Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp173-179)

Privacy and e-Health in Australia

BRUCE LE MARSHALL, MIRKA MILLER
School of Information Technology and Mathematical Sciences
University of Ballarat
PO Box 663, Ballarat, Victoria 3353
AUSTRALIA

Abstract: - One of the most pressing problems in health informatics is how to ensure the privacy of individual patient records, particularly with threats to such privacy from developments in Information Technology and current health care reimbursement systems. In Australia, the problem is exacerbated by the fact that the various Australian states have not been implementing Australian privacy legislation in a uniform manner. In this paper we survey privacy and e-health in Australia.

Key-Words: - Privacy, Confidentiality, Security**,** Privacy Legislation, Health Care, e-health, Australia, Electronic Health Record

1 Introduction

Health care in Australia is generally composed of a complex mixture of community and hospital based services, provided by numerous health professionals in both public and private facilities and organisations. The *Australian Medicare system* provides free access to public hospital services and assistance with the cost of various medical services. The Australian health care system also allows for private health insurance to assist with the cost of services not covered by Medicare in both public and private hospitals. The Commonwealth has a role in policy development, research funding and national and international health issues. While most health professionals are self-employed, individual states and territories manage public health services and community and public health facilities. The focus of health care, however, has been changing. This change has been driven by a number of factors including globalisation, medical and information technology and the formation of large health organisations. The rapid improvements in communication and information technology over the last few decades have seen significant changes in virtually all aspects of everyday life. In the health system, the face-to-face consultation is no longer the only way to interact with health professionals. The use of e-mail, video-conferencing and various electronic consultation mechanisms for e-health and remote health consultations have either undergone trials or are in regular use [15]. The Internet has also been used by many individuals to attend to their own health directly, or to obtain sufficient information prior to a regular consultation. The ever-increasing costs of traditional health care have led to the formation of many large national and trans-national health organisations. Their primary focus tends to be their long-term survival with (hopefully) ever increasing profits. One of the areas of focus to increase profits is to manage health information, which includes biomedical knowledge, patient records and administrative information. Technology is seen as the means of meeting the challenge to effectively manage these large amounts of information. In this paper we examine health informatics privacy issues in Australia, and, in particular the question of compatibility of privacy and e-health. In the next section we set the scene with a short discussion of security, privacy and confidentiality. In Sections 3 and 4, we describe privacy legislation in Australia, and related issues. Section 5 is devoted to Health Information issues. Privacy Enhanced Technologies (PETs) are discussed in Section 6. In Section 7, the Conclusion, we point out some reasons why currently in Australia privacy and e-health are not compatible.

2 Security, Privacy & Confidentiality

Security is a key area of health informatics to maintain the privacy, confidentiality, integrity and availability of stored information [7]. Unfortunately, there is some conflict between confidentiality and availability as access is required to make clinical decisions, but individuals may feel that some information will reflect badly on them in some contexts and prefer it not to be readily accessible. As a result, there has been a significant amount of research and discussion on privacy, various related

concepts and the implementation of adequate legislation. The concept of *privacy* is not absolute. Privacy is both subjective and changeable because it varies according to the views and customs of each society. In addition, other concepts such as confidentiality, secrecy, professional privilege and security are often used interchangeably with 'privacy', particularly with respect to the protection of personal information. *Confidentiality* generally only applies to information imparted by one person to another, where those persons are aware of the special nature of the communication. In comparison, privacy includes both communicated and uncommunicated information. *Secrecy* is a term that tends to be used when the disclosure of information is forbidden, while privacy requires the information to posses a quality making it of a personal nature. Professional privilege only applies to certain professionals (lawyers and doctors) to ensure open and honest communication in the professional relationship. Information imparted to such professional is considered privileged and cannot be disclosed to third parties. *Security* is the measures that are taken to ensure privacy, confidentiality or secrecy of private information. Security is indispensable when considering data privacy. The problem of defining privacy has resulted in the use of the expression *information privacy*, the scope of which has been set out in the eight guidelines published by the Organisation for Economic Cooperation and Development (OECD), which has been adopted by most western industrialised countries. In particular, they were adopted by the Australian Government in December 1984 and were upheld in the Privacy Act 1988. While many countries have enacted legislation to regulate rights in this area, none attempt to define the term privacy, focusing instead on 'personal data' or 'personal information'. Some legislation recognises special categories of information. Data relating to health, politics, religion, police records and sexual preferences are all of a personal nature and there are various legislative protections for each.

3 Privacy Legislation in Australia

When the federal Constitution was written, privacy protection was not mentioned in the list of powers that reside in the Commonwealth Parliament. While privacy is relevant to many areas, it is not dealt with as a separate category. By comparison, the Constitution of the United States expressly protects privacy under its bill of rights. There are three compelling reasons for any country to have central privacy laws applying to both public and private sectors: (i) *Uniformity*: Sparse and inconsistent laws do not protect many categories of people; (ii) *Compliance with international instruments:* The International Covenant on Civil and Political Rights and the OECD Guidelines require broad coverage of privacy in domestic laws; (iii) *Trans-border data flows*: European countries impose restrictions of the flow of data to countries with which they trade.

Only adequate and consistent central privacy laws would eliminate possible trade barriers court actions. The external affairs power in Section 51(xxix) of the Commonwealth Constitution has been used as the basis to enact general federal data protection legislation. This has been upheld in the High Court as the external affairs power is wide enough to allow the federal government to legislate with respect to international agreements to which it is a party. The restriction being that the treaty must be of an international character, not just a matter arising at an international level. It cannot be doubted that data protection is a matter of international concern, particularly as the ability to transfer data around the world virtually instantaneously has made geographical distinctions almost irrelevant. To have any hope of protecting such data, protection needs to commence from a multinational level – which is recognised by the European Commission [16]. Two international instruments already provide the basis for federal legislation: the International Covenant on Civil and Political Rights and the OECD Guidelines. While Australia is legally bound to observe the terms of its ratification of the International Covenant, there is no such legal obligation with the OECD Guidelines. Article 17 of the Covenant provides all individuals with a right of privacy. Implementation of the Covenant by Commonwealth legislation in the Human Rights Commission Act 1981 (Cth) in effect creates a de facto privacy right in Australia. In addition, the ratification of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data by Australia would further enhance the competence of the federal government to enact relevant comprehensive legislation. The Federal Privacy Act primarily provides for the regulation of personal information handled by the federal government and its satellites (information privacy only). Eleven privacy principles are recognised. While based on the OECD Guidelines, they are more detailed and contain additional principles. There is, out of necessity for the public interest, provision for federal agencies to apply for exemptions from the Information Privacy Principles (IPPs) [16]. The Act also provides guidelines for the protection of privacy in medical research to be issued by the National Health and Medical Research Council. The 1983

Australian Law Reform Commission Report on Privacy [5] noted that: "Improvements and efficiencies brought by the informatics industry incidentally cause concern for privacy". Information and protection of privacy laws enacted in Australian should not be significantly different from those applied overseas. The Commission concluded that: "The framework of existing laws, practices and procedures limiting use, safeguarding security and encouraging individual participation in the handling of personal information needs to be supplemented, not only to secure better protection of privacy interests threatened by misuse, inadequate security, and denial of access, but also to secure a suitable threshold level of privacy protection in areas at present largely untouched by laws, standards or guidelines for the handling of personal information" [5]. As a result of the reported theft and sale of personal information [8], the Government is expected to consider amendments to the Privacy Act so as to place an obligation on companies to ensure the protection of personal information that they disclose to third party (contractors) [13].

4 Implementing Privacy Legislation

The Federal Privacy Commissioner reported that Australians appear to be more suspicious about the use of personal information by commercial organisations than the government [16]. This is subsequently supported by the indication that privacy was the main reason goods and services were not purchased over the Internet [16]. One study [12] even suggests that Australians are not confident that healthcare providers keep and use information responsibly. Thus, some patients take steps to minimise the risk to their privacy when seeking health care, only disclosing what they feel is necessary for the care they are after. While there is a tendency for legislation protecting personal information to initially apply to the public sector and subsequently to the private sector, it is important to not only ensure that legislation covers both sectors, but that there is equivalent protection in both sectors. The increasing degree of computerisation of health records kept by various health providers and the push towards an integrated electronic health record system are issues that affect both the public and private sector. While the Commonwealth Government has recognised the implications of mismanaging computerised databases [5], it has encouraged or insisted on outsourcing databases to the private sector. However, only since 1997 it has been able to require in its requests for tender that the Privacy Act 1988 (Cth) must be complied with. The Privacy Amendment (Private Sector) Act 2000 contains ten National Privacy Principles (NPPs) and extends the Privacy Act to the private health sector throughout Australia [9] and private sector organizations [10]. While a number of exemptions are noted, any industry or business dealing with health information is required to comply with the Act.

Unfortunately, the various Australian states have not implemented legislation in any consistent manner. Much of the legislation is related to interception and surveillance, spent convictions and public/state records, more so than privacy in general or medical information privacy in particular. The ACT, NSW and Victoria have passed legislation relating to information privacy. The Victorian Information Privacy Act 2000 covers personal information (excluding health information) held in the public sector, and contains ten Information Privacy Principles (IPPs). The Victorian Health Records Act 2001 covers all health information including employee health information in both the public and private health sector and includes eleven Health Privacy Principles (HPPs) [18]. This legislation attempts to provide uniformity across the public and private sectors, partly in order to facilitate the frequent movement of consumers between the two. Generally, Australian privacy legislation contains privacy principles which are based on the OECD guidelines. The European Union (EU) appears to have shown the way with its member countries coming to agreement and introducing standard protection. The European Commission's *Directive on the Protection of Personal Data* came into effect on October 25, 1998 and establishes a regulatory framework to ensure high level protection for the information of individuals, while facilitating the free movement of personal data within the European Union. The directive further established rules to ensure that data can only be transferred to countries outside the EU when its continued protection is guaranteed, either by similar legislation, voluntary arrangements or via contractual clauses. The U.S Department of Commerce uses a voluntary system, the "safe harbour" framework, agreed to by the EU in 2000, where U.S. companies register their agreement to abide by the principles set out in the Data Protection Directive. In 2001, the EU determined that Australia did not adequately protect privacy, while the Australian government argued that there was adequate protection. However, in order to avoid interruption to business dealings and prosecution by European authorities under European privacy laws, Australia may need to ensure greater protection in line with the EU requirements. The Health Insurance Portability and Accountability Act in the United

States provides for continuity of healthcare coverage via an improved information system incorporating standards and requirements for the electronic transmission of certain health records, including electronic transaction standards, identifier standards, code standards, security and electronic signature standards and privacy standards. The implementation of any integrated system utilizing personal data requires a significant effort in these areas.

5 Privacy of Health Information

Medical privacy concerns people more than most other privacy issues. Health and medical information is personal, some of which is considered very sensitive by having negative social connotations. In addition, some people prefer to keep all health problems private. Fortunately, the medical profession has a long history of concern for patient privacy:

What I may see or hear in the course of the treatment or even outside of the treatment in regard of the life of men, which on no account one must spread about, I will keep to myself holding such things shameful to be spoken about.

Hippocratic oath, fifth century B.C.E.

A physician should respect confidences and protect the patient's secrets. In protecting a patient's secrets, he must be more insistent than the patient himself.

Haly Abbas, advice to a physician, 10th century C.E.

I will respect the secrets which are confided in me, even after the patient has died.

Geneva Declaration, World Medical Association, 1940.

A physician shall respect the rights of patients, of colleagues, and of other health professionals, and shall safeguard patient confidences within the constraints of the law.

Principles of Medical Ethics, American Medical Association.

Although in our age, the general principles of privacy and confidentiality still apply, the line is becoming increasingly blurred. Health insurance companies require evidence of treatment prior to payment. The benefits of integrated electronic health records come with risks to patient privacy because the information can be put to many new uses. Medical records initially provided a detailed history of meetings with medical practitioners so as to facilitate positive outcomes in future encounters. Thus, individuals had a vested interest in ensuring accurate and complete medical records. Prior to the cyber-age, medical records were handwritten notes, made by a medical practitioner, and even though the information related to patients, the notes were considered the property of the medical practitioner. However, with the change to a more integrated approach to medical records, this idea may need to be reviewed. If patients are to have any real say in what their records contain and how they are used, ownership may need to reside with the patient. However, in an evolving electronic environment with the increased sharing of information and the ability to duplicate information, control and access may be more useful concepts than ownership. People should not only have access to information about themselves, they must be able to control who can see it. The difficulty of control is managing the control of information as circumstances change. With e-health being in its infancy, the electronic health record, as with most other aspects of health informatics, "is an evolving, multi-faceted, complex phenomenon" [19]. In Australia, the National Electronic Health Records Taskforce has recognised the value of a national framework for the use of electronic health records to improve efficiency, safety and quality of care compared to paper-based systems [19]. Most health care organisations currently have some level of computerised record system. Much current work is being focused on expanding these to an electronic medical record or an electronic patient record. Recent technological advances that pose particular threats to health privacy include the Electronic Health Records Project, HealthConnect; the Health-e-link Project, formerly ERH*Net (NSW); OACIS (SA); and the proposed SmartCards to replace Medicare cards. These are all designed to create a detailed personal record for the purpose of information sharing between many persons and organisations and can only work if patients are confident that their privacy will be protected [11]. A lack of coordination between state and federal governments, while there are joint state-federal responsibilities for health, will likely create unique problems in Australia. As noted by Paterson the "most pressing need is for a uniform Australia-wide scheme" [11]. Governments in many countries see the development of electronic health records as central to their vision for health care in the future. While many focus on financial aspects, more ambitious schemes hope to provide "a comprehensive lifetime patient record across the health system" [1]. Privacy and confidentiality pose significant problems when each record access should only be made with the knowledge and consent of the patient. However, in addition to being an inconvenient and time consuming process, people often cannot understand the implications of providing or denying access under changing circumstances. Alternatively, using blanket consent does not allow for changing circumstances, nor does it provide truly informed and voluntary consent. It is often the case with many documents that require signatures that the patient (consumer) is given no choice; for example, if they are not in a position to forgo medical benefit payments. For health

information systems to provide services that are more efficient and effective, controls are required to ensure that the required information can be provided to the appropriate people at the appropriate time in the appropriate format. Another as yet unresolved privacy concern pertains to the release of statistics based on subpopulations of individual patient records. Confidentiality problems from the aggregation of data are difficult to manage due to the lack of adequate practical and affordable technological solutions. These problems occur because protected data may be able to be inferred from comparing the answers to a number of apparently unrelated queries. Computerised records can improve medical care and cut costs. However, medical and other personal information in databases and on the Internet face significant privacy risks. It is recognised in Whetton [19] that an ideal system would be a delicate balancing act as it needs to consider a variety of perspectives of key players, who may include: consumers (patients), health care providers, health care managers, health care funders and e-health businesses. The ideal system for one is unlikely to be ideal for another, or any of the others. Intranets are used to help improve communication and the flow of information within an organisation for daily activities and extranets that connect organisations to partner organisations are becoming increasingly common. While each of these on their own have particular privacy issues, most are also connected to the Internet which open them up to significantly greater risk. The development and implementation of any e-health initiative will necessarily be a managed process, as with any large project. In addition, there will be many issues around state and federal jurisdiction and competing interests. Legislation already varies from state to state and between state and federal governments on a variety of issues. As health care is regulated along state lines, e-health will cut across state boundaries and a high level of cooperation will be required to address policy, regulatory and legal questions relating to many aspects of any e-health system. The Western Australia Institute for Medical Research Genetic Epidemiology laboratory is currently working on a database that integrates all of that state's human research information. A BioBank is also planned, which will contain the genetic information of every consenting adult in the state. However, as noted by Senator Natasha Stott Despoja, there are "frightening" privacy and ethical implications and "our laws are not equipped to deal with biobanks". She questions the issue of ownership and use of genetic information [2]. In addition, not withstanding the fact that these projects follow the National Health and Medical Research Council guidelines to de-identify all data before it is provided to researchers, Ms Stott Despoja notes that from previous experience, "de-identified does not always mean unidentifiable".

6 Privacy Enhancements

Privacy enhancing technologies aim to design information and communication systems and technologies so as to minimize the collection and use of personal data (privacy by design). These technologies include not just hardware and software, but also privacy policies and procedures. As such, there are many areas to consider in providing or enhancing privacy. The collaborative environment that an e-health system attempts to create, presents many challenges to privacy. One possible solution would be the use of a trusted network. However, with large highly dispersed networks there is no guarantee that a local health professional will not inadvertently compromise the network in some way. The World Wide Web Consortium's (W3C) Platform for Privacy Preferences (P3P) effort to give users control of their private information is limited to matching policy preferences of users with stated policies on Web sites. However, there is no enforcement of stated policies. An alternative proposed by Skinner [14] allows individuals to control access to their personal information through reconfigurable settings for access and privacy. Privacy information, customised by the user, is stored with their personal data and is used to determine access controls and privileges of the various users and roles within the collaborative environment. In addition, to allow for changing circumstances, the individual to whom the information pertains, can alter the privacy and access settings. This assumes the user is sufficiently informed as to the use and implications of various settings. While various PETs already exist, it is a mistake to become complacent as new threats are continually arising and old threats may persist (from lack of action) or change over time [17]. Two major issues with any security system are (i) selecting the most appropriate set of technologies to provide the most cost effective protection, and (ii) the ongoing monitoring and maintenance of that system. This includes fine tuning the system to reduce or prevent signalling legitimate activity as an attack and prevent missing a real attack. The federal Health Minister Tony Abbott has noted that in pursuing HealthConnect, the Government is "inclined to work with IT-based medical record providers". He also noted that participation in HealthConnect and the online Health Insurance Commission payment

system "could become mandatory". As such, he is warning medical providers to improve their business processes [3]. Australian Medical Association (AMA) President Dr Mukesh Haikerwal does not believe participation should be mandatory. He further indicates that consultation with doctors to provide "electronic systems that met the needs of doctors and patients" would require no such mandate, "compulsion implies a flawed system" [6]. Not withstanding the successful demonstrations of mature e-health systems at the Health Informatics Conference 2005, many of the electronic health projects are on hold, not it appears from privacy concerns, but due to budgetary constraints, jurisdictional issues, major gaps in IT systems in state and private hospitals [4].

7 Conclusion

The future of any integrated system that contains and transfers personal information between numbers of authorised interested parties will rely heavily on the confidence placed in that system by the people it is there to benefit. In the case of an integrated health system, the privacy and confidentiality of patient information is crucial to its acceptance by the public. Increasing community awareness and e-health initiatives such as HealthConnect have helped to drive the development of privacy legislation. Critical issues include standardized, Australia-wide laws for privacy, and ensuring the correct use of the most appropriate Privacy Enhancing Technologies such as encryption, reconfigurable access and privacy settings, time outs and proximity tokens to name just a few. A certain degree of transparency is necessary as ultimately it is about trust, respect and the expectations that patients have of their health care team to provide them with the best possible care while ensuring the privacy and confidentiality of personal information. Other key areas important in the success of any e-health system include data integrity and usability. The information stored and used must be accurate and up-to-date so as to provide appropriate and correct diagnosis to ensure a good treatment outcome. It is also essential that any system be readily usable by all authorised individuals, who should only have access to the information they require - the correct information must be accessible where it is needed at the time it is needed, in an appropriate format. The lack of consistent Australia-wide privacy and health record legislation, due to jurisdictional issues, is just one major hurdle for e-health. Additional problems include security policies, procedures and measures, access control, stakeholder liability, and gaps in Information and Computer Technology across the various health organisations. Therefore, we conclude that privacy and e-health in Australia are currently incompatible.

References:

[1] Cornwall, A. Electronic Health Records: An International Perspective. http://home.vicnet.net.au/~hissues/Text/hicornwall4dec2002.doc (accessed 16/08/05).

[2] Dearne, K., Genetic data under fire, *The Australian*, IT Today, 13 September 2005, p. 31.

[3] Dearne, K., Health providers told to lift their act, *The Australian*, IT Business, 9 August 2005, p. 2.

[4] Dearne, K., Project flatline, *The Australian*, IT Business, 6 September 2005, pp. 1- 4.

[5] Jackson, M., *Hughs on Data Protection in Australia,* Law Book Co. Pyrmont, 2001.

[6] Limprecht, E., Abbott's patience runs out, *The Age*, Next, 6 September 2005, p. 4.

[7] McCabe, B., Privacy of data is key to spread of sharing,*The Australian*,IT Business, 9 Aug 2005, p.2.

[8] McDermott, Q., Your Money and Your Life, *Transcript of ABC Four Corners program* 18/08/05.

[9] Office of the Federal Privacy Commissioner, *Guidelines on privacy in the private health sector*, September 2001.

[10] Office of the Federal Privacy Commissioner, *Guidelines to the national privacy principles*, November 2001.

[11] Paterson, M., *Freedom of Information and Privacy in Australia: government and information access in the modern state*, Lexis Nexis Butterworths, Chatswood, 2005.

[12] Ritchie, J., *Privacy Implications*, Women's & Children's Health, Melbourne, 2002.

[13] Shaw, M., Privacy laws may be tightened, *The Age*, News, 16 August 2005, p. 5.

[14] Skinner, G.D., Dynamic User Reconfigurable Privacy and Trust Settings for Collaborative Industrial Environments. Curtin University of Technology. Perth, 2005.

[15] The Economist, The mobile puts a doctor in your pocket,*The Australian*,IT Business,20 Sept 2005. p.2.

[16] Tucker, G., *Information Privacy Law in Australia*, Longman Cheshire, Sydney, 1992.

[17] Turner, A., Rogue agents aren't a reload of Hollywood rubbish,*The Age*,Next,10 June 2003,p.12.

[18] Victorian Health Records Act 2001 Health Privacy Principles (HPPs), http://www.health.vic.gov.au/hsc/hppextract.pdf (accessed 16/08/05).

[19] Whetton, S., *Health Informatics: a socio-technical perspective*, OUP South Melbourne, 2005.

i