Enhancing Participation in Personally Controlled Electronic Health Records

George Coles, William Smart, Bruce Armstrong
Southern Cross Business School, Southern Cross University,
Locked Bag 4 Coolangatta, QLD 4225, Australia
E-mail: bill.smart@scu.edu.au

Abstract

The introduction of a Personally Controlled Electronic Health Record (PCEHR) system is central to Australia's key e-Health initiatives. This comes at a time when recent research efforts world-wide, report consumer concern about the security and privacy of information accessible via the Internet. Research into possible solutions has been ongoing for decades with Anonymous Credentials recognised as a possible solution. Our study examines whether the use of Anonymous Credentials can address these concerns and enhance participation in the PCEHR system. Preliminary analysis seems to indicate that this is the case, with the sample investigated displaying high levels of concern with security and privacy issues of both the PCEHR system and web based identification as a whole. Additionally enhancement of participation in the PCEHR, by introduction of anonymous credentials is found to be supported amongst respondents.

Keywords: PKI, privacy, security, e-Health, anonymous credentials

1. Introduction

The current e-Health initiative of the Australian Government has been criticised by some commentators as favouring government agencies, insurers and researchers and could be adverse to the welfare of consumers[1,2]. A centralised Personally Controlled Electronic Health Record (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[3,4]. 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[4,5].

The success of the PCEHR system in Australia is dependent upon user participation. The establishment of a centralised EHR system presents the opportunity to use this data for research purposes while reducing the load placed upon the Australian health services sector and minimising the incidence of medical errors[6,7]. The Australian Government's target was to have the PCEHR system in operation by July 1st 2013, one year after its release, with 500,000 users enrolled[8]. Associate Professor David Glance of The University of Western Australia[9] reported that the Department of Health and Ageing (DoHA) stated that the total number of users enrolled by this date was 397,745. Brett Avery[10] of CIO stated that by early March 2013 only 73,648 PCEHR registrations had taken place. The surge in registrations after March has been attributed to DoHA's e-Health travelling road shows, a television advertising campaign and by using consultants to promote the systems at public hospitals[8].

Despite the incentives that the Government is providing to medical providers in an effort to get them involved, many see little benefit in investing time and effort into the use of the system and are also confronted by potentially severe legalities related to disclosure of patients' healthcare identifiers and the privacy of information stored in their health records[11,8]. The cost to maintain the system, which is currently comprised of mostly empty records, is estimated to be around $80 million per year[8]. Avery[10] suggests that the PCEHR system needs to be promoted to the people who stand to benefit the most right now and that a better understanding of peoples' motivations to register and

Published by Atlantis Press

use the service is important in order to realise the benefits that the system has to offer. Meaningful use of the service goes beyond counting the number of registrations and it is considered that as the population ages, enabling older Australians and those with ongoing health conditions and chronic illnesses to actively manage their health, will help them to coordinate their interactions with their health care providers[8,10,12]. An understanding of what will influence and encourage patient and healthcare provider uptake of the PCEHR service is central towards making the most of the benefits it has to offer[10].

2. Identity Management and 'Big Data'

Information technology professionals for decades have recognised the need for an identity management system, which preserves the privacy of individuals and that operates at a global level[13,14,15,16,17,18,19,20,21,22]. This suggests that it is no longer considered adequate to protect user identities stored in the databases of individual web sites distributed across the Internet, by fortifying individual websites themselves[5]. A solution which protects user identities at the global level is required for the survival of real consumer security and privacy into the future[1,5,13,14,15,16,18,19,23].

The proliferation of data matching and cross-referencing of user activity on the Internet has increased at an astonishing rate over recent years with reports suggesting that around 90% of the data now in storage has been generated over the last two years[24]. This phenomenon has been termed 'Big Data' and is practiced increasingly by the major players such as Google, Microsoft, Facebook and Apple[24,25] in their efforts to continuously find new means of making the profits to meet shareholders' expectations[26]. This 'Big Data' phenomenon refers to the correlation of huge volumes of data in order to extrapolate information regarding online user behaviour concerning individual's activities conducted over the Internet[24]. It is anticipated that 'Big Data' will be a key driver behind developments in health, commerce and technology in the near future and that the protection of consumer privacy and the reinforcement of user trust will be an ongoing challenge for e-commerce enterprises, governments, regulators and health in the years to come[24].

3. Cryptography and Anonymous Credentials

David Chaum's[16] work titled 'Security without Identification' foresaw the impending approach of the 'Orwellian' like practice of 'Big Data' and sought a solution that could counter the imminent threats to consumer privacy and security[27]. Chaum's[16] ideas were presented in the form of a number of analogies. These were inspired after the work of Rivest, Shamir and Adleman in their asymmetric key encryption algorithm presented in 1978 and now known as the RSA algorithm[16,21]. Asymmetric key encryption uses two keys in the encryption process i.e. one to encrypt and one to decrypt[21,28]. Diffie and Hellman were the first to present the theory behind asymmetric key encryption in 1976 and later released their Key Exchange Protocol, which was used specifically for key exchange only[29]. Chaum[16] recognised the possibilities for what is termed as Anonymous Credentials that came about as result of the development of the encryption techniques and algorithms presented by Diffie and Hellman[28]and Rivest, Shamir and Adleman[21].

Although the RSA algorithm has been in use for many years now and is the original and remains the most common asymmetric key encryption technique in use today[20,29], the concepts presented by Chaum, are only now coming to realisation in practical form. IBM's 'Identity Mixer'[30] is inspired by Chaum's work and is a continuing project under development and funded as part of the European Union's 'PrimeLife' project which represents "Privacy in Identity Management for Europe for Life[31]". Identity Mixer is built upon the Camenisch-Lysyanskaya Signature Scheme, which was first released in 2001[15] and purposely developed as a foundation by which to develop an 'Anonymous Credential' system.

The development of asymmetric key encryption technologies such as RSA has made it possible to develop 'Digital Signature' schemes[20,32], which have for decades, proven highly resilient against attack (cracking) by adversaries[17]. This kind of technology is termed as Public Key Infrastructure (PKI). However the implementation of these technologies under the current international standard for PKI (i.e. the X.509 standard[33]) provides a very strong identifier when used by individuals on the Internet and places their privacy at risk[34]. A strong identifier used for identification makes it easier to track which websites a user visits on the Internet. The work conducted by IBM Research in

Zurich has sought to resolve this issue by developing a different implementation of PKI based upon the proven security of the RSA algorithm yet has been specifically designed to provide strong security whilst preserving user privacy[30].

In September 2009, the 'German Society for Computer Science' awarded the project with the 'Innovation Award 2009' for establishing an anonymous credential system on a standard Java Card (i.e. SmartCard or chip card)[35]. Members of the team are now in the final stages of establishing an international standard[36], which may change the way in which individuals identify themselves on the Internet.

3.1. *Anonymous credentials*

Anonymous credentials are a digital or virtual form of a common real world credential such as a driver's licence, birth certificate, Medicare card, passport, credit card or any other form of membership credential like a student card or library card[5]. In the physical world, credentials such as these are used to verify an individual's identity. In many cases these are pooled together in order to establish valid proof of identity. In the physical world, these credentials are shown to an authority that may need to verify that an individual has a specific qualification that certifies their eligibility to an entitlement, concession, benefit or licence. Examples would include a police officer checking if the driver of a vehicle is licensed or if an individual is 18+ years of age to purchase alcohol or a traveller has the necessary visa to enter a country. In these cases, the credentials are issued by the respective organisations that know the individual's identity and that authority then gives them some qualification in the form of a credential.

Possession of these credentials can serve as identification for secondary purposes and when used as such is simply checked or shown to someone who may need to verify an individual's name, age or qualification (i.e. the details are not recorded in a database stored somewhere on the Internet). In the digital world, there is currently no equivalent form of digital credential that can be used in a similar manner that preserves the privacy of information about the individual contained in the credential [5]. On websites, a user will enter all of the data regarding their particulars such as their name, address, birthdate, credit card number, Medicare number, gender, nationality, postcode, and so forth, all of which are then recorded on the website's database and stored somewhere on the Internet[5]. Many organisation's conducting websites on the Internet have little knowledge regarding who or where their Internet Service Providers (ISPs) are and no knowledge of who may have access to the data stored there. In many cases, their ISP's may be located in another country. This represents a serious threat to individuals having their identity disclosed to unauthorised parties.

3.2. *Attribute based credentials*

A more recent terminology for Anonymous Credentials has been described as Attribute-Based Credentials or ABC's[37] and two primary projects which have emerged as leaders in the field are IBM"s Identity Mixer and Microsoft's U-Prove project[5]. The development of this kind of credential system for identity management has been the focus of many projects across the globe for well over a decade and have involved many of the world's leading cryptographers in the effort[1,13,14,15,18,20,26,30,31,38]. These systems are now being trialled for use in a multitude of different applications and have many appropriate features highly suitable for use in PCEHR systems[38].

The Australian Government is currently considering a National Trusted Identities Framework (NTIF) that provides for the recognition of online credentials for use by individuals, businesses and the government[24,23]. Similar initiatives include the US National Strategy for Trusted Identities in Cyberspace[24,39], the EU's ABC4Trust project[36,40] and the UK Government's Identity Assurance Programme[24,41].

Anonymous credentials as implemented in the two key ventures to have emerged i.e. IBM's Identity Mixer and Microsoft's U-Prove projects possess the same security properties of conventional digital certificates without compromising the privacy of the user's identity or the traceability of their online interactions[42]. This provides for authentication and authorisation based upon the users attributes without the need for identification and can also be implemented on a smartcard[42]. These privacy preserving features are highly suitable for use in the Australian PCEHR system and offer a level of security superior to that of password authentication[43].

Password authentication is considered to be low cost to implement by comparison to digital certificate schemes[44]. However password authentication is considered to have many inherent security weaknesses[43], whereas conventional digital certificate schemes depend upon a complex infrastructure such as Public Key Infrastructure and the dependence upon specialised hardware and the software to control that hardware. Conventional digital certificate schemes have also been criticised for weaknesses in the preservation of the privacy of users' identity and also for inefficiencies in the revocation process when credentials are compromised.

The developers of IBM's Identity Mixer claim to have solved these issues and were awarded the '2009 Innovation prize' by the 'German Society for Computer Science', for establishing an anonymous credential system on a standard smart card[35]. The award suggests that their system ensures privacy and security in a practical manner that promotes trust in the protection of users' data and also strengthens the social acceptance of solutions in fields such as e-government. These properties are highly advantageous to ensure the usefulness of the Australian PCEHR system.

4. Cyber Threats

In an Australian Computer Society (ACS) presentation by Emeritus Professor William Caelli, AO, he indicated that 9 out of 10 web servers throughout the world have been compromised to some degree by hackers intruding into the systems[45]. Moreover, that many of these attacks take place unnoticed by the webmasters controlling the systems. Professor Caelli is Australia's foremost authority on cyber security and is the only non-US citizen invited as a board member of the CISSE - Colloquium for Information Systems Security Education. In his presentation, he indicated that the defence forces of the world's major powers including the USA and China are now treating information security as a weapon of war.

He stated that efforts are being ramped up to educate and train cyber security professionals in preparedness for the looming possibility of cyber-attack and that the gloves are off regarding cyber defence and cyber offence operations. Because the world's defence forces are now preparing for cyber war, the accumulation of individuals' identity information stored in databases and randomly scattered throughout the Internet, represents serious vulnerabilities, not only to the possibility of identity theft of individual's but also the threats to national security[45].

In a joint media release on the 15th September 2011, the then Australian Foreign Affairs Minister, The Hon Kevin Rudd and the Australian Minister for Defence, The Hon Steven Smith stated that:

"*The US and Australian Governments agreed today that a cyber-attack on either of them would trigger the mechanisms of the ANZUS Treaty*[46]."

In a follow up to these discussions on May 16th 2012, Australian Attorney-General, The Hon Nicola Roxon met with US Secretary Napolitano to sign a 'Statement of Cyber Security Intent', to enhance global cyber security and 'cyber incidence' response capabilities[47,48]. This indicates the seriousness by which cyber security and the associated vulnerabilities are now being treated.

Anonymous credentials have the potential to reduce greatly these vulnerabilities by shifting the focus of authentication away from being identity based and basing authentication more upon rights, roles, privileges and/or restrictions that an individual may have[1,5]. Anonymous credentials are also designed to offer a higher degree of security to online services that need to authenticate those who are accessing the services provided[18]. Currently the majority of website services employ authorisation techniques based upon what is termed 'password' authentication where a registered user after he/she has 'enrolled' at a website is issued a user name and password that he/she then use to access the site[5,40,49]. The security of this is very weak considering that after a user has initially enrolled, he/she can easily give the particulars of their user name and password to someone else who can then easily gain access.

4.1. *Hacking*

An adversary who does not know any particular user's access details can gain access via numerous means available to them[50,51]. This can range from a brute force attack, to packet sniffing, or possibly insider knowledge where the adversary has physical access to the server itself[50,51]. Hackers have devised numerous techniques. This places server computers throughout the Internet highly at risk, especially when an adversary is intent on discovering the super user's access details, which can then provide the personal details of all users who are registered at any specific domain[45]. Many computer viruses are purposely designed to assist adversaries to achieve these objectives[48].

No web server on the Internet is immune to these kinds of attacks[45,51]. However, the objectives of an Anonymous Credential system are aimed at reducing the incidence of user identities being recorded on multiple servers that are distributed across the web[5]. This is achieved using pseudonyms that are cryptographically generated by the system[18]. A user's pseudonym becomes an effective identifier, which is used in place of their actual identity. However, by simply substituting a user's identity with a pseudonym, an individual can still be identified by that pseudonym by cross-referencing the use of that pseudonym across the Internet, which then becomes a viable means by which to identify the user and profile their online behaviours[19,52]. An Anonymous Credential system circumvents this through having the ability to cryptographically generate a multitude of pseudonyms each of which can be verified and used at various domains that the user may visit or become a member of[19,30]. In the case where it is imperative that the web service strictly needs to identify a user as a registered member, a domain pseudonym can be generated, which is then used specifically for that particular service[19].

A problem arises where someone who may have access to some website service based upon his/her credentials, decides to sell or share his/her access with someone who may not qualify. To counter this approach with IBM's anonymous credential scheme each user has his/her own master secret that is contained in every one of his/her credentials that he/she has been issued with by different authorities[53]. Such as a motor registry in the case of a driver's licence, or possibly a credential that is issued by Medicare for use in the e-Health system. Credentials are issued in such a way as to maintain the same master secret in each credential without revealing the secret to any issuer[18,19,53]. The underlying concept is that the master secret becomes the foundation upon which an individual's entire electronic identity or digital persona[1] is formed[5]. This circumvents the ability for any user to share any particular credential with any others without revealing their master secret and thus sharing all of their credentials[18]. This also prevents multiple users from pooling their credentials in any attempt to create a false identity.

Anonymous credentials can be implemented using various means and deployed for use in web browsers on a user's computer or securely deployed on a Smart Card (chip card), thumb drive or mobile device[18]. Credentials can be backed up and later restored in the event that they are lost or misplaced and cannot can be used by anyone other than the rightful owner who alone knows the master secret [18]. Credentials can also be efficiently revoked by the system and they can also have expiry dates or be allocated a specific number of uses[15,18].

4.2. *User understanding*

In efforts to promote consumer trust in Business to Consumer (B2C) e-commerce, much emphasis has been placed upon the development of security measures in the underlying technologies of the Internet (i.e. protocols, encryption, hardware and systems). These efforts, which have primarily been made by technicians and engineers working on the infrastructure, have indeed led to more secure systems over time. However Ulivieri[54] argues that this does not translate well into the minds of consumers who in the vast majority of cases have little comprehension of the technologies involved. The security measures to make the Internet a safer place have not significantly increased consumer trust[55]. The establishment of consumer trust is far more related to sociological principles than it is to technical solutions[54].

Ulivieri[51] states in his report "Naïve Approaches to Trust Building in Web Technologies" that it is more important to consider the 'perceived' security engendered in users as a result of the site's efforts to build trust. He states that:

"*If a user doesn't believe that the environment they are in is secure it will make little difference if it is secure or not* [51]."

This implies that increasing the security of the on-line environment through technical advances, may not influence Internet users as they may have little understanding of how such technologies work and may fail to recognise any benefit. Without a sufficient understanding on the part of the majority of users, the advances in security have had little impact on trust[55]. Ulivieri[54] suggests that what users can relate to is information provided to them about what the technologies do and how they can use them. He suggests that it is only necessary to understand what these security technologies are for in a similar way in which the driver of a car needs only know how to accelerate, turn and stop but does not need to know the full particulars of how a car works in order to drive it[54].

The technologies behind Anonymous Credentials mentioned above are extremely complex for the average user to understand and even highly skilled IT professionals struggle with the workings behind encryption techniques[36]. Encryption itself is purposely designed to confuse interceptors of private messages. The following quote illustrates these points:

> "*… the complexity of ABC technologies and the client-server interactions they entail have so far overwhelmed potential users and consequently hindered their effective large scale deployment. Overcoming these hurdles requires an in-depth comparative study of the functionalities of the different ABC technologies and an analysis of their security and efficiency properties to provide a common understanding of their applicability to diverse application fields and scenarios*[36]."

Considering the complexities of the technologies driving the World Wide Web (WWW) and the lack of understanding in the general population of Internet users, trust plays an important role in the uptake and use of online services and technologies[54]. A group of twenty three researchers from North America and Europe have been studying issues related to online privacy and security in a project titled 'On the Identity Trail'[56]. The project is investigating and reporting upon several aspects related to the use of anonymity in authentication processes conducted over the Internet. The project consists of three streams:

- The nature and value of identity, anonymity and authentication
- Constitutional and legal aspects of anonymity
- Technologies that identify, anonymise and authenticate

Findings of the project indicate that the concept of anonymity itself is complex and often misinterpreted even among tech savvy users of the Internet[56]. Very little is known regarding the perceptions of Internet users towards the use of technologies that are built expressly with privacy by design and especially in Australia, as these Privacy Enhancing Technologies (PETs) are still in development and yet to be standardised[36,37].

This gap in the literature is primarily towards what this research effort seeks to make a contribution to knowledge. The issues related to the privacy of health information and given that in Australia, the Medicare card is used as part of a 100 point identity check as used by Australia Post[57], the Australian PCEHR system is ideally suited for the use of an Anonymous Credential scheme.

On Tuesday March 1, 2011, IBM announced that they had won the contract to deliver the Australian Government's National Authentication Service for Health (NASH) project[58,59,60]. In October 2012, it was announced that the contract with IBM had been terminated due to anticipated delays to complete the work by the 1st July, 2012, launch date of the PCEHR system[61,62,63]. The National E-Health Transition Authority (NEHTA) originally contracted IBM to build a smartcard and public key infrastructure-based user verification system; after realising the complexities involved in building such a system[58]. The $23 million contract with IBM was terminated in favour of keeping to the launch date and an interim solution was deployed. The Interim Authentication Solution was the initial system developed before IBM was contracted and is a modified Department of Human Services (DHS) PKI solution[64].

IBM as a world leader in developing an anonymous credential system were ideally poised to integrate privacy enhancing technologies into the Australian PCEHR system[5,23]. Critics question why the IBM project was dropped and the interim NEHTA system substituted in its place. Especially when IBM had already completed much of the work, and critics also question if the interim system is safe and appropriate to use in view of the fact that at the outset it was not considered to be adequate[65].

5. Methodology

The primary research question to arise from the review of literature was, "*Can Anonymous Credentials enhance user participation in PCEHR?*" The researchers considered that an anonymous online survey would be an appropriate approach to take given the nature of the study. This would ensure that respondents taking part in the survey would also be potential/current users of the PCEHR system. These respondents would also have some degree of online experience that may affect their trust in using online systems.

5.1. *Conceptual model*

In the past doctor – patient confidentiality has defined the trust users have had in usage and storage of their medical records. With the introduction of the online PCEHR system and the associated benefits previously mentioned, many additional technological factors have been added to this basic trust/privacy situation.

A conceptual model containing eight constructs was developed to examine the causal relationships deemed to influence users in signing up to the government's PCEHR system. The model was developed to explore the many factors influencing users in their decision to sign on to the PCEHR system, and in particular discover if the introduction of Anonymous Credentials to the system could enhance user participation. This conceptual model is displayed below (see Fig 1).

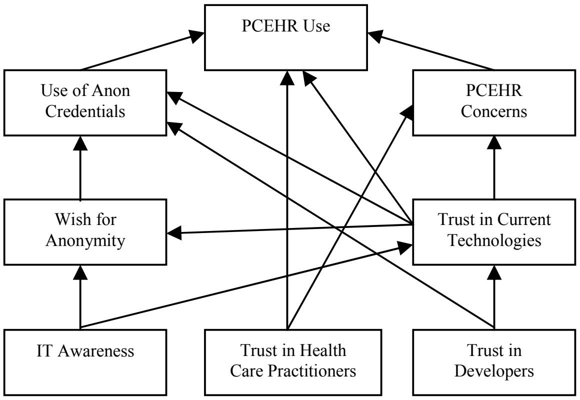

Fig. 1. Conceptual model developed for the research.

The conceptual model and its constructs were drawn from an extensive review of literature covering Technology Acceptance Models[66,67,68,69] and Models of Trust in E-Commerce[70,71,72]. We hypothesise that the Use of PCEHR is influenced by *PCEHR Concerns*, *Trust in Health Care Practitioners*, *Trust in Current Technologies* and the *Use of Anonymous Credentials*. We further hypothesise that PCEHR Concerns are influenced by *Trust in Health Care Practitioners* and *Trust in Current Technologies*. We also hypothesise that the Use of Anonymous Credentials is influenced by *Trust in Current Technologies*, *Trust in Developers* and the *Wish for Anonymity*. Furthermore we hypothesise that the Wish for Anonymity is influenced by *IT Awareness* and *Trust in Current Technologies* and finally that *Trust in Current Technologies* is influenced by *IT Awareness* and *Trust in Developers*. These hypotheses are represented by the arrows connecting the constructs shown in Figure 1.

5.2. *Design and Construction of the Survey*

The following sections outline the design and construction of the survey and discuss the inclusion of a video as a key component of the experiment. It also details some of the questions included in the experimental design and describes how the survey was delivered.

5.3. *Inclusion of a video with the survey*

The review of relevant research established the importance of system security in ensuring the privacy and confidentiality of patient records. It also highlighted the key benefits of PCEHR for medical practitioners as well as patients. More importantly for the research undertaken here, it was also established that there is little understanding of security related to PCEHR. Anonymous Credentials have been established as a key technology to provide robust security as well as simplify and consolidate access across varied systems. Given the general lack of understanding about Anonymous Credentials as a user identification and verification technology, it was decided to expose users to information about its use and implementation prior to undertaking the survey.

Davis, Bagozzi and Warsaw[73] suggested that a key challenge in the development of information systems concerns the difficulty of communicating to users how a system may function. They suggest that paper systems, often utilised in the design phase, may be an inadequate representation of the system being tested and suggest that video mock ups are increasingly being used to convey to potential users what the system will consist of. Albert Bandura, in his paper Social Cognitive Theory[74] suggests that,

> *"The video system has become the dominant vehicle for disseminating symbolic environments both within and across societies[74]."*

Two videos were determined to be suitable for this project, the first was developed for the purposes of this project and the second titled "*IBM Identity Mixer: Scenario 1 - In support of Data Privacy Day 2012*" was publically available on You-tube and produced by IBM Research[30]. Each of the videos was shown to a focus group comprised of ten participants drawn from of Southern Cross University students, staff and researchers. As a result of this process it was determined the video prepared by IBM Research[30] was more suitable as it appeared to convey to participants the necessary concepts and their applications in simple terms. Therefore respondents undertaking the survey in this research were required to watch this video prior to answering the survey questions.

5.4. *Demographic questions*

Demographic measures were included within the survey to allow responses to be categorised by the key measures of gender, education, dependants, age and registration for Australian PCEHR. These questions were asked as basic categorical variables. They present the opportunity to look at responses to attitudinal responses to see if differences emerged based on these variables.

5.5. *Attitudinal questions*

The attitudinal survey questions sought to gain an insight to users perceptions of the eight constructs illustrated in the conceptual model that forms the basis of this study (Figure 1). The conceptual model displays the proposed relationships between the constructs which form the hypotheses that are being investigated in this study. A total of 49 questions were asked seeking users attitudes to the conceptual constructs. The number of items asked about each construct is as follows.

Table 1. Number of questions asked in relation to the eight constructs in the conceptual model.

Attitudinal Questions

Construct	Num. Questions
IT Awareness	7
PCEHR Use	4
PECHR Concerns	6
Trust in Current Technologies	6
Trust in Developers	7
Trust in Health Care Practitioners	5
Wish for Anonymity	8
Use of Anonymous Credentials	6

All attitudinal questions were answered by respondents using seven point Likert scales using the extremes of 'Strongly Disagree' to 'Strongly Agree' as these scales have been found to communicate interval properties to respondents and can be treated as interval data by reseachers[75].

5.6. *Pilot study*

A pilot study was conducted to test the survey questionnaires' functionality and to seek feedback from the pilot study's participants. The invitation to participate in the pilot study was bulk emailed to staff of the SCU Business School and 28 submissions were received. Included in this group were academic experts in survey design and statistics, business and information technology.

The feedback from the pilot study was primarily technical in nature (i.e. tweaks for different browser configurations and settings).

5.7. *Survey delivery*

In the main survey, approximately 15,000 students and 900 staff of Southern Cross University[76] were bulk emailed an invitation to take part in the online survey along with a link to the site hosting the survey. Participants were not required to provide their email address nor identify themselves in any way. Invitations were also bulk emailed to members of the SCU Collaborative Research Network (CRN) and affiliate members of the University of Sydney, University of NSW and the University of Queensland[67] plus members and attendees of the ANZAM Year-End Doctoral Workshop 2012 held at Edith Cowan University, Perth[78].

Each invite when responded to via the link to the survey site included a code identifying which group respondents were from, this plus tracking the IP (Internet Protocol) addresses of the respondents allowed for a check to ensure that each participant was taking part from within Australia or was in an invited group, Any surveys completed from outside Australia and not in an invitational group would have been excluded. In fact only two submissions were received from an off shore IP, however the invitation code identified the respondents as SCU staff. All responses from Australian IP addresses could be considered to be valid as even international students studying in Australia can avail themselves to a PCEHR record. This resulted in the collection of valid submissions.

6. Preliminary Data Analysis

The data analysis for this study is currently still in process. The descriptive analysis and response distributions, describing the characteristics of the studies sample is complete. Additionally, cross tabulations of response distributions examining relationships between demographic variables and key variables related to the constructs in the conceptual model have also been completed. Some of the key findings of the descriptive analysis are reported as following.

6.1. *Demographic description of the sample*

- Of the 240 responses to the survey 44.2% of the respondents indicated they were male and 55.8% indicated that they were female. Porter and Umbach[79] conclude that that this is a typical statistical split between the genders (in samples drawn from higher education) as female students are more likely to respond than males to both paper-based and web-based surveys.
- As expected, due to the sample being drawn from university students and staff the sample is skewed towards higher education with 29.6% having completed or currently studying at an undergraduate level, 22.5% at postgraduate level and 18.8% at PhD/Doctorial level.
- 45% of respondents reported that they had dependants. This was an important question as in most cases dependants are children and a child's PCEHR record is controlled by their parent(s) while they are minors and this may influence a decision to enrol in the PCEHR system.
- Respondents in the sample ranged in age from 18 – 75+. However, the sample contains very few respondents of either gender in the 66+ age range. Table 2 displays the age categories by gender of the sample.

Table 2. Respondents Age by Gender

Age	Male	N=	Female	N=
18-25	7.5%	8	10.4%	14
26-35	17.9%	19	17.2%	23
36-45	25.5%	27	20.1%	27
45-55	21.7%	23	33.6%	45
56-65	24.5%	26	17.2%	23
66+	1.9%	2	1.5%	2
Total	100%	106	100%	134

- Currently the percentage of adult Australians enrolled in the PCEHR system one year into its roll-out is 2.23%[10]. Respondents in this sample reported 12.9% were enrolled. This is approximately 5 times that of the target population, it is considered by the researchers that this difference may be influenced by the skew in education and high levels of Internet skills (several of the questions in the 'IT Awareness' construct).

6.2. *Selected cross tabulations*

Cross tabulations have been performed on all demographic measures between variables in each of the constructs of the conceptual model. Several of these are discussed in the following as they are seen as directly influencing enrolment to PCEHR or demonstrate a moderating effect upon constructs in the conceptual model.

Respondents with dependants already signed up to PCEHR. Of the 105 respondents reported to have dependants 17.6% were enrolled in the PCEHR system, whereas only 9.1% of the 132 without dependants were enrolled in the system. This tends to suggest that respondents with dependants may have a greater incentive to enrol in the PECHR system on behalf of the dependents that in their care.

Respondents already signed up for PCEHR and trust. Many of the variables in the constructs of the conceptual model are based on trust. The results of the first two variables shown in Table 3 was expected as it was thought respondents whom had already availed themselves to PCEHR would tend to have greater trust in the existing security/privacy technologies, in this case the Interim Authentication Solution[64] developed by the government. This is in direct contrast to respondents whom have not registered for PCEHR as they demonstrate a greater level of distrust in the confidentiality and privacy provided by the government's system. It was also hypothesised that trust in health care providers would be similarly affected. The last two variable shown in Table 3 indicate that while there is not as much trust in health care providers amongst respondents not signed up for PCEHR the differences are markedly less pronounced than in the previous example.

Table 3. PCEHR registered and trusting beliefs

Trusting Belief	Disagree	Neutral	Agree
Trust in Government to ensure confidentiality[*]	35.5%	9.7%	54.8%
	47.8%	18.2%	34.0%
Trust in Government to ensure privacy[*]	32.3%	16.1%	51.6%
	48.6%	18.3%	33.2%
Trust in competence of health care providers[**]	9.7%	3.2%	87.1%
	13.4%	20.1%	66.5%
Trust in confidentiality of health care providers[**]	12.9%	12.9%	74.2%
	25.4%	15.8%	58.9%

Clear background is respondents registered for PCEHR
Grey background is respondents not registered for PCE.

[*] Question from the 'Trust in Developers' construct
[**] Question from the 'Trust in Heath Care Practitioners' construct

Respondent self assessed level of health and already signed up to PCEHR. Respondents were asked the question *'I generally enjoy good health and rarely need to see any doctor or other health care practitioner'* as a variable included in the 'PCEHR Concerns' construct of the conceptual model. Response to these questions shows that 67.7% of those that had signed up for PCEHR believed they experienced good health and that 25.8% indicated they had poor health (answered below the scale mid-point). The researchers thought that the opposite would have been evident and that people who thought their health was poorer would be more likely to take advantage of the benefits of PCEHR. However, when considering the response distribution, the researchers thought that:

- People with poorer health may be satisfied with the level of healthcare and record keeping they currently experience.
- They are less mobile and therefore less likely to see the advantage of PCEHR.
- Have established their health support network and don't see any advantage to their records being online and available to health practitioners outside their existing network.
- May experience some discomfort at the thought of their 'condition' being available to people or organisations outside their immediate health support network.

In relation to the group who felt they enjoyed good health, the researchers thought that…

- People who are generally healthier are more health conscious and more likely to take advantage of initiatives that could help them better service or support their health,
- They would be less self-conscious about their health and less likely to be concerned about their health records being available via PCEHR.

6.3. *Selected key variables in constructs*

Several of the variables in the conceptual model's constructs stand out and are included here as they directly support the literature and/or have direct bearing upon the primary research question in this study. All questions used a 7 point Lickert scale '<u>Strongly Agree</u>' to '<u>Strongly Disagree</u>'. The results following are shown as Agree, (above the mid-point of scale) Disagree (below mid-point) and neutral (the mid-point).

- *'I am concerned about the websites I browse being tracked.'* 80.7% agree, 9.2% neutral and 10.1% disagree [ǂ]
- '*I am concerned about using Electronic Health Records as it may expose my health information to those who are not authorised to view it.*' 68.3% agree, 13.8% neutral and 17.9% disagree [φ]
- '*I believe that user name and password authentication is a secure method to authorise access to websites.*' 30.8% agree, 17.9% neutral and 51.3% disagree [±]
- '*I believe that many organisations collect more information about my personal details than they actually need to know.*' 92.9% agree, 4.2% neutral and 2.9% disagree [ɩ]
- '*I like the idea of using a pseudonym to identify myself rather than giving full details of my identity.*' 72% agree, 19.2% neutral and 8.8% disagree [ɩ]
- '*I would like to learn more about Anonymous Credentials.*' 85% agree, 11.7% neutral and 3.3% disagree [ɩ]
- '*I would be more likely to use Anonymous Credentials for online authentication if it were more "secure" than password authentication.*' 88.7% agree, 9.1% neutral and 2.2% disagree [≠]

The respondents in this sample display high levels of concern about being tracked on websites (80.7%) and that PCEHR in its current format may expose their health information (68.3%). In fact, 92.9% of the respondents in this sample believe that organisations collect more personal information about them than is required. These results indicate that potential users of the PCEHR system have concerns about existing security/privacy on the Internet

Over half of the sample (53.1%) is of the opinion that password authentication is not a good authorisation method and would be more likely to use Anonymous Credentials if it was more secure (88.7%). The samples respondents also show high levels of interest in anonymity with 72% agreeing they would like to use a

[ǂ] Question from the 'IT Awareness' construct

[φ] Question from the 'PCEHR Concerns' construct

[±] Question from the 'Trust in Current Technology' construct

[ɩ] Question from the 'Wish for Anonymity' construct

[≠] Question from the 'Use of Anon Credentials' construct pseudonym and 85% expressing an interest in learning more about Anonymous Credentials.

These results at this early stage of the data analysis would seem to support the conceptual model developed for this study.

6.4. *PCEHR use*

The 'PCEHR Use' is the penultimate dependent construct of the conceptual model. Shown following are the results of the four variables that are contained in this construct.

- '*I have no reservations about using Electronic Health Records.*' 32.8% agree, 34% neutral and 33.2% disagree
- '*I consider a government controlled identification system to be the safest option for accessing Electronic Health Records.*' 22.2% agree, 31.8% neutral and 54.6% disagree
- '*I would like to learn more about Personally Controlled Electronic Health Records.*' 85% agree, 11.7% neutral and 3.3% disagree
- '*I would be more likely to use Electronic Health Records if my identity could remain anonymous at all times.*' 65.4% agree, 24.6% neutral and 10% disagree

Respondents seem to be evenly split (agree, neutral and disagree) in their reservations in using PCEHR, and 54.6% indicating that they have concerns about the governments identification scheme. Of particular interest to the researchers is the result of the question about respondents desire for anonymity as a result of 65.4% agreeing tends to indicate that anonymous credentials may indeed enhance user participation in the PCEHR system. Whether this is the case is not yet supported, as additional statistical analysis is yet to be undertaken. With only a small subset of the Australian public (2.23%)[10] currently registered for PCEHR it is encouraging that 85% of respondents indicated an interest in learning more about the PCEHR system.

7. Conclusion

The key objective of this study is "*Can Anonymous Credentials enhance user participation in PCEHR?*" At this early stage in the data analysis indications are that the introduction of anonymous credentials could enhance user participation in the study with 65% of the sample indicating that they would be more likely to use the PCEHR system if their identity could remain anonymous, 85% of the sample expressing an interest in learning more about anonymous credentials and 54.6% identifying their lack of confidence in the current government controlled identification system. The data collected in this study is also showing support for the conceptual model developed to investigate the factors influencing users, although much further analysis need to be completed to verify is this is indeed the case.

Introduction of an anonymous credential system as part of the PCEHR system will practical implications beyond this system alone as there is currently no equivalent form of digital credential that can be used in a similar manner that preserves the privacy of information about the individual. This will have effects on how users access websites, identify themselves to e-commerce sites and web based identification as a whole.

7.1. *Limitations of the study*

The sampling procedure used in this study is classified as convenience sampling. A disadvantage of convenience sampling is that the sample may suffer from bias, leading to under representation or over representation of particular groups within the sample. Because the sample was drawn from university staff and students, some bias may exist in the results of the study and particularly the education measure. Statistical inference cannot be reliably applied to convenience sampling yet it can be useful in exploratory research.

7.2. *Future directions - ongoing data analysis*

The next steps to be undertaken in analysis of the relationships between the constructs of the conceptual model will commence with establishment of the validity of the constructs. This will be followed by a factor analysis to see whether there are higher order factors overlaying the observed variables. Finally the relationships among the constructs will be examined using structural equation modelling (SEM).

References

1. R. Clarke, A Sufficiently Rich Model of (Id)Entity, Authentication and Authorisation, in *The 2nd Multidisciplinary Workshop on Identity in the Information Society*, (LSE, London, UK, 2009-10).
2. R. Clarke, Re: Ehealth – Consumer Consultation and Project Governance, *Australian Privacy Foundation* (Apr.17, 2011), Online available at http://www.privacy.org.au/Papers/Roxon-PCEHR-Ltr-110417.pdf (accessed Sept. 25 2012).

3. Accenture, *Making the Case for Connected Health,* (Jan. 30, 2012) Online available at http://www.accenture.com/us-en/Pages/insight-making-case-connected-health.aspx (accessed Apr. 12, 2013).
4. P. Gray, Protecting Privacy and Security of Personal Information, in the Global Electronic Marketplace, *Internet Consumers Organization* (1999) Online available at http://www.ftc.gov/bcp/icpw/comments/ico2.htm (accessed May 24th 2013).
5. M. Crompton and R. McKenzie, Current Issues and Solutions in Identity Management, *Information Integrity Solutions,* (Oct. 2010) Online available at http://www.iispartners.com/downloads/2010-10%20Current%20Issues%20in%20Identity%20Management%20NICTA%20Jerusalem%2014%20Oct.pdf (accessed Jan.24, 2013).
6. Accenture. 2010. *Information Governance: The Foundation for Effective E-Health*, (Aug. 25, 2010) Online available at http://www.accenture.com/us-en/pages/insight-information-governance-effective-ehealth-summary.aspx (accessed Apr. 13, 2012).
7. A. Boonstra and M. Broekhuis, Barriers to the Acceptance of Electronic Medical Records by Physicians from Systematic Review to Taxonomy and Interventions, *BMC Health Services Research* **10(**231) 2010.
8. D. Glance, *Is the Government's Missed Health Record Target Meaningful?*" (Jul. 3, 2013) Online available at http://theconversation.com/is-the-governments-missed-health-record-target-meaningful-15558 (accessed Sept. 12, 2013).
9. The Conversation, David Glance, *The Conversation Media Group* (Perth, W.A. Australia, 2010-2013) Online available at http://theconversation.com/profiles/david-glance-148/profile_bio (accessed Sept.12, 2013).
10. B. Avery, Opinion: Why National E-Health Is Not for Everyone, in *CIO Magazine, (May 13, 2013)* Online available at http://www.cio.com.au/article/461628 /opinion_why_national_e-health_everyone/ (accessed Sept. 12, 2013).
11. Attorney-General's-Dept. "Healthcare Identifiers Act 2010," Attorney-General ed. (Office of Legislative Drafting and Publishing, Canberra, Australia, 2010) Online available at http://www.comlaw.gov.au/Series/ C2010A00072 (accessed Sept.25, 2012).
12. Australian Bureau of Statistics, *Population by Age and Sex, Australian States and Territories*, (Jun. 2010, Canberra, Australia) Online available at http://www.abs.gov.au/ausstats/abs@.nsf/mf/3201.0 (accessed May 12, 2012).
13. M. Blaze, *Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks* (AT&T Labs - Research Mar 3, 2003) Online available at http://www.crypto.com/papers/mk.pdf (accessed May 12, 2012)
14. S.A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates*. (Massachusetts Institute of Technology Press, USA 2011).
15. J. Camenischand and A. Lysyanskaya, An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation, *International Conference on the Theory and Application of Cryptographic Techniques*, (Springer, Innsbruck, Austria, 2001).
16. D. Chaum, Security without Identification Card Computers to make Big Brother Obsolete, : *Communications of the ACM* **28** (10) (1985) 1030-1044.
17. EMC Corporation, *Cryptographic Challenges - The RSA Factoring Challenge,* (2011) Online available at http://www.rsa.com/rsalabs/node.asp?id=2091 (accessed Jul. 7, 2011).
18. T. Groß, Identity Mixer in Resources for Smart Identity Card, *IBM Research*, (2009) Online available at http://idemix.files.wordpress.com/2009/08/prime2006-primer-ecitizens.pdf 2009a. (accessed Sept. 25, 2012)"
19. IBM Research, *Specification of the Identity Mixer Cryptographic Library*, (April 29, 2010) Online available at http://domino.research.ibm.com/library/cyberdig.nsf/ papers/EEB54FF3B91C1D648525759B004FBBB1/$File/rz3730_revised.pdf (accessed Sept. 27, 2012).
20. G. Kessler, *An Overview of Cryptography*, (updated continuously) Online available at "http://www.garykessler.net/library/crypto.html#skc (accessed Jul 27, 2011).
21. R.L. Rivest, A.Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM* **21**(2) (1978) 120-126.
22. S. Wilson, PKI Online, *The Lockstep Group* (2013) Online available at http://lockstep.com.au/about/pki (accessed Apr.13 2013).
23. Information Integrity Solutions (IIS), *National Trusted Identities Framework*, (Jan. 11, 2012) Online available at http://www.privacy.org.au/Papers/PMC-NTIF-Rpt-130111.pdf (accessed May 12, 2012).
24. International Association of Privacy Professionals, *The Global Changing Privacy Landscape*, (Apr. 29, 2012) IIS (ed.). Online available at http://www.iispartners.com/ downloads/2012_PAW%20_IIS_%20iappANZ_background_paper.pdf (accessed May 12, 2012).
25. Australian Broadcasting Commission, *Is Google Watching You?*, M. O'Neill (ed.). (Video, Feb. 29, 2012) Online available at http://www.abc.net.au/news/2012-02-29/is-google-watching-you/3861158 (accessed Apr. 27, 2012).
26. A. MacGibbon, Inquiry into Cyber Crime, *Internet Safety Institute,* (Jul. 7, 2009) Online available at http://www.internetsafetyinstitute.com.au (accessed May 25, 2012)
27. G. Day, Dealing with Big Data in Cyber Intelligence, *RSA Conference* (Oct. 11, 2012, London, UK) Online available at http://www.rsaconference.com/events/eu12/ agenda/sessions/525/dealing-with-big-data-in-cyber-intelligence (accessed Jan. 12, 2013)
28. W. Diffie, and M.E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory* **22**(6) (1976).

29. EMC Corporation, *RSA Algorithm*, .(2011) Online available at http://www.rsa.com/ rsalabs/node.asp?id=2146 (assessed Jul. 25, 2011).
30. IBM Research, Identity Governance, *IBM Research - Zurich* (Zurich, Switzerland, 2011), Online available at http://www.zurich.ibm.com/security/idemix/ (accessed Jan 12, 2012).
31. PrimeLife, Primelife - Bringing Sustainable Privacy and Identity Management to Future Networks and Services, *Privacy and Identity Management for Europe*." (Kiel, Germany 2008 – 2011) Online available at http://www.primelife.eu/ (accessed Jan 12, 2012).
32. , R. Clarke, Message Transmission Security/Cryptography in Plain Text, *Privacy Law and Policy Reporter,* **3**(2) (1996) 24-27.
33. Telecommunication Standardisation Sector of ITU-T, Itu-T Recommendation X.509, *ITU-T*. (Geneva, Switzerland, 2009) Online available at http://www.itu.int/rec/T-REC-X.509-200811-I/en (accessed Jan 12, 2012).
34. R. Clarke, The Fundamental Inadequacies of Conventional Public Key Infrastructure, *The 9th European Conference on Information Systems*, (University of Maribor, Bled, Slovenia, June 27, 2001).
35. T. Groß, Innovation Award for Anonymous Credential System on Java Card, *IBM Research - Zurich*, (Oct. 1, 2009) Online available at http://idemix.wordpress.com /2009/10/01/gi-innovation-award/ (accessed Jan 12, 2012).
36. ABC4Trust, Abc4trust Project Description, *ABC4Trust Project* (May 2009) Online available at https://abc4trust.eu /download/ABC4Trust-Project-Description.pdf (access Jan 12, 2012).
37. ABC4Trust, Attribute-Based Credentials for Trust, *ABC4Trust*, (2010-2012) Online available at https://abc4trust.eu/ (accessed Jan 12, 2012).
38. Future of Identity in the Information Society, "Structured Overview on Prototypes and Concepts of Identity Management Systems," *FIDIS Information Society Technologies EU* (Sept. 15, 2005) Online available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf (accessed Jan 7, 2013).
39. W.E. Burr, D.F. Dodson, and W.T. Polk, Electronic Authentication Guideline, Recommendations of the National Institute of Standards and Technology, *National Institute of Standards and Technology Computer Security Division*, (Gaithersburg, MD, USA, 2004) Online available at http://www.nist.gov/customcf/ get_pdf.cfm?pub_id=151295 (accessed Feb 11, 2012)
40. J. Camenisch, et al., D2.1 Architecture for Attribute-Based Credential Technologies - Version 1, *ABC4Trust EU Project* (Dec. 22, 2011) Online available at https://abc4trust.eu/index.php/pub/results/107-d21architecturev1 (accessed Feb 12, 2012)
41. S. Wreyford, Cabinet Office Joins the Open Identity Exchange." Government Digital Service (June 14, 2012) Online available at http://digital.cabinetoffice. gov.uk/2012/06/14/cabinet-office-joins-open-identity-exchange/#more-4285 (accessed Jan. 7, 2013)
42. W. Mostowski and P. Vullers, Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards, Springer-Verlag, (Radboud University Nijmegen, The Netherlands 2011), Online available at http://wwwhome.ewi.utwente.nl/~mostowskiwi/papers/securecomm2011.pdf (accessed Nov 4, 2013).
43. ABC4Trust, Attribute-based Credentials for Trust, ABC4Trust, (2011), Online available at https://abc4trust.eu/download/flyer/ABC4Trust-OnePager-About-ABC4Trust.pdf (accessed Aug 6, 2013).
44. Stack Exchange Inc., Certificate based authentication vs Username and Password authentication, Stack Exchange Inc, 2013), Online available at http://security.stackexchange.com/ (accessed Aug 8, 2013).
45. W. Caelli, Protecting Australia's Digital Economy, *Australian Computer Society,* (Speech given Griffith University Gold Coast, Australia, Jul 17, 2012).
46. K.Rudd and S. Smith, Cooperation on Cyber – a New Dimension of the Us Alliance, *The Australian Ministry for Foreign Affairs* Online available at http://foreignminister.gov.au/releases/2011/kr_mr_110916.html (accessed Dec 12, 2011).
47. N. Roxon and J. Clare, Australia and United States Working Together on Homeland Security, *Attorney-General's Department* (May 4, 2012) Online available at http://www.ministerhomeaffairs.gov.au/Mediareleases/Pages/2012/Second%20Quarter/4-May-2012---Australia-and-United-States-working-together-on-homeland-security.aspx (accessed Jul. 7, 2012).
48. US Dept. of Homeland Security, Enhancing Cybersecurity Collaboration with Australia, *US Dept. of Homeland Security,* (May 16, 2012) Online available at : http://www.dhs.gov/blog/2012/05/16/enhancing-cybersecurity-collaboration-australia (accessed Jul. 7, 2012).
49. R. Clarke, Introducing Pits and Pets: Technologies Affecting Privacy, *Privacy Law and Policy Reporter* **7**(9) 181-183.
50. C.P. Pfleeger and S.L. Pfleeger, *Security in Computing,* 4th edn. (Prentice Hall, Upper Saddle River, NJ, USA 2006).
51. R.E. Smith, *Elementary Information Security*, (Jones & Bartlett Learning, Burlington, MA, USA, 2013).
52. IBM Corporation, Solve Your Toughest Challenges with Data Mining, *IBM Corporation, Software Group* (Somers, NY, USA, Oct. 2012) Online available at http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=BR&infotype=PM&appname=SWGE_YT_YV_USEN&htmlfid=YTB03032USEN&attachment=YTB03032USEN.PDF (accessed Jan 7, 2013).
53. J. Camenisch et al., D2.1 Architecture for Attribute-Based Credential Technologies – Version 1, *ABC4Trust* (Dec. 1, 2011) Online available at https://abc4trust.eu/ download/ABC4Trust-D2.1-Architecture-V1.pdf (accessed Jan 12, 2012).
54. F. Ulivieri, Naive Approaches to Trust Building in Web Technologies, *Institute for Cognitive Sciences and Technologies* (National Research Council, Rome, Italy, Jul. 2004).

55. OECD, Measuring Security and Trust in the Online Environment: A View Using Official Data, *OECD Digital Economy Papers*, M. Schaaper ed. (OECD publishing, Jan. 29, 2008) Online available at http://www.oecd-ilibrary.org/science-and-technology/measuring-security-and-trust-in-the-online-environment_230551666100 (accessed Jan. 7, 2012).
56. On the Identity Trail, Technologies That Identify, Anonymize and Authenticate, (continuously updated) Online available at http://www.idtrail.org/content /view/12/34/ . (accessed Apr. 17, 2013).
57. Australia Post, Australia Post Digital Mailbox How to Apply, *Commonwealth of Australia*, (continuously updated) Online available at https://digitalpost.com.au/ html/?gclid=CL2A3M3Sh7sCFShepgodCn4ATQ (accessed Nov 7, 2013).
58. K. Dearne, IBM Wins Government E-Health Security Contract, *The Australian* (Mar. 1, 2011) Online available at http://www.theaustralian.com.au/australian-it/ibm-wins-government-e-health-security-contract/story-e6frgakx-1226013765428 2011 (accessed Jan 23, 2012).
59. M. Freri, Rivals Nash Teeth as IBM Wins E-Health Deal, *Delimiter* (Mar. 11, 2011) Online available at http://delimiter.com.au/2011/03/01/rivals-nash-teeth-as-ibm-wins-e-health-deal/ (accessed Jan. 23, 2012).
60. Medicare, Human Services Ehealth Record and Nash PKI Certificates, *Australian Gov. Dept. of Human Services* (continuously updated) Online available at http://www.medicareaustralia.gov.au/provider/vendors/pki/dhs-ehealth-record-and-nash-pki-certificates.jsp (accessed Sept. 17, 2013).
61. A. Brino, IBM Loses $23 Million Contract for Australian EHR System, *Government Heath IT* (Oct. 24, 2012) Online available at http://www.govhealthit.com/ news/ibm-loses-23-million-contract-australian-ehr-system (accessed Dec. 22, 2012).
62. K. Dearne, E-Health Record Service Delayed by Incomplete Infrastructure, *The Australian* (June 19, 2012) Online available at http://www.theaustralian.com.au/ australian-it/government/e-health-record-service-delayed-by-incomplete-infrastructure/story-fn4htb9o-1226399179988 (accessed Jan 7, 2013).
63. J. Gliddon, IBM Loses Key E-Health Contract, *ITNews* (Oct. 23, 2012) Online available at http://www.itnews. com.au/News/320322,ibm-loses-key-e-health-contract.aspx (accessed Jan. 7, 2013).
64. Dept. Health and Ageing, Frequently Asked Questions: Healthcare Professionals, *Commonwealth of Australia* (Nov. 2012) Online available at http://www.nehta.gov.au /component/docman/doc_download/1576-healthcare-provider-faqs-v1-0-17012013?Itemid= (accessed Jan. 7, 2012).
65. D. More, Australian Health Information Technology," in: I Think This Makes It Clear NASH Won't Happen Anytime Soon. The Have A Long Term Interim In Place!. *Australian Heath Information Technology* (Sept. 6, 2012) Online available at http://aushealthit.blogspot.com.au /2012/09/i-think-this-makes-it-clear-nash-wont.html)accessed Jan. 7, 2013).
66. F.D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, **13**(3) (1989) 319-340.
67. M. Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, (Addison-Wesley, Reading, USA, 1975).
68. V. Venkatesh and F.D. Davis, A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, *Management Science*, **46**(2) (2000) 186–204.
69. V. Venkatesh, M.G. Morris, G.B. Davis, and F.D. Davis, Unified Theory of Acceptance and Use of Technology., *MIS Quarterly*, **27**(3) (2003) 425-478.
70. D.H. McKnight, V. Choudhury, and C. Kacmar, Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, *Information Systems Research*, **13**(3) (2002) 334–359.
71. A. Ganzaroli, Y.H. Tan and W. Thoen, The Social and Institutional Context of Trust in Electronic Commerce, (1999), Online available at http://libra.msra.cn/Publication /5681213/the-social-and-institutional-context-of-trust-in-electronic-commerce (accessed 23/06/2012).
72. F.N. Egger, From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce, PhD Thesis (Eindhoven University of Technology, Netherlands, 2003), Online available at http://www.ecommuse.com/egger2003trust.pdf (accessed Jan. 24 2012)
73. F.D. Davis, R.P. Bagozzi and P.R. Warshaw User Acceptance of Computer Technology: A comparison of Two Theoretical Models, *Management Science* **35**(8) (1989)
74. A. Bandura, Social Cognitive Theory, (Stanford University, USA 1989) Online available at http://www.uky.edu/~eushe2/Bandura/Bandura1989ACD.pdf (accessed Jul. 7, 2012).
75. I.E. Allen and C.A. Seaman, Statistics Roundtable: Likert Scales and Data Analyses, *Quality Progress* **40**(7) (2007) 64-65.
76. Southern Cross University, Annual Report 2012 (Gold Coast, Australia, 2012) Online available at http://www.scu.edu.au/docs/annual_report/download.php?doc_id=4833&site_id=223&file_ext=.pdf (accessed May 12, 2013).
77. R. Keast, Policy and Planning Research for Sustainable Regions, (Southern Cross University Collaborative Research Network, Gold Coast, Australia, 2012) Online available at http://www.scu.edu.au/research/download.php /?doc_id=12207&site_id=319 (accessed May 12, 2013).
78. ANZAM, ANZAM Year-End Doctoral Workshop, (ANZAM, Perth, Western Australia, 2012) Online available at http://www.anzam.org/anzam-year-end-doctoral-workshop-perth-western-australia-3-4-december-2012/ (accessed Mar. 3, 2013).
79. S.R Porter and P.D. Umbach, Student Survey Response Rates Across Institutions: Why Do They Vary?, *Research in Higher Education* 47(2) (2006).