice	41
Josephine Holman, Manager Medical Records, Gold Coast Health Service District (personal submission)	42
Cerner Corporation	43
Centre for General Practice Integration Studies, School of Community Medicine, University of New South Wales	44
Verinet Solutions	45
Dr Tom Hartley, Senior Scientist, Pathology IT Group, Royal Hobart Hospital	46
Mr Stan Stanfield and Ms Ferne Panambalana (private submission)	47
Staff of the Bachelor of Health Information Management, School of Public Health, La Trobe University	48
Office of the Federal Privacy Commissioner	49

NAME OF PERSON/ORGANISATION MAKING SUBMISSION	SUBMISSION NUMBER
Clinical Services, Ballarat Health Services	50
Mr Len W. Ashby, DMR Consulting	51
The New Children's Hospital, NSW	52
B2G.com Ltd	53
Australian Health care Association	54
Mr Michael Harvey (personal submission)	55
National Allied Health Casemix Committee	56
Health Informatics Association of NSW	57
Price Waterhouse Coopers	58
Health Issues Centre	59
Health Technologies Pty Ltd	60
Central Australian Division of GPs	61
Globix Telemovers	62
Territory Health Services, NT	63
General Practice Computing Group	65
Attorney-General's Department	66
Health Department of Western Australia	67
National Centre for Epidemiology and Population Health	68
National Informatics Committee, The Royal Australian College of General Practitioners	69
ISOFT	70
Health Information Management Association of Australia Ltd	71
Information and Business Management Branch, Queensland Health	72
Public Health Services – Queensland Health	73
Professor Beth Reid, School of Health Information Management, University of Sydney	74
Mr Doug Golley Director, Information Service, and Ms Bev Bowen, Manager, Medical Record Service, Flinders Medical Centre (personal submission)	75
Dr Ross White	76

NAME OF PERSON/ORGANISATION MAKING SUBMISSION	SUBMISSION NUMBER
Federation Health	77
Inner South East Melbourne Division of General Practice	78
Department of Veterans' Affairs	79
Allegiance Systems	80
Committee of Presidents of Medical Colleges	81
Australian and New Zealand College of Anaesthetists	82
Redcliffe-Caboolture Health Service District – Queensland Health	83
Royal College of Nursing Australia	84
Allmed Sun RHE Alliance	85
Australian Physiotherapy Association	86
Health Insurance Commission	87
NSW Health	88
Medical Benefits Fund (MBF)	89
Victorian Department of Human Services	90
Consumers' Health Forum	91
Dr R. T. Bright (personal submission)	92
South Western Sydney Area Health Service	93
Mr Ronan Herlihy (personal submission)	94

B COMMISSIONED STUDY ON THE BENEFITS AND DIFFICULTIES OF INTRODUCING A NATIONAL APPROACH TO ELECTRONIC HEALTH RECORDS IN AUSTRALIA

C ISSUES PAPER

The Taskforce released the following Issues Paper on 21 March 2000 seeking public input on the many issues raised by its terms of reference (see p.ii of the report). As of 16 May 2000, 93 submissions had been received.

The Taskforce gratefully acknowledges the time and effort people went to in order to contribute their ideas on a system of electronic health records for Australia, especially in view of the short period available for canvassing views for incorporation in this report.

Issues Paper

A National Approach to Electronic Health Records for Australia

March 2000

NATIONAL ELECTRONIC HEALTH RECORDS TASKFORCE

FOREWORD

The health sector is on the threshold of great changes as a result of new and evolving information technologies and their power to transform the way health care is delivered and, indeed, the very nature of the industry. Consumers will be the big beneficiaries of this health care revolution, as new techniques are brought to bear to secure improved health outcomes for consumers and to improve the quality of that care.

Yet we run a risk that, unless we can build on the myriad of initiatives currently underway or on the drawing board in every State and Territory, and across the public and private sectors, we may well end up paying the price of substantial duplication and wastage of resources nationally.

In November 1999, the National Health Information Management Advisory Council (NHIMAC) released *"Health Online: A Health Information Action Plan for Australia"*. *Health Online* is a national strategy for information management and the use of online technologies within the health sector, and also spells out a series of action plans for nationally significant projects. *Health Online* attempts to map where we should be going in terms of our use of health information, and describes the steps Australia needs to take to get there.

One of the key recommendations in *Health Online* is the development of a national framework for the use of electronic health records. Increasingly, the ability of electronic health records to improve the efficiency, safety and quality of care compared with paper-based systems is being recognised across the health sector.

The National Electronic Health Records Taskforce was established to develop a national framework for a system of electronic health records in Australia. Underpinning the work of the Taskforce is a commitment to ensuring that a robust framework is created to protect the privacy of personal health information. This is because personal health information is extremely sensitive and consumers need to be confident that their information is valued, that their privacy will be respected, and such information will be used to both improve their own health or that of the public at large.

On behalf of the Taskforce, I would invite you to make a submission to the Taskforce on issues relating to or raised by a national approach to electronic health records in Australia. Your views will help inform the Taskforce in terms of its recommendations to Australian Health Ministers in July this year. I encourage you to read this paper and respond to any or all of the issues raised (or other issues you believe to be relevant to the work of the Taskforce).

Lynelle Briggs
Chair, National Electronic Health Records Taskforce
March 2000

HOW TO RESPOND TO THIS PAPER

Submissions responding to the questions or raising important issues that are not canvassed in this paper, may be made by:

- Writing to 'The NHIMAC Secretariat', Department of Health and Aged Care, MDP 12, GPO Box 9848, Canberra ACT 2601:

or

- Sending an email to mailto:NHIMAC.secretariat@health.gov.au

or

- By Fax to (02) 6289 4083 marked 'Attn: Chris Mount'

Should you have any queries, please phone (02) 6289 7418

The closing date for submissions is **Friday, 21st April 2000**.

CONTENTS

THE NATIONAL ELECTRONIC HEALTH RECORDS TASKFORCE

A key underlying imperative in the development of a system of electronic health records in Australia is for there to be consistency of approaches to information management across Commonwealth, State and Territory jurisdictions, in both the public and private sectors, and across health care settings (eg acute, primary and community).

The establishment of a National Electronic Health Records Taskforce was included as a recommendation in *Health Online – A Health Information Action Plan for Australia* as a way of bringing a coordinated approach to electronic health record systems and to avoid the potential for duplication and incompatible systems. Electronic health record systems are complicated, especially if a national approach is taken. In this context, it is particularly necessary to have a clear idea about what direction to take and what to develop.

The Taskforce was established in November 1999 under the auspice of the National Health Information Management Advisory Council (NHIMAC).

The objectives of the Taskforce are to:

- develop the framework for a national electronic health records system; and
- recommend a way ahead to Australian Health Ministers in sufficient detail to enable them to make decisions and commit resources.

Terms of Reference

The Taskforce's terms of reference are to:

(1) Evaluate the benefits and difficulties of introducing a national approach to electronic health records that respects the dignity of each health consumer and allows them to enjoy improved health outcomes delivered more effectively.

(2) Consult widely with stakeholders to identify the form and key components of electronic health records suitable for Australia.

(3) Develop specifications (including the functions – administrative, clinical and policy/planning uses – core data items etc) for the key components of electronic health records, drawing on work in progress and seeking advice from relevant sources.

(4) Describe the building blocks that will need to be put in place to enable electronic health records to operate (such as issues concerning record linkage, security/authentication, telecommunications, messaging, imaging standards and coding)

(5) Review progress that has already been achieved, define the additional work program that needs to be undertaken and determine who should undertake the work, including, where necessary, the creation of new working partnerships

- to develop and implement the key components of electronic health records;
- to develop and establish the building blocks that will underpin the operation of electronic health records; and
- to define the implementation and ongoing governance arrangements for electronic health records.

(6) Develop a plan, nominate priorities and provide a timetable to develop electronic health records in Australia.

(7) Cost the plan and provide an indicative timetable.

(8) Report to Health Ministers by July 2000, recommending a way ahead for the development of nationally consistent electronic health records for Australia.

Guiding Principles

The following guiding principles are taken from *Health Online* and are being used for planning the way ahead:

- Consumers, providers and managers are encouraged to innovate in appropriate use of information and communication tools;
- Information which is collected about individual health consumers is transferred and used with their knowledge and authority;
- Information needed for research, policy and planning purposes should be generated as a by-product of operational systems primarily designed for other purposes (eg to achieve better health outcomes for individuals and groups, or to organise payments);
- Health consumers and providers are engaged at all stages of planning and development of new information services;
- The public and individual interests will be protected — particularly in relation to privacy;
- Governments should concern themselves with leadership, direction setting, and providing encouragement to the private sector, health providers and consumers to participate fully in the information economy;
- Planning and coordination should be undertaken at the national level to ensure a high level of coherence and consistency, and to eliminate duplication and waste;
- The costs and benefits of proposals to improve information management are assessed to ensure a value for money approach to investment.

BACKGROUND

Currently, the majority of health care records in Australia exist as discrete paper-based entities held at a variety of different locations, resulting in a fragmented picture of individuals' health needs and health histories. Increasingly, the potential for electronic health records to improve efficiency, safety and quality of care over paper-based systems is being recognised across the health sector. An analogy would, perhaps, be a jigsaw puzzle where it is not possible to begin because some — if not most — of the pieces are missing (the paper-based world) compared with the puzzle being able to be solved in a flash because not only are all the pieces readily available but the way to fit them together is already known (the world of electronic health records).

Access to appropriate information at the time of care delivery is central to good clinical decision making – practitioners and consumers need the right information at the right time. An increasing focus on striving for 'seamless delivery of care', particularly for the frail aged, the chronically ill and others with complex care needs has highlighted the need to improve information exchange between health service providers. A reduced emphasis on hospitals in favour of community care (where this is appropriate) has also led to a wider range of services being utilised, often resulting in duplication of time and effort through repeat assessments and history-taking.

Thus, electronic records and transmission of personal health information can provide a powerful tool to link the isolated islands and fragments of information that currently exist between services and allow providers immediate access to essential clinical information. Integrated electronic health record systems will also provide consumers with the capacity to provide essential information about their health care to the providers of their choice at any time.

The potential benefits to health consumers and providers are substantial, including:

- reduced numbers of adverse events caused by lack of information about health consumers at the point of care;
- reduced duplication of diagnostic tests due to unavailability of previous test results;
- enhanced decision making for practitioners and consumers (and therefore increased quality of care and health outcomes) through online access to decision-support tools such as clinical practice guidelines, prescribing alerts the latest information on prevention, diagnoses, and treatment;
- greater coordination and integration of care across the care continuum through increased exchange of information between service providers in the health and community sectors;

- individual consumers being confident that, subject to appropriate privacy protection and their consent, regardless of where they seek or need health care, the health care professional treating them has full access to relevant clinical histories and treatment information. This will mean they don't have to go over the same questions and assessments each time they see a different provider; and
- efficiency gains through time saved in retrieving information and reduced duplication in ordering tests. Ordering of tests and treatments and arranging appointments and referrals can be substantially sped up with direct electronic requests. Data will be collected and made available more quickly, thereby increasing the time available for direct consumer care.

In addition, better clinical information has an important role in securing long-term benefits for all Australians through improved policy, planning and management of the health system.

Privacy

The Taskforce recognises that there are major issues to be dealt with in terms of privacy and security of information from both the perspective of providers and consumers. Health consumers must be satisfied that their personal health information is treated as being extremely sensitive and that it will be safeguarded from unauthorised access and that it will be used wisely not only in the interests of the individual to whom it relates but also in the interests of the community as a whole (eg in calculating immunisation rates).

General privacy issues are progressively being addressed in Australia and the Attorney-General intends to introduce data protection legislation for the private sector early this year. This legislation, based on the *National Principles for the Fair Handling of Personal Information* will, for the first time, provide a legislative framework to support and strengthen privacy protection in the private sector. It will set out guiding principles for the appropriate handling of personal information, including covering issues of access, collection, use and disclosure and complaints mechanisms.

In recognition of the especially sensitive nature of personal health information, the Attorney-General asked the Federal Privacy Commissioner to consult widely with the health sector on the application of the National Principles to health information. Subsequent to this consultation process, the Attorney-General has released the draft provisions of the legislation for public comment, to be followed by introduction to Parliament in early 2000.

State and Territory Health Ministers have also indicated a willingness to promote parallel legislation, based on the Commonwealth legislation. In addition, the Department of Health and Aged Care, the Office of the Privacy Commissioner and the Attorney-General's Department are working together to develop guidelines which will assist in the day-to-day application of the legislation to health information, and to promote the considered and strictly controlled use of such highly sensitive information.

PURPOSE OF THIS PAPER

The purpose of this paper is to seek input on issues that need to be addressed in any proposal for a national approach to electronic health records for Australia. The National Electronic Health Records Taskforce is inviting submissions from interested parties to help it in reporting to Health Ministers on this important subject.

This paper provides guidance on the issues that are currently being considered by the Taskforce. The paper includes five major sections, each of which contains a series of questions to which you might respond. The Sections are:

Section 1 — Objectives

Section 2 — Purposes

Section 3 — Uses

Section 4 — Structure

Section 5 — Pre-requisites – the 'Building Blocks'

You may also wish to raise other issues as part of your submission or provide more general comments. Your comments will contribute to the deliberations of the Taskforce before it makes its recommendations to Australian Health Ministers in July 2000.

What is an electronic health record?

The Taskforce considers an electronic health record to be:

> An electronic longitudinal collection of personal health information, usually based on the individual or family, entered or accepted by health care professionals which can be distributed over a number of sites or aggregated at a particular source, including a hand-held device. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of a known party.

SECTION 1: OBJECTIVES

A key first step in spelling out a national approach to electronic health records is to articulate the common objectives to be achieved. A suggested objective's statement is as follows:

Improved delivery of health care and better quality of care and health outcomes for all Australians by:

- *empowering consumers to be able to take a greater responsibility for their own health care;*
- *ensuring better decision-making by health providers at the point of care and at the right time;*
- *providing a more seamless and integrated process of care through the sharing and better exchange of information;*
- *building a better evidence based health system;*
- *having better, more targeted health policy;*
- *supporting research, learning and training;*

through the effective and innovative use of electronic health information.

Q. 1 What objectives do you think should be achieved through the introduction of a national approach to electronic health records?

Q. 2 What priority would you give to each of the objectives?

SECTION 2: PURPOSES

The health care record is an important tool supporting quality of clinical care. Just as there will be many different situations in which it is accessed, the record can play many roles in the provision of care to individuals and to the community as a whole (or sub-populations). The following six broad purposes have been identified for electronic health records:

Supports consumer involvement

- Protects personal privacy and security
- Supports cultural diversity
- Provides consumer view of information
- Accommodates consumer decision support and self care
- Ensures clinician accountability
- Accesses information for consumer

Supports consumer care

- Forms the basis of a historical account
- Anticipates future health problems and actions.
- Describes preventative measures
- Identifies deviations from expected trends
- Accommodates decision support

Supports communication

- Supports continuing, collaborative care and case management
- Accesses medical knowledge bases
- Allows automatic reports
- Supports email generation and electronic data interchange (EDI)
- Enables record transfer
- Enables record access when required
- Supports selective retrieval of information

Supports management and quality improvement

- Enhances the efficiency of health care professionals.
- Supports continuing professional assessment
- Facilitates management tasks and reduces routine reporting
- Demonstrates and improves cost-effective practice
- Accommodates future developments
- Provides a legal account of events
- Provides justification for actions and diagnoses

Supports population health care

- Supports policy development
- Provides evidence for development and evaluation of programs

Supports enquiry and learning

- Supports clinical research
- Assists with clinical audit
- Supports medical education

Q. 3 Do you think there are other purposes that electronic health records ought to satisfy?

Q. 4 Which of the purposes are most important?

Q. 5 Are any of the listed purposes unnecessary?

SECTION 3: USES

It is the uses to which electronic health records will be put that will determine whether or not the desired objectives are achieved. An understanding of the ways in which consumers, health providers and policy makers and administrators might use the information from electronic health records will assist the Taskforce to plan for a national approach.

There is no doubt that there are many potential uses of electronic health records. The more uses that are supported, the more complex will be any system required to deliver them. The Taskforce will need to come to a position on the range of uses that a national approach to electronic health records should support — too few and the costs may exceed the benefits, too many and the development of the system may take too long to justify the costs involved). The Taskforce will also have to consider whether any proposed use can satisfy the necessary privacy and security framework, (however some uses may be able to be satisfied through the use of encrypted, aggregated or de-identified data[61]).

The following list includes examples of uses ranging from immediate consumer safety through to planning and policy-making.

- A clinician in an emergency department checking the record of a consumer for potentially life-saving information on existing conditions, medications and allergies.
- Consumers looking up their treatment plan because they are unsure when they are due for a check up.
- A general practitioner calling up a summary of a person's health record to help with a new clinical decision.
- A pharmacist obtaining a list of medications prescribed for a consumer in order to dispense an appropriate drug.
- A public health professional obtaining data on communicable diseases in order to look for early signs of an outbreak.
- A planner using aggregated data to examine patterns of service use in a region to support decision-making on future service provision.
- A researcher using de-identified data to examine the relationship between a particular treatment and the subsequent health status of recipients of that treatment.

61 That is, personal health information where it is not possible to identify the individual to whom the information relates.

- A regulator monitoring for unexpected adverse events associated with a new medication or treatment.
- A policy-maker using aggregated data to inform the development of new policy initiatives.

Q. 6 What are some further uses you would like to suggest?

Q. 7 Which uses do you think are the most important?

SECTION 4: STRUCTURE

The preceding sections on Objectives, Purposes and Uses have focussed on the reasons for having electronic health records. This section considers the elements involved in implementing a national approach to electronic health records.

Record architecture

This section looks at the form and organisation of the data that might be held in electronic health records. The main issue is to determine what level of standardisation is required so that the data can be made available in the form required by consumers, health providers and policy makers and health care administrators. For example, if data were stored in an idiosyncratic fashion the desired objectives could not be met.

Data to be captured

Establishing what data electronic health records need to capture is an important starting point. The answer is ideally determined from the identified information needs of the electronic health record users. However, there are limits to the extent to which data can be captured, particularly given the range of providers and the amount of data that they capture for their own use.

Q. 8 What data should be captured?

Data standards

Data standards will be required in order to achieve any useful integration of data from different sources. Considerable work on data standards such as the National Health Data Dictionary, National Minimum Data Sets, classification and coding systems and the National Health Information Model and subsidiary data models have placed Australia in a good position to establish agreed national data standards. Are there any other types of data standards required? Is more work required in particular areas?

Q. 9 What data standards are required for a national approach to electronic health records?

Electronic health record architectures

Exchange of data and integration of different components of an individual's record would be greatly facilitated by the adoption of a standard record architecture by all health care providers. However, requiring the use of a single electronic health

record architecture may stifle innovation and impose unnecessary costs on information system developers and operators.
The Good Electronic Health Record and the HL7-XML (Kona) proposal are two examples of standard electronic health record architectures. Are there others that the Taskforce should consider? Which one would be the preferred option for Australia?
If a standard electronic health record architecture were not adopted nationwide what arrangements would be necessary to achieve the desired objectives?

Q. 10 Should a standard electronic health record architecture be adopted?

Q. 11 If so, which standard electronic health record architecture would be best suited for Australia?

Network architecture

This section considers the issues involved in the capture, storage and distribution of the data held in electronic health records.
For a national approach to electronic health records to be meaningful two assumptions need to be made: first, that most health providers will have electronic clinical record systems for their own use, and second that they will have the ability to transmit data electronically to other health providers and other relevant parties via a suitable communications network.
Realising these pre-requisites will take time and simply achieving them would result in considerable benefit in terms of the quality of health care. To support the development of a national approach to electronic health records this preliminary work would need to occur within an agreed national framework.

Data capture

If health care providers have their own electronic clinical record systems it would be easy to have them send agreed information as long as their systems conform to the agreed national data and record architecture requirements discussed earlier.
Consumers also have an interest in their health records. Some consumers, such as those with asthma or diabetes, take frequent physiological measurements that would be useful to their health care providers.

Q. 12 How should the network capture relevant data?

Q. 13 How could consumers contribute useful data to their own record?

Online storage

Currently, an individual's health data is largely scattered among different health care providers. This fragmentation makes the data difficult to access (if not simply

unavailable) for clinical care and other uses. Storing data online, that is in easily accessible form via a communication network, would make such potentially vital information more readily available to other health care providers, and consequently improve the utility of the data while at the same time creating potential security concerns.

Would it be possible to satisfy the objectives simply through improved communications and use of electronic clinical record systems by providers, thus avoiding the need for online storage of data? Could such an approach meet the information needs of consumers, clinicians, policy-makers, planners and researchers?

Q. 14 Should data be stored online?

Existing technology can support both centralised and distributed storage of data and make it available online. Are there any reasons to prefer one form to the other? For example, regionally based storage points might be more effective at supporting local needs compared to larger, centralised databases. Are there security or performance reasons for choosing one over the other?

Q. 15 Should any online storage be centralised or distributed?

If a distributed storage approach were to be adopted, it is necessary to consider where such stores should be located. There could be State and Territory and/or large regional based stores. Alternatively, data could be distributed by provider type with stores based at major provider organisations. Maybe it could simply be held on the provider's computers where it was first captured. Or it may be appropriate to adopt a combination of approaches.

Q. 16 If distributed storage technology were adopted where do you think those stores should be located?

Consumer-held electronic storage devices

The use of consumer-held electronic storage devices, such as smart cards, to support clinical decision making has been promoted by a number of groups. The use of smart cards has been trialed recently in Melbourne. The final evaluation report is being prepared currently. Initial indications are that consumers were supportive of them but that smart cards were not yet suitable for general use. Overseas experience, however, is more encouraging.

Q. 17 Would consumer-held electronic storage devices help meet the objectives?

Communication network technology

Electronic transmission of health messages can be achieved through a number of different technologies. The Internet, private and virtual private networks all offer a different mix of benefits and risks. In the context of a national approach to

electronic health records is there a reason for preferring one particular technology over another?

Q. 18 Is there a preferred communication network technology?

Access control

The issue of who should have access to records and under what circumstances is of understandable concern to consumers, and one that needs to be addressed within the context of measures aimed at protecting personal health information. The measures taken involve agreement on both the overarching principles of access control and the implementation of suitable systems that realise those principles. The later section on 'consumer consent and control of records' considers the principles of access control. This section addresses possible mechanisms whereby access could be controlled.

There are several elements to controlling access. First, the consumer must provide consent for access to occur. This requires the authentication of the consumer's identity to ensure that access is granted to the correct record. The consent then needs to be recorded by the system. Once a right of access is established the identity of the person accessing the record needs to be authenticated to ensure that access is only granted to approved parts of the record.

Authentication of identity can be achieved through a number of mechanisms. Currently in health this is often achieved through identification by a trusted third party — for example by a health provider or through use of the Medicare card. In other fields alternative techniques are used, for example:

- Drivers licences rely on photographs and signatures;
- Some high security facilities use biometric measures such as thumbprints and iris scans; and
- The banking industry uses a magnetic stripe card and personal identification number.

Q. 19 What mechanisms should be used to control access to data?

Health care providers

There are many different types of health care providers including general practitioners, specialists, pharmacists, nurses, community care workers, allied health professionals, and complementary health practitioners. Involving all of them in electronic health records (particularly from the start) would be overly challenging. On the other hand, having an overly restricted list of participating providers could result in important health information not being available when required. For developmental reasons it might be appropriate to start with a few types of providers and gradually add more over time. If so who should be involved initially?

Q. 20 Which health care providers should supply data to the EHR's?

SECTION 5: PREREQUISITES - 'THE BUILDING BLOCKS'

To be able to proceed with implementing a national approach to electronic health records, there are some key issues that need to be addressed at the outset. These are the 'building blocks' that must be put in place to underpin all of the activity discussed in previous sections of this paper. They include:

Privacy and data protection

Consumers and the general community currently have a level of trust in the way in which highly sensitive health information is handled within the health sector. However, the capacity for emerging information and communications technologies to assemble, store and transfer information in unprecedented amounts has understandably generated concerns that individuals' health information privacy might be lessened in an electronic age. Providers, likewise, have expressed concerns that their privacy could be eroded as electronic information exchange increases across the health sector.

Before the development and implementation of electronic health records can proceed on a national scale, therefore, both consumers and providers need to be convinced that their personal health information will be protected and that boundaries are firmly drawn to restrict access to information to a need-to-know basis. While confidentiality and security are clearly important aspects, the concept of information privacy goes much wider, covering all aspects of the handling of personal information including:

- the right of individuals to be informed about why their information is being collected;
- having access to their information; and
- having a say in how their information is used and to whom it is disclosed.

In this context, there has been a growing realisation that Australia's approach to health information privacy and the ethical use of such information should be strengthened, to respond to current demands for data sharing and to plan for the increasingly complex issues that are emerging as advances in technology open up new possibilities for using information. These initiatives can only successfully proceed within an environment in which consumers can be confident that their privacy is protected and where they can understand and maintain a reasonable level of control over how their personal health information is handled.

Consumer consent and control of records

Consumer records have conventionally been considered the property of the treating doctor. This has, at times created, considerable tension between health consumers on the one hand asserting that information concerning the individual belongs to that individual and medical practitioners on the other maintaining that medical records belong to the doctor who created them (for their own use).

The evolving world of electronic health records is now shifting the focus from who owns medical records to who can have access to information contained in them. The way in which electronic health records are now being created in practice is very much about the consumer and doctor working together to assemble the health record, with the computer screen being viewed by both during the process. The concept of sharing health summaries (as opposed to complete records) is also gaining support. With the increased transfer of information between locations, access for consumers is essential not only to ensure that they fully reap the benefits of electronic records in terms of compiling life-long, portable records of their health care, but also to enable them to verify the accuracy, currency and completeness of such information. In addition, it reduces loss of information over time with, for example, an important medical problem ten years previously being retained within the health summary, whereas it may not be recalled by the consumer in the anxiety of a new medical event.

Currently, the responsibility for protecting the privacy of information held about a consumer rests with the holders of individual parts of the record. However, as electronic health records and the transfer of information across organisational boundaries become increasingly commonplace, concepts of custodianship (versus ownership) and consumer consent and control in terms of access will likely supersede former practices. Once these concepts are integrated fully into electronic health records systems, consumers will have far greater control over their personal health information than is currently the case with paper-based systems — making them, in effect, empowered gatekeepers of their own health information.

Consumer consent is also of fundamental importance. Clearly, consent should be informed, including the benefits and risks inherent in the electronic exchange of health information. From a medico-legal perspective, such consent will need to be documented and the opportunity provided for consumers to ‘opt-out’ of such exchanges at any time.

Security and authentication

With the continuing progress towards computerisation of the health care industry, all stakeholders will need to work together to develop systems that not only facilitate the integration of health services through the storage, transmission and rapid access to information, but also to ensure that information is managed within a transparent and robust security framework. This framework will need to be

developed as a practical approach to the day-to-day management of privacy, confidentiality, data protection and security.

An electronic health record security framework may support a standardised approach to security and authentication management. The framework would set out administrative and technological security requirements to allow health care providers to adopt and support the implementation of an electronic health record system. Such a framework needs to be comprehensive, multi-layered and able to be adopted by individual health care providers as well as large institutional players. Without such a framework the risk is one of technology mismatch, inadequate management systems, lack of clarity about system requirements and lack of confidence among consumers and health care providers alike.

Underpinning all these issues is the need for both consumers and providers (and possibly locations) to be accurately identified so that:

- health information that is recorded relates to the correct individual (attribution);
- personal health information is accessible only to the individual to whom it relates, or to those for whom that individual has provided explicit consent (security);
- the identity of people seeking access to information can been verified (authentication).

Messaging and communication

Information related to consumer health care is currently held in a variety of data formats and information structures using a range of health care computer applications and paper based systems. The adoption of common messaging standards will enable communication and sharing of consumer health care information between disparate systems. This process will enable the building and access of an electronic health record through the exchange of information in a consistent and non-proprietary manner.

Telecommunications

The use of telecommunication technologies in health continues to expand rapidly as a means of achieving better and more appropriate care.

Imaging and audio standards

Technical standards for the storage and transmission of images and audio data, as well as text and binary data, are required to ensure that electronic health records will be interoperable in a multi-vendor environment.

Classification and Coding

For a national system of electronic health records to mean anything, adoption of common understandings of terms and standard classification systems are essential. National statistical collections also require agreed terms to be used within their data sets to ensure consistent interpretations and inferences are drawn from data captured in electronic health record systems.

National and international terminology standards are necessary to describe, measure and communicate concepts about a person's health. These standards will also address issues relating to the use and exchange of health terms and ways in which those terms might be represented and classified to allow a common language to be used in health records to represent concepts such as diseases, investigations and interventions.

Reference terminology, coding and classification systems have been of interest in the past for the collection of health statistics and activity reporting. However, it is the benefits promised by the introduction of electronic health records that makes it imperative that standards for term and concept representation be implemented. Compliance with such standards will ensure that data extracted from the electronic health record is meaningful to both the provision and management of health care.

Q. 21 Are there any issues you would like to raise in relation to any of these building blocks?

AND FINALLY

The issues involved in the consideration of a national approach to electronic health records are many and few of them are simple. It is quite likely that this paper has failed to raise issues that you consider very important. Please take the opportunity to address them in your submission.

Q. 22 Are there any other issues you wish to bring to the Taskforce's attention?

INDEX OF QUESTIONS

D HEALTH INFORMATION STANDARDS

Lack of widely agreed and implemented standards for health information has hindered implementation of health records in electronic form. Until health care providers collect data in a standard format according to widely accepted definitions, it is virtually impossible to link data generated in various parts of the health care system in any meaningful way. This is a challenging task, if only because the health care system has highly heterogenous data and information needs.

D1 What is a standard?

There are various kinds of standards. For example: the inch is a standard of measurement; money is a standard of exchange; words are standards of communication; traffic lights are safety standards; octane ratings for petrol are quality standards; and "no more than 1 per cent shrinkage is an example of a performance standard. Standardisation has had a long and remarkable history (see Box D1 for a somewhat US-centric view).

A standard has been defined by the US National Standards Policy Advisory Committee as:[62]

> A prescribed set of rules, conditions, or requirements concerning: definitions of terms; classification of components; specification of materials, performance, or operations; delineation of procedures; or measurement of quantity and quality in describing materials, products, systems, services, or practices.

Though often unrecognised, standards can help to assure health and safety and to increase the quality of life. Standards are vital tools of industry and commerce. They often provide the basis for buyer-seller transactions, hence they have tremendous impact on companies and nations, and even on the economic fabric of the international marketplace.

Benefits and difficulties of standardisation

On the whole, the benefits of standardisation far outweigh the difficulties and potential for abuse. Standards promote understanding between buyer and seller and make possible mutually beneficial commercial transactions. Product attributes cannot always be evaluated by individual purchasers by inspection or even from prior experience. However, a product's conformance to accepted standards readily provides an efficient method of conveying complex information on the product's

[62] National Standards Policy Advisory Committee (1978), *National Policy on Standards for the United States and a Recommended Implementation Plan*, Washington DC, p.6.

suitability. Architects use standards in a shorthand manner when drafting plans for buildings.

Purchasing agents can also use standards as an easy way of communicating their needs to potential suppliers. In a host of situations, standards are, or may be used to replace large quantities of complex information.

Standards underlie mass production methods and processes. They promote more effective and organised social interaction, such as the example of the standardised colours for traffic lights and many other widely accepted conventions. Standards are essential in efforts to improve product quality and safety and to clean up the environment. Standardised and interchangeable parts can reduce inventory requirements and facilitate product repairs. They can also promote fair competition by facilitating the comparison of prices of standardised commodities.

In general, standards permit society to make more effective use of its resources and allow more effective communication among all parties to particular activities, transactions, or processes. Indeed, standards are crucial to every form of scientific and industrial process. Without standards, the quality of life would be significantly reduced.

In part, problems result from the sometimes substantial costs of participation in standards development, making it difficult (if not impossible) for small firms and non-industry representatives to be active in the process. The standards themselves may cause problems if highly technical in nature. It is frequently difficult, if not impossible, to get qualified consumer representatives to participate actively. This seriously complicates the attempts to achieve balanced representation by all interests concerned.

Other problems may occur when a standard undergoes review and revision. Unless the original writers of the standard participate in its revision, the reviewers may not be able to understand how the document was prepared, what was eliminated from consideration, and the reasons or assumptions underlying decisions and the resultant provisions. Problems can also occur in the application of specific provisions if the intent behind them is unclear. *Rationale statements*, which sometimes accompany a standard, are specifically designed to define the purpose and scope of the standard, to explain the criteria used in developing its requirements and to provide all other relevant information at the disposal of the developers. However, the use of rationale statements is not yet extensive.

Certification

Product certification is intended to confirm that a particular product conforms to one or more specified standards, thus providing the user with explicit or implicit information about the characteristics and/or performance of the product. Certification is a method for increasing a buyer’s confidence in a product and for furnishing product information.

Box D1: Historical importance of standardisation

The history of standardisation is both fascinating and demonstrative of the scope and variety of such activities. A predecessor of the American National Standards Institute (ANSI) noted that one of the first known attempts at standardisation in the Western world occurred in 1120. King Henry I of England ordered that the ell, the ancient yard, should be the exact length of his forearm, and that it should be used as the standard unit of length in his kingdom.

That history also notes that, in 1689, the Boston city fathers recognised the need for standardisation when they passed a law making it a civic crime to manufacture bricks in any size other than 9x4x4. The city had just been destroyed by fire, and the city fathers decided that standards would assure rebuilding in the most economic and fastest way possible.

Eli Whitney is sometimes referred to as "the Father of Standardisation" in the area of interchangeability, having originated and implemented the concept of mass production in the United States in 1780. He was awarded a contract to produce 10,000 muskets by then Vice-President Thomas Jefferson. Though standardised parts had been successfully used in other parts of the world, Whitney brought the concept to this country when he divided the manufacturing process into individual steps and put different groups to work on each step of the process. All parts of the same type were copied from a model musket and were made to be interchangeable. Subsequently, when he appeared before Congress with a collection of assorted parts and proceeded to assemble ten working muskets by selecting the required parts at random, Congress was convinced of the benefits of mass production made possible by standardisation.

Standards are known to have existed as early as 7000 B.C. when cylindrical stones were used as units of weight in Egypt. However, the great blaze in downtown Baltimore in February 1904 and other, similar catastrophes provided tragic and undeniable evidence of the importance of standards. While the fire in Baltimore burned, fire engines from as far away as New York rushed to the scene only to discover that their hoses would not fit Baltimore hydrants. Those "alien" fire engines were useless! The inferno burned for more than thirty hours, destroying 1526 buildings covering more than seventy city blocks. All electric light, telephone, telegraph, and power facilities were also razed. In contrast, 23 years later, help from 20 neighboring towns saved Fall River, Massachusetts from destruction since hydrants and hose couplings had been standardised in these communities.

As late as 1927, a colour-blind motorist had as good (or as bad) a chance as anyone else when trying to interpret traffic signals. Purple, orange, green, blue, yellow, and red lights greeted him as he drove from state to state. In some states, green meant "Go," in others "Stop." Red, not yellow, lights meant caution in New York City. In 1927 a national code for colors was established through the work of the American Association of State Highway Officials, the National Bureau of Standards and the National Safety Council. Imagine the chaos that would occur during rush hour in any major U.S. city today if newcomers and tourists did not know what traffic signals meant!

Probably the most significant standard ever developed in the United States, however, was the railroads' standard track gauge. This standard, now used in Great Britain, the U.S., Canada and much of continental Europe, enables railroad rolling stock to cross the country.

It was the Second World War, however, that brought the urgency of extending domestic standardisation to the international level. Allied supplies and facilities were severely strained

because of the incompatibility of tools, replacement parts, and equipment. The War highlighted the need for standards aimed at reducing inventories and increasing compatibility.

Source: National Institute of Standards and Technology.

Third-party certification is the term applied to the process by which an organisation, independent of either the manufacturer or supplier, assesses a product's conformance to one or more standards. A manufacturer's overall quality-control program may also be examined as part of the certification process.[63] Thus, certification programs are communication tools designed to reduce the cost of exchanging information between buyer and seller.

D2 Standards-making processes

Standards can be thought of as agreements on how to implement technologies allowing, for example, buyers to choose compatible medical equipment and software from a variety of vendors (thus encouraging both innovation and price competition).

Sometimes de facto *proprietary standards* emerge when a single vendor controls a large share of the market for a particular item (eg the Windows operating system for personal computers). The ultimate criterion for a successful standard is the impact it achieves in its target environment (ie the extent to which any standard is adhered to in practice).

Consensus standards are developed by committees with representatives from those with a stake in the outcome. The committees can include representatives of vendors, the medical community, government and other interested parties who choose to participate in the laborious processes that writing and agreeing on standards can involve.

Standards committees are accredited by organisations such as the American Society for Testing and Materials (ASTM), the American National Standards Institute (ANSI), or by other national or international organisations — such as the International Standards Organisation (ISO) at which Standards Australia represents Australia's interests. They meet over a period of years and develop drafts that members of the committee vote on after extended revisions and public review. Such standards bodies can have problems reaching decisions as rapidly as new technologies are developed.

Purchasers of medical equipment and software can more easily build extensible systems by buying items that store and exchange information according to one or more of these consensus standards, rather than proprietary standards.

[63] A quality-control program is a series of activities designed to assure that quality is being maintained at all phases of production.

Increasing interest in electronic health records has underscored the important role that standards play in the whole electronic health record endeavour to ensure compatibility and transferability of patient records from one setting to another.[64] For example, in its 1991 study, *The Computer-based Patient Record: An Essential Technology for Health care*, the (US) Institute of Medicine (IOM) noted that:

> A variety of standards must be developed, tested, and implemented before the computer-based patient record can realise its full potential.

Specifically, the IOM cited the need for messaging standards (see below) and security standards (also see below). The (US) General Accounting Office, in a 1993 study titled *Automated Medical Records: Leadership Needed to Expedite Standards Development*, discussed the critical need for standards in four areas:

- structure and content;
- vocabulary;
- messaging; and
- security.

As is the case with many other standards, developing health information standards is an ongoing process. While there has been some progress on actually getting some standards implemented (eg in the messaging area) progress in other areas has been slow (eg with structure and content standards). What is needed is more input and impetus from health care professionals, and this in turn depends on the usefulness of health records to providers. Also, as standardisation progresses and the usefulness of exchanging health information via electronic health records becomes established, the standards themselves will need to evolve in line with changing circumstances and new applications for health information.

D3 Vocabulary standards

Vocabulary standards establish common definitions for medical and other health care terms and determine how information will be represented in health records. The intent of such standards is to encourage consistent descriptions of medical conditions by all practitioners and so avoid the situation where different terms are used to describe the same condition. Use of the same vocabulary greatly enhances communication among health care providers and makes the health record that much more valuable to all who have access to it.

Codes are abbreviated representations of medical terms, and are usually numeric or alpha-numeric.

Developing vocabulary (data) and coding standards is a difficult task given the complexity of medical terminology and the number of extant, competing systems.

---

64 Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.xiv).

Data standards and coding and classification systems

High-quality information is a prerequisite for health care, planning and resource allocation decision making. There is an increasing expectation that decisions will be made on a holistic basis, taking into account the different forms of care and treatment that the patient receives in all settings. For this to be able to happen, information needs to be shared between all decision makers, whether for clinical or service management and planning purposes. To be effective it is critical that common definitions and classifications are adopted across different types of health (and welfare) services.

Common data definitions have been developed for use across Australian health services by the National Health Information Management Group (NHIMG). These are contained in the National Health Data Dictionary (NHDD), now in its 9th edition.[65] These are available electronically through the 'Knowledgebase' maintained for NHIMG by the Australian Institute of Health and Welfare (AIHW). The NHDD can form the basis for an expanded set of definitions needed for the development of electronic health records.

Clinical coding and health classifications are also well developed internationally and in Australia, although the coordination of effort is not as well established as for data definitions. Nevertheless, the strong base that exists is well placed to support the development of electronic health records.

Existing resources

Internationally, the World Health Organisation (WHO) takes the lead in the development and implementation of health classifications. The best known health classification is the International Classification of Diseases (ICD), which has existed for over 100 years and is now in its 10th revision (ICD-10). The second core WHO classification is the International Classification of Impairments, Disability and Handicaps (ICIDH).

The WHO has a network of Collaborating Centres across the world to assist it in its health classification work. The AIHW is the Australian Collaborating Centre, with the National Centre for Classification in Health (NCCH) playing a key role in the Centre. There is an active work program across both classifications, and Australia is playing key roles in ICD updating (NCCH), ICIDH redevelopment (AIHW) and developing linkages between health classifications (AIHW). A key piece of work in hand is considering the desirable scope of the WHO Family of Health Classifications: this work is drawn on in more detail later in this paper.

In Australia, the classification of cause of death and diagnosis and interventions for hospital in-patients, and the associated coding, is well developed. The Australian Bureau of Statistics (ABS) classifies causes of death, including underlying cause of

[65] Complementary arrangements exist for community services definitions.

death; NCCH provides expert advice and support to the ABS in this work. Hospital classifications are developed and supported by the NCCH, which produces the comprehensive classification ICD-10-AM for this purpose — implementation is the responsibility of clinical coders within each hospital. The classification is the basis for 'casemix' arrangements in hospitals throughout Australia, showing the value of a well-developed classification going far beyond statistical and planning purposes.

In other fields, there is much less consensus on methods of classification, and this reflects the position internationally. A General Practice Coding Jury is now seeking consensus on a standard classification for general practitioner use, and some work has been done to develop classifications or coding systems for areas such as community health and ambulatory care.

The National Health information Management Group established a Health Classification Strategy Working Group in 1999. This group was formed to:

- identify and report on the scope of the family of health classifications needed to support health and related data collections and the mechanism to choose classifications for inclusion into the 'family';
- gather information on health classifications in use for national collections;
- report on quality, overlaps or issues and relationships between classifications;
- identify additional health classifications determined to be necessary for Australia; and
- report on developmental priorities.

The inaugural meeting was held in June 1999. As a result of both the initial meeting and a paper prepared by the AIHW on Gaps in Health Classifications, a National Audit of Health Classifications has been undertaken to identify the current status of classification development and gaps in existing classifications. The scope of the audit included all classifications, vocabularies and nomenclatures used in health.

Drivers for further development of clinical coding and classification

There are significant business drivers compelling the health system to develop and implement a coherent clinical coding and health classification strategy. These include:

- improving coordination of care between different health services;
- increasing focus on the measurement of outcomes;
- identifying the cost and benefits of alternative treatment regimes;
- providing structure for the development of clinical practice guidelines;
- allowing the compilation of consistent aggregate statistics for policy, planning and research purposes; and
- progressing the development of an electronic health record.

Electronic health record systems must have the capacity to exchange, manipulate and integrate data from multiple sources.

As health care providers in different settings have differing requirements there are valid reasons why the use of multiple coding and classification systems may be used.

Unless classifications used in one setting can be mapped accurately to classifications used in other settings, there can be no meaningful comparison between interventions or activities occurring in, for example, an admitted patient setting with a community health setting.

At present, different classifications are used between settings, and there are also cases where multiple classifications are used within a single setting (eg mental health).

Towards a clinical coding and classifications framework

The array of instruments covered by the audit described earlier show how essential it is to determine a framework for discussing the breadth of clinical coding and classification issues.

The WHO work in progress on defining the WHO Family of Health Classifications is attempting to draw all these 'instruments' together. The extract below is drawn from a current working paper, principally authored by Dr John Ashley, formerly Chief Medical Officer at the UK Office for Population and Census (now part of the UK Office for National Statistics).

> **Instruments**
>
> The rapid development of information technology [IT] in health care with the increasingly extended use of electronic medical records calls for instruments that can handle the much more complex data sets than those previously used to provide data for statistical and related purposes. Also, the development of electronic transfer of data between health providers is facilitated by standardised 'coding' of structured information. IT is an international discipline, which will benefit from an international set of classifications and vocabularies covering all relevant aspects of health care.
>
> Medical and health care science need such instruments. Matters of public health as well as the distribution and use of health care services are no longer just of interest to individual countries or professions. The internationalisation of research related to the health sector needs structured information which is as comparable between as many systems and countries as possible.
>
> There is also a need for a common 'language' covering all the basic elements of health care in which, as far as possible, it must be ensured that one word or one code only have one meaning, and it should be perfectly apparent in which context it is being used. In consequence overlapping of the sphere of influence of individual instruments should, for the most part, be avoided. All this can only be achieved if there is an authoritative body such as WHO to develop, adopt or control a comprehensive international family of instruments, basing it on an agreed concept which can be explained and understood.
>
> **The granularity of instruments**

Relevant instruments which are presently, or potentially, available to describe phenomena related to health and disease are designed to operate at one of three broad levels of increasing 'granularity'. These levels are those of:

- vocabularies;
- classifications; and
- composite groupings.

Vocabularies, sometimes otherwise known as terminologies or nomenclatures, are the finest level of granularity. As each entry normally incorporates sufficient elements to differentiate one individual entity from another, the essential characteristic of a vocabulary is that of *discrimination.* Thus Medical specialists need their own vocabularies for their own use, and which are crucial for communication between the various health settings, including between the hospital and the GP surgery.

Nevertheless some individual terms in vocabularies, particularly 'Diagnostic' terms, may have different interpretations in different contexts. Thus their development and handling within a profession may be far more complicated than one single nomenclature can ever cover. Although vocabularies used in different settings may differ in basic structure, the individualistic nature of the entities they include should ensure that it is normally possible to aggregate (or 'map') to an 'appropriate' (ie, related to a relevant dimension) instrument based on a coarser level of granularity.

Classifications like the tenth revision of the *International Classification of Diseases* (ICD), and its modifications in Australia and the USA can be viewed as having a content typical of the 'second' level of 'intermediate' granularity. They incorporate generalist hierarchies of aggregation designed to make them useful for multiple purposes including national statistics, management information, and reimbursement. They are less appropriate instruments for communication, as the terms that are included (eg, diseases) at this level are primarily labels in medical language for use outside the physician's examination and treatment of the patient.

(Core) members of the FIHC, are and have been, designed to fulfil the requirements of this level of granularity, and to conform with general principles which apply to statistical classifications. For example ICD-10 *(Vol 2 para. 2.3)* and Miriam Gersinovich in her related paper *(Meth. Inform. Med. 1995 Vol 34, pp 172-175)* list a number of general principles which apply to a statistical classification of diseases. They identify that ' *a statistical classification of diseases must be confined to a limited number of mutually exclusive categories able to encompass the whole range of morbid conditions. The categories have to be chosen to facilitate the statistical study of disease phenomena. A specific disease entity that is of particular public health importance or that occurs frequently should have its own category. Otherwise, categories will be assigned to groups of separate but related conditions. Every disease or morbid condition must have a well-defined place in the list of categories'.* Furthermore *'it is the element of grouping that distinguishes a statistical classification from a nomenclature, which must have a separate title for each known morbid condition'.*

Some other, related, instruments represent selections, regroupings or refinements of (core) members; for example, in the case of the ICD, national modifications, or applications for a specific user group, such as oncologists (ICD-0-2). However, it remains appropriate that, like (core) members, these derived instruments should also conform to the generally established structural characteristics associated with this level of granularity.

Composite groupings are of coarse granularity. They include the special tabulation lists of ICD and Burden of Disease Groups. They can also incorporate concepts from two or more domains (eg, Diagnosis Related Groups [DRG's]). A sentinel operations list (or a skeleton grouping of the nature of interventions) would be a further candidate for membership of this level. Any exclusion of instruments of this nature from consideration as classifications as such is not meant to imply they are not of use to national or international bodies like WHO, for inclusion in, for example, the burden of disease project.

None of these levels is sharply demarcated from its neighbour(s), and it is possible for an apparently individual concept to be identifiable at all levels. However the professional languages of the health sector have a limited number of terms to use in the attempts to describe problems, items and concepts. So, users should be aware that the same term may be used with different meaning depending on the context in which it is used, including which of the professional groups is using it.

Similar problems may be found when comparing the professional vocabularies of the health professions. Nurses and other professional groups have developed instruments which cover their interventions, as well as including concepts which are already part of other classifications such as those in the ICD. If these instruments are used together there may be two or more assignments for the same item, where the only difference is that it is related to different professionals as providers. To avoid problems of this nature there must only be one code for one category or item. Otherwise it is necessary to record the context in which the code is used even if this is merely a reference to the profession of the person using the specific category.

There are also links between the levels of granularity, exemplified by multi.-axial classifications such as *ICD-0-2 and SNOMED.* These concept systems are meant to bridge the gap between ICD-10 and the use of diagnostic terms in daily clinical practice, scientific research or other professional activities.

This concept of granularity has two other inherent related implications:

- detail in the information is inevitably lost by moving from a finer to a coarser level because the 'individual granules' at the latter level frequently embrace multiple discrete concepts at the former one; and
- mapping between levels is unidirectional and is usually in the form of n-to-l.

A clinical coding and health classification system to support electronic health records in Australia

A high-quality, universally accepted health classification system has a key place in an electronic health record. Past health conditions and interventions in the in-patient hospital setting are well and uniquely described in terms of the ICD-10-AM classification. The work of the clinical coder can be easily and economically retained in the form of a code in the record, and provided back to a user of the record in generally understood terms. A health care provider can rely on this source of information from the past with minimal fear of misunderstanding.

The WHO working paper indicates how the Family of Health Classifications can grow to provide over time similarly authoritative recording of past events in settings other than the hospital in-patient. An Australian structure to draw on the international work and to decide on inclusions in the Australian family is essential.

Vocabularies need to be agreed for use across Australia, developed where not available, and updated regularly. Similarly, linkages between and across classifications and vocabularies are essential. Through maps to the Unified Medical Language System (UMLS), foundational work in this area has commenced, but it needs to be systematic and used universally once in place.

The NHIMG Health Classifications Group referred to above provides a platform for addressing this need for coordination and development of clinical coding and classification across domains and settings. A more broadly based expert group, representative of the various domains and settings, could be tasked to:

- determine a framework for an Australian Family of Health Classifications (taking the WHO work as its starting point);
- determine the existing classifications that would fit into this framework;
- identify and prioritise gaps in classifications, for further work; and
- consider the need for linkages between the different classifications within this framework and recommend how such linkages might be developed.

Membership of this expert group should include key players in health classification in Australia plus expert representatives of users of the classifications for electronic health records, planning, statistical and research purposes.

Given NHIMG's central role in clinical coding and health classifications, and its capacity as a decision-making body in the field, it would be appropriate for NHIMG to continue to auspice this work.

Resources

Beyond the maintenance and updating of ICD-10-AM, there is little resourcing of vocabulary and classification work in Australia. A significant work program, including the development of electronic tools, over a sustained period will be needed if the desired benefits in terms of quality, consistency of language and terminology in electronic health records are to be achieved. These resources would need to be in addition to those now provided by the Australian Health Ministers' Advisory Council (AHMAC) to NHIMG for its existing information work.

Given the known costs of developing the ICD-10-AM electronic database and initial estimates of other possible developments (such as an Australian Clinical Thesaurus), at least $500,000 for 3 years (with a review after that time) will likely need to be provided.

In the USA, the National Library of Medicine has combined a number of vocabularies covering various specialised areas of medicine into a Unified Medical Language System (UMLS) and one part of the project is the UMLS Metathesaurus — a tool and guide for finding medical information in databases designed for those who develop health information systems.

As mentioned, NHIMG has established a Health Classification Strategy Working Group. A National Audit of Health Classifications is being undertaken to identify the current status of classification development and gaps in existing classifications. The scope of the audit includes all classifications, controlled vocabulary, nomenclature and thesauruses used in health.

The WHO is also reviewing the second version of the International Classification of Impairments, Disabilities and Handicaps (ICIDH). The World Organisation of Family Doctors (WONCA) has also developed a classification for primary care (ICPC2) which provides a common nomenclature for health issues to facilitate international comparison in the primary health care sector.

In Australia, one of the common coding standards for describing medical diagnoses and procedures is ICD-10-AM (an Australian Modification of the international ICD-10 standard). A round of consultation on potential changes to ICD-10 was undertaken in Australia in February 2000. The ICD 10 Australian Modification was implemented nationally in 1999. Version 2 is being introduced by all jurisdictions from July 2000. While it is a detailed classification system, the focus of ICD-10-AM development is driven by funding concerns and it does have some deficiencies for clinical purposes.

In addition, standardised vocabularies, such as the Systematised Nomenclature of Medicine (SNOMED), have been developed in an attempt to consistently and unambiguously define medical terminology.

A national project to develop a code set for Community Based Health Services was completed in 1998. A process to refine this and align it with other national standards was completed in early 2000. A proposal has been endorsed by NHIMG and forwarded to the AHMAC to maintain the code set as a national resource.

A General Practice Coding Jury was convened in 1999 to determine an appropriate coding system for use in general practice. A process to invite public submissions was undertaken and responses are being evaluated. A report of the Jury's findings will be published in 2000. Work has also been undertaken to develop a data model for general practice and a core data set. This project, in conjunction with the Coding Jury, is defining the key information and classification requirements and setting priorities for general practice.

The NHDD provides a core set of standards, nationally agreed classifications to describe the full range of health services and population parameters, including health status and determinants. It aims to promote uniformity, validity and consistency in data, and aligns with nationally and internationally agreed protocols and standards wherever possible. It is available electronically through the National Health Information Knowledgebase which is a repository for health information standards and classification systems maintained by the AIHW. The NHDD has in the past included only data elements required for statistical purposes, but as indicated earlier, is proposed to be expanded to include a broader range of clinically useful elements.

Another relevant development is the Australian Clinical Thesaurus. Its purpose is to provide:

- a mechanism to ensure that data collected using different classifications are as comparable as possible;
- a single reference point for people selecting a coding system so they can make an informed decision about an appropriate tool (rather than reinventing classifications);
- infrastructure for a coding system and mapping table refinement and quality assurance;
- infrastructure and economies of scale for converting paper-based classifications to new electronic forms; and
- maximum re-use of coded data by helping to delimit domains within classifications.

The Taskforce acknowledges the importance of work in this area, notwithstanding its at times chaotic nature and lack of an immediate 'turn key' coding and classification strategy which could be embraced. The Taskforce proposes that focus of activity be directed at:

- finalisation of work undertaken by the AIHW on the audit of health classifications, identifying gaps and priorities for development;
- development of a health classification strategy for Australia;
- development/enhancement/endorsement of key classifications;
- resolution of inter-sectoral classification anomalies;
- development of an Australian Clinical Thesaurus; and
- detailed feasibility and costing of tools to support the integration of multiple classifications, such as the use of a lexicon engine.

D4 Record structure and content standards

Standards for structure and content are needed to give a clear description of the data elements that will be included in electronic health records. This involved identifying essential data elements (such as temperature and blood pressure) and standardising such things as the field length, data type, and acceptable content of each data field.

Hospital discharge summaries

A hospital discharge summary could be expected to contain, at a minimum, data elements for:

- standard demographic information (eg name, address, date of birth, sex);
- patient and hospital identifiers;
- attending and operating medical practitioners;

- principal and secondary diagnoses;
- procedures performed; and
- patient disposition.

Ambulatory care

An ambulatory care patient record could be expected to contain, at a minimum, data elements for:

- standard demographic information (eg name, address, date of birth, sex);
- patient identifier;

and, for each encounter:

- provider and location identifiers;
- date and reason for encounter;
- diagnostic service(s) ordered;
- problem, diagnosis or assessment;
- therapeutic services provided;
- preventive services discussed; and
- patient disposition.

Long-term care

In the case of patients in long-term care facilities (such as a nursing home) a long-term care record could be expected to contain, at a minimum, data elements for:

- standard demographic information (eg name, address, date of birth, sex);
- patient and facility identifiers;
- admission history to long-term care facilities;
- daily pattern of activity;
- physical functioning;
- psychological status;
- health problems; and
- specific body systems review.

Emergency care

In the case of hospital emergency departments, a patient's record could be expected to contain, at a minimum, data elements for:

- standard demographic information (eg name, address, date of birth, sex);
- patient, hospital and medical practitioner identifiers;
- arrival and first assessment;
- history and physical examination;

- procedure(s) and result(s);
- medication; and
- disposition and diagnosis.

Information storage standards

A crucial component of the proposed Health Information Network Australia (HINA) is the use of standards to define the structure of the storage facilities wherever they are located. Unless a standard format is used for the storage the value of the Network will be seriously compromised — information will not be able to be shared, and the various Network applications will not function.

The search for a practical, workable solution to this requirement occupies health informaticians around the world. To date possible candidates include the use of structured messaging typified by Health Level 7 (HL7), system interoperability typified by CORBAMed and record architecture proposals such as the Good Electronic Health Record (GEHR).

The Taskforce reckons that, given the state of play currently, there is insufficient evidence to recommend a single solution. The GEHR appears to have the best prospects and is the subject of a current trial within Australian general practice via the General Practice Computing Group (GPCG).

The Taskforce therefore proposes that further work proceed in this area and, depending on evidence coming from the GPCG trial, that the GEHR architecture be further tested in formative work associated with HINA.

D5 Messaging standards

Information related to consumer health care is held in a variety of data formats and information structures, using a range of computer applications and paper-based systems. The adoption of common messaging standards will enable communication and sharing consumer health care information between disparate systems.

A model of communications published by the ISO describes seven different levels of computer communications, beginning with physical interconnections and ending with the standards that specify how messages are passed between software applications (the seventh level). One of the most widely used messaging standards is the HL7 standard for electronic interchange of health data (see Box D2). HL7 was originally a standard for communicating laboratory data and other clinical observation data between software applications, but it now includes structures for communicating clinical orders, billing information, and patient admission, discharge, transfer, and registration information within single institutions. This suite of standards has brought a modicum of order to the varied approaches to sending messages within and among health care institutions.

Box D2: HL7 messaging standard

Standards for interchanging health data and assigning codes to medical concepts underlie all efforts to make patient records electronically accessible.

Messaging standards specify the *syntax* of an electronic message and coding standards specify its *semantics.* A similar distinction exists for more familiar messages, such as postcards. The syntax of a postcard corresponds to the arrangement of its elements: the addressee's name appears in a standard position, the city in another, the message is placed in a box on the left half and the stamp in the upper right, and so on. The arrangement is set by international postal conventions.

The meaning of the letters appearing within a given element (its semantics) is determined by an entirely different set of conventions, namely the language employed by the correspondent. Similarly, HL7 and other messaging standards specify the order of the many discrete elements that make up a message and indicate which elements are required and which are optional. ICD-10-AM and other coding systems assign meaning to the characters in the message.

Electronic Messages

HL7 messages are streams of text that are relatively simple to interpret, As an example, the portion of the message that carries the patient's address might be represented as "...1432 Hosteler Street 'Apt 232ˆChlcagoˆILˆ60603ˆUSA... " In addition to demographic information identifying the patient, an HL7 message delivering the results of a laboratory test might include hundreds of other data elements containing numerical values for the measured parameters, the measurement units, and portions of the message that bore the initial request so that the request and response can be matched and reconciled.

The data elements contain internal indications of the coding standards to be used. For instance, one small portion of the standard message defined by HL7 contains the patient's diagnosis. This slot might be filled with the characters "410.1ˆI9C. " The software application receiving this message knows from the position of the characters within the message that this is a diagnosis, and it simply has to assign mean-ing to the character by looking up diagnosis number 410,1 in the set of codes published by the ICD-9-CM Committee. The table would indicate that the diagnosis is '(anterior myocardial infarction. " Alternatively, the same diagnosis could be conveyed in a different coding scheme employing an entire-Iy different code set, but still using the same HL7-defined structure. This allows the software application sending a message to choose whatever coding scheme is most appropriate for the data it processes. Libraries of disease and procedure descriptions can evolve without necessitating any changes in the software governing how messages are sent.

Source: Adapted from OTA 1995.

D6 Security standards

Information security is now a major issue facing today's electronic society, and is a particular challenge when it comes to health information — given the particularly sensitive nature of personal health information.

Cryptography

With a history arguably as long as writing itself, cryptography — the scrambling of messages to secure communications between sender and receiver — has come to the fore as a way of adding security to insecure networks (such as the Internet) in

order to conceal information from those not authorised to see it. The idea is that only those who possess the key (or cipher) to unscramble a message will be able to interpret and use the information.[66] Encryption is the process of converting messages, information or data into a form which is unreadable by anyone except the intended recipient. Thus, encrypted information must be deciphered (or decrypted) before it can be read by the recipient.

Encryption — achieved by applying a mathematical algorithm to convert plain text, data or other information to 'ciphertext' — is becoming increasingly pervasive (eg even simple e-mail massages are routinely encrypted before transmission). The cipher (ie the rules followed to encrypt a message) and the encryption algorithm — often also using a 'key' — can be considered as two essential components of an overall security approach to sending messages over a network.

The same key used to encrypt the message is often used to decrypt it, and the key must therefore be sent across the network from sender to receiver.[67] Just how to do this safely remains an active area of research.

But not all keys are identical at each end. This is the idea behind public key infrastructure (PKI), where only one of the two differing keys must remain private (the other can be made public).

However, it must be borne in mind that two-way encrypted messages can be attacked by anyone that intercepts them on the 'untrusted' portion of a network. One method of systematically attacking the problem is for those intent on interception trying all possible keys to the solution — an approach made increasingly feasible by the increasing processing power of computers. This can be countered by increasing the length of keys, or resorting to more and more sophisticated encryption algorithms (eg by repeated use of or combining different algorithms). For example, 128 bit keys are becoming increasingly common — with some applications using up to 2048 bit keys.

Data encryption standards

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. Government that its export was restricted initially. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of possibilities. Like other private key cryptographic methods, both the sender and the receiver must know and use the same (private) key.

DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered

[66] No crptographic technique is 100 per cent safe, however, since cracking the code can be achieved with enough time and computing power.

[67] Keys are usually changed regularly to maintain security.

"strong" encryption, many companies use "triple DES", which applies three keys in succession. This is not to say that a DES-encrypted message cannot be "broken." Early in 1997, RSA, owners of another encryption approach, offered a $10,000 reward for breaking a DES message. A cooperative effort on the Internet of over 14,000 computer users trying out various keys finally deciphered the message, discovering the key after running through only 18 quadrillion of the 72 quadrillion possible keys! Few messages sent today with DES encryption are likely to be subject to this kind of code-breaking effort.

DES originated at IBM in 1977 and was adopted by the U.S. Department of Defence. It is specified in the ANSI X3.92 and X3.106 standards and in the Federal FIPS 46 and 81 standards. Concerned that the encryption algorithm could be used by unfriendly governments, the U.S. government has prevented export of the encryption software. However, free versions of the software are widely available on bulletin board services and Web sites. Since there is some concern that the encryption algorithm will remain relatively unbreakable, NIST has indicated DES may not be recertified as a standard and submissions for its replacement are being accepted. The next standard will be known as the Advanced Encryption Standard (AES).

Public key infrastructure

Securing the exchange of health information over a communications network can be likened to an electronic equivalent of writing the information down on paper, signing it, sealing it in an envelope and posting it. The signature attests to authenticity and the sealed envelope provides confidentiality. In the electronic world, the parallels include things like digital signatures and use of cryptography.

Public key infrastructure (PKI — see Box D3) provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for electronic transactions (including safe electronic exchange of health information):

- confidentiality — keep information private;
- integrity — to prove that information has not been manipulated
- authenticity — to prove the identity of an individual or application; and
- non-repudiation — to ensure that information cannot be disowned.

Lack of security is often cited as a major barrier to capturing, transmitting, accessing and storing personal health information by electronic means — barriers that will only be overcome when those involved are confident that such information will be protected by these core functions.

A PKI is a combination of hardware and software products, policies and procedures which together provide the means to transmit (in this case) sensitive health information about individuals in such a way that authorised users, who may not

know each other, or are widely distributed, can be confident that they can communicate securely over what might otherwise be regarded as an insecure, untrusted network — such as the Internet.

PKI is based on digital identifiers known as 'digital signatures' which act like 'electronic passports,' and bind the user's digital signature to his or her public key. A PKI should consist of:

- a security policy;
- Certificate Authority (CA);
- Registration Authority (RA);
- certificate distribution system; and
- PKI-enabled applications (in this case, for example, able to add value in various ways to the data contained in individual electronic health records).

Security Policy

A security policy sets out and defines an organisation's top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically it will include statements on how the organisation will handle keys and valuable information, and will set the level of control required to match the levels of risk. *Certificate Practice Statement* (CPS): some PKI systems are operated by Commercial Certificate Authorities (CCAs) or Trusted Third Parties, and therefore require a CPS. This is usually a detailed document containing the operational procedures on how the security policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users.

Box D3: A PKI primer

Background

Cryptography is the discipline that treats the principles, means, and methods for making plain information unintelligible and reconverting the unintelligible information back into an intelligible form. Cryptography has been around for hundreds of years but awareness of it has taken off with the wide use of the computer and open networks (eg the Internet). Faster and more complex computers and communications systems have pushed the use and development of new cryptographic systems, which rely on the use of Public Key Cryptography.

What is Public Key Cryptography?

Conventional cryptography consists of a single mathematical key used for both encryption and decryption of data. If you want to send a secure message to an addressee, you encrypt the message using a key known only to the sender and the recipient and then you pass both the key and encrypted message to the recipient so that the message can only be decrypted by the intended recipient.

Public Key Cryptography uses two keys. One key is kept private and the other key is made public. If the Public Key is used to encrypt a message, the Private Key can decrypt the message. In other words, if you want to send an addressee a message, you encrypt the message with the addressee's Public Key and pass the message to the addressee. The addressee can then use the Private Key to decrypt it.

What is a Digital Signature?

With the invention of Public Key Cryptography, another process known as a digital signature is possible. A digital signature is much like a hand signature in that it provides proof that you are the originator of the message (Authentication). If you want to sign the message which you sent to an addressee, you pass the message through a mathematical function (known as a hash function) which provides a summary (hash code) of the message. This summary is unique for every message and is much like a fingerprint. You then encrypt this hash code with your Private Key and attach the code to the end of your message. This attached code is known as a digital signature. The addressee can then verify that the message was sent by you by decrypting the digital signature, using your public key, to get the hash code. The addressee then passes the received message through the same hash function. If the two hash codes are the same, then the message was sent from you (Non-repudiation) and was not altered (Integrity). All this sounds complicated but, in practice, selecting an icon on your computer screen is all that it takes to make it happen.

What is a Public Key Infrastructure?

A Public Key Infrastructure is a Cryptographic key and Certificate delivery system which makes possible secure financial electronic transactions and exchanges of sensitive information between relative strangers. A PKI will provide Privacy, Access control, Integrity, Authentication, and Non-repudiation support to information technology applications and electronic commerce transactions.

A PKI will:

- manage the generation and distribution of Public/Private Key pairs; and

- publish the Public Keys with the user's identification as "certificates" in open bulletin boards (i.e., X.500 Directory Services).

A PKI provides a high degree of confidence that:

- Private Keys are kept secure;
- specific Public Keys are truly linked to specific Private Keys; and
- the party holding a Public/Private Key pair is who the party purports to be.

How does it work?

A PKI is made up of several central systems known as Certification Authorities (CA). These CAs are logically set up in a tree-like hierarchical structure. Each user's Public Key and identification are placed in a message (certificate). The user's CA will digitally sign each certificate and make the user's Public Key certificate available through publicly accessible bulletin boards (i.e., X.500 Directories) along with all other users' certificates. Therefore any user will be able to get any other user's Public Key from a bulletin board and verify that it is authentic by using the CA's Public Key to verify the CA's signature on the certificate. The CA at the top of the hierarchy will sign the certificates containing the Public Keys of CAs directly subordinate to it and these CAs will sign the certificates of any other CAs below themselves and so on. This process allows Public Keys that are signed by other CAs in the infrastructure to be verified, since a chain of trust has been set up between CAs in the infrastructure.

Source: Canadian Government, available at www.cse-cst.gc.ca/cse/english/gov.html.

Certificate Authority (CA)

The CA system is the trust basis of a PKI as it manages public key certificates for their whole life cycle. The CA will:

- issue certificates by binding the identity of a user system to a public key with a digital signature;
- schedule expiry dates for certificates; and
- ensure certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs).

When implementing a PKI, an organisation can either operate its own CA system, or use the CA service of a Commercial CA or Trusted Third Party.

Registration Authority (RA)

An RA provides the interface between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.

Certificate Distribution System

Certificates can be distributed in a number of ways depending on the structure of the PKI environment, for example, by the users themselves, or through a directory service. A directory server may already exist within an organisation or one may be supplied as part of the PKI solution.

PKI-enabled applications

A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits. Examples of applications are:

- communications between web servers and browsers;
- e-mail;
- electronic data interchange (EDI);[68]
- credit card transactions over the Internet; and
- virtual private networks.

D7 Summary

Standards are a complex area and the vision of the electronic health record in Australia will largely determine the work on standardisation that is required. The kind of system the Taskforce has in mind would require the following kinds of standards:

- a shared set of data-representation standards (such as DICOM, JPEG, HL7);
- a shared set of conceptual representation schemes such as SNOMED-CT or UMLS; and
- a common (and therefore easily retrievable) structure for electronic health record data across all storage nodes on the Network.

A more comprehensive solution that is not technology dependent would require:

- an electronic health record architecture (an emerging focus on conceptual models that build uon, rather than are driven by, available technology);
- a coding system for drugs;
- a syntax for health care data interchange;
- standards for enabling exchange of medical images and related data; and
- reliable methods of consumer, provider and institution/location identification.

---

[68] The basic unit of an EDI transfer is the message. Its format and content are totally dependant on agreement to conform to a common standard (eg HL7) and an interchange between two parties contains the message itself, along with information about the parties to the transaction.

E NETWORK AND COMMUNICATIONS CONSIDERATIONS

With its proposal for the Health Information Network Australia, what the Taskforce is effectively advocating is the construction of what is now commonly called a virtual private network — an Internet-based network with in-built security measures to protect privacy and so overcome the otherwise insecure nature of communications over the Internet. Without such security features users will not accept HINA and no virtual private network will be used unless users are comfortable with it.

Despite the incorporation of high technology into almost every other aspect of clinical practice, information technologies have not, so far, been fully embraced by the health sector (where 1 in 12 dollars of national income are spent). That will change as the health care sector becomes an integral part of Australia's emerging 'information economy.' This report explains how that can happen sooner rather than later — with the public and private sectors acting in concert (rather than in an uncoordinated way) to build a national network devoted to health information.

The global communications industry is undergoing major changes, the most significant of which are the shift from voice to data and a spectacular growth in the demand for services and the capacity of networks to provide them. The fact is that we live in an increasingly networked society.[69] This change is underpinned by significant developments in: communications technology to reduce the unit cost of carrying information; commercial and financial arrangements to facilitate e-commerce/e-transactions; and regulatory structures to promote competition.

The practice of medicine is information intensive, and therefore an obvious candidate for utilising modern information and communication technologies (see Box E1). There has been a change in emphasis form tertiary care at a single site (eg acute care provided in a hospital) to ambulatory care provided at multiple sites (eg GP consultations, community care and home care).

An integrated network supporting electronic health records can be expected to break down the organisational barriers that have tended to growth up between care

[69] In assessing a country's readiness for the 'digital economy', a joint Harvard/IBM guide (www.readinessguide.org) poses the following questions: What is the availability, cost and qualilty of information and communication technology (ICT) networks, services and equipment? Does the educational system integrate ICTs into its processes to improve learning? Are there technical training programs in the community that can train and prepare an ICT workforce? To what extent are individuals using ICTs at work and in their personal lives. Are there significant opportunities available for those with ICT skills? How are businesses and government agencies using ICTs to interact with the public and with each other? To what extent does the policy environment promote or hinder the growth of ICT adoption and use? In response, Australia seems well placed generally — but lagging in the health sector.

providers, medical researchers, and health administrators. These barriers have, for example, supported a clear demarcation between clinical and administrative health information and reinforced a long-standing distinction between treatment of disease and preservation of health.

Box E1: Changing nature of the practice of medicine

To start with, a systematic and comprehensive review of diseases and their treatments is presented at medical school, and students strive to memorise as much of the vast corpus of the science of medicine as they can. After leaving structured education, doctors try to keep up with progress by reading professional journals or engaging in other like activities (eg attending conferences). This continuous self-education approach was more feasible at the turn of the 20th century that it is now.

The first major change occurred after World War I, in the 1920s, when the pace of basic and clinical research activities greatly increased and progress on all frontlines of medicine greatly accelerated: it was no longer enough to devote 2 to 3 hours a week to read two or three journals. Since then, both the scientific bases and the clinical applications have kept changing, outpacing the capability of the physician to follow progress.

The response to this accelerated pace of advances was specialisation. This gave a dermatologist or a gastroenterologist a drastically reduced domain of knowledge to follow. The result of specialisation was, however, rapid escalation of cost and unavoidable fragmentation of care; a specialist treated an organ, not the patient's body system as a whole.

After World War II, research efforts further increased, and American medicine emerged as a world leader in dealing with poliomyelitis and many other diseases. But this spectacular progress had a negative effect. Even the specialists had growing difficulties in keeping up with new important developments. *A gap developed between the frontlines of knowledge and the clinical applications of the new concepts and methods.*

When the leaders of medicine recognised the growing gap, they responded with the only available measure: mandatory continuing education. Despite the best intentions, this force-feeding of new knowledge proved to be a complete failure. Continued classroom education was aimed at the symptom of the problem, not at its cause. The cause was simply the volume of total knowledge, which exceeded the capacity of the human memory. But this conclusion was in direct conflict with the culture of medicine. Physicians are proud to be healers who know how to deal with all diseases. The patient community was kept unaware of the crisis in knowledge updating. Even today, it could be unpopular to declare that memory-based practice of medicine is no longer desirable. But the knowledge crisis is real, and predictably it will only increase unless some entirely new paradigm is developed to replace the obviously failing memory-based practice of patient care.

Source: Based on Gabrieli (1999), in Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (pp.603-4).

E1 Public, private and virtual private networks

Public networks are what Australians are most familiar with, the leading example being the public switched telephone network — so called because connectivity can be switched from one end-point device to another (telephone to telephone) by simply dialling the appropriate number. The public switched telephone network has been adapted to accommodate data by using modems that computers use to dial in and link to the public switched telephone network. Thus, with modems the public switched telephone network treats a computer as if it were a telephone. There can also be publicly available networks which are devoted just to transmitting data (such as frame relay and asynchronous transfer mode services).[70] Public networks differ from private ones in that any public network user is reachable by another user of the network unless there is active intervention to prevent the connection from being made. As a result, a public network has less built-in security than does a private one (where it is easier to address such 'quality of service' issues).[71]

Traditionally, private networks were built using owned or leased private lines by firms seeking to establish secure communications among a 'closed' group of users.[72] Thus, they were deliberately designed to restrict communications to users of devices which were directly linked by these point-to-point private lines. Such limited access could more easily ensure that communications were secure and private to the firm's employees (because no one outside the closed group can easily intercept information being transmitted or compromise devices attached to the network).

Virtual private networks are relatively new, but becoming increasingly necessary for the conduct of business as the Internet takes the world by storm.[73] Use of the term 'virtual' is common in networking parlance and can usually be taken to mean "looks and acts identical to …" whatever term follows (although the virtual version of the concept is not the same as the actual idea. Thus, a virtual private network "looks like a private network," although it is not actually a private network built on a system of private lines. When built on top of a public data network featuring virtual circuits, a virtual private network creates the same environment of security and privacy through use of virtual circuit closed user groups and much more.

---

[70] Public frame and asynchronous transfer mode networks provide users some security and privacy by placing virtual circuits between end-point devices — with the virtual circuit making connections appear and behave as if they were private line circuits.

[71] Apart from security, other quality of service concerns can include access to sufficient bandwidth to undertake a particular task, any delays that may be involved, the stability of such delays, network reliability and the risk of information distortion or loss. A measure of security and privacy can be added to a public switched telephone network by, for example, including unlisted numbers, caller identification and call-screening methods.

[72] Private lines are purchased by the kilometre and by the speed at which they communicate.

[73] One of the greatest attractions powerfully reinforcing the popularity of the Internet is that it costs the same to use for e-mail and file transfers irrespective of the distance the bits that comprise the message have to travel. It is little wonder, then, that businesses and individuals alike are increasingly using the global, public Internet to satisfy daily needs.

Ironically, the most widely used public data network is not a virtual circuit network: the Internet is public data network based on the concept of universal connectivity, without virtual circuits blocking off user groups. Although building them is a challenge, Internet-based virtual private networks dominate the marketplace. Thus, as ubiquitous and successful as the Internet is, its security and privacy levels are poor: a virtual private network adds these missing but valuable ingredients to enable its use for transactions where security and privacy are an issue.

Adding privacy and security to a virtual private network needs to satisfy the following basic requirements:

- privacy, with the ability to scramble or encrypt messages across an unsecured network;
- access control, determining who is given access to the network as well as what and how much information someone can receive;
- authentication, which verifies the identity of the two parties to an exchange of information (or transaction) on the network;
- integrity, ensuring that files or messages have not been altered in transit; and
- non-repudiation, which prevents the two parties to an exchange of information across the network from denying that they sent or received the information (or transaction).

E2 Authentication

Authentication ensures the identity of all communicating parties. Without strong authentication procedures in place, network access may be effectively unprotected — allowing an intruder to access private information stored on the network.

Having to establish one's identity has become a commonplace activity in daily life and certificates of various kinds are a way of doing this. Thus a birth certificate is valid for a lifetime and a driver's licence can be used for authentication (ie that one is who one says one is), as well as for its primary purpose (to authorise certain actions — such as being qualified to drive a passenger motor vehicle). Yet any certificate has its limitations: certificates expire and have to be renewed; and there is always the issues of the validity of any certificate (eg a driver's licence would be useless if one could easily be forged). Mechanisms for verifying the validity of a certificate — such as special markings, distinctive paper, seals, or other signs — are critical.

What prevents any user from making his own certificates? In the physical world, the control factor may be a seal of approval with an official signature. In the electronic world, authentication in usually based on passwords (shared secrets) or 'digital certificates'.

Password authentication is the most prevalent form of user authentication used in computer systems today, but it is also one of the weakest because passwords can be guessed or stolen.[74]

Digital certificates are also becoming more prevalent as an authentication mechanism for virtual private networks. A digital certificate is an electronic document that is issued to an individual by a 'Certificate Authority' that can vouch for an individual's identity. It essentially binds the identity of an individual to a public key. A digital certificate will contain a public key, information specific to the user (name, organisation, etc.), information specific to the issuer, a validity period and additional management information. This information will be used to create a message digest which is encrypted with the Certificate Authority's private key to 'sign' the certificate. The digital signature ensures that the message came from the reputed sender and that the message content, encrypted or in plain text, has not been altered during network transmission.[75]

Authentication typically occurs when a user first logs onto the network. Once accepted as a legitimate user, continual authentication during the course of a logged session may be enforced to verify that the user continues to be the same as originally authenticated. Additional authentication may also be demanded if a user requests access to increasingly sensitive information.

The most important aspect of authentication certificates for virtual private networks is that they are issued by a trusted authority — usually a third party that is trusted by both issuer and user. In the health arena, such a certificate authority (CA) may indeed need to be a third party (ie a body which is not involved in health care transactions). Indeed, users might wish to see more than one CA operating in the health sector, so that they can use a CA of choice.

E3 Authorisation

The distinction between authentication and authorisation can be ambiguous. Authorisation is generally the next step after the authentication process is complete (or the first step if authentication is not required). For example, if doctors were not required to authenticate themselves in order to access to certain information on HINA, the authorisation process would merely establish entitlement to access to that part of the network where the information is held.

---

74 Multi-factor authentication is generally a stronger form of authentication and is based on the premise of utilising something you have in conjunction with something you know. This process is similar to how most ATM cards are used; a user possesses the physical ATM card and 'unlocks' it with a password.

75 Digital signatures are as important in virtual private networks as ordinary signatures are in the physical world of contracts and traveller's cheques. A sender can encrypt a message and append his or her digital signature. The receiver decrypts the message and simultaneously generates the digital signature. If the digital signatures match, the message is presumed to be genuine and unaltered.

Authorisation is typically accomplished by associating users with lists of access rights. Access rights grant or deny clients permission to read, write, delete, modify or create information held on various parts of the network (eg at particular storage nodes). Because access rights can be granted or revoked by an appropriate authority, coordinating and maintaining them can consume a lot of network administrator time.

If restrictions are inadequate, confidentiality, security, and privacy are jeopardised. If restrictions are too stringent, not everyone can access the information they need to perform their tasks effectively. In the case of very sensitive information, even a particular field in a record (or the entire record) might be accessible only to users with the highest levels of authority.

E4 Accountability

In the commercial world, accounting concerns the theory and practice of setting up, maintaining, and auditing an organisation's financial records. Accounting's function in the virtual private network world is similar. Virtual private networks must keep a record of (or log) user and system actions for security-reporting purposes. Accounting addresses issues such as what part of a network a user accessed and when, how often, and how long he or she had access. The accounting function is generally invoked once the authentication and authorisation functions are complete, although it does not depend on these two functions.

Strict accounting can involve recording literally every keystroke and mouse click that users make. This means that the accounting/audit trail can generate enormous log files. While authentication and authorisation are preventive security measures, accounting is a detection security measure to monitor possible infractions of the network access rules. Effective security is a combination of prevention and detection.

E5 Quality-of-service desiderata

Although quality-of-service criteria are not yet standard, most industry observers cite at least two quality-of-service complaints when it comes to applications running on a network:

- the network must have adequate bandwidth for the application and deliver information across the network with minimal (or at least acceptable) delay; and
- bandwidth and delay can vary from network to network (and within a single network as the volume of traffic fluctuates), however, if bandwidth for the application is insufficient or if users must wait too long for information, then the application will not run on that network.

The essentials desiderata are therefore bandwidth and delay. Other quality-of-service parameters can be added to enhance the network, but there is disagreement on the next most important attribute. For example, as applications increasingly feature voice and image/video support aspects like stable delays, reliability and information loss become significant — since stable delays prevent distortion of audio and video sequences, reliability indicates network availability and the likelihood of failure and information loss reflects the percentage of bits sent across a network that fail to arrive at the destination (most likely because of errors on the network).

Security is another quality-of-service feature that is essential for virtual private networks — comprising network privacy and authentication (in addition to creating and adding counter-hacker devices). Thus the quality-of-service parameters needed for trusted networks can be categorised as:

- essential — adequate bandwidth, minimal delay;
- highly desirable — stable delays, reliability and no information loss; and
- required for virtual private networks — security.

Bandwidth considerations

There is a widespread recognition that the market conditions for ‘bandwidth’ (broadly speaking, communications capacity for data services) is likely to be a key factor of production for the emerging information economy.[76] The bandwidth requirements of data network applications vary considerably, from a few bits per second for text-only e-mail messages to megabits per second (Mbps) for complex graphics file transfers. Many data network applications (and many new voice or video applications) are 'bursty' in nature, generating different numbers of bits per second, and may be able to work for long stretches without transferring any bits between origin and destination — a further complication.

The recent Bandwidth Inquiry’s conclusions for Australia are that the market outlook for the trunk network, particularly in the inter-capital markets, is reasonable, with competition likely to develop further over the next few years. However, while the trunk infrastructure to provide services is largely already in place, substantial anecdotal evidence suggests that there are problems with making data services available in a timely and affordable manner in practice, particularly outside the central business districts of Sydney, Melbourne and Brisbane. If this shortfall in customer available bandwidth is not addressed, there is a risk that Australia’s ultimate performance in the global information economy will be adversely affected.[77]

---

[76] National Bandwidth Inquiry(1999), Report of the Australian Information Economy Advisory Council, Commonwealth of Australia, AGPS.

[77] National Bandwidth Inquiry(1999), *op. cit.*.

While the Inquiry felt that competition could more or less be relied on to supply the market's demand for bandwidth in metropolitan areas it was not so sanguine about prospects in regional Australia:

> … the problems of the supply of diverse services to regional and rural Australia appear to involve structural issues at two levels. First, the real costs of supply of these services are greater and this is inevitably reflected in pricing. While technological developments may reduce the differential and encourage competition in many areas, the greater attraction of 'low hanging fruit' represented by dense metropolitan markets will mean regional areas will probably always lag behind their urban counterparts in achieving equivalent levels of services and prices. Second, where these prices are contained by regulatory measures, this can result in undesirable supply and service outcomes. Again, the solution set must be one that takes account of both the transitional and structural issues, while minimising any negative impact of responses to one category of issues on the other category.

Relevant inquiry findings

The Inquiry identified the following as key industry segments which are likely to have a particularly high demand for bandwidth: retail trade, property and business services, health and community services and education.

Currently installed domestic backbone bearers (eg installed trunk optic fibres) are likely to be capable of supplying adequate bandwidth capacity to meet current and likely future demand in most parts of Australia over the next five years. However, some rural and remote routes do not currently have sufficient capacity or it is often not provided in a timely manner. Moreover, the installed capacity is immaterial if it is not in fact available to the customer. Capacity can be substantially increased through new technologies, principally dense wave division multiplexing (DWDM), which makes it possible to upgrade the capacity of existing optic fibres by huge multiples easily, although commercial viability will be a consideration.

There is strong anecdotal evidence to suggest that there are problems in practice with the translation of the potential trunk capacity on the optic fibre network into actual capacity available for data services, particularly in regional Australia. This lack of customer access to bandwidth on a timely basis would seem to flow from problems in the customer access network and from the provisioning priorities within carriers' systems.

Backbone bandwidth capacity is currently subject to highly concentrated ownership with Telstra dominating almost all markets and the sole provider of a ubiquitous network. While infrastructure competition will broaden to include a number of fixed and mobile operators, many rural and remote areas will not experience significant competition over the period being considered by the Inquiry (through to 2005).

However, it should be noted that bandwidth alone cannot address the quality-of-service needs of all network applications today. For example, even simple bandwidth is not dependable over the Internet (or any other network using Internet protocols). All packets appear identical on the Internet. They are all routed as

quickly as possible to their destinations. If individual packets do not arrive in time, the higher levels of the protocol stack, most notably TCP, must determine how to manage lost or missing information.

Privacy and security

Virtual private networks allow electronic transactions with at least some measure of privacy and security. But there will always be some risks to privacy and security on networks, whatever measures are taken. The trick is to incorporate sufficient measures so as to provide a level of privacy and security that people accept as appropriate under the circumstances. An what is considered appropriate and acceptable in the circumstances will change over time — for example there is a growing expectation that new cars will be fitted with air bags as well as seat belts (accepting that such measures will not eliminate fatalities when traffic accidents occur).

Adding privacy and security to a public network such as the Internet will usually involve making hardware and software modifications in order to achieve the added level of surety sought. The main discussion on security standards (including encryption) is in Section D6 of Appendix D on security standards.

Understanding virtual private networks means coming to grips with a new language: including such things as firewalls, proxy servers, secure remote access, tunnels, authentication certificates, and the mathematically complex world of encryption (see Box E2).

Box E2: A VPN primer

A virtual private network (VPN) is a secure, encrypted connection between two or more points across the Internet. Information is sent via tunnelling (see below), which is the practice of encrypting and encapsulating traffic in Internet protocol (IP) packets. Wide area networks (WANs), security products, and routers are all components of the overall VPN. The use of the Internet and the Web for e-commerce is a major impetus of the development of VPNs, which offer a way to send private IP data over a public network infrastructure. The basic idea is to provide an encrypted IP tunnel through the Internet that permits distributed sites to communicate securely. The encrypted tunnel provides a secure path for network applications and requires no changes to the application.

Cryptography

The cornerstone of many forms of security, even authentication, is using some for of encryption. Encryption is the goal of network cryptography, a term that has been extended from its root of secret writing to indicate any use of encryption techniques. Because current cryptographic techniques in use are complex, only more recent, powerful computers can apply them in the time frames required for networking.

Tunnelling

Normally, the bits flowing across the Internet are organised into frames, which contain IP packets. In turn, the IP packets usually contain TCP segments, and a field in the IP packet header identifies the packet content.[78] Each process is technically a form of encapsulation: segments encapsulated in packets and packets encapsulated into frames. Any receiver knows that an IP packet is inside a frame, and the IP header indicates whether a TCP segment, or something else, is inside. The receiver must know the content type to process it correctly; otherwise the content will appear to be merely a haphazard collection of bits.

Tunnelling obscures the true structure of the content of frame, packet or segment (or all three). Thus what may appear to be a regular IP packet might not contain a segment (regardless of what the packet header claims), but rather a frame. If the packet is intercepted, however, the interceptor might not know what information is contained within the packet. A virtual private network tunnelling gateway establishes secure tunnels between itself and similar gateways to ensure that packet contents — even if they are intercepted — will not be easily understood.

Firewalls

Firewalls are critical to VPNs. Firewalls separate the inside of a network (Intranet) from the outside of the network (Internet), while allowing access to authorised users. They are also used to limit employees' activities on the Intranet and screen downloads for viruses.

Source: Based on Computer Technology Research Corporation, *Virtual Private Networks: Achieving Secure Internet Commerce and Enterprisewide Communications* (www.ctrcorp.com).

[78] Hence reference to the Internet connectivity protocol as TCP/IP.

F LEGAL CONSIDERATIONS

In 1996, the High Court of Australia in *Breen v Williams* held that medical records were "the sole property of the doctor who held all rights associated with ownership and that the records remained the intellectual property of the medical practitioner who had written them".[79]

The only exception to this general rule recognised in *Breen v Williams* is investigative reports such as pathology and radiology reports. The High Court stated that the physical reports are owned by the patient or the organisation paying for the investigation to be conducted.

In relation to records created in a health care facility where treatment is provided, records created by employees are owned by the employer. Whether records created by independent contractors are owned by the facility will depend on the nature of the contract between the contractor and the facility employer.

In any case, the present law in Australia is that patients do not own the health records which pertain to them.

Applying the *Breen v Williams* principles to the electronic health record is difficult as the decision was limited to medical records only. In the USA, the issue of who owns the data in computer-based patient records has not been resolved.[80]

The electronic health record will include entries authored by numerous individuals. Applying *Breen v Williams* principles literally, each of the individuals and facilities where recorded treatment is provided will have an ownership claim over their respective entries. These principles will lead to an unworkable situation where the consent of each author and facility could be needed before information can be accessed or used by any other party. This outcome suggests legislative involvement is required.

NSW Health has recently recognised a view that "ownership of data is an outdated concept"[81]. Noting the existence of concepts more relevant to the electronic age it stated: [82]

> With the development of electronic records and more widespread use and sharing of data, perhaps a more useful concept is that of custodianship.

It is suggested that the focus should not be on 'ownership' of health records, that being a concept which is more closely aligned to a traditional 'document'. Rather,

---

79 (1996) 138 ALR 259.

80 Tang PC and Hammond WE (1997), *A progress report on computer-based patient records in the United States*, in *The Computer-based Patient Record: An Essential Technology for Health Care*, rev edn, National Academy Press, Washington DC, p.11.

81 NSW Health (1999), *Ethical Management of Health Information*, discussion paper, p.13.

82 *ibid.*

what is relevant to both health consumers and providers is the ability to exercise control over the content and the use of health record data. NSW Health put forward the suggestion that it may be desirable to develop principles which recognise the rights of the "data collector, the intellectual rights of the provider and the rights of the community at large and individuals to whom the information relates".[83] Concepts concerning control and use of the electronic health record are discussed below.

F1 Privacy, confidentiality and security

Privacy, confidentiality and security are inextricably linked. The House of Representatives' Standing Committee examining health information management and telemedicine defined those concepts terms relevant to this discussion as follows:

- *Information privacy* — the ability of an individual to control the use and dissemination of information that relates to him or her self.
- *Confidentiality* — a tool for protecting privacy. Sensitive information is accorded a confidential status that mandates specific controls, including strict limitations on access and disclosure. These controls must be adhered to by those handling the information.
- *Security* — all the safeguards in a computer-based information system. Security protects both the system and the information contained within it from unauthorised access and misuse, and accidental damage.*[84]*

Health Online[85] recognised that the degree to which individual consumers' privacy is actually protected (and perceived to be protected) is critical to the success of initiatives aimed at greater sharing of personal health information by electronic means. It has been said that "security, privacy and confidentiality concerns have become major barriers to widespread implementation of (computer-based patient record) systems and sharing data" in the USA.[86] In addition, virtually unconditional trust placed by a patient in his or her health care provider that information imparted to the provider will remain confidential, is fundamental to the patient's relationship with the provider as well as the quality and appropriateness of the care received.[87]

---

83 *ibid.*

84 House of Representatives Standing Committee on Family and Community Affairs (1997), *Report on Health Information Management and Telemedicine*, Paragraph 5.7.

85 National Health Information Management Advisory Council (NHIMAC 1999), *Health Online: A Health Information Action Plan for Australia*, Commonwealth of Australia, Canberra.

86 Tang and Hammond, *op. cit.*, p.11.

87 The classic protection of medical privacy, of course, is the 'medical secrecy' compact, originating with the Hippocratic ideals, that is embodied in the licensing of medical practitioners and other health care providers, and that is embraced in most health care contracts and medical confidentiality laws. Despite considerable erosion in recent years, this confidentiality undertaking still has validity, is thought to encourage patients to enter fully into

Coupled with the issue of privacy is the related notion of confidentiality. Health service providers owe to their patients a duty to keep confidential information disclosed to them in the course of the professional relationship. The duty may be based on legislative provisions or at common law. Exceptions to the duty are generally prescribed in specific terms in legislative enactments. Given the sensitive and personal nature of information recorded on the electronic health record, consumers will have real concerns about the level of access granted to 'strangers' to information they imparted to their health care providers and which was recorded in an electronic health record. On the other hand, the public interest may be served through access to such information for policy, planning and research purposes. The dilemma has been expressed as follows:[88]

> The ethical problem is to maintain the paramount welfare of the individual while continually exploring new ideas which may improve that welfare.

Security safeguards are inextricably related to the concepts of privacy and confidentiality. Mechanisms must be in place to prevent unauthorised access and misuse of the health information contained in the electronic health record. For example, the fundamental challenge for health research is to respect individuals' privacy while at the same time pursuing justified access to personal data in order to provide health benefits to society as a whole. Further, many of the patient identifiers currently used (eg name and address) could be omitted if a reliable, but suitably controlled, coded identifier could be used to support identification — and this could add to (rather than detract from) privacy because the mapping between individuals and patient identifiers can be tightly controlled (eg on a need-to-know basis).

The legal environment in which an electronic health record exists has to accommodate all of these conflicts and concerns.

Current legal environment

Public sector

The Commonwealth, the States and the ACT, each have Freedom of Information legislation which grants to the public a general statutory right to obtain access to documents held by public agencies. This right is subject to limitations and exemptions based on a range of concepts, including the public interest. For example, in some circumstances, information communicated in confidence by or to an agency may be exempt from disclosure as may information about an individual which is reasonably likely to harm that person if disclosed to him or her.

---

health care and research transactions, and is valued by the public and by health care providers. All OECD nations have laws protecting medical confidentiality to varying degrees (Source: OECD DSTI/STP/BIO(99)3, *Scoping study for an OECD project on data protection in transborder flows of health research data*, Dr. William W. Lowrance).

88 *Health Online: A Health Information Action Plan for Australia*, p.20.

Public hospitals and community health centres are public agencies for the purposes of Freedom of Information legislation. Accordingly, members of the public are generally entitled to access their health records relating to them which are in the possession of these bodies unless there is a statutory power to withhold the records or parts of them. The person concerned has a right of appeal against a decision refusing access.

The *Privacy Act 1988 (Cth)* presently extends only to Commonwealth and Australian Capital Territory Government agencies and certain businesses providing or reporting on consumer credit. The Commonwealth's limited involvement in delivery of health services means that most health service providers are not bound by that Act.

The only other Acts of Parliament which confer public rights of access to health information are the ACT *Health Records (Privacy and Access) Act 1997* which came into force on 1 February 1998 and the NSW *Privacy and Personal Information Protection Act* 1998. The *Health Records (Privacy and Access) Act* applies to records kept by any health service in the ACT, in both the public and private sectors. It also applies to personal health information in documents kept by organisation other than health services. The NSW Act establishes privacy principles that must be observed by all NSW public sector agencies and entitles individuals to access information which relates to them.

Private sector

Only the ACT has legislated to provide members of the public with a general right of access to private sector records. New South Wales has given limited rights of access under regulations governing private hospitals, day-procedure centres and nursing homes.[89] Apart from these legislative provisions and the right to obtain court orders for the production of health records in some circumstances, there is currently no statutory right of access to records created in the private sector. As stated earlier, the writer of the health record in the private sector is generally entitled to determine whether patients can access that record, unless a Court orders otherwise.

The situation in the Australian private sector differs from many other countries. As one commentator said "Australia is now lagging behind most of the developed world (in regard to patient access to their medical records)."[90]

This situation will change if the *Privacy Amendment (Private Sector) Bill 2000*, currently before the Parliament is passed in its current form. The Bill would give statutory force to the *National Principles for the Fair Handling of Personal Information* — principles widely accepted as representing good practice for the handling of personal information. Under the Bill, consumers will have the right of

89 Private Hospitals Regulations 1996 (NSW), Day Procedures Centres Regulations 1996(NSW) and Nursing Homes Regulation 1996 (NSW).

90 Carter M (1998), *Should patients have access to the medical records?*, MJA (vol. 169) p.596.

access to records relating to them which are held by private doctors and private organisations. Specifically, the Bill states that individuals must be given access to health information held by those individuals and organisations to which it applies unless, amongst other things, providing access would pose a serious threat to life or health of any person.

Introduction of electronic health records

Unless Parliament specifically legislates in respect of the electronic health record or enacts legislation, with the co-operation of States and Territories, which establishes generic national rights of access for all patients to their health information, regardless of where services are received and whether a person is treated publicly or privately, all the different access principles which exist today will apply to the electronic health record. This will be the case even after the enactment of the *Privacy Amendment (Private Sector) Bill*.

Because an electronic health record is a virtual integrated record, each individual will be able to gain access through a variety of channels depending on where the request is made. The principles applicable will depend on to whom a request is made and whether principles pronounced in *Breen v Williams* continue to apply. For example, under Freedom of Information legislation members of the public are entitled to access documents in the possession of government agencies, subject to various statutory exemptions. In Victoria, the *Freedom of Information Act* specifically provides for access to be given to computerised information. In addition the concept of 'possession' has been interpreted widely in Victoria to include both actual or physical possession and constructive possession. 'Constructive possession' of a document is a right to immediate possession of, or a right and power to deal with a document.[91] Therefore, with the introduction of the electronic health record throughout Australia, Victorian public hospitals, for example, could immediately access all parts of such record (unless restrictions are imposed on access). A member of the public will be able to access their entire electronic health record (even non-hospital records) if a request for access is made to a public hospital. However, if such request for access is made to a doctor in the private sector (assuming *Breen v Williams* still applies), access may not be granted to the doctor's notes held in the private sector. Similarly, if a request is made in NSW, the NSW *Freedom of Information Act*, or the various regulations governing nursing homes, day procedure centres and private hospitals will apply. Put simply, introduction of the electronic health record on a national basis will result in numerous different legal principles applying to requests for access to the same document.

---

[91] Re Guide Owners' and Friends Association (1988) 2 VAR 405, Re Midenhall and Department of Premier and Cabinet (No.2) (1995) 8 VAR 478 and Birrell and Victorian Economic Development Corporation (1989) 3 VAR 358.

The introduction of a nationally uniform statutory framework which sets out consumers' rights of access to the electronic health record would address these problems. On a preliminary review, such legislation will have to be enacted by the Federal Parliament and all State and Territory Parliaments. Alternatively, State Parliaments may need to refer specific powers to the Commonwealth Parliament as the Australian Constitution does not empower the Commonwealth to enact legislation to grant access to documents held by all health care providers and facilities.

Introduction of a national statutory framework will necessarily require judgements to be made by the legislatures about the extent of consumer rights of access and control. Given that consumer acceptance of the concept of electronic health record is critical, Parliaments may choose to give consumers a statutory right of access to their own records and those of their young children, as a matter of law. The granting of such a statutory right would reverse the current position in the private sector and is consistent with the *Privacy Amendment (Private Sector) Bill*.

There appear to be good public interest reasons why consumer rights of access should be limited rather than absolute. The medical profession accepts valuable benefits for patient care result from encouraging third parties to provide information about patients on a confidential basis. Health care providers may not be able to obtain relevant information if the person possessing those details fears that source details will be passed to the consumer. Similarly, receipt of some information (in particular, information relevant or relating to mental health) may detrimentally affect an individual consumer, either mentally or physically. Numerous Acts of Parliaments, including Commonwealth and State *Freedom of Information Acts*, infectious diseases notification legislation and the *Privacy Amendment (Private Sector) Bill* recognise that the individual right to privacy is not absolute, justifying some exceptions on public interest grounds.

Parliament will also need to make judgements regarding third party access to health information and the duty of confidentiality owed to patients. As stated above, health service professionals generally have a duty to maintain confidentiality over the information imparted to them during the course of a professional relationship. As a general rule, the common law prohibits confidential information from being disclosed by a health service provider without the consent of the patient. Unless Parliament legislates for specific exemptions, the common law duty will require express consent to be obtained from each patient before information entered onto the electronic health record can be shared with a third party. Otherwise, by entering data onto the electronic health record a treating professional will disclose confidential and identifying information to a third party.

Parliament will need to determine what, if any, exceptions to the duty of confidentiality will be permitted. Such determination requires a balance to be drawn between protection of confidentiality and other public interests. This approach is adopted in the proposed *Privacy Amendment (Private Sector) Bill*. There are perceived benefits to society through policy makers, planners and

researchers accessing health information. Parliament may choose to grant to specific parties, or categories of entities and individuals, access to non-identifying data for the purposes of policy making, planning and/or research. The 1997 House of Representatives' Standing Committee supported the view that "health data and information for secondary purposes is contingent on that information being deidentified".[92]

In addition, situations arise when specific individuals seek access to a consumer's health information for the benefit of the consumer, although he/she is unable to consent to such access. For example, a treating practitioner may require such information urgently to facilitate life protecting medical treatment. In these circumstances, the electronic health record should be available. Parliament may need to define the criteria which determines whether and to what extent access is granted to third parties without the individuals approval. The mechanisms introduced to protect health consumer privacy should not be so onerous that a treating professional is denied immediate access to urgently required health information for treatment purposes. A similar recommendation was made by Health Information Management and Telemedicine Standing Committee in 1997.[93]

Consistent with the granting of consumer access to their own records, consumers should be informed who else has had access to their records and when that access was granted.

Parliament will also need to consider the extent to which third party access to health information should be limited in terms of time and content. Currently, health information relating to an individual consumer is held by a number of different individuals in various locations. For example, general practitioners, specialists, hospitals and pharmacists may all hold different information about an individual health consumer. Introduction of the electronic health record enables all health information relating to a health consumer to be brought together as a virtual integrated record. Unless restrictions are introduced, any individual who has or had a role in a person's treatment could access all of that person's health information. Parliament may choose to require health consumers to nominate individuals (specifically or by description) who are entitled to access specific information. This option is consistent with the notion of providing patients with at least a degree of control over their own health information.

Another issue to be considered is whether consumers are to be able to 'opt out' of the electronic health record, wholly or partly. Will consumers be able to require that information be not included in their electronic health record? As recognised by NSW Health, an 'opting out' system will result in data held on the electronic health

---

92 House of

0.Representatives Standing Committee on Family and Community Affairs *op. cit.*, Paragraph 5.72.

93 *Ibid*.

record being incomplete. The benefits of the electronic health record could be significantly reduced.[94]

Storage and retention of records

One of the guiding principles in making retention decisions is the statute of limitations (the period during which a person is able to bring a claim against a provider of health care services).

A major reason to retain records is to have the information available for future care. A number of decisions can be made about information that is to be available to guide future care. For example, the value of information that might have been critical to monitor the hour-by-hour progress of an individual admitted to intensive care unit will likely fade with time — suggesting retaining all possible information (leaving aside considerations of expense) in a longitudinal health record may make little sense. What is needed is consensus on this issue to guide retention decisions — a consensus that can be expected to change over time.

A range of storage media is available for storing electronic health records (and the range can be expected to widen over time). Apart from considerations of durability, what medium to use will depend on the urgency with which various kinds of information may need to be retrieved (so that, for example, as storage-hungry components of the electronic health record — such as x-rays or CT scans — date they may be stored off- rather than on-line).

F2 Medico-legal issues

While the primary purpose of the medical record is to benefit the patient particularly as to continuity of care, the secondary purpose is to provide a medico-legal record of the care provided. There are significant medico-legal implications associated with the introduction of the electronic health record. They relate to the duty of care owed by a health service professional and the usefulness of the electronic health record as a means of legally documenting care provided to a patient.

94 NSW Health, *op. cit.*, p.14.

Duty of care and risk of liability

Health service providers owe their patients a duty of care to exercise reasonable care and skill in the provision of professional advice and treatment With the introduction of the electronic health record, the standard of care required of these professionals is likely to alter as the environment in which they operate changes. Health service providers will have access to more complete information in a timely and accessible fashion. If they fail to access and incorporate all available information into their decision making, such failure is likely to constitute a failure to achieve the required standard of care.

Further, once health service professionals become aware that their entries form part of a national integrated electronic system which can be accessed by other professionals throughout Australia, they are more likely to ensure that their own entries are meaningful, comprehensive and accurate. Currently, only a very limited number of providers can access the notes made by a treating colleague. With the introduction of the electronic health record, this number will increase as more individuals will be able to access health information. As the ability to access increases, so does the risk of harm being suffered by a patient if information on the electronic health record, entered by a provider is incomplete or inaccurate. If another professional accesses the incomplete or inaccurate information, relies upon it and makes a wrong and damaging decision as a result, the author of the first entry could be held liable for that error.

On the other hand the electronic health record has the potential to reduce liability risks and improve quality of care if the system incorporates computerised alerts which warn providers of such matters as unwanted interactions between medications or the need to check the effects of a medication on specific functions. Additional benefits will flow from computers being able to retrieve information in any order, perform rapid information searches and data processing.[95] Paper records suffer the problem of data being fixed in an exact sequence. Also, the problem of illegible writing will disappear.

Many studies have shown that a principal reason why patients chose to sue health service providers is poor communication. Theoretically, the electronic health record will improve communication between health consumers and providers since consumers will have greater access to their health information. Therefore, at least theoretically, the institution of legal proceedings against health service providers and the risk of liability may be reduced.

It is uncertain what the legal impact of the introduction of the electronic health record will be. To remove the uncertainty Parliament may choose to enact legislation which clearly outlines the duties of health service providers in relation to the electronic health record.

---

95 Powsner, Wyatt and Wright (1998), *'Opportunities for and challenges of computerisation'*, The Lancet vol 352, 14 Nov, p.1617.

Use of the electronic health record in court

There are difficulties to overcome if the electronic health record is to be relied upon for legal purposes. In general, computerised documents can be admitted as evidence in court. However, the processes which currently have to be followed are cumbersome.[96] In addition, it is not difficult to envisage allegations being made by consumers and their lawyers of incorrect transcribing of data onto the computer system and of data being altered some time after the initial entry was made, so that the electronic health record allegedly does not reflect what actually occurred at the time in question. Further potential difficulties are associated with the content of the electronic health record. Unless these problems are addressed, the evidential value of computer generated data in a court will be limited.

Problems of incorrect transcribing can be overcome by avoiding transcribing altogether and having health service providers enter information directly onto the electronic health record. Utilisation of specialist technology, such as voice recognition equipment, may make this proposal viable. The second problem of alteration of an entry can usually be resolved through the existence of a computer audit trail. While the electronic health record must allow entries to be updated, it must be virtually impossible to over write or erase previous entries. All alterations must be recorded as such.

In order to at least maintain the level of protection currently afforded to health care professionals by their notes, the electronic health record must be comprehensive and able to accommodate a wide range of health care disciplines and settings. In terms of comprehensiveness, the electronic health record must make provision for the same type of information to be recorded as is presently recorded in paper documents; including facts, observations, interpretations, plans, actions and outcomes. This is consistent with clinical user requirements acknowledged by the Good Electronic Health Record (GEHR).[97]

Further, the electronic health record must also be able to identify the author of each entry and the time the entry was made. With paper records, this is done by way of a signature and noting the relevant time. Of itself a signature has no legal value. The value lies in the fact that the author of an entry attests to the correctness of that entry and is able to be identified as the person who made the entry. The electronic health record must accommodate like attributes.

F3 Overseas views on legal aspects electronic health records

Timely completion of record entries supports patient care and meets expected standards for business records. The paper environment is very forgiving in this area.

---

96 See, for example, section 55B *Evidence Act 1958* (Vic).

97 Schloeffel, *GEHR (the Good Electronic Health Record) and other EHR Architectures*, p.4.

Individual rights

Laws must protect individuals' rights in relation to the information about them contained in electronic health records, including penalising inappropriate access to, and use of, personal health information. In the USA, a couple of states have addressed the issue of appropriate use and disclosure (see Box F1).

Box F1: Appropriate use and disclosure: Washington State

1 Health care information is personal and sensitive information that, if improperly used or released, may do significant harm to a patient's interests in privacy and health care or in other areas that may concern patients.

2 Patients need access to their own health care information as a matter of fairness to enable them to make informed decisions about their health care and correct inaccurate or incomplete information about themselves.

3 To retain the full trust and confidence of patients, health care providers have an interest in ensuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information.

4 Persons other than providers obtain, use, and disclose health record information in many different contexts and for many different purposes. It is the public policy of Washington State that a patient's interests in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers.

5 The movement of patients and their health care information across state lines, access to and exchange of information from automated data banks, and the emergence of multi-state health care providers create a compelling need for uniform law, rules, and procedures governing the use and disclosure of health care information.

Source: Murphy, G. F. *et al*. (1999), *Electronic Health Records: Changing the Vision*, Harcourt Brace & Co., Philadelphia (p.71).

Data should be collected and used for a purpose — and this should be reflected in applicable law. In health care the primary purpose is to assist in decisions about health care for the individual in respect of whom personal health information is collected. Such data may also have other valuable uses, for example to contribute to the evidence basis of what kind of care seems to work for whom (and under what circumstances), and to aid in planning future health services. But it is important that the individual is aware of such secondary purposes and, ideally, consents to such uses — particularly if such uses retain data that are capable of identifying the individual concerned (rather than being used in de-identified form for, say, population health purposes).

Individuals increasingly expect to have access to their personal health information and to consent to having their health records (or parts of them) made available to health care providers other than those who may have created the record. They also

expect that their personal health information will be kept confidential and that systems designed to store that information will be secure.

Provider rights

The law usually regards that part of the patient record created by a provider as a business record of that provider. The ownership of an electronic health record to which many providers may have contributed (particularly over a lifetime) — as would be the case with an electronic health record — is arguably more problematic (except in the above contributory sense).

Consumers also have an interest in health information held in their health record(s), and in the manner in which they are handled (including how and under what circumstances their personal health information may be accessed by others). In recognition of this aspect of personal health records, there is now a world-wide trend to grant consumers right of access to such records. Thus, rights of access are being considered as well as ownership and control.

Nevertheless, as with consumers, providers have the right not to participate in a system of information exchange should they elect not to. This would create a difficulty in the case of consumers who did want their personal health information made available to other providers — in which case they would have to seek out providers who were prepared to comply with their wishes.

Some providers might seek to distinguish health information (eg in its factual dimension) from what they may regard as their intellectual property (eg the recording of the diagnosis) and only wish to contribute the former kind to any system set up to exchange health information. Again, that is their right, but again also, consumers unhappy with such a decision could be expected to seek out health care providers who are prepared to act without such a restriction on their patient's behalf.

F4 Summary

When it comes to health information, the law must protect both patients' and providers' rights and penalise inappropriate use and disclosure of such information, most particularly personal health information (ie health information identifiable with an individual).

G COMMISSIONED STUDY: COSTING THE PROPOSAL

The Taskforce appointed Planning And Review Consultants to prepare indicative costings of its proposal for a national health information network (HINA), including required infrastructure, the necessary 'building blocks' (see Chapter 10) and appropriate governance arrangements. While the costings are an attempt to estimate what would be involved in creating and operating the Network, no attempt has been made to apportion costs between the Commonwealth and the States and Territories (or between the public and private sectors).

The approach taken by the consultants divides the work on the project into three major streams:

- governance;
- development; and
- implementation.

Establishment of network governance arrangements will be one of the first activities undertaken. There will be an initial period of development of the legislative and operational environment for HINA. Following the initial development, work will commence on the implementation of the Network. There will be some ongoing development work in the first years of implementation.

While there are significant costs involved in governance and development, these are reasonably well defined. Detailed financial modelling therefore focused on the implementation stage.

The HINA financial model developed by the consultants estimates the costs of building and operating the Network over a 10-year period. The model identifies costs by major sector (medical practitioners, medications, pathology, imaging, public and private hospitals), the data processing and storage components required for network development, capital and recurrent costs and approximate timing — before focussing on the ongoing costs of operating the Network. This appendix does not, however, identify the savings that will be achieved by virtue of the existence of HINA (refer Chapter 13 for a consideration of this aspect).

G1 Governance

While there are two suggested options for governance in the Report, costing of the governance arrangements was based on the existing structures approach, namely a Unit in the Commonwealth Department of Health and Aged Care.

The costing allows for a 15-person Unit and a smaller Access Control body. It is estimated that the governance arrangements will cost $2 million per annum.

Table G1: HINA governance ($m)

Item	*2001/02*	*02/03*	*03/04*	*04/05*	*05/06*	*06/07*	*07/08*	*08/09*	*09/10*	*10/11*	*Total over 10 years*
Governance	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	20.00
Total	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	20.00

Source: Planning and Review Consultants.

G2 Development

There is a number of areas of work involved in preparing for the implementation of HINA, namely:

- privacy and confidentiality;
- security and authentication;
- standards;
- telecommunications strategy;
- lead implementation and satellite sites;
- uptake of information technology; and
- community liaison.

Privacy and confidentiality

There is considerable work that needs to be undertaken in creating the appropriate privacy and confidentiality environment in which HINA will operate. However, others are funding much of this work. An allowance of $0.3 million has been made for development of a uniform privacy code covering public and private sectors. Support for government privacy regulators is also provided to cover extra work arising from establishing a complaints mechanism for the Network ($5 million over 8 years).

Security and authentication

The major work included in the costing is the establishment of the public key infrastructure (PKI) across the Network. Based on work undertaken by the Health Insurance Commission (HIC), this is estimated to cost approximately $15 million over the first 5 years. A further allowance has been included for development of a health sector security standards framework and processes for uniquely identifying providers and facilities.

Standards

One of the major activities in the development phase will be the specification of national standards covering data, classifications, messaging and storage (refer Chapter 10). This work is estimated to cost approximately $4 million. Allowances

are also included for ongoing standards work and on international harmonisation of those standards (estimated at $0.3 million per annum for 10 years).

Telecommunications strategy

This component of HINA development costs includes work on developing a strategy for health communications for the next 5 years — estimated to cost $0.25 million in the first year. No allowance is made for any physical infrastructure that is not health-specific (expected to be funded through other sources).

Lead implementation and satellite sites

Development of a lead implementation site will be a complex process and will be the focus of development work for the national rollout of the Network. An amount of $8.4 million has been estimated to cover the development work involved in the lead implementation site, covering the development of standard 'event summaries', applications, standards implementation, source system interface development network planning study, project team costs and evaluation. A further sum of $4.5 million for the construction and operation of a data centre is included later in the implementation costs. These funds will be spent in the first 2 years.

Uptake of information technology

Facilitating the uptake of information technology by health care providers will be an important element of the change-management work required to successfully implement HINA. A sum of $0.65 million has been allowed for the development of education and training tools and the identification of key infrastructure and standards barriers. A further sum of $53 million has been allowed for the provision of incentives to some providers to adopt technologies necessary to connect to the Network.

Community liaison

Ensuring community support for HINA will require considerable resources. The costing includes a sum of $2 million for an extensive consultation process and $8 million for a public communications strategy. A further sum of $2 million has been included to support training of network users.

Cost estimates for development work

Total development costs of the project are estimated at around $100 million (Table G2).

Table G2: HINA 'building blocks' ($m)

Item	*2001/02*	*02/03*	*03/04*	*04/05*	*05/06*	*06/07*	*07/08*	*08/09*	*09/10*	*10/11*	*Total over 10 years*
Privacy and confidentiality	0.30	0.30	1.00	1.00	0.50	0.50	0.50	0.50	0.50	0.50	5.60
Security and authentication	6.14	4.08	2.89	2.30	-	-	-	-	-	-	15.41
Standards development	1.13	0.63	0.30	0.30	0.30	0.30	0.30	0.30	0.30	0.30	4.15
Telecommunications strategy	0.25	-	-	-	-	-	-	-	-	-	0.25
Lead implementation site	5.20	3.20	-	-	-	-	-	-	-	-	8.40
Uptake of information technology	0.65	-	17.70	17.70	17.70	-	-	-	-	-	53.75
Community liaison	3.00	3.50	2.50	1.50	1.50	-	-	-	-	-	12.00
Total	16.66	11.71	24.39	22.80	20.00	0.80	0.80	0.80	0.80	0.80	99.56

Source: Planning and Review Consultants.

G3 Implementation

From the beginning of the third year of the project, the installation of data processing capacity will begin and health service providers and consumers encouraged to use the Network. The costs incurred in this work include capital and recurrent expenditure on the construction and operation of the data centres and associated communications and software. However, before discussing these costs it is necessary to explain the model in order to understand how these costs were derived.

In essence, the model takes known activity data on the use of health care services and a series of assumptions are made that allow this activity data to be converted into storage and performance requirements for the Network. These requirements are converted into a system specification that can then be costed in terms of capital and recurrent outlays. An important feature of the model is that it is designed to allow for exploration of different possible scenarios for the distribution of network storage nodes and changes in uptake rates.

The assumptions in the model used to convert the level of forecast service activity into needed data processing and storage capacities include:

- average event summary size;
  - Most 4 KB (1KB = 1024 bytes);
  - Hospital discharge summaries 8 KB;
  - Prescriptions and dispensing reports 1 KB;
- data archiving policies;
  - 3 years of online data;
  - 1 year of live online backup;
  - 7 years of near online archived data; and
- a contingency for extra growth of 30 per cent.

A key assumption was made about the likely rate of joining of the Network on the part of consumers. The rate of take-up was generally assumed to follow the following profile.

Table G3: Assumed overall take-up rate

Year	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
% take-up	0	0	8	15	27	38	50	61	69	77

Source: Planning and Review Consultants.

Information arising from contact by consumers with health service providers was identified as the source data. Six major streams of source data were provided for in the Network, and these are defined broadly by the type of provider involved in the health event:

- medical practitioners (general practitioners and specialists, excluding pathologists and radiologists);
- medications (includes both prescriptions and dispensing events);
- pathology;
- imaging;
- public hospitals and community health; and
- private hospitals.

In addition, the model incorporates a network management function that provides backup for all the specific data processors and archive facilities, as well as other administrative and analytical services.

Detailed activity statistics for health services were forecast over a 10- year period utilising Australian Bureau of Statistics population forecasts and forward estimates of health services by the Department of Health and Aged Care. These forecasts of 'health events' by type of service provider became the prime driver of the information needs for each sector. For each 'health event' involving consumers who have decided to participate in HINA, a standard event summary is generated for lodgement on the Network. Service providers would be able to access details (with the consumer’s consent) from event summaries lodged by other service providers.

Network demand is projected to be modest in the early years but increases rapidly. Coupled with increases in the base levels of activity, the increasing rate of participation on the Network is projected to result in an exponential rise in capacity requirements and activity levels (Tables G4 and G5).

Processing capacities — in terms of processors and online storage units — were estimated from a combination of data volume estimates, equipment capacities and the expected distribution of data centres. It appears that equipment capacities exist to enable a concentrated management of the Network, however, economies may need to be sacrificed if an overly distributed data centre network model were adopted.

Table G4: 10-year network storage requirements (Gigabytes)

Item	*2001/02*	*02/03*	*03/04*	*04/05*	*05/06*	*06/07*	*07/08*	*08/09*	*09/10*	*10/11*
Online storage capacity	-	-	317	809	1,551	2,450	3,459	4,580	5,644	6,695
Near online archive capacity	-	-	242	805	1,830	3,353	5,379	8,021	11,211	14,951
Total	-	-	558	1,614	3,381	5,803	8,837	12,600	16,855	21,645

Source: Planning and Review Consultants.

Table G5: Year 10 activity forecasts

Item	*Event summaries (millions per annum)*	*Reports accessed (millions per annum)*	*Estimated daily transactions ('000)*	*Data storage (GB)*
Medical practitioners	129	129	538	1,270
Medications	489		2,037	2,030
Pathology	23		95	310
Imaging	8		33	110
Public hospitals	51	47	211	930
Private hospitals	4	4	16	100
Online back-up	-		1,520	1,950
Near online archive	-			14,950
Totals	703	179	4,450	21,650

Source: Planning and Review Consultants.

Table G6: Year 10 network capacity and distribution

Item	*Greenfield data centres*	*Expansion of existing data nodes*	*Servers*	*Storage units*	*Storage capacity (GB)*
Medical practitioners	1	2	11	4	1,600
Medications	0	9	41	6	2,400
Pathology	0	1	2	2	800
Imaging	1	0	2	2	800
Public hospitals	0	8	16	16	6,400
Private hospitals	1	0	2	2	800
Network back-up and archives	1	7	39	43	17,200
Totals	4	27	113	75	30,000

Source: Planning and Review Consultants.

Cost estimates for implementation

The financial model calculates capital and operating costs based on the estimated system capacity and the costs of each system component. No external funding has been included at this stage, though there is a provision for such.

The financial model incorporates estimated standard cost profiles for three types of data centre — a centralised function, a new 'greenfield' centre and an existing data centre which could be incrementally expanded. The differences in operating costs are significant and highlight the importance of the extent to which data centres are distributed throughout the Network.

Total 10-year implementation costs broken down by recurrent and capital costs are shown in Table G7 (noting also that a 10 per cent contingency allowance is included, as well as the construction and operational cost of the lead implementation site data centre).

Table G7: 10-year network implementation: capital and recurrent costs ($m)

Item	*2001/02*	*02/03*	*03/04*	*04/05*	*05/06*	*06/07*	*07/08*	*08/09*	*09/10*	*10/11*	*Total over 10 years*
Capital	1.15	0.12	10.45	2.41	3.71	4.76	5.06	6.46	7.47	8.08	49.66
Recurrent	1.55	1.68	17.24	21.82	24.45	27.72	30.37	32.95	37.79	40.00	235.57
Contingency	0.27	0.18	2.77	2.42	2.82	3.25	3.54	3.94	4.53	4.81	28.52
Total	2.97	1.98	30.46	26.65	30.98	35.73	38.97	43.35	49.79	52.89	313.75

Source: Planning and Review Consultants.

G4 Summary

The overall indicative costs of the HINA project over 10 years (before inflation, GST and capital user charges) are estimated at $433 million and are summarised in Table G8.

Clearly, the cost estimates are sensitive to assumptions as to the take-up rate for consumer and provider participation and the size of the event summaries. Capacity calculations are also sensitive to backup and archiving policies and what is assumed in relation to consolidation of event summaries. Major risks to the capital cost estimates include: Network operations and management function migrating to a different technology; users downloading all event summaries (rather than extracts); applications increasingly drawing on other databases; and access by non-service providers becoming significant. The cost estimates can be refined as detailed capacity planning studies and 'proof of concept' projects are undertaken.

Table G8: 10-year governance development and implementation costs ($m)

Item	*2001/02*	*02/03*	*03/04*	*04/05*	*05/06*	*06/07*	*07/08*	*08/09*	*09/10*	*10/11*	*Total over 10 years*
Capital costs											
Implementation – capital	1.15	0.12	10.45	2.41	3.71	4.76	5.06	6.46	7.47	8.08	49.66
Development	16.66	11.71	24.39	22.80	20.00	0.80	0.80	0.80	0.80	0.80	99.56
Total Capital	17.81	11.83	34.84	25.21	23.71	5.56	5.86	7.26	8.27	8.88	149.22
Recurrent Costs											
Governance	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	20.00
Implementation-recurrent	1.55	1.68	17.24	21.82	24.45	27.72	30.37	32.95	37.79	40.00	235.57
Total Recurrent	3.55	3.68	19.24	23.82	26.45	29.72	32.37	34.95	39.79	42.00	255.57
Contingency	0.27	0.18	2.77	2.42	2.82	3.25	3.54	3.94	4.53	4.81	28.52
Total	21.63	15.69	56.85	51.45	52.98	38.53	41.77	46.15	52.59	55.69	433.31

Source: Planning and Review Consultants.

The development of a financial model for the Network has helped crystallise some of the issues requiring further consideration. Major issues that require further consideration include:

- the balance between decentralised data storage operations (with events summaries held close to point of generation) versus fewer (but larger) stroage nodes — where economies of scale can reduce both capital and operating costs;
- how applications will consolidate the data held in the event summaries to form reports and so reduce the amount of information required to be transmitted across the Network;
- backup and archiving policies as the compounding effect of accumulation of event summaries, combined with increasing participation rates and growth in demand for services leads to an unexpectedly rapid increase in data-storage requirements;
- whether archives will be held centrally or distributed throughout the Network; and
- the extent to which incentive funding may be required to accelerate the uptake of computerised systems by health care providers.

Considering the benefits of HINA to various parts of the health sector, there appears to be sufficient incentive for most providers investing in connections to the Network. Incentive funding may be required for some providers where the level of computer use in clinical practice and the requisites skill levels appear to be low. However, prospective productivity improvements and the ability to provide better advice to consumers argue for little inducement being required for most providers to cooperate in entering data for consumers wishing to participate. As vendors of clinical and health administration systems upgrade their products, they will be able to improve their competitive advantage by including interfaces to HINA as integral to their products.

The overall cost of HINA of approximately $433 million over a 10-year period is a very small proportion of total expenditure on health services in Australia. For example, it translates to approximately $23 per person per year or 6 cents per person per day. The major contributors to this low cost are:

- the large investment that has already been made by Commonwealth and State Governments in health-related information technology means that much of the public sector infrastructure requirement is already in place (or is planned for implementation); and
- the rapid development of electronic commerce technologies means that, by the time that the Network is operational, most of the infrastructure required for the source systems will be in place.

H HEALTH IDENTIFIERS: OPTIONS IN AN ELECTRONIC WORLD

H1 Context

New information and communication technologies create opportunities both to improve patient care and simultaneously give consumers more control over health care decisions that vitally affect them. The use of these new technologies can also lead to better quality information about our health services, allowing better planning and the provision of more cost-effective health care services, including for people living in regional Australia.

The key to this opportunity is the potential for new technology to provide the right health care information, wherever it is needed, when it is needed.

Currently, the vast majority of health care records exist as discrete paper-based entities held at a variety of locations, resulting in a fragmented and inevitably incomplete picture of a person's health needs and history. Traditional boundaries around health and community care settings further impede the flow of essential health information and effective communication. At the same time, access to relevant aspects of a person's health information at the point of care delivery is central to good clinical decision-making — providers and consumers need the right information to be available when health care decisions are being made.

In this context, the reliable electronic linking and transmission of personal health information can provide a powerful tool to bridge isolated 'outcrops' of information — and allow providers immediate access to essential clinical information. In the longer term, with the advent of a national health information network supporting a system of electronic health records, consumers will have the capacity to enable essential information relevant to their health care to be available at any time to health care providers of their choice.

In a world in which health consumers and health professionals will increasingly base their decision-making on health information exchanged electronically at the point of care, absolute certainty is required in the following three areas:

- the identity of the person to whom the information relates — the 'patient identifier';
- the identity of the facility or location from which the information has originated —the 'facility identifier'; and
- the identity of the person who has created each piece of information – the 'provider identifier'.

In principle, this is no different from the processes currently used by health professionals to assess the provenance and status of information that they receive in hard copy format. However, in an electronic world the tools for identifying people, providers, locations (and even individual items of medical equipment) will need to be both accurate and instantly verifiable at the point of care. Otherwise, many of the benefits of being able to exchange health information electronically will simply not be realised.

The need to develop a personal health identifier was identified in *Health Online: A Health Information Action Plan for Australia* (*Health Online*) as one of the key building blocks that needs to be in place to enable the safe and secure transfer of health information electronically — and as such, has been accepted by the National Health Information Management Advisory Council as an issue of high priority on its agenda.[98]

Increasingly, the Australian public has come to accept and use a whole range of identifiers in going about their daily business and lives. Examples include bank and credit cards; Medicare cards; Tax File Numbers; Medicare provider numbers; and, most recently, Australian Business Numbers.

This appendix focuses on the issue of identification (ie establishing who a person or place or thing is) — rather than the wider issues of proof of identity and authentication processes which are considered elsewhere in this report.

H2 Patient identification

The issue of a national patient identifier has been singled out as a high priority for action by the National Health Information Management Advisory Council — and for sound reasons.

There are many people in Australia who share the same name and some of these may even see the same general practitioner, specialist or other health professional. Australians often change address and sometimes their names. This causes confusion when it comes to matching the right health information with the right person, especially in an electronic world.

Unless critical health information exchanged electronically can accurately identify the individual to whom it relates, the benefits of new technologies for the health sector will go largely unrealised.

There is the potential for serious misadventure and adverse patient outcomes if transfer of clinical information — such as prescription data or medical history — is not accompanied by a foolproof and unambiguous system of patient identification. Current methods of identification using name, sex and date of birth, were recently

[98] National Health Information Management Advisory Council (NHIMAC 1999), *Health Online: A Health Information Action Plan for Australia*, Commonwealth of Australia, Canberra.

evaluated using Australian data and found to provide a sensitivity (accuracy) of only 89%.[99] This level of certainty is hardly adequate for health care decision making.

In addition to the critical issue of patient safety, there are other benefits to be gained by being able to more accurately identify individual health consumers across the health sector, including:

- improved continuity of care by being able to bring together health records held in different locations more efficiently and effectively — and building up a longitudinal health record;
- improved integrity, comprehensiveness and completeness of the information held in records by being able to more accurately assign the correct record to the right person;
- better quality data for: evidence-based decision-making; evaluation of service quality and health outcomes; development of clinical practice guidelines; and research;
- enhanced privacy through:
- having an identifier as the tool for pulling files and test results together rather than having to use readily identifiable names and addresses when transferring information electronically;
- the ability to easily scramble numerical identifiers or replace with a numerical pseudonym ('pseudonymisation'); and
- administrative efficiency gains by being able to access and file information more quickly and simply.

Health identifiers for individuals have now been introduced successfully in New Zealand and the United Kingdom. Also, the use of a health identifier has been mandated under the USA's Health Insurance Portability Act which requires that the Department of Health and Human Services adopt a number of standards to support the electronic exchange of administrative and financial information in the health sector — including identifiers for individuals, employers, health plans and health care providers.[100] In the Australian context, as far back as 1997, the House of Representatives Standing Committee on Family and Community Affairs in its report *Health on Line: A Report on Health Information Management and Telemedicine* advocated the assignment of a unique patient identifier in conjunction with an electronic health card. It also viewed with concern the slow progress in

[99] Kelman CW. (2000) *The Australian National Death Index,* Australian and New Zealand Journal of Public Health, 24-2 p91-2.

[100] *Unique Health Identifier for Individuals: A White Paper,* US Department of Human Services and Health, http://.aspe.os.dhhs.gov

resolving the issue of a patient identifier at the national level as it "directly affects the deployment and use of technologies."[101]

Some States and Territories have already developed their own systems for identifying individuals within their services, setting up the potential for providers and consumers encountering insuperable problems in accessing critical information around Australia, thereby negating the benefits to be gained through a national approach to electronic health records.

H3 Options for a national health identifier for individual consumers

While there are many that could be utilised for uniquely identifying individuals in an electronic world, these options generally fall into three categories:

- options that do not require a universal, unique identifier — such as Patient Master Indexes;
- biometric identification — which are based on unique physical attributes (eg finger prints, iris scans, DNA analysis, voice pattern recognition etc); and
- an identifier based on the assignment of a number unique to each individual — this number could be an entirely new one or based on an existing one, such as the Medicare number.

The first group of options includes such systems as Patient Master Indexes (or PMIs). PMIs link a patient's medical record number with a common set of other identifying characteristics — such as an individual's first name, last name, date of birth and other characteristics sufficient to achieve unequivocal identification. The Northern Territory has established such a system through its Client Master Index for individuals receiving services from community and/or hospital settings.

The second group of options (biometric identifiers) would be costly, requiring a substantial infrastructure and specialised equipment. They are also potentially more intrusive. Moreover, as some biometric forms of identification (such as fingerprints and DNA samples) are used for law enforcement purposes, the potential to link such information beyond the health sector poses a potential threat to privacy and could even deter people from seeking health care.[102]

The third option (assigning a number unique to each individual) is the one which would appear to be most easily implemented — either through the introduction of an entirely new 'health identifier' (which could be assigned to an individual on the

---

[101] House of Representatives Standing Committee on Family and Community Affairs (1997), *Health on Line: A Report on Health Information Management and Telemedicine*, AGPS, Canberra, p. 90- 92.

[102] US Department of Health and Human Services (1998) *Unique Health Identifier for Individuals: A White Paper*, Washington DC. Available at http://.aspe.os.dhhs.gov.

first encounter with a health service or sent out to every Australian individually), or by extending the current use of an existing number.

An option for a health identifier that has been flagged in several arenas (including *Health Online*) is to build on the existing Medicare card system. The Medicare card is already out there, is well accepted by the Australian community and is recognisable across the health sector. Much of the infrastructure for recording the number is already in place via embossing machines or magnetic readers. Expanding the use of the Medicare card would largely obviate the considerable costs that would be incurred in introducing an entirely new system of identification.

However, the number that appears on existing Medicare cards is not unique to the individual — a person can appear on several cards and may change card numbers over time. However, an identifying number which is unique to the individual and which is linked to the Medicare card number is held by the Health Insurance Commission (HIC). This number (commonly referred to as the HIC PIN) is currently not available on the card or to the consumers and is not used outside the HIC.

A relatively simple and cost-effective option, then, could be to either extend access to the HIC PIN or to reissue the Medicare card and include the HIC identifier.

Regardless of what option might be chosen for identifying an individual health consumer, there would clearly have to be stringent safeguards in place to ensure that privacy and confidentiality are maintained. Unless consumers and providers have confidence that their privacy is assured, any such tools will not be utilised.

Clearly, there is a number of risks that have to be recognised and appropriate counter measures put in place to manage those risks within acceptable limits.[103]

In brief, these risks include:

- potential breaches to privacy and confidentiality;
- unauthorised access to health information;
- unauthorised use of a health identifier;
- inadequate/incorrect identification through lack of agreed standards for identification; and
- widening of uses over time ('function creep').

Before the Commonwealth were to embark on developing any such system of patient identification it would therefore be likely to be required to meet the following strict criteria:

- use of a patient identifier would be limited to the health sector;

[103] No system is risk free, including existing manual (paper-based) methods of keeping personal health information.

- there would need to be absolute transparency and accountability — with control over an identifier's use residing with the consumer;
- participation by consumers and providers would be voluntary;
- it would need to be backed by a robust privacy/legislative framework which limits the circumstances in which a health identifier could be used (with appropriate penalties for misuse);
- appropriate security measures and standards would need to be in place throughout the health sector to maintain privacy and confidentiality of health information; and
- agreed standards would need to be in place to provide assurance of the integrity and quality of the information being exchanged electronically.

Clearly, issues of security would be of paramount importance and safeguards would need to be in place to ensure that:

- a person cannot use someone else's identifier to access that person's record without permission. This is particularly important in the case of minors or people with impaired decision-making ability;
- consumers are able to maintain control over who has access to their personal health information — with mechanisms in place to allow them to see who has accessed their information; and
- providers or organisations that have access to identifiable personal health information have adequate security precautions in place to protect and safeguard such information.

While the potential for breaches of privacy must be acknowledged, the introduction of a health identifier could also provide the opportunity to *enhance* individual privacy by helping to set boundaries around the use of information — that is, can be as much about privacy as it is about information. Control over their health identifier will provide consumers with the key to unlock essential health information held elsewhere in order that the health professionals of their choice can access the critical information they need for sound decision-making.

H4 Provider identification

Providers also need to be able to be uniquely identified:

- to ensure that the information is only accessed by the provider (at a particular location) authorised by the consumer;
- to ensure that a provider is a bona fide health professional (via links to professional registration bodies or other appropriate sources);
- for professional accountability purposes (such as to establish duty of care); and
- to facilitate the efficient payment of any relevant professional fees or rebates.

Provider authentication will ensure that information is sent to the appropriate person at the correct destination. In addition, a provider may supply professional services from a variety of locations. A system of electronic health records also needs to be able to access information from the location at which it is stored, and transmit information to the location at which the information is required — that is, a location or facility identifier is also integral to the system.

H5 Identification of facilities

A facility may be defined in a number of ways, including:

- the location at which services are actually provided;
- the location at which health records are electronically stored; or
- a combination or linkage of these locations.

A facility identifier could also be used to administer health programs that need to differentiate between locations at which a service is rendered by a particular provider, as well as distinguishing between providers rendering services at a specific location.

Finally, particularly for some highly sophisticated medical technologies, the actual piece of equipment used may need to be identified to allow a clinical decision to be made (for example the reliance to be placed on a result depending on the resolution of imaging equipment), or an administrative process to occur (such as the differential payment of a rebate).

H6 A way forward

This appendix has focussed almost exclusively on the issuing and use of health identifiers, and in particular on the need to accurately identify the individual health consumer, in an electronic world. However, even in the current climate where such initiatives are relatively few in number and extent, the need for such an identifier for the individual consumer is readily apparent. These needs are multiple but include: the tracking of individuals exposed to the risk of contracting HIV/AIDS or another infectious disease following possible exposure in a public hospital; the recall of individuals with faulty implantable medical devices; reducing the potential for mix-up between test results or procedures due to confusion between individuals with similar or the same names; the failure to bring together critical information because of misspelt names, illegibility of handwriting and the individual benefits to be gained from the surveillance of medical treatments in general.

Ultimately, however, most of the direct benefits to the individual consumer or provider from the use of such an identifier will be delivered within the context of widespread use of electronic health records and electronic communication of critical health information.