Pseudonymity And Anonymity In Identity Management: Can Anonymous Credentials Enhance User Participation In Electronic Health Records

George Coles, Southern Cross University, Australia
William Smart, Southern Cross University, Australia

Abstract

The introduction of a Personally Controlled Electronic Health Record System is central to Australia's key eHealth initiatives. This comes at a time when recent research efforts in Australia, Britain and the US, indicate that a majority of consumers are concerned regarding the security and privacy of information accessible over the Internet. Primary concerns are related to the potential for identity theft and the exposure of personal information. Research into possible solutions has been ongoing for decades however; the technological solutions that are slowly emerging have complexities that make it difficult for the average consumer to comprehend. The research proposed here concerns user perceptions and preferences towards the key technologies that have evolved in efforts to protect the privacy of personal information. This includes various implementations of Public Key Infrastructure (PKI) with a focus upon Anonymous Credentials.

Keywords: PKI, privacy, security, eHealth, anonymous credentials

Introduction

The recent Australian Healthcare Identifiers Act 2010 (Attorney-General's-Dept. 2010), provides for the assignment of unique identifiers for Health Care Providers and Health Care Recipients in order to facilitate the access of Personally Controlled Electronic Health Records (PCEHR) (NEHTA 2012). A centralised PCEHR system can bring many benefits to Health Care Recipients, either directly through the increased accessibility of their health information for their own treatments or indirectly through the increased accessibility of information for the purposes of medical research. However, these benefits come at a cost, which is an increase in the possibility that a recipient's privacy may be endangered through the exposure of their information to unauthorised parties.

Whilst the world is still coming to terms regarding the vulnerabilities associated with the protection of privacy concerning credit card and other financial transactions conducted over the Internet (OECD 2008). Google has recently released changes to their privacy policies, which now effectively allow them to data mine any information they collect from the users of their services on a day-to-day basis. This includes what is searched for such as words, medical conditions, jobs, prospective partners and virtually anything a user clicks. Google's new policy now allows them to cross reference and data match personal information across more than 60 of their products, including their web search engine, u-tube, g-mail, mobile phone and tablet location finders among others. Google can record what a user is doing, what they wish they were doing, when they are doing it, where they are and with whom they are communicating (ABC 2012). This exposes users to the possibility of being traced online when interacting with the PCEHR systems and then subsequently conducting searches related to their health conditions.

Alistair MacGibbon (2012) a graduate of the FBI's National Academy and the founding director of the Australian High Tech Crime Centre reports that as competition between the major players such as Google, Microsoft, Facebook and Apple has increased so too has the number of privacy breaches both against them and by

them (ABC 2012). These issues contribute to an Orwellian atmosphere of distrust among users regarding the use of the Internet. Users are becoming increasingly aware that there are now many Big Brothers keeping watch over them. Evidence of this has recently been unveiled in a large-scale joint study conducted by RSA Laboratories, Microsoft Research and Microsoft Corporation where it was found that service providers (websites) can recognise and track up to 88% of the users returning to a website. Of these users 33% demonstrated efforts to preserve their privacy through the use of private browsing mode or by utilising browser options to clear tracking cookies (Yen et al. 2012)

Furthermore as a ramification of the recent "do-not-track" initiative of the U.S. Federal Trade Commission (FTC 2011), ensighten.com a UK based industry leader in international website privacy compliance, claims that 93% of Internet users would use a Do Not Track browser feature (Ensighten.com 2012). In addition to this a recent Australian survey indicates that 90% of respondents indicated their support for regulations which could control the capture and use of their personal information with 56% showing their disapproval of targeted advertising based upon their personal information (Andrejevic 2012). Amidst these uncertainties, a total of $466.7m was allocated in the 2010 Australian Federal budget to build e-Health over two years for launch in 2012. This is expected to be only a small part of the Government's overall e-Health investment (Tay 2010).

For centuries, medical practitioners have instilled trust in their patients through adherence to the Hippocratic Oath (Croll 2010b; Hulkower 2010). The oath is said to outline 12 principles, one of which clearly relates to confidentiality between a patient and physician as follows:-

> *"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about",* (Tyson 2001).

Confidentiality plays a significant role in the doctor/patient relationship, without it, trust is shattered to the extent that a patient will soon discontinue any treatment and seek help elsewhere and may even enter into some form of litigation seeking retribution. A patient also needs to have a high degree of confidence in the 'competence' and 'professionalism' of their health carers including employees associated with the practice concerned. This now needs to extend to the security technologies deployed in the ICT systems, which store and process their data and the underlying infrastructure of the systems in use (Croll 2010a). With the development of the Internet and now, the establishment of a centralised database for Electronic Health Records (EHR) and considering the privacy implications that the Internet poses, patients now need to invest more trust in the entire health system than ever before.

Progress towards establishing consumer trust regarding the use of the Internet has primarily concerned the development of security technologies for the authentication, authorisation and access of users. However, users generally have little comprehension of how these technologies work (Ulivieri 2004). Increased security does not necessarily translate into a consumer's understanding as an increase in trustworthiness. Ulivieri (2004) suggests that it is more important to consider how users perceive security in efforts to build trust. If a user does not believe that the environment they are in is secure, they will avoid using it and it will make little difference if it is secure or not.

User Participation

The success of the proposed Personally Controlled Electronic Health Records (PCEHR) system is highly dependent upon user participation. Without user participation there will be little data made available by the system for research purposes. Currently the primary source of research data is extracted from medical records held by health care practitioners, which is held under their protection in their archival systems and within the confines of their premises. Such records are generally stored in the form of paper-based records, film and/or computer based records. Access to the data of interest to research contained in these records is fraught with complications ranging from patient consent to the resource intensive efforts on the part of medical practitioners to make it available for use in research. The establishment of a centralised EHR system is seen to greatly facilitate the access of this data for research purposes whilst simultaneously reducing the load placed upon the Australian health services sector and minimising the incidence of medical errors (Accenture 2010; Bartlett et al. 2008; Boonstra and Broekhuis 2010).

Currently patients can readily gain access to their own medical records from their healthcare providers and may also have such records sent to other practitioners who may also be treating them, such as their GP, Dentist or other health care specialists. This is a common practice among health care professionals. Although the taking of the Hippocratic Oath is no longer obligatory in many medical schools, it is still observed in a traditional sense by medical practitioners throughout the world. In this way it has served the preservation of the privacy of highly sensitive health information of patients for centuries (Hulkower 2010; Tyson 2001). Incentives for user participation in the proposed PCEHR systems concern benefits which either directly affect patients, such as the reduction of medical errors (Kohn et al. 2000) or indirectly improvements in research and a perceived reduction of workloads for their health care practitioners (Boonstra and Broekhuis 2010). These benefits will be realised over time as the population ages and places an increasing burden upon an already overloaded system.

Quantin et al. (2011) suggest that currently there are no indications that any country has successfully implemented a centralised PCEHR system at the national level. Researchers are now re-evaluating the possibility of deploying distributed systems as a solution (Quantin et al. 2011). However distributed systems are not considered to deliver the cost savings and efficiency that a centralised system is expected to bring (Accenture 2010; Bartlett et al. 2008) yet a distributed system is considered to be a safer alternative regarding the protection of the privacy of individuals' information (Quantin et al. 2011). Distributed systems have other complications that have yet to be addressed such as the legal responsibilities of medical practitioners regarding the protection of patient privacy.

Faced with the increasing erosion of privacy of information regarding the use of the Internet, users are now being asked to participate in EHR by allowing their highly sensitive health information to be placed in a centralised database that is accessible via the Internet. With few incentives for participation, trust in the systems is being pressed to extremes (Fernando 2012). Security technologies have not yet developed to the extent where the Internet is considered a safe environment. However, developments in security technologies have made the Internet safer over time. The measures taken have mostly concentrated on fortifying individual domains by reinforcing authentication, authorisation and access control mechanisms. These mechanisms primarily focus upon strong identification procedures (Clarke 2009-10). This indeed strengthens the security of access, however the collection and storage of the identities of users in data stores erodes the privacy of user information and becomes a target for identity theft.

Security Technologies

IT professionals for decades have recognised the need for an identity management system, which preserves the privacy of individuals and that operates at the global level (Blaze 2003; Brands 2011; Camenisch and Lysyanskaya 2001; Chaum 1985; Clarke 1998; Ellison 2004; EMC Corporation 2011; Groß 2009; IBM Research 2010; Kessler 2011; Quantin et al. 2011; Rivest et al. 1978; Wilson 2012). However, the complexities associated with the design and implementations of such a system are vast. Researchers continue to seek out solutions in response to these problems. Encryption technologies are central to these efforts and Public Key Infrastructure (PKI) is the primary technology to have evolved.

The current ITU Telecommunication Standardization Sector (ITU-T) recommendation and ISO standard ISO/IEC 9594-8 (ITU-T 2009) describes a framework for PKI commonly known as the X.509 Digital Certificate scheme. X.509 based PKI is subject to extensive criticisms concerning the shortcomings of the technology to protect the privacy of information of individuals and is more suited for corporate use (Clarke 2001). The Gatekeeper PKI Framework is the foundation for PKI in Australia as defined by the Australian Government Information Management Office of the Department of Finance and Deregulation and is based upon the X.509 Digital Certificate scheme (AGIMO 2009; Andison 2008). The Gatekeeper PKI Framework is the basis upon which The National E-Health Transition Authority (NEHTA) are building the PCEHR system (Tay 2011). IBM Australia have been contracted by NEHTA to build the National Authentication Service for Health (NASH) which will facilitate user access to the PCEHR system (Roxon 2012; Tay 2011).

This approach can be loosely described as a form of Government Controlled PKI (GPKI) whereby the encryption keys involved in the process are fully controlled by a government department (Clarke 2009-10). Clarke (2011) takes a strong stance regarding the intrusive nature of the implementation of many of the electronic security practices in common use. He suggests that for proper functionality, all forms of conventional PKI are intrusive to

some extent. However, he maintains that conventional PKI based upon the X.509 standard is particularly harsh in this regard. The International Telecommunication Unions' (ITU), X.509 standard is the foremost standard currently used as a foundation for PKI today, now in version 'X.509 (11/2008)' (Clarke 2001; ITU-T 2009). Clarke (2009-10) identifies numerous weaknesses in the scheme that include; Privacy Invasiveness, Limited Assurances, Technical and Implementation Weaknesses, Private-Key Insecurity, the use of a Single Identifier with a Single Key-Pair and that X.509-based PKI is based on a hierarchy of trust.

In order for e-trust systems to be effective, Clarke (2001) suggests that the focus must move away from the identity of individuals and that security mechanisms should be accommodating of both anonymity and pseudonymity. He highlights the following needs:-

- Organisations and individuals both need on occasion to have software agents act on their behalf.
- Individuals need to be able to carry out tasks without the necessity of declaring their identity.
- Individuals need to be able to convey certain attributes without the necessity of declaring their identity.
- Persistent relationships need to be supported without necessarily identifying either party.

Security technologies have been primarily driven by the needs of e-commerce. Clarke (2001) suggests that in order for e-commerce to become accepted, the perception was that merchants needed to be able to identify themselves and to allow authentication of the identifiers they provide. However, marketers sought schemes whereby consumers also needed to identify themselves.

He presents a model in his work titled, "A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation", and suggests that the theory behind identification and identity authentication practised over the last 20 years has been highly inadequate (Clarke 2009-10). In his model, he introduces concepts such as 'entifiers' and 'entification' as distinguished from 'identifiers' and 'identification'. Another concept he terms as 'nymity', which is associated with both anonymity and pseudonymity. Clarke (2001) suggests that the inclusion of the concept of a 'nym' into conventional PKI may possibly satisfy the above-mentioned needs.

Although there is no suggestion that the approach taken by NEHTA regarding the construction and design of the system is flawed, the security technologies incorporated into the solutions will at most only protect users of the system itself, which represents a single domain. Finding a solution that can operate across all domains at the global level is yet to be realised, however research continues towards this outcome. Technologies within this field are loosely termed as 'Anonymous Credentials', the concept of which was first conceived in 1985 by David Chaum (1985). IBM Research in Zurich has been developing an open source solution, known as 'Identity Mixer', along these lines since 1998 and is now in the final stages of establishing an international standard. Similar work has been conducted by Brands (2011) since 1999 and later in conjunction with Microsoft on their U-Prove product.

Parallels of EHR to e-Commerce

Any study that attempts to evaluate the success of PCEHR systems can benefit greatly from the insight and knowledge gained through the implementation of e-commerce systems. E-commerce originally evolved from Electronic Data Interchange (EDI), which allowed established business traders to trade over private networks. Later the commercialisation of the Internet in 1995 provided a more affordable means for businesses to conduct their trade using a single and open network. As a result Business-to-Business (B2B) e-commerce flourished. Businesses quickly embraced this avenue for trade as commercial relationships between businesses are formed on the basis that the trading partners know and trust each other.

As the Internet grew so too did the number of private users. This led to the advent of Business-to-Consumer (B2C) e-commerce (Egger 2003). With the emergence of B2C e-commerce, where consumers are able to shop online to make purchases, conduct their banking or pay bills and so forth, there came an increase in the number of vulnerabilities to the privacy, safety and security of personal data and information. These vulnerabilities are related to crimes such as identity theft and other fraudulent behaviours perpetrated by cyber-criminals who seek to identify one's personal information such as name, address, date of birth, gender, passwords and credit card details etc. in order to steal a user's identity, money and/or goods and services.

At the outset it was anticipated that B2C e-commerce would see similarly high levels of growth and acceptance in the community as did B2B e-commerce (OECD 2008). However, the issues of consumer trust emerged, due to the transient nature of the relationship between retailers and their customers. This usually involves a single transaction between unknown parties, unlike that of B2B transactions, which primarily take place between established business trading partners (i.e. supplier/distributor, wholesaler/retailer etc.). Although there are many similarities between the uses of e-commerce systems to that of EHR systems, there are also highly significant differences between the two.

Whilst e-commerce systems, used in online banking and online shopping, involve the transmission of sensitive data and information such as names, addresses, credit card numbers and account details etc., EHR systems concern a very different type of user data and information. The problem is compounded by the fact that traditionally workers employed in the health industries are not expected to have a comprehensive understanding of the technologies driving the World Wide Web (WWW). The financial sectors, which include the banks and credit card companies such as VISA and MasterCard and other similar services, have been developing electronic systems, since long before the advent of the Internet and the WWW. In contrast, EHR systems are a relatively new concept by comparison (KPMG 2008).

Medical Records and EHR

The practice of keeping medical records predates Hippocrates. Until the recent information revolution, medical records have been kept primarily on paper and filed in the archives of healthcare practitioners and hospitals. Medical records (MR) and Electronic Medical Records (EMR) should not be confused with Electronic Health Records (EHR). Medical records and their electronic equivalent EMR remain the property of the doctor or practice attended by the patient. The electronic version of a medical record is simply a record kept by the practitioner in electronic form on a computer system. These records are essentially notes taken by the doctor regarding a patient's consultation and hence remain the property of the doctor or practice. However, in the Australian public health sector, generally a patient is entitled to access to information contained within medical records concerning that patient (AMA 2002; MCNSW 2010; Samford 1999).

Medical Records (MR) are essentially legally binding documents from which the data contained in an EHR is drawn (Garets and Davis 2006). The terms EMR and EHR are often used interchangeably and are known by other monikers such as Patient Care Records (PCR), Computer-based Medical Records (CMR), Electronic Patient Records (EPR) or Summary Care Records (SCR) among others. What is of concern in this study is essentially referred to as Electronic Health Records (EHR) or more specifically Personally Controlled Electronic Health Records (PCEHR). Currently throughout the world, health carers and organisations are developing EHR systems with the purpose of improving individual patient and public health standards (Accenture 2010; Liu et al. 2009). These outcomes are being achieved through an effort to increase the accessibility and quality of healthcare to patients in need, whilst simultaneously lowering the costs involved.

Benefits of EHR

Benefits of EHR include the provision of access to practitioners of patients' medical history and clinical data from previous episodes of care provided by other practitioners. This facilitates personalised treatment plans, supports decision-making, reduces the risk associated with errors made in diagnoses and prescriptions and reduces the cost and time involved with sharing records across various healthcare providers. By connecting healthcare providers through health care networks, accessibility of specialist care is improved as clinical data, images etc. can be sent electronically to specialists for assessment. Networking also, helps reduce the cost of care by reducing the reliance upon dedicated diagnostic laboratories and specialists. Furthermore, anonymised EHR data can greatly improve the outcomes of clinical research. This data can also be used in the development of Intelligent Decision Systems (IDS) thus helping to improve the effectiveness of disease management, public health campaigns and the development of preventative health strategies (Accenture 2010; Commonwealth of Australia 2012).

Cost savings expected from the Australian PCEHR system are reported to be up to a possible $5.6 billion over the first 10 years of operation based upon an independent state by state implementation and up to $20.8 billion

from a system deployed at the national level (Bartlett et al. 2008). This represents a huge reduction in costs and heightened efficiency in the Australian health care system. Similar effects in efficiency and savings have been identified in the analysis of the German and Canadian health care systems. It is now acknowledged by the European Union that a cross-border EHR solution for all the EU member states, would realise similar benefits in savings and efficiency and it is now planned to achieve this by 2015 (Bartlett et al. 2008).

The beneficiaries of these improvements include, the users of health services and their carers, healthcare providers, health managers and planners and the government. Although these benefits are widely recognised, organisations and governments throughout the world have struggled to implement effective solutions (Accenture 2010; Quantin et al. 2011). Primary challenges are related to information governance, which concerns the processes, functions, standards and technologies that enable highly sensitive health information to be collected and used effectively in a secure and safe manner.

Privacy Concerns

Issues of trust and privacy in e-commerce greatly concern the privacy of a user's information regarding access to their bank accounts and credit card services (Coles 2010; Coles and Smart 2011). Other concerns involve trust in merchants to fulfil their obligations according to expectations. However, the data and information stored in eHealth records concerns a very different data type which when the security of that data is compromised there is very little in terms of compensation that can be offered.

Privacy and data security issues continue to escalate at a rapid pace. The Australian Privacy Commissioner, Timothy Pilgrim addressing the Emerging Challenges in Privacy Law Conference held at Monash University, Melbourne in February 2012 (Monash 2012), warned that data security has become a major challenge for organisations throughout Australia. He states that with the advent of cloud computing, portable devices, database storage and the activities of hackers', dramatic changes have taken place regarding data security and document storage. Even when strict measures are put in place to protect data, breaches can still occur. He warned that organisations should have comprehensive contingency plans in the event that a data breach may occur and that damage to an organisation's reputation can be made worse if any attempt at a cover-up is seen to take place. This applies also to non-profit organisations if they earn over $3 million per year and or hold health information (ProBono 2012).

On the 29th February, 2012 (ABC 2012) Pilgrim, along with 36 US attorneys general plus regulators in Korea and the European Union unsuccessfully appealed to the online search engine giant Google to delay the release of their new privacy policies. These policies now give Google unprecedented access to the personal information of users who use their services. Ben Edelman of Harvard Business School suggests that Google has amassed the most extensive database ever conceived on who does what, who wants what and who reads what over the Internet. Although Google makes claim to an informal motto of "Do No Evil" (i.e. putting the interest of users before profit), with annual revenues of around $40 billion there are great concerns regarding whether this motto really means anything (ABC 2012).

Considering the fragility of the current state of privacy protection of the average user, the situation is exasperated further when taking into account the confidentiality that a patient places in health care practitioners, their practices and associated employees. This includes the systems in use to manage and control day-to-day operations of the practice concerned. Croll (2010a) suggests that when dealing with healthcare providers, patients have high expectations regarding the confidentiality of their private health information. This means that the confidence a patient places in their doctor, dentist or other health care provider, to keep secret from anyone else the status of their health, would be severely broken if anything were to be divulged without their consent. This includes spouses, other family members, other relatives and anyone else for that matter. However, this expectation of confidentiality is variable when considered in different contexts i.e. in a life threatening circumstance it may save a patient's life if the attending emergency crew were privy to specific information that would otherwise be kept private. Information such as medications, allergies, mental health and other ongoing or past conditions etc., can help greatly in a patient's diagnosis particularly when that patient may be unconscious. In certain cases, a patient would be thankful that their conditions be made known to those concerned on a need to know basis yet not to others.

Proposed Research

The research problem at hand is to determine whether the characteristics of Anonymous Credential systems can enhance user participation in the Australian PCEHR systems. Although there are no working models currently in use in Australia and due to the complex nature of the technology involved, the average user has little comprehension of what an Anonymous Credential system is and how the technology works. However, the characteristics of these technologies can be presented graphically in a short video, which can be presented to users as part of an online survey in order to evaluate user preferences and attitudes towards various identity management and access control technologies.

Croll (2010a) presents a 'Privacy Model for Health' that places Safety at the centre of Confidentiality, Trust, Security and Privacy (see Figure 1 below). This model was designed to help healthcare organisations determine the adequacy of the privacy policies they implement, and how well they adhere to these policies. The model was tested against differing case studies and then compared to the 10 National Privacy Principles (NPPS) (OAIC 2006), which in 2000 were amended to the Privacy Act of 1988 (ComLaw 2012). These principles are applicable to all private health care providers in Australia and across some public services under State legislation. Conclusions drawn in the study suggest that the model could be used as an overview from which detail can be drawn through decomposition of its constructs in an effort to develop policy. The model is simple and easily understood and may help the average user to evaluate the risks and safety concerned with the use of EHR. The model will also assist in the formulation of the survey questions as part of the research design the survey questionnaire and will assist in the evaluation of the outcome.

The video animation describes characteristics of the key technologies under examination and presented as an introduction to the survey.

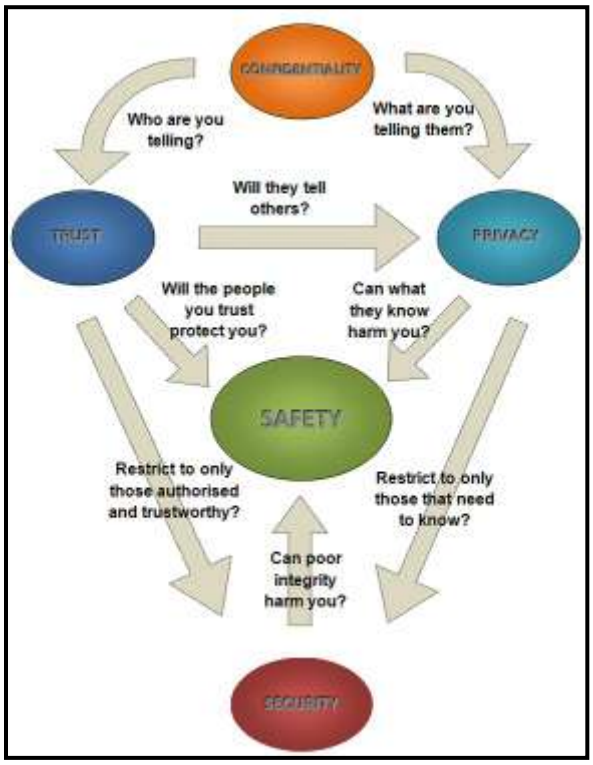

Figure 1 - Privacy Model for Health (Croll 2010a)

Author Information

George Coles is currently a casual academic teaching IT at Southern Cross University, whilst undertaking his PhD. The focus of his research is primarily related to user trust issues concerning the privacy and security of information stored on the Internet.

Dr William Smart is a lecturer with the Southern Cross Business School, based at Southern Cross University's Gold Coast Campus, Australia. Bill's research interests are Information Success Modelling, e-Health, Web Navigation, Web Development, Wireless Technology, National Broadband Network, Online Learning, Telecommunications and programming in multiple languages.

References

1. ABC. 2012. "Is Google Watching You?," M. O'Neill (ed.). Australia: Australian Broadcasting Commission, from http://www.abc.net.au/news/2012-02-29/is-google-watching-you/3861158
2. Accenture. 2010. "Information Governance: The Foundation for Effective E-Health." Accenture, from http://www.accenture.com/us-en/pages/insight-information-governance-effective-ehealth-summary.aspx
3. AGIMO. 2009. "Gatekeeper Public Key Infrastructure Framework," Australian Government Information Management Office (ed.). Online: Department of Finance and Deregulation, from http://www.finance.gov.au/e-government/security-and-authentication/gatekeeper/docs/Gatekeeper_PKI_Framework.pdf
4. AMA. 2002. "Guidelines for Doctors on Providing Patient Access to Medical Records - 1997. Revised 2002." Australian Medical Association, from http://ama.com.au/node/469
5. Andison, D. 2008. "Gatekeeper Public Key Infrastructure Framework." Online: Australian Government Information Management Office, from www.landgate.wa.gov.au/docvault.nsf/web/NEC_PRES8_PKI_FRMWK/$FILE/NEC_PRES8_PKI_FRMWK.ppt
6. Andrejevic, M. 2012. "Australians Concerned for Online Privacy." The University of Queensland: UQ News Online: , from http://www.uq.edu.au/news/?article=24504
7. Attorney-General's-Dept. 2010. "Healthcare Identifiers Act 2010," Attorney-General (ed.). Canberra, Australia: Office of Legislative Drafting and Publishing (OLDP), from http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/3F407B27709A1442CA257757008155A9?OpenDocument
8. Bartlett, C., Boehncke, K., and Haikerwal, M. 2008. "E-Health: Enabler for Australia's Health Reform." National Health & Hospitals Reform Commission, from http://www.racgp.org.au/Content/NavigationMenu/ClinicalResources/ehealth/Resources/Booz_eHealth_Report.pdf
9. Blaze, M. 2003. "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks." AT&T Labs – Research: crypto.com, from http://www.crypto.com/papers/mk.pdf
10. Boonstra, A., and Broekhuis, M. 2010. "Barriers to the Acceptance of Electronic Medical Records by Physicians from Systematic Review to Taxonomy and Interventions," *BMC Health Services Research*), 06/08/2012.
11. Brands, S.A. 2011. "Rethinking Public Key Infrastructures and Digital Certificates." Massachusetts Institute of Technology, from http://mitpress.mit.edu/catalog/item/default.asp?ttype=2&tid=3801
12. Camenisch, J., and Lysyanskaya, A. 2001. "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," *Advances in Cryptology—EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques*, Innsbruck, Austria: Springer.
13. Chaum, D. 1985. "Security without Identification," in: *Card Computers to make Big Brother Obsolete* New York, USA: Communications of the ACM (The Association for Computing Machinery), from http://www.chaum.com/articles/Security_Wthout_Identification.htm
14. Clarke, R. 1998. "Public Key Infrastructure Position Statement." from http://www.rogerclarke.com/DV/PKIPosn.html
15. Clarke, R. 2001. "The Fundamental Inadequacies of Conventional Public Key Infrastructure," *ECIS 2001* -

The 9th European Conference on Information Systems, Bled, Slovenia: University of Maribor.
16. Clarke, R. 2009-10. "A Sufficiently Rich Model of (Id)Entity, Authentication and Authorisation," *IDIS 2009 - The 2nd Multidisciplinary Workshop on Identity in the Information Society*, LSE, London, UK: Identity in the Information Society (IDIS).
17. Clarke, R. 2011. "Ebusiness, Information Infrastructure, Indentiy Matters, Dataveillance & Privacy ". from http://www.rogerclarke.com/DV/APM-091112.html
18. Coles, G. 2010. "The Effects of Website Design on Consumer Trust in E-Commerce," in: *School of Commerce and Management*. Lismore: School of Commerce and Management - Southern Cross University, from http://www.gcoles.com/node/3
19. Coles, G., and Smart, W. 2011. "Building Trust in Online Customers," in: *SNPD 2011, 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*. University of Technology, Sydney, Australia: SNPD 2011, from http://ieeexplore.ieee.org/xpl/tocresult.jsp?reload=true&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A6063522%29&refinements=4283766288&pageNumber=1&resultAction=REFINE.
20. ComLaw. 2012. "Privacy Act 1988 ". Online: Australian Government, from http://www.comlaw.gov.au/Details/C2012C00271
21. Commonwealth of Australia. 2012. "Expected Benefits of the National Pcehr System." Online: Department of Health and Ageing, from http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/content/pcehr-benefits
22. Croll, P. 2010a. "Determining the Privacy Policy Deficiencies of Health Ict Applications through Semi-Formal Modelling," *International Journal of Medical Informatics* (80:2), 2011.
23. Croll, P. 2010b. "Privacy, Security and Access with Sensitive Health Information," in: *Health Informatics - an Overview*, E. Hovenga, M. Kidd, S. Garde, C. Hullin and L. Cossio (eds.).
24. Egger, F.N. 2003. "From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce." J.F. Schouten School for User-System Interaction Research., PhD, Eindhoven University of Technology (The Netherlands). <http://www.ecommuse.com/egger2003trust.pdf >.
25. Ellison, C. 2004. "Spki/Sdsi Certificates." from http://world.std.com/~cme/html/spki.html
26. EMC Corporation. 2011. "Cryptographic Challenges." *The RSA Factoring Challenge* Retrieved 25/07/2011, from http://www.rsa.com/rsalabs/node.asp?id=2091
27. Ensighten.com. 2012. "Website Privacy Standards." Online: Ensighten, from http://www.ensighten.com/website-privacy-standards-infographic
28. Fernando, J. 2012. "Apf Submission to Pcehr System: Proposals for Regulations and Rules Paper." from http://www.privacy.org.au/Papers/DoHA-PCEHR-Regs-120411.pdf
29. FTC. 2011. "Ftc Testifies before the Senate Commerce Committee on Privacy; Industry Efforts to Implement "Do Not Track" System Already Underway." Online: U.S. Federal Trade Commission, from http://www.ftc.gov/opa/2011/03/privacy.shtm
30. Garets, D., and Davis, M. 2006. "Electronic Medical Records Vs. Electronic Health Records: Yes, There Is a Difference." HIMSS Analytics, from http://www.himssanalytics.org/docs/wp_emr_ehr.pdf
31. Groß, T. 2009. "Identity Mixer," in: *Resources for Smart Identity Card*. Zurich: IBM Research, from http://idemix.files.wordpress.com/2009/08/prime2006-primer-ecitizens.pdf
32. Hulkower, R. 2010. "The History of the Hippocratic Oath: Outdated, Inauthentic, and yet Still Relevant." New York: Albert Einstein College of Medicine, from http://www.einstein.yu.edu/uploadedFiles/EJBM/page41_page44.pdf
33. IBM Research. 2010. "Specification of the Identity Mixer Cryptographic Library." from http://domino.research.ibm.com/library/cyberdig.nsf/papers/EEB54FF3B91C1D648525759B004FBBB1/$File/rz3730_revised.pdf
34. ITU-T. 2009. "Itu-T Recommendation X.509." Geneva, Switzerland: Telecommunication Standardisation Sector of ITU-T, from http://www.itu.int/rec/T-REC-X.509-200811-I/en
35. Kessler, G. 2011. "An Overview of Cryptography." Retrieved 21/07/2011, from http://www.garykessler.net/library/crypto.html#skc
36. Kohn, L.T., Corrigan, J.M., and Donaldson, M.S. (eds.). 2000. *To Err Is Human: Building a Safer Health System*. Washington, D.C. USA: National Academy Press.
37. KPMG. 2008. "An Evaluation of the Healthelink Electronic Health Record Pilot." NSW Health, from

http://www.healthelink.nsw.gov.au/__documents/evaluation/evaluation_of_healthelink_pilot_summary_report_3566534_1client-job.pdf

38. Liu, V., Franco, L., Caelli, W., May, L., and Sahama, T. 2009. "Open and Trusted Information Systems/Health Informatics Access Control (Othis/Hiac)." Proc. 7th Australasian Information Security Conference (AISC 2009), Wellington, New Zealand: Faculty of Information Technology and Information Security Institute - Queensland University of Technology.
39. MacGibbon, A. 2012. "Internet Safety Institute." Online: Internet Safety Institute, from http://www.internetsafetyinstitute.com.au
40. MCNSW. 2010. "Medical Records - a Guide for Patients." The Medical Council of New South Wales, from http://www.mcnsw.org.au/index.pl?page=64
41. Monash. 2012. "Emerging Challenges in Privacy Law: Australisian and Eu Perspectives." Melbourne: Monash University, from http://www.law.monash.edu.au/about-us/events/privacylaw/
42. NEHTA. 2012. "What Is a Pcehr?." Online: National E-Health Transition Authority Ltd & the Department of Health and Ageing, from http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcher
43. OAIC. 2006. "Information Sheet (Private Sector) 1a: National Privacy Principles." Online: Office of the Australian Privacy Commissioner from http://www.privacy.gov.au/materials/types/infosheets/view/6583#npp1
44. OECD. 2008. "Measuring Security and Trust in the Online Environment: A View Using Official Data," in: *OECD Digital Economy Papers*, M. Schaaper (ed.). OECD publishing, from http://www.oecd-ilibrary.org/science-and-technology/measuring-security-and-trust-in-the-online-environment_230551666100
45. ProBono. 2012. "Not for Profits Warned on Privacy and Data Security." online: Pro Bono Australia, from http://www.probonoaustralia.com.au/news/2012/03/not-profits-warned-privacy-and-data-security
46. Quantin, C., Jaquet-Chiffelle, D.-O., Coatrieux, G., Benzenine, E., and Allaert, F.-A. 2011. "Medical Record Search Engines, Using Pseudonymised Patient Identity: An Alternative to Centralised Medical Records," in: *Special Issue: Security in Health Information Systems*. International Journal of Medical Informatics, pp. e6-e11 from http://dx.doi.org.ezproxy.scu.edu.au/10.1016/j.ijmedinf.2010.10.003
47. Rivest, R.L., Shamir, A., and Adleman, L. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Cambridge, Massachusetts USA: Laboratory for Computer Science, Massachusetts Institute of Technology, from http://securespeech.cs.cmu.edu/reports/RSA.pdf
48. Roxon, N. 2012. "Ibm Selected for E-Health Authentication Service." Online: Australian Labor, from http://www.alp.org.au/federal-government/news/ibm-selected-for-e-health-authentication-service/
49. Samford, K. 1999. "Access to Medical Records," in: *Research Bulletin No 6/99*. Brisbane: Queensland Parlimentary Library, from http://www.parliament.qld.gov.au/documents/explore/ResearchPublications/researchBulletins/rb0699ks.pdf
50. Tay, L. 2010. "Healthcare Identifiers Legislation Passed." from http://www.itnews.com.au/News/217806,healthcare-identifiers-legislation-passed.aspx
51. Tay, L. 2011. "Nehta Inks E-Health Authentication Deal." Online: ITNews for Australian Business, from http://www.itnews.com.au/News/249797,nehta-inks-e-health-authentication-deal.aspx
52. Tyson, P. 2001. "The Hippocratic Oath Today." *NOVA, Body and Brain*, from http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html
53. Ulivieri, F. 2004. "Naive Approaches to Trust Building in Web Technologies," 15426B_2004, Rome, p. 17.
54. Wilson, S. 2012. "Pki." Online: The Lockstep Group, from http://lockstep.com.au/about/pki
55. Yen, T.-F., Xie, Y., Yu, F., Yu, R.P., and Abadi, M. 2012. "Host Fingerprinting and Tracking on the Web: Privacy and Security Implications." Network and Distributed System Security Symposium (NDSS) 2012: San Diego, California.: Internet Society, from http://www.internetsociety.org/host-fingerprinting-and-tracking-web-privacy-and-security-implications