

PUBLIC
INTEREST
ADVOCACY
CENTRE

Level 1, 46-48 York Street
Sydney 2000
Australia
DX 643 Sydney
Tel: (612) 9299 7833
Fax: (612) 9299 7855
Email: piac@piac.asn.au
A.C.N. 002 773 524
A.B.N. 77 002 773 524

Connecting health

**A review of electronic health record projects in Australia,
Europe and Canada**

AMANDA CORNWALL - 2002 Churchill Fellow

November 2002

CONTENTS

Acknowledgements	i
Summary	ii
Programme	iv
Section 1: the schemes	
Introduction	1
EHR projects in Australia	2
EHR projects in Canada	4
EHR projects in Europe	8
EHR projects in England	8
EHR projects in Germany	10
EHR projects in France	12
EHR projects in Ireland	13
Section 2: the issues	
Testing the objectives	14
Privacy laws	16
Privacy and EHRs	17
Consent and control	19
Security of EHRs	21
Role of privacy commissioners	23
Section 3: conclusions	
Conclusions and recommendations	24
Implementation	25
References	26
Appendix 1 – Summary of EHR schemes	

This report details the findings of a 2002 Churchill Fellowship visit to Canada and Europe to investigate programs for electronic storage and linkage of patient records across the health care system.

The Fellowship gave me invaluable experiences and insights into how the different systems work in practice, as distinct from promises made in policy documents.

Acknowledgements

My visit to Canada and Europe and the experience I gained were made possible with the support and assistance of a number of organisations and individuals.

The Winston Churchill Memorial Trust provided financial support and the respect accorded to Churchill Fellows.

The Public Interest Advocacy Centre gave me the opportunity to develop and extend my professional expertise by incorporating the Fellowship into my work program.

The Office of the Federal Privacy Commissioner provided introductions to Information and Data Protection Commissioners in each country. These offices were enthusiastic and helpful contacts, particularly in France and Canada.

The Federal Department of Health and Ageing and the office of the NSW Minister of Health assisted with introductions and suggestions on who to visit.

Thanks to the Hon Judge Kevin O'Connor, Associate Professor Merrilyn Walton and Meredith Carter for initial support in making the application.

Special thanks to my mother, Patrice Cornwall for her tireless assistance with travel and accommodation.

Churchill Fellow

Amanda Cornwall
Senior Policy Officer
Public Interest Advocacy Centre
Sydney NSW 2000
Tel: 02 9299 7833
fax: 02 299 7855
piac@piac.asn.au

© Winston Churchill Memorial Trust, November 2002. Reproduced with permission.

SUMMARY

Project description

The objective of the Fellowship was to investigate the impact of information technology in health services on consumer access to information and privacy. It examined nationally significant programs for electronically linked patient records, in Canada, Germany, France, England and Ireland, focussing on the potential benefits and measures to protect privacy. The lessons from those systems are applied to equivalent programs in Australia.

Over 65 individuals from 30 organisations were interviewed, including people responsible for managing and administering EHR programs, health informatics experts, academics, policy officers, senior staff of information and privacy commissioners, doctors and consumer representatives.

What are EHRs?

Electronic health records have been developed for a range of purposes. Most of the established EHR schemes are used for purposes such as electronic billing and are designed for individual institutions or for a limited network of health services.

EHR projects are now being developed at the national and state level in Australia, Canada and Europe to provide a lifetime summary of patient's records, linking information about their health care across the whole health system. The primary objective of these EHR schemes is to improve the quality of health care services. They offer health care providers access to a more complete medical history of a patient, with the patient's consent. They also promise consumers more complete information to assist them to better manage their own health care.

EHRs promise a more integrated approach to health care, so that services are more patient focussed. In Canada, England and Ireland EHRs have been explicitly linked to reforms in health care delivery, particularly primary care, rather than relying on EHRs to achieve change in themselves.

Australia is well advanced in developing EHR projects, with trials of proposed schemes commencing in late 2002 and 2003. The National Health Information Advisory Council was established in 1998 to bring together state, territory and federal government health information technology initiatives.

In England the government has made a long term commitment to testing, developing and evaluating EHR proposals to learn from the best and worst of local initiatives. The Canadian Government has also adopted a collaborative approach to EHR development. It has established a number of organisations to foster co-operation and build on provincial government EHR projects. A summary of the nationally significant schemes in Australia, Canada, France, England, Germany and Ireland is set out in Appendix 1.

Conclusion and recommendations

The EHR schemes in the countries reviewed in this study demonstrate that there are many common challenges to be met and some important lessons for Australia.

The pilots of EHR schemes in England and Canada demonstrate the benefits of a long term commitment to research and evaluation of different EHR models. The

HealthConnect and BMMS trials and evaluations in Australia in 2003 may need longer than planned to provide useful results.

In Australia public policy debates about the privacy and security requirements of EHRs have not yet commenced. As a result there is a lack of understanding and consensus about the issues among stakeholders.

The Canadian Government and the European Union have advanced these discussions by incorporating privacy and security issues into the health information technology agenda. The privacy requirements of EHRs should be explicitly part of the funded work program of National Health Information Management Advisory Council or its successor.

The lessons from Europe and Canada in particular show the need for patient consent processes to be simple and easy to use for consumers and doctors. Processes need to be developed that are responsive to peoples' desire to control how their personal health information is shared with others.

EHR schemes in Australia would benefit from privacy commissioners taking an active and public role in providing advice on privacy issues. Their Canadian and European counterparts have done so very successfully.

In Europe and Canada government agencies and health informatics experts have highlighted the shortcomings of PKI and favour the use of Public Key Infrastructure (PKI) in combination with other security measures. Australian governments should consider the use of Trust Management system, biometric devices and smart cards in combination with the PKI provided by the eHealth Signature Authority.

Implementation

The findings of the Fellowship have been used in a numerous submissions to the NSW and federal governments on privacy issues and EHR schemes.

Briefings and presentations have been given to a number of organisations, including the Australian Consumers Association, the Office of the Federal Privacy Commissioner and the Better Medication Management System Development Group.

An article has been submitted to *Health Issues* journal and several other articles will be submitted to other publications. This report has been distributed widely, including to state and federal departments of health, health care provider groups, consumer groups and privacy commissioners.

The report is available at www.piac.asn.au.

PROGRAMME

Vancouver and Victoria, British Columbia, 5 May–12 May

- College of Pharmacists of British Columbia
- Ministry of Health, British Columbia
- Centre for Health Services and Policy Research, University of British Columbia
- Information and Privacy Commissioner, British Columbia – meetings with the Commissioner and staff, and a lunchtime presentation to staff about EHR and privacy issues in Australia
- Ministry of Management Services BC, Corporate and Information Programs Division
- School of Political Science, University of Victoria
- BC Public Interest Advocacy Centre
- School of Health Information Science, University of Victoria, British Columbia

Toronto, Ontario, 13–15 May

- Information and Privacy Commission of Ontario
- The Hospital for Sick Children, Electronic Child Health Network and Information and Diagnostic Services
- University Health Network
- Smart Systems for Health, Ministry of Health, Ontario
- ePhysician project, Family Health Network, Ministry of Health, Ontario
- Canada Health Infoway Inc.

Ottawa, 16 and 17 May

- Privacy Commissioner of Canada
- Public Interest Advocacy Centre, Canada
- Office of Health and the Information Highway, Health Canada - meetings over two days with the Director General of OHIH, staff from the Privacy and Knowledge Division, the EHR and Telehealth Division, the Strategic Alliances and Priorities Division and a lunchtime presentation to OHIH staff about EHR and privacy issues in Australia

London, 20–24 May and 4–7 June

- ACHEW – Association of Community Health Councils of England and Wales
- Patients Association (UK) (telephone interview)
- National Health Service - Information Authority (telephone interview)
- Hadfield Medical Centre, Manchester (telephone interview)
- National AIDS Trust

Manchester (Cheshire), 29 May

- Information Commission, UK – Compliance manager, Health team; Policy manager, FOI team and Compliance Manager, Law Enforcement and Justice

Leeds, 30 May

- Direct Care Team, Information Policy Unit, Department of Health

Bonn, 14 June

A one day conference organised by the German Ministry for Health with participants from:

- German Ministry for Health, legal officers and health informatics officer
- National Association of Statutory Health Insurance Physicians
- German Health Telematics Action Forum (non-government forum)
- Centre for Health Telematics

Paris, 17–21 June and 26–27 June

- Mission pour l'Informatisation du System de Santé, secretariat d'état a la Santé et aux Handicaps, Ministre de l'Emploi et de la Solidarite
- Bureau des Systems 'Information, Direction Generale de la Santé, Ministre de l'Emploi et de la Solidarite
- Caisse Nationale l'Assurance Maladi (major health insurance provider)
- Commission Nationale de l'Informatique et des Libertes - Division of European and International Affairs and Division des Affaires Publiques et Sociales
- Group pour la Modernisation du Systeme d'Information Hospitalier
- D'un collectif d'association des defense de droits de maladies

Dublin and Cork, 1–5 July

- Faculty of Law, University of Cork, Ireland
- Department of Health and Children, Ireland

Introduction

Development of electronically linked patient records or Electronic Health Record schemes (EHRs) is a priority for governments in many countries, including Australia. It is part of a vision for delivering health services electronically, making use of information technology, telephone call centres, websites, the internet and telehealth.

Electronic Health Record schemes provide a means for health care providers to access a more complete medical history of a patient, with the patient's consent. In this way they promise to improve the quality of health care services and promote a more integrated approach to care. EHRs also offer patients more information about their condition and treatment so that they are better able to manage their own health care.

According to opinion surveys in Australia, England and Canada people generally embrace the benefits of EHRs, but only if the confidentiality and security of their medical record is protected. The surveys indicate that people expect to be able to control whether personal information in their EHR is shared with others, including other health care professionals, government agencies and researchers. People are also concerned about unauthorised people accessing their record and security risks when information is transmitted over the internet.

The Churchill Fellowship provided the opportunity to examine nationally significant EHRs in Canada, England, Germany, France and Ireland. In all of these countries EHR projects are part of publicly funded health care systems, operating within a privacy law framework.

This report outlines the features of the EHR schemes in those countries and the place of EHRs within the health system. It reviews the privacy laws in each country and how the privacy and security of patient information is protected through the design of EHRs.

What are EHR schemes?

Types of EHRs

EHRs have been designed to perform a number of different functions. Most of the established EHRs are designed for single organisations, such as hospitals, or limited networks of health services in a defined geographical area. EHRs have so far been applied primarily for administrative and financial purposes, such as patient billing, rather than to record patients' clinical information.

The governments of British Columbia, Canada and France established EHR schemes in the mid-1990s to provide electronic processing of claims for government health benefits and health insurance. More ambitious EHR projects are being developed in Australia, Canada and Europe to provide a comprehensive, lifetime patient record across the whole health system. The focus of this report is on these broader, national EHR schemes that link patients' clinical information.

The definitions of clinical EHRs vary slightly depending on how the information is organised and the purposes for which it will be used. Different EHR models have developed in different parts of the health system, reflecting the different nature of

care and work practices in community care, acute care and primary care. The English have distinguished an electronic patient record, which is a record kept by a health service about a patient's contact with the service, from an electronic health record, which provides a longitudinal record of a patient's health and health care. They have also promised an electronic patient held record – a record of patients' health care in a format that will assist patients to manage their health care.

The planned national EHRs seek to cut across these boundaries to provide summaries of patient consultations including treatments, diagnosis, test results, medications, immunisations, outcomes of treatment, referrals and discharge summaries. The summary information in the EHR is extracted from the more detailed records kept by clinics, doctors and hospitals. The EHR does not replace those records.

Electronic decision support

Clinical EHRs are used in conjunction with 'electronic decision support' systems for health professionals, providing objective and accurate clinical information such as best practice guidelines, protocols and advisories. Some electronic decision support systems include software that can perform automatic checks, such as adverse drug interactions and duplication of ingredients in medicines. Research has found that the use of electronic decision support significantly reduces adverse outcomes, particularly in prescribing and administering medicines.

Health infostructure

An obvious prerequisite for clinical EHRs is an information technology infrastructure that provides appropriate and secure systems to share patient information. This is referred to as health 'infostructure'. Major components of infostructure include:

- standards for health information management and information technology;
- data definitions, coding and classification systems of information so that common language is used to describe medicines, test results and diseases;
- architectures that describe how information and technology will be used to provide a framework for clinical and administrative purposes;
- appropriate software for electronic decision support systems;
- privacy and security frameworks that establish the legal framework and describe operational functions such as patient consent and control processes.

Successful EHRs also require computerisation of health services, training of health professionals and managers and changes to work practices so that the systems are used effectively.

EHR projects in Australia

The major national EHR initiative planned in Australia is *HealthConnect*—an internet based network providing for the collection, storage and exchange of summary patient information, with the patient's consent. It is a joint initiative of federal, state and territory governments to research and develop the proposal for two years. Two 'fast track' trials commenced in 2002 and pilots in NSW and Queensland will commence in March 2003. Evaluation of *HealthConnect* will assess whether it can prove its value, requirements for managing privacy and a preferred implementation model. Feasibility and cost will also be assessed.

A related initiative is the Better Medication Management System, to be called *MediConnect*. It is an initiative of the federal government, with the support of all Australian Health Ministers. It will be administered by the Health Insurance Commission (HIC), which also administers the Medicare Benefits and Pharmaceutical Benefits Schemes (PBS).

The BMMS will provide a central patient medication record, using information about a patient's medications held by doctors, pharmacists and hospitals. It will include prescription medicines, over the counter medicines and complementary medicines that the patient agrees to be included on the record. The BMMS will also provide drug alerts and record information such as patient allergies. Doctors and pharmacists will be able to download information from the BMMS to incorporate into their patient files. Two pilot sites for the BMMS will commence in March 2003, with an initial phase of three months and second phase of six months, followed by an evaluation.

Participation in both schemes is voluntary for health care providers and for patients who can register at the point of care or at an HIC office.

There are also EHR programs being developed by state governments. The most advanced statewide scheme is the New South Wales Government's NSW EHR**Net*. It will provide web-enabled access to a life time summary record of patient information held by the NSW public health system. The two lead implementation sites commence in late 2002. They build on existing projects at Area Health Services in NSW for co-ordination of the care of people with chronic heart conditions and children with acute and chronic health care needs. They are also trial sites for *HealthConnect*.

In South Australia the Department of Human Services is implementing the Open Architecture Clinical Information System to bring together patient and clinical information across health units. It is an essential first step to providing patient access to personal health information and sharing information among their health care providers.

An example of a local scheme is a project at the Alfred Hospital in Melbourne to allow admission and discharge information to be shared electronically between the hospital and local 20 General Practice surgeries.

The HIC is committed to increasing public access to online claiming and improving peoples' access to personal health information to assist them to better manage their health care. Electronic lodgement of claims for reimbursement from Medicare via doctors' surgeries is planned under a scheme called *Medicare connect*. PBS online is also planned. It will initially allow pharmacists to make claims for remuneration for medicines covered under the PBS by email. A new claims processing system is to be available in 2003-2004 and online prescribing is planned for 2004-2005, eliminating paper based claims processing. Medicare *two way* claiming is already available for people with private health insurance, providing electronic transmission of 'gap' claims for in-hospital claims.

Medicare online is being developed to give people access to personal information held by the HIC in formats that will help them to understand and manage their

treatment and medications. It is to be available via the HIC website. An example is a project providing information and reminders to people with diabetes to assist them to prevent or delay complications such as nerve, eye, kidney and blood vessel damage.

The HIC also established the Health eSignature Authority in 2001 to provide Public Key Infrastructure (PKI) for transmission of confidential information in the health sector in Australia– a world first. PKI is a combination of technology, policies and practice to achieve secure use, storage and transmission of information.

Australian governments have invested substantial funding into computerisation of health services and training of health professionals in the use of information technology. However, development of electronic decision support systems has been fragmented and lacks co-ordination, leading to problems of accessibility, scale, duplication and lack of integration of systems. A National Electronic Decision Support Taskforce was established in May 2002 to establish stakeholder support for a co-ordinated approach and to identify national governance arrangements. It has commissioned reports on *Electronic Decision Support Activities in Different Health Care Settings in Australia* and *Electronic Decision Support Systems Requirements*. The Taskforce provided a report to the Australian Health Ministers Council in November 2002.

Australian Health Ministers sought to bring together the various health information technology activities of state, territory and federal governments through the National Health Information Management Advisory Council, established in 1998. A strategic national framework called *Health Online: a health information action plan for Australia* was published in 1999, with a revised edition in 2001. A key element of the strategy is *HealthConnect*.

The Council was reviewed in 2002 to assess how well it had met its role, identify barriers and assess its structure and relationships with other advisory structures in the field. A parallel review was conducted as part of the review of Australian Health Care Agreements. It was particularly concerned that a separate body, the National Health Information Management Group, is responsible for access to health information for research and statistical uses of data. The review recommended that the two functions be combined in an Australian Council of Health Information supported by a proposed national Infostructure Unit to co-ordinate the national health infrastructure framework. Both reports were provided to the Australian Health Ministers Council meeting in November 2002.

EHR projects in Canada

As provincial governments are responsible for health service delivery and funding in Canada, the EHRs are being developed at provincial level. There are nationally significant EHRs in British Columbia, Alberta and Ontario.

British Columbia – PharmaNet and HealthNet

The British Columbia *PharmaNet* system was introduced in 1995 to assist with administration of Pharmacare, the provincial pharmaceutical benefits scheme and other relevant benefits. It provides an online real-time claim system that processes a wide range of entitlements and benefits for residents of BC (not including third party insurers). *PharmaNet* provides pharmacists with a province-wide patient medication

history, comprehensive drug information and automatic checks such as drug to drug interactions, duplicate ingredients, appropriate dose and known patient allergies. All prescription medicines are covered, except HIV/AIDS drugs. Over the counter medicines can be added to the record if it is thought necessary. PharmaNet has been available in hospital emergency rooms for some years. There are plans to extend it to doctors, but unlike the current scheme, it would require patient consent.

PharmaNet is administered by the British Columbia College of Pharmacists, which verifies all new drugs and corrects errors and other data integrity. The College conducts regular audits to check pharmacists are appropriately accessing and using the system. An audit in 2001 found five pharmacists had inappropriately accessed patient records and disciplinary action was taken. PharmaNet is also used as part of the College's general professional monitoring and compliance role. The College is covered by the BC *Information and Privacy Act 1993*, which also covers hospitals. The privacy obligations of pharmacists under PharmaNet are set out in the legislation establishing the scheme.

HealthNet/BC was started by the British Columbia Ministry of Health to enable the secure sharing of integrated patient information across the province. It started in 1993 with on-line patient records as part of the vision. Specific PharmaNet transactions have been accredited as HealthNet/BC Products and are now being offered as part of the HealthNet/BC Product Suite.

Alberta Wellnet and Pharmaceuticals Information Network

Wellnet was established by the Alberta Government to provide an umbrella for provincial and regional initiatives to build an integrated health information network. Its focus shifted to providing a provincial EHR in 2001, offering health care professionals patient information, including medications, laboratory and diagnostic imaging, discharge summaries and other medical history. Decision support and reference tools are to be provided concurrently. The EHR is evolving as a series of co-ordinated projects over time, leveraging existing data sources to the extent possible.

The foundation project of Wellnet is the Pharmaceutical Information Network (PIN), which will enable electronic exchange of patient medication information between doctors, pharmacists and hospitals. It will also provide current best practice information on medicines, prescription information, dosage checking and validation, checks on interactions, prescription status, list current medications and allergies and other clinical support tools. PIN is being implemented through staged introduction to pharmacists and pilots to engage doctors commenced in early 2002.

A precursor to the PIN is the Seniors Drug Profile, which allows hospital emergency rooms in Alberta to access a patient medication history from their pharmaceutical benefits claims. The information is provided by the pharmaceuticals claims body, Blue Cross, with the consent of the patient. Wellnet also includes an Integrated Cancer Care Network.

Smart Systems for Health and ePhysician, Ontario

Smart Systems for Health is a project of the Ministry of Health and Long Term Care in Ontario. It was established four years ago to provide the base infrastructure to facilitate the secure communication and exchange of personal health information among Ontario's health care providers. It supports a number of initiatives, including

the ePhysician Project, a voluntary emergency health record, Integrated Services for Children Information System and Health Network System (Ontario Drug Benefits). When fully operational it will allow the secure collection, storage and exchange of personal health information and provide information tools and resources for the delivery of integrated health services.

The ePhysician Project is a joint initiative of the Ministry of Health and Long Term Care and the Ontario Medical Association. It is using the Smart Systems for Health infrastructure to provide an information technology tool to support an integrated primary care program, the Family Health Network (FHN). The FHN supports networks of general practitioners and nurse practitioners who have agreed to cover for each other in providing after hours care and telephone advice to their patients through Primary Care Networks. The payments system under the FHN moves from fee-for-service to payment according to a profile of patients and their needs. There are 13 Primary Care Network pilots to evaluate the primary care reform model. The networks are voluntary for patients and providers.

The Ontario Government has invested C\$100 million in incentives for GPs to join FHNs and C\$150 million for information technology to support the Networks. Initially doctors chose software to suit their needs from vendors approved by the government and they were provided with computer servers. However, uptake of the technology by doctors was highly variable, with some using it only for billing and scheduling appointments while others used it fully to link with pharmacists and laboratories. A major limitation was that the doctors were accessing their software in a way that did not allow them to communicate with each other. It was also very expensive, at a cost of about \$50,000 per doctor.

The ePhysician Project developed a model offering a clinical management system software application that was accessed through a secure, centrally located server provided by SSH. The first IT Transition Pilot Project was set up by the ePhysician Network in November 2001 at Chatham-Kent, with eight participating GPs at six different locations. It successfully demonstrated the benefits of a centralised system that provides connectivity, security, on-site training support and back up.

Smart Systems for Health, as a public sector agency, is covered by the Ontario *Freedom of Information and Privacy Act 1990*, but doctors and software developers participating in ePhysician are not.

National initiatives

The Canadian Government has fostered a collaborative approach to health information technology, based on the vision in *Canada Health Infoway: paths to better health*, the final report of the Advisory Council on Health Infostructure in 1999. *Health Infoway* pointed out the need to create a Canadian Health Infostructure that builds on the initiatives of provincial and territorial governments. It identified electronic health records and telehealth as pivotal to the future of health care services in Canada. Four strategic goals were identified: empowering the public; strengthening and integrating health services; creating information resources for accountability, and improving privacy protection in the health sector.

In 2000 the federal, provincial and territorial Deputy Ministers of Health established an Advisory Committee on Health Infostructure to provide advice on strategies to support the development of a national health infostructure. It is made up primarily

of Chief Information Officers in provincial and territorial health departments, a privacy commissioner and representatives of health care providers. The Committee is responsible for a *Tactical Plan for a pan-Canadian Health Infostructure*, which is updated annually. In November 2001 the Canadian Government made a C\$500 million funding commitment as part of implementing the *Tactical Plan*.

The Office of Health and the Information Highway (OHIH) was established as part of Health Canada to provide project leadership and funding for government health infostructure programs. OHIH provides the secretariat for the Advisory Committee on Health Infostructure and it has prepared important reviews and analyses of international developments in health information technology. For example, it prepared an international overview of EHR projects in January 2001, *Toward Electronic Health Records*.

OHIH is working on a health care network, discussed in the 2001 *Tactical Plan*. It is comprised of many systems but with common architecture to allow systems to talk to each other in a secure environment. It is also developing an Information and Communications Technologies Health Initiatives Database to profile Canadian telehealth, EHR, education and training and health information infostructure initiatives.

OHIH has invested in health infostructure programs under the Canada Health Infostructure Partnership Program (CHIPP), a 2-year, C\$80 million funding program to support national implementation of information and communications technologies in health care delivery, particularly electronic health records and telehealth for rural and remote residents. The 30 CHIPP projects provide a realistic illustration of the barriers and opportunities in building interoperability solutions that cross jurisdictions and go beyond one organisation or health region.

OHIH works closely with Canada Health Infoway Inc, a not for profit organisation established to foster industry based development of communication technologies. It has created a National Registry of EHR initiatives to foster collaboration and help identify partners and investment opportunities. The first stage was reported on in mid-2002.

CHI is also documenting the current state of developments in building EHRs, with regular updates as the required infostructure is developed. In 2002 it mapped out an 18-month strategy and tactical plan for 2002-2003, *Accelerating development of electronic health information systems for Canadians*. It gives priority to developing enabling technologies to make EHRs interoperable and to protect privacy.

The Canadian Institute for Health Information is responsible for health research activities. It produced *The Roadmap Initiative* (revised in 2000) to provide a national vision and action plan to modernise Canada's health information system. The report is a collaborative effort with Statistics Canada, Health Canada and many other groups at the national, provincial and local levels. A National Data Model has been developed as part of *The Roadmap Initiative*.

EHR projects in Europe

The European Union has supported EHR projects and related telehealth initiatives in a number of different areas with substantial programme funding to develop various applications. The driving force is to promote interoperability of national health information systems. The initiatives include:

- a European Health Card launched by the European Commission in February 2002 primarily to verify health insurance status. It does not contain clinical data;
- an eEurope Smart Card Charter that pleads for interoperability of national information systems in the health care sector.

The eEurope 2002 Action Plan, *An Information Society for All* sets out goals to be achieved through national action plans by 2002. These include establishing a health telematics infrastructure, identifying and benchmarking best practice in ehealth services and establishing quality criteria for websites providing health information. The revised eEurope Action Plan 2005 commits member states to, among other things, developing systems for exchange of information between points of health care by 2005.

The European Commission supports a common approach to electronic health records architecture to provide secure, extended use of personal health information. Its current focus is on systems to provide access to essential patient information in medical emergencies, for residents of the EU.

Netlink, a collaboration between Italy, France and Germany commenced three years ago to demonstrate the technology available to link patient records when they are in another European country and need emergency treatment. It is intended to provide a 'cookbook' of international interoperability of patient records. The project initially found some significant differences between the health information systems of each country and the patient information that could be disclosed to governments.

The EC's Programme of Community Action on Health Monitoring is planning an information system to network de-identified health data for population health purposes.

EHR projects in England

England is widely accepted as the world leader in setting a national agenda for health information. It has had a national health information strategy since the late 1980s, with a number of health care policies and health informatics policies developed and implemented over the past 10 to 15 years. EHRs are a major component of England's National Health Service information strategy, *Information for Health*, launched in 1998.

An important feature of the success of the English approach is that the information strategy is integrated with reforms to health service delivery, set out in the *NHS Plan 2000*. The vision of the reforms is to give the people of England a health service designed around the patient. It set out a completely new way of delivering health care.

Information for Health supported the vision of a 'service designed around the patient.' It would ensure that information is used to help patients receive the best possible

care, enabling health professionals to have the information they need to provide care and improve the quality of people's health. It would do this through:

- providing a lifelong EHR for every patient;
- round the clock online access to patient records and information about clinical practice (electronic decision support) for clinicians;
- co-ordination of care provided by hospitals, GPs, community care services through sharing patient information across the system;
- providing health planners and managers with the information they need; and
- public access to information about health care through online information and telemedicine.

The strategy set targets and action items to be achieved within specific time frames:

- 35% of the acute hospitals would have level 3 Electronic Patient Records—an institution based record of health care provided to each patient, providing functions such as ordering diagnostic tests and electronic prescribing - by 2002;
- first generation Electronic Health Record initiated (providing a complete, longitudinal record of a patient's health care over a lifetime) by 2002;
- first generation electronic health records to be fully implemented at primary care level, all acute hospitals would have level 3 EPR by 2005; and
- 24 hour emergency care access to patient records by 2005.

The English Government committed over £1 billion over the seven year period of the strategy. In the first two years the focus of investment was on connecting GPs to NHSnet, developing information services for primary care and funding to assist with local implementation.

NHSnet is provided by the NHS Information Authority to give health care professionals access to protected email, NHSweb and the internet. It is used by health care providers to transfer information between applications and organisations within the NHS. The NHS IA also promotes the use of information management systems in GP practices through a GP computer systems accreditation policy. It ensures that the systems deliver benefits to patients and clinicians and facilitate implementation of the NHS strategy.

Local implementation strategies are an important feature of *Information for Health*. Each of the 98 local health communities is required to develop a local implementation strategy, which also requires developing local IT expertise. The local implementation strategies must address local health care priorities. Consultation and participation are emphasised as part of ensuring projects service the needs of consumers and clinicians.

The *Information for Health* was revised in January 2001 with *Building the information core* and again in 2002 with the release of the *NHS Information Technology* strategy in July. The 2002 strategy extends a number of the deadlines in *Information for Health* and commits an extra £5 billion to national IT support. An immediate priority in the 2002 *Information Technology* strategy is to upgrade IT infrastructure. It re-commits to EHRs in all health trusts and electronic booking of appointments by 2005. A national electronic prescription service is also made a priority for the end of 2005, with full implementation by December 2007.

The *NHS Plan 2000* reinforces the emphasis on local implementation. The 2002 *Information Technology* strategy also supports local implementation and further 'ring

fences' funds for IT. Funding is to be released from a central fund directly to local health care trusts using accredited IT systems that comply with new national standards.

Another important feature of the English approach to electronic record development is a long-term commitment to learning from the best and worst of local EHR initiatives. The Electronic Record Development and Implementation Programme (ERDIP) was established to support in-service project work to explore a variety of aspects of electronic patient records. Four initial pilot projects were announced in April 2000 with £2.4 million and further projects were announced in June 2000 with an additional £5.8 million. Seven of the 19 ERDIP sites have reached or are nearing completion, by mid 2002. A great deal of learning has occurred and much of the original design of EPRs and EHRs has been reassessed.

An electronic Personal Health Record, a patient held record of their health care, was developed as part of ERDIP. It is to be offered as a service by NHS Direct by 2004. It uses a web portal established for patients to view their records, organising data collected by the NHS to map a patient's health profile.

Evaluation was a significant feature designed into ERDIP from the start, with £1.5 million to assess roll out nationally. Standards and specifications have now been published based on what has been learned at the ERDIP sites. Evaluation reports for each ERDIP project has been produced and a national evaluation is to be completed by March 2003.

EHR projects in Germany

A number of electronic and digital systems have been used to provide authentication of insurance status and reimbursement for hospital services, prescription medicines and other health services in Germany. The German Department of Health is planning to introduce a patient smart card by 2003-2004. The new smart card was recommended in a 1998 report commissioned by the Department to review the use of telematics in health, *Telematics in health care—perspectives for telemedicine in Germany*. It recommended a telematic platform to interlink isolated information systems in the health care sector. The introduction of electronic prescribing was recommended as a key application, requiring a common network for doctors and hospitals as well as the telematic platform.

A comprehensive EHR scheme providing for transmission of information across an intranet or the internet is still being debated in Germany. There are substantial concerns about data protection requirements, whether or not a secure communications infrastructure can be provided and controls on who can access patient information access. The proposed patient card will store information on the card rather than using a network or database.

The objectives of the proposed electronic health card are to improve quality of care by providing patient information, empowering patients, optimising workflow and supporting efficiency in the care process. Co-ordination of information about patient's medications is a priority. However, the major motivation for the upgraded card is the substantial financial gains from the efficiencies of electronic processing of insurance claims.

The card will store four different types of patient information collected from doctors, pharmacists and hospitals:

- insurance information;
- electronic prescriptions;
- emergency health data (name, address, blood group, chronic illnesses, allergies and certain specified priority diseases including heart disease, diabetes and asthma);
- medication management information (all medications, prescribed and otherwise).

The information is stored on a 'smart card', with each category of information to be stored in separate areas on the card. All the applications will be connected within a common telematics architecture, but there will be no centrally stored data.

The Department of Health proposes that the card is voluntary for emergency data and medication management functions (clinical information), but compulsory for insurance purposes and electronic prescriptions (financial and administrative information). Patients will control who can access to the record through use of the card and a 'key' that is required to access information stored on the card.

The German Government is developing a smart card to be used by health professionals to restrict access to the information on the card to authorised professionals. It would provide a digital signature and encryption.

Implementation of the electronic patient health card and the professional card is being overseen by a steering committee composed of High Level Committees in Health Care and other organisations including the federal Data Protection Commissioner and patient groups. Arrangements for the cards are set out in the *Agreement of the Federal Ministry of Health and High Level Committees in the Health Sector concerning the use of telematics*, signed in May 2002.

The card will commence regional and functional pilots in late 2002 - early 2003, which will then be evaluated before a phased nation-wide introduction. The objective of the regional pilots is to demonstrate 'on time verification and optimisation of available technical and organisational solutions with cost saving potential'.

The cost of implementing the new technology is estimated to be DM1.1 billion. Most is for communications and security (44%) and the patient smart card (33%).

The Action Forum for Telematics in Health Care was established in 1999 by the German Health Care Associations to achieve a consensus among stakeholders in this area. It is constituted by the major health sector organisations such as the health insurance funds, the National Association of Statutory Health Insurance Physicians and the German Medical Association. A separate health telematics working group has been established for the Laender or state governments.

EHR projects in France

SESAM Vitale has operated nationally in France since 1996. It provides verification of insurance status and secure electronic billing for all the population covering all 'payers' (insurers and government benefits), processing an average of 10.8 million electronic bills a week and covering 30 different health insurance regimes.

SESAM Vitale is comprised of a consumer held smart card (Vitale card), a card for health professionals to access the system and a social health network that provides information to health professionals. The social health network utilises Intranet technology to transfer health care information among users and to offer a secure database of information. It also offers secure mail exchange, an index of all registered users, electronic address book, transmission of health care forms, medical news, databases, some medical education information, sanitary alerts and diagnostic and prescription advice.

The professional smart card ensures that only authorised health care providers can access the system. Access to the patient record is only available with the consumer's Vitale card. The Vitale card contains name, social security number, identity of beneficiaries, the health office responsible and validity of entitlements. Cards are issued for family groups at present rather than to individuals.

Any payment made to health service providers is recorded in a central database. The database is used to provide statistical records and information to contribute to quality control and monitoring of expenditure. Statistics are sent to the health insurers risk analysis division, to income tax administration and professional organisations. Global information on the cost of health care are reported to Ministry of Health. The SESAM Vitale system has provided the French Government with de-identified information on population use of prescription drugs since 1998, said to be the most detailed collection of such data in the world.

The French Ministry for Health plans to expand the SESAM Vitale system to include some clinical information and improve the exchange of information. Known as Vitale 2—the final phase of the Hebergeur system, it is comprised of :

- an upgraded, individual Vitale card for each citizen;
- the professional smart card providing authentication of ID, digital signature and encryption (PKI); and
- a web-based, secure network operated by a private consortium providing information for clinicians on the Health and Social network and access to patient records (with Vitale 2).

Caisse Nationale l'Assurance Maladi, the largest national insurer, is responsible for the development of technical aspects of the SESAM Vitale project.

It is proposed that the patient record will include clinical data, such as blood type, vaccinations, allergies, treating doctor, type of treatment, test results and prescriptions (last 20 medicines prescribed) for use in emergencies. However, officers of the Ministry of Health that I interviewed doubt that much clinical information will be included. It is not proposed to offer electronic prescribing as part of the system and alternative projects will provide for medication management.

The clinical data would be stored in a protected area of the card, separate from financial and administrative information. The new cards are also to contain a 'key' to allow health professionals to access patient records held by hospitals. Vitale 2 was originally to be delivered by 2003, but is now proposed by 2005. Legislation providing the legal framework for Vitale 2 was passed in 2002. The system is to be administered by a non-government organisation, following a tender process to be completed in 2002-2003.

Hospitals in France use EHRs for limited, administrative and billing purposes. The Group pour la Modernisation du System d'Information Hospitalier is drafting proposals on privacy and information standards in French hospitals, due for release in late 2002.

EHR projects in Ireland

The Irish Government has promised a national networked computer system to support integrated health services and the phased introduction of electronic patient records to enhance quality and safety of care. Details of the EHR and the location and forms of pilot projects are to be set out in a National Health Information Strategy, expected to be released before the end of 2002.

Information for Action, a national health strategy for 2002–2009 and Health Information – Guiding Principles were released by the Department of Health and Children in 2001 to inform public consultations about a National Health Information Strategy. Two consultancies were commissioned to assess the current state of development of electronic health information systems in 2001. They found that there has already been considerable parallel development of different electronic health information systems by different areas of the health system in Ireland and each of the 17 Health Boards have developed their own systems. However, they are mostly for administrative and financial functions rather than for clinical purposes.

Information for Action contemplates moving towards a common approach to health information technology through standards and coding schemes with the potential to provide evidence based data. However, it acknowledges the risks of this strategy, which requires expanding local initiatives to large scale projects.

Information for Action considers patient held smart cards are appropriate for specific purposes such as emergency care, pharmaceuticals, and eligibility and reimbursement for benefits. A patient electronic record is promised. The forms in which it is to be piloted is to be set out in the NHIS.

Developing the information and communications infrastructure of the health sector in Ireland is part of other reforms promoting quality improvement and better primary care services. An electronic patient record is promised as part of investment in a national health system in the national Health Strategy 2001, *Quality and Fairness: a health system for you*. EHRs are also part of primary health care reforms, set out in *Primary care a new direction: Quality and Fairness, 2001*. It emphasises the need for a more team based approach to health care and makes a commitment to providing more health services in the community. The strategy promises primary care networks to support primary care teams and an improved information and communications infrastructure for the primary care teams.

The Department of Health and Children plans specific health information legislation to enable the uses of information contemplated under the National Health Information Strategy. Some commentators have called for the government to develop an electronic health record strategy to address the needs of an EHR, to supplement the wider National Health Information Strategy.

Testing the objectives of EHRs

Cost benefit

The huge cost of government investment in EHRs is justified on the basis that the benefits of improved safety and quality in health care will eventually outweigh the cost. However, there is little research and evaluation of the how EHRs will improve the safety of health care. Most of the field tests assume the benefits will follow, without necessarily evaluating how they will be achieved or to what extent.

Electronic linkage of information about patients' medicines is a priority for all of the planned EHR schemes, reflecting the international research about the high level of injury from medication errors. However, the research on computer based solutions to medication injury demonstrates the benefits of electronic decision support systems, providing clinical information to clinicians, not EHRs.

The research also demonstrates that less technological measures are effective to minimise medication errors, according to the *Second National report on patient safety: improving medication safety*, July 2002 of the Australian Council for Safety and Quality in Health Care. These include use of hospital discharge summaries and care plans, medication management services, case conferencing and patient education.

Improved monitoring of entitlements

A major financial benefit of EHRs for governments is that they allow much better monitoring of entitlements to health benefits. Many of the people interviewed as part of the Churchill Fellowship said this is the major driving force for government investment in EHRs, even though it is often not stated.

The SESAM Vitale 2 and the German electronic health card proposals are exceptions because they are explicitly designed for electronic processing of claims for health insurance and benefits. Cost benefit analyses conducted for these proposals show that the efficiencies of electronic processing over manual processing offer sufficient financial benefits to cover the cost of investment.

In Australia improved entitlement monitoring is not part of the objective of the BMMS or HealthConnect, but concerns have been raised about the likelihood that this is a major benefit for government. Improved Entitlement Monitoring of Pharmaceutical Benefits was introduced in 2001, requiring Medicare numbers to appear on all prescriptions.

Testing what works best

The pilot sites for HealthConnect, which includes the NSW EHR*Net sites, will test aspects of a single HealthConnect architecture and the field tests for the BMMS will test the BMMS architecture. They will not explore different models for EHRs. In England and Canada the approach favoured exploring the benefits and weaknesses of different models of EHRs that have been developed in the field.

In England thorough testing of different EHR models has been a hallmark of EHR development through the Electronic Record Development and Implementation Programme (ERDIP). Some examples of the 19 ERDIP sites include:

- a community wide Electronic Patient Record (an organisation based record of patient care) demonstrator used in Cornwall to develop an integrated community health record, linking primary, community and acute care, with a 24 hour emergency care record. It has delivered a range of clinical systems, tested key concepts in implementing electronic records and helped develop new integrated models of care. The project set out to continue development of an electronic record to support health care across Cornwall and the Isles of Scilly. To speed implementation and roll-out of systems the Cornwall site adopted standard integrated information architecture, avoiding the need for many different integration engines to link systems together. A series of condition specific, community wide modules have been developed for mental health, diabetes and heart disease to demonstrate the value of the core clinical record to support integrated services.
- a working emergency Electronic Health Record (a record of the patient's health and health care) based on a common primary care system in Bradford, providing complete access to the live GP record to a range of health care providers.
- a system for patients to consent to sharing information via an EHR at the Maternity and Child Health at Kingston and Richmond Local Health Community.
- a Personal Health Record for patients developed at Hadfield Medical Centre available through a web portal. It used 'read codes' to organise data already held by the NHS to map a patient's health profile. People could add documents such as letters, prescriptions and clinical test results (there are frequently long delays in informing patients of results). Patients had access to the record in the medical practice and at home via the Internet. The project tested devices to authenticate the patient, using biometric devices and smart cards. The project found that people were able to see what they wanted, but not always as quickly as they hoped.

The ERDIP projects have demonstrated the best and worst of EHRs. The Cornwall project has demonstrated the shortcomings of the distinction between an EPR and EHR, developing a record that combines aspects of both. The personal health Records developed at Hadfield has provided a model for implementation nationally by 2004. A distinguishing feature of ERDIP is that it has taken a long term view – two years to produce meaningful results in the Cornwall site. While such a long-term approach sits uncomfortably with politicians' desires for short-term outcomes and an annual funding cycle, the results are widely regarded as a great success.

The experience of the ePhysician Project in Ontario, Canada also demonstrates the benefits of exploring different options in the field before designing an EHR model for widespread implementation. Initially implementation of the IT tools by the doctors in the Primary Health Networks was left to individual doctors to choose. The ePhysician Project's IT transition pilot project at Chatham-Kent demonstrated the benefits of a centralised system that connected the doctors to each other and to services such as pharmacies and laboratories in a secure network. The uptake of the system was much faster than at any previous sites. Doctors also reported a number of benefits of the specific features of the IT tool:

- more precise note taking through the use of templates;
- checking drug interactions more frequently;

- significant time saving for doctors because it encouraged timely recording of information and the use of 'tablets' meant there was no duplication of data entry.

The Canadian Government's collaborative approach to the development of EHRs encourages learning and exchange among the EHRs developed at provincial and regional level.

Privacy laws

Privacy and health care

The privacy framework gives people control of personal information that is collected about them and assurances that it will be kept up-to-date, accurate and secure. It requires that personal information cannot generally be shared with others unless the person gives consent. People have a right to access their record and to have errors corrected.

EHRs, which facilitate sharing of information by a wide network of people, potentially conflict with privacy principles unless patients control how the record is shared and appropriate security measures are in place. A coherent legal framework to appropriately protect the privacy and confidentiality of personal health records is therefore an essential first step for successful EHRs.

In all of the countries reviewed in this study, health services are having to adjust to relatively new privacy requirements that have demanded changes to established practices. Traditionally medical practitioners have ownership and control of patient records, while placing a high ethical value on doctor-patient confidentiality. The privacy framework gives patients the right to control how their personal information is used and a right to access their health records. The common difficulties being experienced in each country are reflected in guidelines on privacy laws in the health sector prepared by data protection and privacy commissioners in Australia, England and Ireland.

A common national privacy standard

In Australia, Canada and Germany a federal system of government has further complicated matters by producing a confusing matrix of privacy laws that impose different privacy standards on different parts of the health system. The approach taken by the Canadian Government and the European Union offer some lessons for Australia in making progress towards a common privacy standard for the health sector.

In Australia the private health sector, such as GPs, private hospitals and pharmacists are covered by National Privacy Principles (NPPs) in the federal *Privacy Act*, under amendments that came into effect in December 2001. Federal government agencies, such as the Department of Health and Ageing and the Health Insurance Commission, have been covered by Information Privacy Principles under the *Privacy Act* since 1988. Health services run by state governments, such as public hospitals, are governed separately. Some have introduced privacy laws covering state run health services, but most states have only policies or codes of practice.

The Federal Department of Health and Ageing have been working on a National Health Privacy Code with a National Health Privacy Working Group of the Australian Health Ministers Advisory Council. However, after several years there

has been little progress. A draft Code was released for public comment on 1 December 2002. The HealthConnect and BMMS proposals have promised special privacy measures in the laws establishing the schemes, but this may only add to the confusion by creating yet another layer of privacy obligations.

In Canada provincial and territorial governments are responsible for regulating privacy in the health sector and each of them has privacy laws covering public sector agencies. Some of these laws cover hospitals and universities, but others do not. At the beginning of 2002 none had privacy laws governing the private sector, except Quebec. The Canadian Government provided an incentive for provinces to introduce consistent privacy and data protection laws for the private sector with the *Personal Information Protection and Electronic Documents Act 2001*. In January 2004 the law will apply to the private sector in any province that does not enact 'substantially similar' legislation.

Other organisations have taken action to promote a national approach to privacy standards. The Canadian Standards Association (CSA) developed a *Model Code for Privacy Implementation* that sets out 10 practices for fair information handling. The Model Code has been used in the Ontario Government's *Privacy of Personal Information Act 2002*. The Act covers collection, use and disclosure of personal information by the private and not-for-profit organisations in Ontario. It incorporates provisions for 'health information' and 'health information custodians' and creates an Assistant Commissioner with responsibility for the health sector.

Canadian Health Ministers have agreed to a harmonised privacy framework in the health sector. The Advisory Committee on Health Infostructure, serviced by the OHIH, established a working group on privacy in 2000. A nationally harmonised approach to the protection of personal health information has been drafted and the working group is developing a set of guidelines based on the CSA *Model Code*.

The European Union provides a strong model for achieving common privacy and data protection standards. The European Commission's *Data Protection Directive 95/46/EC* sets out privacy standards that must be adopted by all member states. France, Germany, Ireland and England passed laws to fully implement the Directive in 2001 and 2002, including new provisions applying to health information. The Directive establishes an EU Working Party on Data Protection, made up of the European data protection and information commissioners. Members of the working party are currently considering the European *Directive on Personal data and electronic communications*, July 2002, which addresses digital technologies in public communication networks and electronic communication services via the Internet.

The EU also published a report on *Legal aspects of ehealth* in 2001 to clarify applicable legislation to assist companies entering the market for EHRs in Europe.

Privacy and EHRs

EHRs raise particular privacy issues. These include how much control patients will have over the content of the record and who can use it, how much access to the information will be allowed for governments, researchers and others and how the security of the record will be protected.

The privacy and security requirements for EHRs have not been substantially debated in Australia. It is addressed in only general terms in the draft *National Health Privacy Code* recently released for comment by the National Health Privacy Working Group. As a result, the operational design of EHRs may not meet the strong privacy and security measures expected by the public.

In Canada and Europe organisations responsible for supporting health information technology have done considerable work to promote understanding of privacy and security issues for EHRs. In Canada privacy and security issues are part of the work program of OHIH and Canada Health Infoway. For example, OHIH's Privacy and Knowledge branch commissioned a *Privacy technology review* in 2001, providing a survey and assessment of commercial privacy technology available for EHRs and makes recommendations on the best way forward.

Canada Health Infoway's 2001 Tactical Plan, *Accelerating Electronic Health Information Systems*, highlighted the obstacle posed by the patchwork of privacy laws in Canada. It is currently conducting a review to identify the priority privacy issues for implementation of EHRs for provincial and territorial governments.

In England the extent to which government agencies access personal health information is highly controversial and poses a potential barrier to the implementation of a national EHR. The work required to ensure confidentiality of patient information in the NHS was outlined in *Building the information core: protecting and using confidential patient information, a strategy for the NHS* in 2001. Elements included bringing data quality, clinical governance and data protection standards together in one place under 'Information Governance' standards and clarifying when explicit patient consent is required for use and disclosure of information. The strategy promises the development of a guide on the structure and functionality of electronic records covering privacy rights of patients and options for respecting demands for absolute privacy.

The NHS Information Authority recently commenced national consultations about a new confidentiality management system. The proposal includes a *National Charter for Sharing Information* to inform consumers what to expect and a draft *Code of Practice* for NHS staff. A joint survey conducted by the NHS and the UK Consumers Association in 2002 found that just under half of the respondents were reassured that a published Sharing Agreement would protect the confidentiality of their records.

In Ireland there is considerable confusion about how data protection laws apply to the health sector and privacy is seen as a major barrier to the development of EHRs. The Irish Department of Health and Children regards freedom of information and data protection laws as posing a number of potential legal challenges for the National Health Information Strategy. Of particular concern is lack of clarity about the legal definition of when explicit patient consent to sharing of information is required and the hesitancy of some agencies to share patient information with disease registries. Some commentators have called for the Irish Government to prepare an Electronic Health Record Strategy as the privacy needs of EHRs are not expected to be adequately dealt with in the National Health Information Strategy.

Consent and control

The planned EHR schemes in Canada, Europe and Australia are voluntary, requiring consumers to explicitly consent to join the schemes. The consent processes for EHRs therefore need to offer meaningful choice to patients while at the same time being 'user friendly'. The process needs to be flexible, incorporating a simple, standard consent arrangement with other options that can be more tailor made for individuals.

Defining consent

The ERDIP pilots in England confirmed that obtaining informed and explicit patient consent to sharing of information contained in an EHR is essential. Informed, explicit patient consent was a fundamental element of the strong support expressed for the EHR as a valuable means for health professionals to obtain comprehensive information.

It is important that the consent process is also easy to use for doctors and other health care providers who will be the ones obtaining patient consent. Doctors have resisted EHRs in some places because of the perception that they are responsible for the integrity and management of the information contained in the EHR. In a recent pilot implementation of the Pharmaceuticals Information Network in Alberta, Canada, doctors were taking more than 30 minutes to explain the system, driven by concerns about professional liability.

Part of the problem for doctors is that 'informed consent' in the context of health care requires doctors to provide comprehensive information about the potential risks of a course of treatment and to make sure that the patient understands. In the context of privacy 'informed consent' is much less onerous.

The HealthConnect trials will test different models for informed consent, including a site in Katherine, where the population is predominantly Indigenous people. It also hopes to develop a model for obtaining consent electronically, which will require processes for authentication of the patient's identity and verification that consent has been given.

Clear information about who is responsible for managing the accuracy and security of information in the EHR is essential. Often EHRs are promoted in a way that highlights the role of trusted health professionals, while the government agency responsible for the scheme is almost invisible. The *Privacy review: Chatham-Kent IT Transition Pilot Project* conducted by the Ontario Information and Privacy Commissioner recommended that the Ministry of Health and Long Term Care improve the information provided to consumers by making available brochures and signage in doctors clinics with following information:

- the benefits and risks associated with EHRs;
- the roles performed by the Office of Family Health Networks, the ePhysician Project, the SSH and physicians;
- the technology used in the project;
- how the privacy of their personal information is protected;
- who is accountable for protecting their personal information; and
- contact details at ePhysician Project/SSH for more information.

The printed information provided to consumers about the BMMS will be tested as part of the BMMS pilots in 2003.

Patient control of information

People's desire to control how their health information is shared, even among the people providing their care, has been strongly stated in opinion surveys in Australia and England. Patient surveys about consent and privacy issues conducted by ERDIP projects in England showed that patients were concerned about confidentiality and security of personal information in an electronic record. Patients were very clear that they want to decide who has access to their record.

The ERDIP project at Maternity and Child Health at Kingston and Richmond Local Health community found that a one-off consent process to join an EHR scheme was not enough. People needed to revisit who the information is being shared with at later stages of the care process. Processes had to be established during the course of a project to gain patient consent at every stage of the pregnancy and after delivery. Patients who were health workers expressed concerns about who would have access to the information. Assurances were given, based on professional standards of behaviour. The evaluation of the project concluded that the 'reality of gaining informed consent is not so clear cut and defined.'

A survey conducted for the NHS Information Authority and the UK Consumers Association in 2002 found that a quarter of people wished to exclude sensitive information (eg terminations of pregnancy, mental illness, sexually transmitted diseases) from routine sharing of information in an EHR. More than a third wanted to be consulted each time their details were shared with other health care providers (regarded as not feasible by the NHS).

Another survey, conducted by the UK Patients Association, found that 95% of people surveyed wanted to be asked before their personal information was given to government agencies. The NHS conducted a national workshop for consumers to discuss consent and control processes in September 2002.

In Australia, the Roy Morgan Research survey conducted for the Office of the Federal Privacy Commissioner in 2001 found that over 60% of people thought that an individual's permission should be sought before their de-identified health information was used for research purposes. When asked whether health professionals should be able to discuss the medical details of an individual (to better treat them) without the patient's consent, the results were split with just over half agreeing and 44% disagreeing.

The HealthConnect project plans to develop structures to allow consumer control over who has access to their records. A number of options were presented in a discussion paper released by HealthConnect in July 2002 on *Consent and EHRs*. A national Consent workshop was held in May 2002 to seek to develop a simple and workable approach to managing consent. The most favoured process is to give consumers the opportunity to agree to specific 'events' or treatment episodes to be added to the HealthConnect record. Options that would allow consumers to select who sees what information are regarded as too complex technically.

The Acute and Co-ordinated Care branch of the Department of Health and Ageing is conducting a research project on electronic forms of consent. It has commissioned

four projects to identify and trial potential mechanisms that allow a consumer to record the conditions or instructions under which their information may be transmitted from one person to another.

The BMMS field tests will explore two options for patients to control access to the record after the initial consent to join the scheme. A patient can give 'standing' or ongoing permission to a specific doctor and pharmacist to access the record whenever they see them. Alternatively, a patient can give permission to access the BMMS record every time they visit a doctor, hospital or pharmacist. Patients can also direct a pharmacist or doctor not to include a particular medication on the BMMS record.

The German Government proposal for an electronic health card offers consumers a high degree of control over their record because the information is stored on the smart card. Consumers will be able to direct health care providers as to what clinical information is to be entered or deleted from their card and control what data each health care provider can access. The card will also provide a digital system that allows a patient to record their consent for specific uses of the record (such as for emergencies) or to control access.

Smart cards and keywords

Some EHR schemes provide physical barriers to accessing patient information with the use of consumer held smart cards or a keyword known only to the consumer. The BC PharmaNet scheme provides for consumers to set up a keyword, but the option is not well known and many pharmacists do not know how to set it up. As a result, only about 2,000 people have taken up the option, out of a population of 4 million people. The BMMS field tests will test the option of a key word.

The proposed French and German schemes both use a consumer held smart card, which gives patients physical control over access to their record. Under the German proposal, patients will hold a 'key' to use the smart card, which is passed to the health care provider. Two types of key are available. One for one-off use, another for regular or continuous use. A major topic of debate in Germany is whether the keys need protection by requiring them to be used in conjunction with a Personal Identification Number or keyword.

In France, the legislative framework for the Hebergeur System or SESAM Vitale 2, passed earlier this year, specifies that patients can control the health professionals that see different parts of their record. Patients can direct a professional to put a copy of specified data onto a specified database within the System or the doctor can seek the patient's consent to put information in a database. The consumer held Vitale card continues to control access to patient information in the System.

Security and EHRs

EHR schemes need to have systems in place to ensure only authorised people are able to access patient records and that sensitive information is encrypted or scrambled. Internationally these needs are addressed by a number of measures, known as 'privacy enhancing technologies'. The most widely understood tool is Public Key Infrastructure (PKI), a combination of technological devices, policies and procedures.

In Australia the Health eSignature Authority has been established to provide PKI for the health sector - a world first. The Authority provides Digital Certificates (electronic passports) that bind a person's identity or location to their digital keys. The 'keys' operate in matching pairs and are used to protect the content of the message. The public key encrypts the message and only a matching private key, held by the recipient, can be used to decrypt it. When used together the keys provide a 'digital signature', which prevents the copying or transfer of documents or messages. People providing or receiving health care services can apply for a certificate.

The Authority claims PKI will allow the health sector to transmit confidential information securely. However, in Europe and Canada government agencies and health informatics experts are much more cautious, highlighting the shortcomings of PKI. They express concerns about the heavy reliance the PKI places on governance and policy management and on users maintaining the confidentiality of their key. In England the Department of Health emphasises the significance of people, policy, processes and services in effective PKI, not just technology. The NHS is not planning to implement national PKI infrastructure immediately because of these concerns.

In Canada a *Privacy technology review* conducted for the Office of Health and Information Highway expresses similar reservations. It concludes that the most promising technology for EHRs is a combination of PKI and Trust Management, possibly enhanced with smart cards and biometrics. It says PKI can provide many of the required safeguards such as strong encryption for confidentiality and digital signatures. Trust Management design can propagate the certificates that are used by the access control components to enforce privacy-supporting practices. The report recommends that smart cards and biometrics (such as face, hand or fingerprint recognition) be explored to enhance privacy where stronger controls on access are required.

Germany and France have been working with other EC countries to establish a PKI as the central security infrastructure. Under their respective EHR schemes PKI technology will be provided on the health professional smart card, which provides the certificates (and signatures) and encryption software. The specifications for the German health professional card are set out in the *Use of Telematics Agreement* signed earlier this year and the specifications for the French card are in the Hebergeur legislation passed this year. The French Data Protection and Liberties Commission's 2001 annual report expressed concerns about encryption provided on the card. It prefers encryption software to be provided on the health provider's computer.

In France health informatics experts support the use of smart cards in combination with PKI. For example, the director of the SESAM Vitale project at Caisse Nationale l'Assurance Maladi, favours the use of PKI in combination with smart cards to provide a higher level of control and access to SESAM Vitale.

The data protection commissioners in both countries have favoured use of biometric devices such as hand or fingerprint recognition to verify someone's identity. The Data Processing and Liberties Commission has supported use of such biometric devices that are proportionate and appropriate to the purpose and where the information is not kept on databases. The German Data Protection Commissioner favoured the introduction of biometric characters on personal identification papers

for German citizens to prevent falsification, following 11 September 2001. The data is stored on a microchip for comparison with the owner's fingerprints.

The Ontario Information and Privacy Commissioner supported the use of biometric devices to identify authorised health care providers in the *Privacy Review: Chatham-Kent IT Transition Pilot Project*. It supported the security measures put in place by the ePhysician Project, which included passwords for doctors plus a physical token or 'key fob'. However, the Commissioner was concerned that a 'key fob' can be easily lost and shared among staff who have each other's passwords.

Role of Privacy Commissioners

Privacy and information commissioners in Canada and Europe have an established public profile and actively promote compliance with privacy laws in the health sector. They have also been active in providing independent, expert advice on the privacy and security aspects of EHRs.

Privacy commissioners and privacy laws in Australia have a low profile and the commissioners have had a very limited role in the health sector and EHRs. Just over two in five people are aware that federal privacy laws exist according to the Roy Morgan survey conducted for the Office of the Federal Privacy Commissioner in 2001. A quarter of people said they did not know where to report breaches and of the remaining people, most said they would report it to the Ombudsman (22%), the organisation complained about or consumer affairs agencies. Only 5% of people said they would report misuse of their personal information to a privacy commissioner.

Data protection commissioners in Canada and Europe use a range of measures to promote compliance and awareness of privacy laws in the health sector. The Data Processing and Liberties Commission in France and the Information and Privacy Commissioner (IPC) in British Columbia conduct regular audits of agencies, notifying the agency beforehand so the audit is carried out with a high degree of co-operation. The Data Protection Commissioner in Ireland has given notice that he plans to carry out random privacy audits on a sector basis.

Privacy Impact Assessment (PIA) has been developed in Canada as a tool for agencies to gauge whether new technologies, information systems and proposed programs or policies meet basic privacy requirements. Smart Systems for Health in Ontario conducted a PIA before commencing the ePhysician Pilot Implementation project this year.

Surveys are also used to assess practices and potential privacy breaches in evolving areas of the health sector. In British Columbia, for example, the IPC conducted a survey in 2001 of organisations administering health registers, such as cancer registries. It found none were complying with privacy obligations and none had conducted a PIA (compulsory in British Columbia for public sector agencies). In France, the Data Processing and Liberties Commission reviewed websites providing health information to see if they complied with privacy requirements. It identified many problems, especially about people being informed of their privacy rights.

IPCs in Canada and Europe are actively involved in the development of EHRs and the associated public debate. The Data Processing and Liberties Commission works closely with Caisse Nationale l'Assurance Maladi on the SESAM Vitale project. The

Commission's opinion on the legal framework for the various incarnations of SESAM Vitale is tabled in Parliament. Its views on EHR projects, such as a recent trial of a proposed system using the Internet to connect GPs and hospitals, are regarded as an essential element of project and policy development.

Smart Systems for Health in Ontario worked closely with the IPC in developing the ePhysician Project. It requested the IPC to conduct a *Privacy Review* of the Chatham-Kent IT transition pilot implementation project following allegations in the *Globe and Mail* newspaper that:

- patients were not fully informed of what happens to their records;
- the system could be hacked into over the Internet;
- three private companies (two of them software developers) had been granted access to patient information; and
- a computer technician took unencrypted backup tapes, containing thousands of medical records, to his home and three of the tapes were lost.

It found none of the major allegations about hacking and lost tapes were substantiated, but recommended some improvements.

Privacy Commissioners in Canada and Europe are acutely aware of the importance of striking a balance between protecting personal privacy and the public interest in freedom of speech. Governments frequently use personal privacy arguments to prevent publication of embarrassing information. An example is the role played by the Data Protection and Liberties Commission in France in a dispute between the French FOI agency (Commission d'Access aux Documents Administratifs) and the Ministry of Health over publication of a 'league table' on the best and worst hospitals in France. The Ministry of Health resisted release of the report on the grounds that it contained data that could be re-identified. The dispute resulted in legislative reform, making the Data Processing and Liberties Commission responsible for authorising such releases of information, which it has never refused.

The privacy and data protection commissioners in British Columbia, Ontario, England and Ireland are responsible for administering both privacy laws and 'access to information' or FOI laws. Even where those roles are not combined, such as in France, the data protection commissioners see themselves as agents for government transparency - not government censor. Combining the two roles, particularly at state level, may help to improve the low profile of privacy laws in Australia.

Conclusions and recommendations

The EHR schemes in the countries reviewed demonstrate that there are many common challenges to be met and some important lessons for Australia.

The pilots of EHR schemes in England and Canada demonstrate the benefits of long term research and evaluation of different EHR models. The HealthConnect and BMMS trials and evaluations in Australia may need longer than planned to provide useful results.

The need for consensus on the privacy and security requirements of EHRs is more likely to be addressed successfully if it is incorporated into the national health information technology agenda. It should be explicitly part of the funded work

program of NHIMAC or the proposed Australian Health Information Council and Infostructure Unit.

The lessons from Europe and Canada show the need for patient consent processes to be simple and easy to use for consumers and doctors. Processes need to be developed that are responsive to peoples' desire to control how their personal health information is shared with others.

EHR schemes in Australia would benefit from privacy commissioners taking an active and public role in providing advice on privacy issues. Their Canadian and European counterparts have done so very successfully.

In Europe and Canada government agencies and health informatics experts have highlighted the shortcomings of PKI and favour the use of PKI in combination with other security measures. Australian governments should consider the use of Trust Management system, biometric devices and smart cards in combination with the PKI provided by the eHealth Signature Authority.

Implementation

The findings of the Fellowship have been used in a number of ways:

- a submission to the Federal Government on a confidential draft National Health Privacy Code in August 2002;
- a submission to the review of the National Health Information Advisory Council in 2002;
- representations to the New South Wales Government about the *Health Information Privacy Bill 2002* (now an Act) and further representations are planned about the NSW EHR*Net as a member of the NSW EHR Steering Group;
- briefings to a number of organisations, including the Australian Consumers Association, the Office of the Federal Privacy Commissioner and the Better Medication Management System Development Group.

An article has been submitted to a refereed journal and several shorter articles will be submitted to other publications. This report has been distributed widely, including to state and federal departments of health, health care provider groups and consumer groups.

A summary of this report has been distributed to a number of email discussion forums for privacy advocates and health consumer advocates.

The report is available at www.piac.asn.au.

Select bibliography

(full references available on request)

- *Health Online, an information action plan for Australia*, 2nd edition, September 2001, National Health Information Management Advisory Council
- *Health Connect newsletter*, vol 1, number 1, August 2002
- *NSW Health Strategy for the Electronic Health Record*, NSW Health, February 2002
- *NSW EHR*Net, The Electronic Health record Newsletter*, NSW Health, Issue 1, June 2002
- Australian Council for Safety and Quality in Health Care, *Second National report on patient safety: improving medication safety*, July 2002, pages 41-51
- *Panacea or placebo?*, Report of the NSW Ministerial Advisory Committee on Privacy and Health Information, 2000
- Wendy Bloom and Associates, *Investigation of concerns and Information Needs re the BMMS – a qualitative research report*, August 2000
- Office of the Federal Privacy Commissioner, *Privacy and the Community*, July 2001, prepared by Roy Morgan Research
- *Health eSignature Authority*, Fact Sheet, Health Insurance Commission, March 2001
- Information and Privacy Commissioner Ontario, April 2002, *Privacy Review: Chatham-Kent IT Transition Pilot project*
- *Toward Electronic Health Records*, Office of Health and the Information Highway, Health Canada, January 2001
- *Privacy technology review*, prepared by EXECOM Group Inc for Office of Health and the Information Highway, Health Canada, 30 August 2001
- Privacy Commissioner of Canada, *Annual Report, 2000-2001*
- *Information for health*, December 2001, Department of Health, England
- *Building the Information Core – overview*, 2001, Department of Health, England
- *Delivering IT in the NHS – a summary of the national programme for IT*, Department of Health, England
- *Electronic Record Development and Implementation Programme*, NHS Information Authority, 2002,
- Information Commissioner (UK), *Use and Disclosure of health data: Guidance on the Application of the Data Protection Act 1998*, May 2002
- ICM Research Survey, for the Patients Association UK, 2002
- Dr G Dietzel, *Health Telematics and eHealth in Germany – Current Developments*, 2001
- S Schug, *European and International perspectives on telematics in health care*, ATG and GVG, 2001
- Commission nationale de l'informatique et des libertes, 22nd Annual Report for 2001, extracts of chapter 3, Current debates – 'A century of Biometrics' and 'E Administraiton' (English translation)
- Commission nationale de l'informatique et des libertes, *La reforme du Systeme de Sante Le Dispsitif SESAM Vitale*, April 1998
- Department of Health and Children, Ireland, *Information for Action, a national health strategy for 2002 – 2009*, July 2001
- *Primary care a new direction: Quality and fairness – a health system for you*, Health Strategy, 2001
- Data Protection Commissioner, Ireland, *Third Annual Report*, 2001

Summary of electronic health record projects

Appendix 1

Australia

The major national EHR initiative planned in Australia is *HealthConnect* - an Internet based network providing for the collection, storage and exchange of summary patient information over a patient's lifetime. A related initiative is the Better Medication Management System (BMMS), which will provide a central record of patient medications information held by doctors, pharmacists and hospitals, with the patient's consent. Regional and state EHRs are also well advanced and many of these will provide pilot sites for *HealthConnect*. Pilots and evaluation will be completed, by the end of 2003, before national implementation.

Canada

The major EHR schemes being developed by provincial governments in Canada include:

- the *PharmaNet* system in British Columbia, Canada. Established in 1995 to provide online processing of pharmaceutical benefits, it gives pharmacists a province-wide patient medication history and offers them comprehensive drug information and automatic checks such as drug interactions. It is available in hospital emergency rooms and will be extended it to doctors in future;
- the Pharmaceutical Information Network in Alberta, Canada. It provides a complete record of patient medications held by doctors, hospitals and pharmacists and drug information and automatic checks. Pilot implementation commenced in 2002. It is part of Alberta's *Wellnet* scheme, which aims to provide an umbrella for provincial and regional initiatives to build an integrated health information network;
- Smart Systems for Health, an initiative of the Ontario Ministry of Health and Long Term Care. It commenced four years ago to provide the infrastructure for secure communication of patient information among healthcare providers across the province. The ePhysician Project in Ontario used SSH to provide a secure Intranet for GPs who have agreed to provide after hours care for each others patients to access each other's patient records, with the patient's consent. Other SSH initiatives include the Health Network System (Pharmaceutical Benefits).

Europe

The EHR schemes being developed in Europe include:

- a patient centred EHR, electronic booking of appointments, electronic prescribing and a patient held record promised across the English National Health Service by 2005. The English are world leaders in setting a national agenda for health information technology and integrating the information strategy to changes in how health services are delivered. A feature of the English approach is a desire to learn from success and failures, with funding for long term development and evaluation;
- the Department of Health in Germany is planning an electronic health smart card to process health insurance claims and provide electronic prescriptions, with the option of also storing other clinical information. Pilots will commence in late 2002-2003, which will be evaluated before implementation;

- the SESAM Vitale system in France. The system has operated nationally since 1996 to provide secure electronic processing of health insurance claims for all the population. It is comprised of a consumer held smart card (Vitale card), a smart card to identify health professionals and a social health network that provides information to health professionals. There are plans to expand SESAM Vitale in coming years using a web-based network. It will include clinical information about patients, such as prescription drugs, immunisation, blood type;
- phased introduction of electronic patient records proposed in Ireland as part of a yet to be released National Health Information Strategy.