Preliminary Investigation to Explore Perceptions of Security Issues Associated with Wireless Technology in Healthcare in Australia

Chee TI, Hafeez-Baig A, Gururajan R and Soar J

Collaboration for Ageing and Aged-care Informatics Research

Faculty of Business

University of Southern Queensland, Toowoomba, Australia 4350

Gururajan@usq.edu.au

Tiong, I. C. and Hafeez-Baig, Abdul and Gururajan, Raj and Soar, Jeffrey (2006) 'Preliminary investigation to explore perceptions of security issues associated with wireless technology in healthcare in Australia.' In: Westbrook, J. and Callen, J., (ed.). *HIC 2006 Bridging the Digital Divide: Clinician, consumer and computer*, Health Informatics Society of Australia Ltd. (HIC 2006, 20-22 August 2006, Sydney, Australia.)

Abstract

The adoption of wireless technology is expected to be especially beneficial to the healthcare industry because of the potential it offers to improve the adoption of health systems, provide more timely access to information and capture of data in care settings [28], [57], [81], [91]. Wireless user devices are expected to facilitate access to information and entry of data at the point of care. This may better fit practice settings where clinicians are moving between patients such as in wards rather than, for example, clinics where desk-based devices may be appropriate. Wireless technology will provide a component of infrastructure necessary for better sharing of health information for quality care planning and delivery. A major issue for the adoption of wireless technology in healthcare is the ability of wireless technology to secure sensitive health data during the exchange of information [41], [28], [60], [73], [83], [98].

This paper reports on the first stage of a research programme involving gathering user perceptions using qualitative approach. Further stages will involve quantitative approaches based upon issues identified in the first stage.

Introduction

Information and communication technologies (ICT) have been a key driving force in reshaping and improving our quality of life [91]. ICTs are perceived to have the potential of breaking down communication barriers across nations and geographical locations, and bringing about economic growth and prosperity [23], [91]. The concept of information and communication technology could be explained as electronic devices that are used in the organisation and management of data and information [23]. The term communication is included in the concept because information by itself is of little use to people. It is when the information is shared and utilised among people, it would be of importance to people. Communication technologies refer to devices that are used in the exchange of information between two or more sources [23], [62], [97].

Communication technologies can be divided into wired and wireless technologies. Wired technologies consist of cables, twisted pairs and fibre optics. While wireless technologies would consist of microwave, radio waves, infrared and laser [9], [23], [58]. In particular, radio wave technology has received a great amount of attention and growth over the recent years in local area network deployment [29], [52], [80]. Otherwise known as wireless local area network (WLAN), the technology promotes mobility and reduced deployment cost compared to its wired counterpart [8], [9], [44], [47], [77], [95].

The expectation is that wireless technology will enable sharing of health information more effectively and efficiently among health care professionals and consequently will enable more timely and effective treatment of patients. However, there are still concerns and issues in the ability of WLAN to secure sensitive health information during the exchange of information [41], [28], [60], [73], [83], [98]. In a recent series of workshops with health professionals in Queensland and Western Australia conducted by one of the team member of this project, it was discovered that a major barrier to the uptake of this technology appears to be user concerns over various security issues including physical, logical and data security [47], [70]; [83], [69]; [47]. This is particularly evident from recent interviews conducted by team members the supervisor of this project with Queensland Nursing Council staff which clearly demonstrated their concerns for loss of equipment in a wireless domain, security of data due to unexpected breakage in wireless communication, and privacy legislation when data are transmitted between various stakeholders [89] [47], [98], [68], [47].

There are also new concerns in wireless security breaches that may prove to have serious impacts such as wireless hacking and mobile phone viruses [17] [82]. Therefore, users will need to consider wireless security features when they opt for a wireless healthcare environment. While the current research addresses technical components associated with this complex environment, it appears that user issues specific to healthcare in the Australian healthcare have been neglected [47]. Even some informal models used in public healthcare in terms of security appeared to have attached little importance to user perceptions and concerns [41], [73], [98].

User perception is a good indicator of how a system will be accepted. Therefore, it is important to investigate user perception in regards to the usage of wireless security in Australian health care [38], [36], [10], [35], [83]. Recent solutions that are emerging in public health appear to have ignored this issue because of the emphasis on technical security concerns rather than user perceptions. This has given impetus to this study

Literature Review

The uptake of some new technologies has been rapid in healthcare; laboratories make use of robotics, results are transmitted electronically and diagnostic images are increasingly digital. The sector is still very cautious on the use of wireless technology in healthcare facilities [15], [21], [57]. There are concerns about the maturity of the technology and the fit with organizational culture and work practices. While the technology has been in existence for some decades, recent developments have made it more accessible and affordable. Wireless technologies have captured global attention in a variety of industries [52], [80]. Wireless technology is also being tested in some hospitals. The risks of wireless security in health care will also increase with more people using it [47], [83], [69]. Wireless technology promises efficiency gains for the healthcare sector in Australia because of the mobility offered [88], [96]; [94], [19]. There are indications of efficiency gains including data capture and validation at point of entry. Despite this, its adoption rate is slow in health care industry [24]; [30], [54] [60].

Security and privacy issues appear to inhibit the adoption of wireless in healthcare. Security and privacy are issues that need to be addressed in healthcare information systems strategies and there is a common perception that wireless technology is not secure. Confidentiality refers to privacy of health information, specifically patient health record. Patient health record will normally contain a history of treatment and medication of a patient. This is necessary for clinicians to plan, deliver and evaluate care. Sensitive areas such as HIV/AIDS status, sexually transmitted diseases, substance abuse, mental health and other personal information will also be part of a person's health history [13], [21], [23], [51], [91]. The perceived shortcomings of wireless will need to be addressed before clinicians and patients are comfortable with sensitive data being transmitted through this technology {[6], [8], [16], [21], [57], [62], [76].

Besides protecting confidentiality of health information, there is also the issue of protecting the data from alteration especially during the process of data exchange. Wireless data transmission is prone to interception [5], [8], [9], [16], [76]. It does not have the shielded protection of wired technology. Any information modified or altered may cause inaccurate information supplied for treatment planning and delivery. Besides preventing alteration to information, it is also important to detect alteration of health information [6], [43], [62], [97].

Therefore, it is crucial to ensure the flows of data in a healthcare environment are not at risk. The solutions to these issues can be achieved through proper security infrastructure and advancement in technical specification of wireless technology standards. There are already new standards underway to address the limitations such as 802.11i, 802.1x and Advanced Encryption Standard [5], [19], [32], [44], [62], [76], [97].

Fisher [41] conducted a technical review on the security of wireless standard from past surveys and literature. He proposed a five layer of security framework consisting of hardware protection, wireless security policy, monitoring and intrusion detection, business and technology integration, virtual private networking, and transport layer security [43], [22]. Misra [69] conducted a case study on security challenges in a mobile healthcare setting. The study suggested a wired equivalent security standard that makes mobile devices as secure as wired transactions. The basis of the common framework would be a security model that assures authenticity, confidentiality, integrity, availability and non-reputability for any transaction whether wired or wireless [70]. Their research also suggested additional problems between the provider and mobile device, the mobile device and the mobile infrastructure operator, the mobile infrastructure operator and the wireless application gateway of the merchant, and the wireless application gateway and the web services of the merchant. Their analysis was more user and content centric [69].

Zeeshan [98] conducted a case study of wireless security in an Australian healthcare. His study investigated a bare minimum wireless security framework specifying the essential and desired components of wireless security in health care industry. Patient confidentiality is protected by numerous legislations in Australia. It suggested numerous technical limitation and threats of current wireless standards. It is obvious that no ‘out of box’ wireless security solution provides the level of security desirable in health care area.

The literature review indicates that much of the research is of very technical nature [66], [10], [38], [35], [69]. There are few studies of the management and the user aspects of wireless technology in healthcare. The research in progress outlined in this current paper is investigating the user concerns and perception of security in both public and private hospitals [4], [7], [11].

Research Question

This study explores user perception of the wireless technology in question. Any measurement taken is based on the user perceptions rather than measurement of the technology. It is possible to investigate user perceptions as there are common elements in the use of health information among many stakeholders such as clinicians.

The main research question for this study is:

“What are the users perceptions regarding the use of wireless technology in regional Queensland healthcare facilities with respect to security and privacy requirements?”

This research investigates user concerns for wireless technology and security requirements in healthcare in order to obtain a view for security management in Australian healthcare.

The Importance of User Perceptions

It is important to know the socio-technical aspects of information technology usage besides the technical aspects. Coakes [27] describes socio-technical aspects as the study of relationships

between the social and technical part of any systems in helping organisations to explore and adjust to conflicts and complexity in the human, organisational and technical aspects of change. In particular, these principles emphasise an ethical principle relating to the individuals participation in decision making and control over their immediate working environment.

The implementation of wireless technologies in healthcare organisations causes changes and would result in a wide variety of impacts upon the design of business, economic performance and the working conditions of staff. It can cause either positive or negative impacts [34]. Therefore, it is important to investigate how information collection, storage and dissemination strategies could affect people's attitudes, beliefs and behaviours [84]. The measurement of user perceptions on features and concept of wireless application security would be a good indicator of what constitutes a secure wireless environment in health care.

Fisher [41] described several elements that contributed to a successful system from a user's perspective. They include understanding user requirements and perspective, user and developer communication, effective user involvement, accessibility of quality user information, ease of use, and appropriateness of the design of user interface. Therefore, it is possible to measure user perceptions on WLAN security by associating certain attributes or factors to the technology, and measure the user needs. This study uses Unified Theory of Acceptance and Use of Technology (UTAUT) model derived from the Information Systems literature to measure user perceptions specific to wireless security issues. Thus far, the model could predict up to 70 percent of user variance in usage intentions because it combines the strength of eight previous user acceptance models: Social Cognitive Theory (SCT), Theory of Reasoned Actions (TRA), Technology Acceptance Model (TAM), Motivational Model, Innovation Diffusion Theory (IDT), Model of PC Utilisation, Theory of Planned Behaviour (TPB), and combined TAM-TPB [38], [10], [78], [35].

Research Theory and Methodology

This research will base on the Unified Theory of Acceptance and Use of Technology (UTAUT) model. This model is a predictive model on user acceptance of technologies. It measures user intentions and predicts uses of technology with four constructs and four moderators [10], [35], [38], [49], [66], [78]. The four constructs of the UTAUT model are performance expectancy, effort expectancy, social influence and facilitating conditions. The four moderators are age, gender, experience and voluntary use [38], [10], [78]. These four constructs will be the four main categories of attributes in measuring user perceptions on wireless technology security. The model is shown in figure 1.

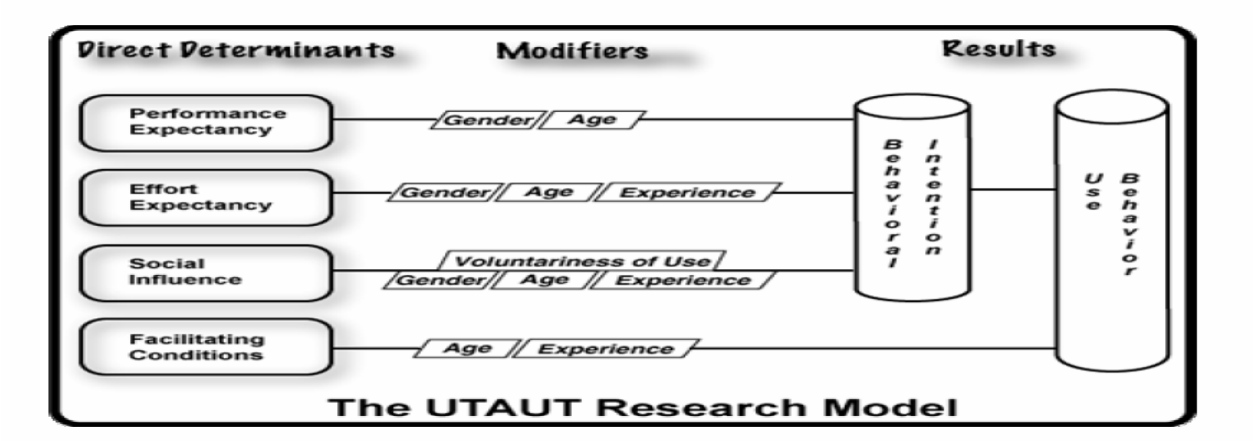

Figure 1: UTAUT Model adopted from Emanavin [38]

Based on the preliminary literature review, this study will employ a mixed research methodology. A mixed research methodology is the use of more than one research method in testing one's

hypotheses [26], [33], [50], [65], [85]. The mixed research methodology has recently gained popular attention among social science research. Morse [71] stated that the aim of social science research is to understand the complexity of human behaviour and experience, which is a part of the objectives in this study. The use of mixed research method in a single study may allow researchers to obtain broader view of human behaviour and experience through different sets of data collection [33]; [71].

Therefore, in this research mixed research method will consist of both qualitative and quantitative methods. The mixed method would be implemented in the sequential exploratory style as described by Clark [25]. It consists of the execution of a qualitative method, and follow by a quantitative method. The reason for inclusion of both qualitative and quantitative methods is because qualitative research can help to explore initial themes needed for the research as the domain of the research is relatively new [26]; [99]. The mixed methods will be conducted in two phases: exploratory and confirmatory. The first phase would utilise a focus group session to gather and explore the user opinions of wireless technology security in health care. The initial themes would be derived from literature reviews. The confirmatory phase would be used to confirm the findings of the exploratory phase. Figure 2 provides an overview of the mixed research methods used in this study.

Data Analysis

After the final transcript is produced, data analysis was conducted using qualitative data analysis software – NVIVO. NVIVO provides an easy documentation of qualitative data for storage and retrieval during analysis. Current study applies a logical analysis approach by revealing the interrelation of keywords in the feedback provided by the focus group participants, and reveal the logical shape of the focus group participants' idea [18].The approach begins by searching for keywords within the focus group transcript that leads to either positive or negative argument. The keywords could be an interesting word, reoccurring comments, intense word, extended comments or consistent words. These keywords are later grouped under a category to be confirmed through the next stage of the mixed research methodology. The group keywords are later used for the development and administration of the questionnaire survey [18], [18], [67].

The data analysis identified several themes. These themes were repeatedly analysed in order to condense them into a meaningful form. The repetitive analysis yielded 25 specific themes as shown in the following table.

Table 1: Consolidation of themes from focus group interviews

Performance Expectancy
1. If I could quickly see benefits of wireless security to my work, I would accept it. 2. If wireless security increases my work efficiency, I would accept the technology. 3. If wireless security enables me to move around at workplace, I would accept it. 4. If wireless security is reliable in protecting my work, I would accept the technology. 5. If wireless security shortens my work time, I would accept the technology
Effort Expectancy
6. If I feel comfortable with wireless security, I would use accept the technology. 7. If I am more computer-literate, I would accept wireless technology. 8. If the wireless security is user friendly. I would accept the technology.

9. If it doesn't take long to learn to use wireless security, I would accept the technology. 10. If I am more familiar with the use of wireless technology, I would accept it.
Facilitating conditions
11. A person's credibility has influence on my decision to accept wireless security. 12. Management Decision has influence on my decision to accept wireless security. 13. People's total commitment has influence on my decision to accept wireless security. 14. The people I work with have influence on my decision to accept wireless security. 15. My workplace culture has influence on my decision to accept wireless security.
Social Influences
16. Education provided on wireless security increases my acceptance to the technology. 17. It is very important that enormous resources support wireless security system. 18. The cost effectiveness in supporting wireless security system is very important. 19. Existing infrastructure has to support the implementation of wireless security system. 20. Wireless security system should not have negative effect on existing system.
Other Mediating Factors
21. A formal system that manages wireless security is better than setting policies. 22. Adopting right practices will increase security of wireless environment. 23. Clinical data should have higher protection priority compared to non-clinical data. 24. Knowing the limitations of wireless security increases my acceptance to the technology. 25. If I work in a place with no technology, I would welcome wireless technology

It can be noted from the above 25 themes that they were slotted into the model constructs. The last section was slotted as 'others' because the focus group data revealed themes that are beyond the current scope of the literature. For example, theme 23 indicates the perception from healthcare staff that clinical data require more protection. Some themes also refer to organisational culture in a subtle manner (example: theme 22). The themes can further be regressed into an initial model. The four main constructs can further be grouped into sub-themes arising from the focus group discussion. This aspect is crucial as this data is yet to emerge in the literature. The four major constructs, while clearly highlighting the relevance, were able to provide a drilled-down version of specific aspects as applicable to the selected organisation. The following table depicts the initial model. The model consists of the four main themes and an additional theme named 'mediating factors' as the members of the focus group highlighted themes that may not have any reference to the main themes.

Table 2: Five major themes and facilitating factors

Performance Expectancy • Benefit to work	**Social Influences** • Credibility

• Increased efficiency • Mobility • Consistency • Reduce work time cycles	• Management Decisions • Commitments • Collegiality • Culture
Effort Expectancy • Comfortable • Technology Awareness • User Friendliness • Learning Times • Familiarity	**Other Mediating Factors** • Formal Systems • Right Practice • Clinical data protection • Knowing Limitations • Availability of new technology
Facilitating conditions • Training • Resources • Cost Effectiveness • Infrastructure • Positiveness of Existing Systems	

The first main factor performance expectancy yielded 5 sub factors namely (i) benefits to work, (ii) increased efficiency, (iii) mobility, (iv) reliability and (v) reduced work tile cycles. Participants of the focus group felt that any security measures of wireless LAN should be able to bring significant benefits to their work. The implied meaning of this sub factor is that security measures should be implemented in such a way that automated cross-checking of patients records can be facilitated by the system. The inherent meaning is that current health records lack strong cohesion in terms of data modelling and hence there is a necessity to address this. Further, healthcare employees are naturally mobile in conducting their daily work functions. Therefore, there is a positive perception that wireless technology coupled with strong security features would bring benefits to work. This has an impact on the efficiency factors and this is identified as the second sub factor. Mobility refers to their ability in performing various activities while moving between patients in wards. The sub factor reliability indicates that the current levels of reliability of health records is not sufficient as manual checks required to be conducted prior to clinical procedures and this requires accessing several documents both paper and computerised and hence the level of reliability expected is not facilitated by current systems. The four sub factors collectively imply reduced work cycles. These five factors collectively define performance expectancy.

In conducting their work, effort is expended by healthcare employees. This is indicated in the second main factor effort expectancy. This main factor was regressed in terms of (i) comfort, (ii) technology awareness, (iii) user friendliness, (iv) learning time and (v) familiarity. The sub factors are different to that of TAM models as the TAM models assume that, in the current climate of technology adoption, due to technology maturity, there is no necessity to provide training to users. However, there is clear indication from the participants that technology should be comfortable to use indicating ease of use. Technology awareness is crucial in healthcare domain because of the use of a variety of medical technology and their reference to computing systems. User friendliness is crucial in terms of user interfaces as the time available on hand to complete a given task is minimal in healthcare settings. This has profound impact on various learning sequences and information processing sequences. Finally, due to the focus on patients, healthcare employees require familiarity of IT components so that they can ‘mechanically’ perform the tasks. This is discussed in terms of familiarity. These five factors collectively lead to effort expended in

conducting a task. It can be inferred from these five factors that these sub factors are related to each other.

The third main factor social influences was further regressed into five sub factors namely (i) credibility, (ii) management decision, (iii) commitment, (iv) collegiality and (v) culture. The sub factor credibility was discussed in terms of the technology and its credibility as well as users' confidence in using the technology as this may be linked to perceptions of security aspects. The participants felt that any problem due to technology fault may impact their credibility. Similarly, the management decision was discussed in terms of deploying the technology and various policies associated with such decisions. This aspect also brought out issues surrounding various privilege levels assigned to employees to access patient data. Commitment refers to the continual support by the management for wireless technology adoption and diffusion. Collegiality indicates the confidence level placed on clinical staff on support staff in order to ensure various security parameters are maintained. The culture of the organisation is important in establishing appositive attitude in terms of social influence. According to participants, these five sub factors collectively defined social influence that can impact wireless technology security issues.

The fourth main factor, facilitating conditions, was grouped in to five sub factors. They are (i) training, (ii) resources, (iii) cost effectiveness, (iv) infrastructure and (v) positive effect on existing systems. The discussion on this main factor mainly focussed on the on-going support for wireless technology in the given healthcare setting. While the discussion centred on 'doubts' in participants' minds, the points made appear to be valid. Again these five sub factors were related to one another. As indicated earlier, training appears to be assuming paramount importance in healthcare. While the technical features of wireless security are beyond the scope of participants' work practices, they insisted that 'training' to handle various security operations as dictated by the software applications is crucial in performing their daily tasks. This includes data access, validation etc. Collectively, these five sub factors defined facilitating conditions.

The last main factor, other mediating factors, was also regressed into five sub factors namely (i) formal systems, (ii) right practice, (iii) clinical data protection, (iv) knowing limitations and (v) availability of new systems. The participants felt that there should be formal procedure sin place prior to any implementation of new systems as the change over from existing systems to new systems may be complicated in a health environment. They also indicated that clinical data requires high level of protection as there is a statutory requirement to maintain clinical data. This aspect has profound impact on off-shoring software development as overseas developers may not be fully aware of this aspect due to varying regulatory frameworks. The fourth sub factor indicates that the healthcare workers were keen to know the limitations of the ICT systems in order to define their work practices. They were reluctant to use the system without knowing the limitations. This would, perhaps, have arisen from the fact that their culture demands limitations of a prescribed medication or clinical procedure. The final sub factor indicates that they would like to see some form of assurance that a new system is available on a continued basis for them to conduct their daily operations. Collectively these factors establish the mediating factors.

Future Work

The data analysis indicated that these 25 factors are related to each other and to some extent succinctly define the unified theory of acceptance of wireless security for a given setting. Based on these 25 factors, a survey instrument was prepared and currently this survey is administered for empirical data to verify these factors and their correlations.

References

[1]. ABS 2004, Year Book Australia, Australian Bureau of Statistics, viewed 04 March 2005, <http://www.abs.gov.au.ezproxy.usq.edu.au/ausstats/abs@.nsf/94713ad445ff1425ca25682000192af2/2955a5ec4f53191fca256dea00053974!OpenDocument>.

[2]. 2004, Population, Australian States and Territories - Electronic Delivery, Australian Bureau of Statistics, viewed 27 March 2005,

<http://www.abs.gov.au.ezproxy.usq.edu.au/Ausstats/abs@.nsf/1020492cfcd63696ca2568a1002477b5/8ca5022b2135f162ca256cd0007bee22!OpenDocument>.
[3]. 2004, Private Hospitals, Australia, Australian Bureau of Statistics, viewed 20 March 2005, <http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/EEEB143EAFB2D027CA2568A9001393FA>.
[4]. ACHS 2003, The Australian Council of Healthcare Standards Annual Report 2002-2003, Australian Council of Healthcare Standards, Ultimo.
[5]. Ahmed, F & Siyal, M 2005, 'Security Services and Issues in WLANs', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[6]. Ahson, S & Bhaskar, S 2005, 'Minimizing WLAN Security Risks', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[7]. AIHW 2004, Australian Institute of Health and Welfare Annual Report 2003-2004, Australian Institute of Health and Welfare, Canberra.
[8]. Aktar, S 2005, 'WLAN Performance', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[9]. Alesso, H & Smith, C 2002, The Intelligent Wireless Web, Addison-Wesley, Boston.
[10]. Anderson, J & Schwager, P 2004, 'SME Adoption of Wireless LAN Technology: Applying the UTAUT Model', paper presented to 7th Annual Conference of the Southern Association for Information Systems.
[11]. APHA 2003, APHA Annual Report 2002-2003, Australian Private Hospitals Association, Deakin.
[12]. AstraZeneca 2002, 2002 HIMSS/AstraZeneca Clinician Survey, Healthcare Information and Management Systems Society, Chicago.
[13]. Baase, S 2003, A Gift of Fire: Social, Legal, and Ethical Issues for Computers and the Internet, 2nd edn, Pearson Education Inc., Upper Saddle River.
[14]. Baker, D 2003, Wireless (In)Security for Health Care, SAIC Enterprise and Health Solution, viewed 15 March 2005, <http://www.saic.com/healthcare/wireless_insecurity.pdf>.
[15]. Bargh, M, Benz, H, Eijik, R, Heer, J, Hesselman, C, Salden, A & Tokmakoff, A 2005, 'Mobile WLAN Application Services', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[16]. Becerra, J, Kawaguchi, A, Miyata, C, Qian, G & Russell, S 2005, 'Integrated WLAN Deployment: Implementation of a Mobile Wireless Diabetes Management System', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[17]. Biever, C 2005, 'Phone Viruses: How Bad is it?' New Scientists, no. 2489, 05 March 2005, p. 25.
[18]. Bloor, M, Frankland, J, Robson, K & Thomas, M 2001, Focus Groups in Social Research, SAGE Publications Ltd, Thousand Oaks.
[19]. Boyd, J 2005, 'A cellphone is the only gadget you need', New Scientists, no. 2489, 05 March 2005, p. 28.
[20]. Boyd, T & Dasgupta, P 2005, 'Security in Wireless Networks', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[21]. Buckley, P, Togno, J, Hovel, J, Cesnik, B, McPhee, W, Lundin, R, Hart, G & Skippngton, P 1996, Telehealth in Rural and Remote Australia, Monash University - Australian Rural Health Research Institute, Moe.
[22]. Buckley, N 2004, An Exercise in Wireless Security, Partners Healthcare, viewed 28 March 2005, <http://www.mahealthdata.org/forums/security/2004/SOF_20040910-PartnersHC.pdf>.
[23]. Burke, L & Weill, B 2005, Information Technology for the Health Professions, 2nd edn, Pearson Prentice Hall, New Jersey.
[24]. Chau, S & Turner, P 2004, 'Implementing and Evaluating a Wireless Handheld Clinical Care Management System at an Australian Aged Care Facility', paper presented to HIC 2004, Brisbane, Australia.
[25]. Clark, V, Creswell, J, Gutmann, M & Hanson, W 2003, 'Advanced Mixed Methods Research Designs', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[26]. Clarke, S & Drake, P 2003, 'A Social Perspective on Information Security: Theoretically Grounding the Domain', in S Clarke, E Coakes, M Hunter & A Wenn (eds), Socio-TEchnical and Human Cognition Elements of Information Systems, Information Science Publishing, Hershey.
[27]. Coakes, E 2003, 'Socio-Technical Thinking - A Holistic Viewpoint', in S Clarke, E Coakes, M Hunter & A Wenn (eds), Socio-TEchnical and Human Cognition Elements of Information Systems, Information Science Publishing, Hershey.
[28]. Coiera, E 2004, 'Four Rules for the Reinvention of Health Care', Bristish Medical Journal, vol. 328, no. 7449, pp. 1197-9.
[29]. Collins, G 2005, 'Evolving Architecture Drives Enterprise WLAN Growth', Business Communication Review, pp. 28-30.
[30]. Crow, A 2004, 'Defining the balance for now and the future - Clinicians perspective of implementing a care coordination information systems management', paper presented to HIC 2004, Brisbane, Australia.

[31]. Czaja, R & Blair, J 1996, Designing Surveys: A Guide to Decisions and Procedures, Pine Forge Press, Thousand Oaks.
[32]. Degen, S & Veugen, T 2005, 'General Security Analysis of an IT Configuration Based on WLAN', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[33]. DeMarco Jr, G, Newman, C, Newman, I & Ridenour, C 2003, 'A Typology of Research Purposes and Its Relationship to Mixed Methods', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[34]. Doherty, N & King, M 2003, 'From Technical Change to Socio-Technical Change: Towards a Proactive Approach to the Treatment of Organisational Issues', in S Clarke, E Coakes, M Hunter & A Wenn (eds), Socio-TEchnical and Human Cognition Elements of Information Systems, Information Science Publishing, Hershey.
[35]. Doktor, R, Bangert, D & Valdez, M 2005, 'Organizational Learning and Culture in the Managerial Implementation of Clinical e-Health Systems: An International Perspective', paper presented to 38th Hawaii International Conference on System Sciences, Hawaii.
[36]. Donaldson, L 2005, 'Patient Safety: Do Not Harm', Perspective in Health, vol. 10, no. 1.
[37]. Edmunds, H 1999, The Focus Group Research Handbook, NTC/Contemporary Publishing Group, Chicago.
[38]. Emanavin, C 2004, 'Testing Lessig: Applying User Acceptance Theory to Internet Use and Behavior for Privacy and Security Applications', Master of Art in Communication, Culture and Technology thesis, Georgetown University.
[39]. Fern, E 2001, Advanced Focus Group Research, Sage Publications Ltd, Thousand Oaks.
[40]. Fernandez, E, Jawhar, I, Petrie, M & VanHilst, M 2005, 'An Overview of the Security of Wireless Networks', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[41]. Fisher, J 2003, 'Human Factors and the Systems Development Process', in S Clarke, E Coakes, M Hunter & A Wenn (eds), Socio-TEchnical and Human Cognition Elements of Information Systems, Information Science Publishing, Hershey.
[42]. Forthofer, M 2003, 'Status of Mixed Methods in the Health Sciences', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[43]. Fullerton, C 2004, The need for Security Testing: An Introduction to the OSSTMM 3.0, Charles W. Fullerton Institute of Analysis, viewed 17 March 2005, <http://www.infosecwriters.com/text_resour_es/pdf/need_for_security_testing.pdf>.
[44]. Gadh, R, Gerla, M, Kong, J & Prabhu, B 2005, 'An Overview of Network Security in WLANs', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[45]. Gillies, J & Whetton, S 2005, 'Electronic Health Records', in S Whetton (ed.), Health Informatics: A Social-Technical Perspective, Oxford University Press, Oxford.
[46]. Gritzalis, S & Lambrinoudakis, C 2005, 'Security in IEEE 802.11 WLANs', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[47]. Gururajan, R, Rai, S & Edward, D 2003, 'The Study in the Use of Hand Held Devices in an Emergency Department for a Hospital in Western Australia', paper presented to IEEE TENCON International Conference, Bangalore, October 2003.
[48]. Gururajan, Quaddus, Fink & Vuori 2005, 'Driver and Inhibitors of the Adoption of Wireless Handheld Technology in the Healthcare Industry: Views from Selected WA Stakeholders', paper presented to HIC 2005, Melbourne Australia.
[49]. Han, S, Mustonen, P, Seppanen, M & Kallio, M 2005, Does Fragmentation of Working Time and Working Space Influence the Acceptance of Mobile Technology? A Case of Finnish Physicians, 657, Turku Centre for Computer Science.
[50]. Harre, R, Moghaddam, F & Walker, B 2003, 'Cultural Distance, Levels of Abstraction, and the Advantages of Mixed Methods', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[51]. Hartnett, J & Whetton, S 2005, 'Building the Knowledge Base', in S Whetton (ed.), Health Informatics: A Social-Technical Perspective, Oxford University Press, Oxford.
[52]. Havenstein, H 2005, Industry Focus: Wireless in Healthcare, Techworld, 15 August 2005, <http://www.techworld.com/mobility/features/index.cfm?featureid=1469&Page=1&pagePos=15>.
[53]. Head, V 2004, Defining the Requirements for Third Generation Wireless LAN Security from Location to Application, Meru Networks.
[54]. Hession, M, Gaudry, P & Hudson, R 2004, '802.11b wireless communication in an emergency department', paper presented to HIC 2004, Brisbane, Australia.
[55]. Hoglund, D 2002, Dynamics of the Wireless Change in Health Overview and Synopsis, Integra System Inc., viewed 23 March 2005, <http://www.codebluecommunications.com/Documents/Dynamics%20of%20the%20Medical%20Wireless%20Marketplace-Hoglund.pdf>.

[56]. IDC 2005, 119% Growth for Australian Wireless LAN Market, Reveals IDC, PC World, viewed 10 April 2005, <http://www.pcworld.idg.com.au/index.php/id;623803113>.
[57]. Ilyas, M & Qazi, S 2005, 'Applications of WLANs in Telemedicine', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[58]. Jamalipour, A 2003, The Wireless Mobile Internet: Architectures, Protocols and Services, John Wiley & Sons Ltd., West Sussex.
[59]. Johnson, B 2002, Wireless 802.11 LAN Security: Understanding the Key Issues, Systems Expert Corporation, viewed 12 April 2005 2005, <http://www.systemexperts.com/tutors/wireless-issues.pdf>.
[60]. Johnson, B & Turner, L 2003, 'Data Collection Strategies in Mixed Methods Research', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[61]. Johnson, C 2004, 'Realising Value From Health Technology Investments: Improving the Selection and Delivery of a Portfolio of Projects', paper presented to HIC 2004, Brisbane, Australia.
[62]. Khan, M 2005, 'WLAN Security: Issues and Solution', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[63]. Kruegar, R 1998, Developing Questions for Focus Groups, Sage Publications Ltd, Thousand Oaks.
[64]. ---- 1998, Analyzing and Reporting Focus Group Results, Sage Publications Ltd, Thousand Oaks.
[65]. Loomis, D & Maxwell, J 2003, 'Mixed Methods Design: An Alternative _pproach', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[66]. Lu, J, Yu, C, Liu, C & Yao, J 2003, 'Technology Acceptance Model for Wireless Internet', Internet Research: Electronic Networking Applications and Policy, vol. 13, no. 3.
[67]. Macnaghten, P & Myers, G 2004, 'Focus Groups', in G Gobo, J Gubrium, C Seale & D Silverman (eds), Qualitative Research Practice, SAGE Publicaiton Ltd., London.
[68]. McGeera 2005, Wireless Security, Hewlett Packard Development Company, viewed 28 March 2005, <http://h200007.www2.hp.com/bc/docs/support/SupportManual/C00290881/C00290881.pdf>.
[69]. Misra, S, Wickramasinghe, N & Goldberg, S 2003, 'Security Challenge in Mobile Healthcare Setting', paper presented to Wireless I.T. Committee Meeting, Cleveland.
[70]. MMC 2002, Wireless Security and Management in Healthcare Organisation, Maine Medical Center, viewed 26 March 2005, <http://www.bluesocket.com/solutions/Healthcare-BluePaper.pdf>.
[71]. Morse, J 2003, 'Principles of Mixed Mehods andd Multimethods Research Design', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[72]. MRI 2004, Medical Records Institute's Sixth Annual Survey of Electronic Health Record Trends and Usage for 2004, Medical Records Institute.
[73]. Oleshchuk, V 2003, Wireless Security and Health Care Information Systems, Agder University College, viewed 12 April 2005, <http://www.mif.vu.lt/cs2/wimv/Wireless%20Security%20for%20Health%20Care.pdf>.
[74]. Onwuegbuzie, A & Teddlie, C 2003, 'A Framework for Analyzing Data in Mixed Methods Research', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral Research, Sage Publications, Thousand Oaks.
[75]. Pabrai, U 2005, Wireless Security, HIPAA Academy, viewed 30 March 2005, <http://www.hipaaacademy.net/pdf/WirelessSecurityWP.pdf>.
[76]. Qazi, F & Qazi, S 2005, 'WLAN Security', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[77]. Rehman, T 2005, 'IP Mobility', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[78]. Schper, L & Pervan, G 2004, 'A Model of Information and Communication Technology Acceptance and Utilisation by Occupational Therapists', paper presented to Decision Support in an Uncertain and Complex World: The IFIP TC8/WG8.3 International Conference 2004.
[79]. Schwandt, T 2000, 'Three Epistemological Stances for Qualitative Inquiry: Interpretivism, Hermeneutics, and Social Constructionism.' in N Denzin & Y Lincoln (eds), Handbook of Qualitative Research, 2nd edn, Sage, Thousand Oaks, pp. 189-214.
[80]. Sciannamea, M 2005, Study Says WLAN Growth to Triple within Two Years, therfidwebblog, 21 October 2005, <http://rfid.weblogsinc.com/entry/1234000053064524/>.
[81]. Showell, C & Whetton, S 2005, 'Health Informatics Tools, Techniques, and Applications', in S Whetton (ed.), Health Informatics: A Social-Technical Perspective, Oxford University Press, Oxford.
[82]. Sinnot, D 2004, Wireless Insecurity, ProActive Network and Security, viewed 24 march 2005, <http://www.e-nc.org/pdf/Sinnot.pdf>.
[83]. Stanford, V 2001, 'Pervasive Health Care Applications Face Tough Security Challenges', Pervasive Computing, vol. 02, no. April-June 2002.
[84]. Stanton, J 2003, 'Information Technology and Privacy: A Boundary Management Perspective', in S Clarke, E Coakes, M Hunter & A Wenn (eds), Socio-TEchnical and Human Cognition Elements of Information Systems, Information Science Publishing, Hershey.
[85]. Tashakkori, A & Teddlie, C 2003, 'Major Issues and Controversies in the Use of Mixed Methods in Social and Behaviral Sciences', in A Tashakkori & C Teddlie (eds), Handbook of Mixed Methods in Social & Behavioral

Research, Sage Publications, Thousand Oaks.
[86]. Thomas, R 2003, Blending Qualitative and Quantitative Research Methods in Theses and Dissertations, Corwin Press, Thousand Oaks.
[87]. Trumble, B (ed.) 2002, Reader's Digest Wordpower Dictionary, 2nd edn, Reader's Digest Association Limited, London.
[88]. Turisco, F 2000, 'Mobile Computing Is Next Technology Frontier for Health Providers', Health Financial Management, vol. 55, no. 11, pp. 78-82.
[89]. Vergara, A 2003, Wireless Network Security, Proxim Corporation, viewed 16 April 2005, <http://www.proxim.com/learn/library/whitepapers/wireless_security.pdf>.
[90]. Walker, J & Whetton, S 2005, 'Health Informatics in Action: Rural and Remote Health', in S Whetton (ed.), Health Informatics: A Social-Technical Perspective, Oxford University Press, Oxford.
[91]. Whetton, S 2005, 'The Health Care Environment and Health Informatics', in S Whetton (ed.), Health Informatics: A Social-Technical Perspective, Oxford University Press, Oxford.
[92]. ---- 2005, 'What is Health Informatics?' in S Whetton (ed.), Health Informatics: A Social-Technical Perspective, Oxford University Press, Oxford.
[93]. WHO 2002, The World Health Report 2002, World Health Organisation, New York.
[94]. Williams, D 2003, $1.3M BOOST FOR HEALTH AND TRANSPORT LOGISTICS, Departments of Communications, Information Technology and Arts, viewed 18 April 2005, <http://www.darylwilliams.dcita.gov.au/Article/0,,0_7-2_4011-4_117516,00.html>.
[95]. Wong, K 2005, Wireless Internet Telecommunications, Artech House, London.
[96]. Wu, J, Wang, S & Lin, L 2005, 'What Drives Mobile Health Care? An Empirical Evaluation of Technology Acceptance', paper presented to Proceedings of the 38th Hawaii International Conference on System Sciences - 2005, Hawaii.
[97]. Yang, T & Zahur, Y 2005, 'Security in WLANs', in S Ahson & M [57] (eds), Handbook of Wireless Local Area Network: Applications, Technology, Security, and Standards, Taylor & Francis Group, Boca Raton.
[98]. Zeeshan, A 2003, Wireless Security In Health Care, University of South Australia, viewed 01 April 2005, <http://www.cs.mu.oz.au/~bir/auscc03/papers/ahmad-auscc03.pdf>.
[99]. Zikmund, W 2003, Business Research Methods, 7th edn, Thomson: South Western, Ohio.