Winter 12-9-2003

Barriers to Uptake of Wireless Healthcare Applications – A Review

Raj Gururajan

Joshua Last

Shri Rai

Barriers to Uptake of Wireless Healthcare Applications – A Review

Raj GURURAJAN, Joshua LAST & Shri RAI

School of Information Technology

Murdoch University

Perth, Western Australia

r.gururajan@murdoch.edu.au

ABSTRACT

Wireless technology is growing and a number of vendors are providing solutions in the area of healthcare. These solutions include electronic prescriptions using handheld devices, data capturing at point of entry using wireless devices, communication of patient information and accessing patient databases using handheld devices. While these new systems appear to be providing solutions to some of the problems encountered by the healthcare industries, there are a number of barriers associated with the wireless technology itself, prohibiting the uptake of this technology in healthcare settings. This paper provides a review of such barriers.

INTRODUCTION

Recent advances in wireless and mobile technology have enabled healthcare industries to provide more responsive service to their customers. Wireless applications that are emerging in the market address some of the problems of the healthcare industries such as data management. This development has prompted renewed interest in technological issues associated with healthcare industry and how the emergence of wireless technology can be applied to the healthcare settings. Current research and development in the area of healthcare includes prescriptions, pharmacy and billing applications. According to a report released in the Wireless News in 2003, it appears that the hospital systems are the fastest growing market for wireless technology. According to [1], wireless technology sector is expected to become a $2 billion industry within five years. According to GE Medical, the number of clinicians using wireless tools will increase from 1 in 100 today to 1 in five by 2004. Therefore, hospitals are investing money into wireless technology that will augment the management of hospital operation.

However, there is still doubt as to whether wireless mobile technology would provide anticipated benefits as the introduction of such technology in hospital environment is still in its infant stages. A number of barriers associated with the performance of wireless technology are yet to be answered in the literature as the applicability of wireless technology to healthcare is just emerging [2]. The objective of this paper is to identify some barriers to wireless technology in a healthcare setting.

WIRELESS MOBILE TECHNOLOGY

Wireless technology includes the concept of mobile computing, which consists of portable devices that can connect to traditional networks without the utilisation of cables [3]. In a wireless network, computers in an office are linked to one another. These computers communicate using radio signals. The network itself is built around an access point and this point may have a wired connection to another network. This access point can receive data and transmit the same to wireless adapters found in the base computers [4]. In healthcare settings, this technology can be used to access data about a patient, to enter certain predefined terms in order to process billing details or to capture patient data at the point of entry.

The need for wireless technology in healthcare is justified by many studies. For example, [5] provides initial thoughts of applicability of wireless technology in addressing the financial crisis encountered in many healthcare systems. [6] elaborates how wireless technology can be utilised to address the increasingly complex information challenges currently encountered by healthcare information systems. [4] mentions the role of wireless technology and hence the mobility of data using wireless devices in order to comply with the rigorous regulatory framework. [7]'s study provides insights into how wireless technology could be used to reduce medication errors and to generate affordable healthcare applications that allow for

greater mobility and ease of use in entering, sending and retrieving data. Similar views can be found in [8].

While these studies provide justification to the use of wireless technology in healthcare settings, [1] raise warnings as to the infancy stages of the devices in the area of wireless technology that are used for data management. [9] warns of the slower speed of wireless devices compared with the desktop computers. [10] points out the high costs to initially set up these wireless networks and their impact on the financial resources of already struggling healthcare industry. [11] is concerned with the lack of real time connectivity due to the mobility of the wireless devices and their adverse influence at critical times. [12] discusses the limited size of screens found on many mobile devices such as PDAs and argues on their lack of suitability in displaying critical data – especially in medical imaging. [13] provides a discussion on the hard-to-see display screens of current mobile devices and the potential difficulty that these screens can introduce for medical professionals. [14] points out the adverse effects of wireless devices on healthcare industry in terms of the need for high quality graphic displays in specific healthcare settings such as operating theatres. While there is general agreement that wireless technology would provide solutions to some of the problems encountered by healthcare industries, it appears that there are some barriers to the uptake of this technology in the healthcare industry.

Further literature review indicated that it is possible to construct a taxonomy for these barriers. We have grouped these barriers into hardware barriers, software barriers, protocol barriers, cost barriers, logistics barriers, interfaces barriers, wireless coverage barriers, security issues, patient care specific to healthcare settings, efficiency of wireless systems, performance barriers and perhaps workforce issues. Some of these are reviewed in the following sections.

HARDWARE BARRIERS

The hardware barriers of wireless technology applicable to healthcare include the demand for more processing power, potential interference to other existing medical devices, range issues, problems associated with bandwidth and energy consumption by current devices [15-17]. Current healthcare applications process a lot of data and hence the information storage at main memory level is crucial for this processing. Due to their sizes, mobile devices have limited memory power (compared with desktop computers) and this appears to be a barrier in implementing major applications with voluminous data on mobile devices. The size of the devices also place some constraint on the Central Processing Unit (CPU). Increasing the power of the CPU adversely affects battery life. Battery life is very important for mobility. Due to the limited power possessed by batteries in mobile devices, frequent charging becomes necessary. This introduces usage limitations. When the hardware is not robust enough, various user settings may be erased by weaker battery and the device may need to be reset. This is a source of major concern and seen as a barrier as this restricts long period of mobility without charging.

The hardware devices also cause problems with other existing medical devices by interfering with them. For instance, mobile telephones are not allowed in a number of hospital environments. These interference problems appear to be limiting the usage of certain mobile devices and is considered a barrier. Due to their nature, current mobile devices used for data processing can communicate only up to certain physical distances and this physical range appears to be a major barrier in hospital environments as these environments, can for some very large hospitals, span over a few square kilometers. As the devices move away from their wireless nodes, the communication signal strength becomes weaker and this may introduce unforeseen problems in terms of data management and communication. This is seen as a hardware barrier and healthcare industries are wary of this problem.

Current research in the area of hardware for wireless technology includes the combination of electronic and mechanical components to reduce interference, improved processing power, long battery life, devices going to 'sleep' mode automatically when they are not in use in order to conserve battery life and higher bandwidth [16]. While the comparative analysis of wired and wireless costs has been extensively covered by [16], it is only within the last five years that wireless hardware has become cost effective and hence a cheaper alternative to wired systems. [18] highlights that 'many healthcare providers are extremely adverse to risks associated with adoption of new information technologies' (p.80). In essence, the hardware barriers include the slower information-transfer speeds due to device restrictions, lack of real time connectivity due to device compatibility, small, hard to see display screens due to size restrictions and limited graphic capabilities due to processing power restrictions.

SOFTWARE BARRIERS

A major barrier in terms of software products for the healthcare industry appears to be the incompatibility of off-the-shelf products with specific environments. An area of common

agreement found in the literature is that hospital systems are custom applications that may seldom be applied to other hospitals [19, 20]. Research into this problem includes the design of generic wireless hospital toolsets that can be applied and customised to any hospital [21] and the abstraction of network connection components within the software that will allow for adaptation to either wireless or wired environments [22]. Further, due to lack of technical expertise and costs associated with software training, the healthcare industry is not in a position to attempt new wireless applications. This appears to be a major barrier in the area of wireless software solutions.

In terms of software, research into wireless mobile software is currently scattered in terms of issues ranging from use of web technology [23] to computing language and protocol support [24]. There is also a significant rivalry between proprietary languages for dominance over the wireless market [25]. [26] question the capability of wireless applications in the area of data management. One specific problem raised was the problems encountered due to the mobility offered by wireless. This mobility has created software technical issues of resolving a user based on the location details due to mobility. [26] also question the software issues associated with security and privacy as users move from one service provider to another. The security issues have been highlighted as major barriers in the uptake of mobile devices by many researchers.

PROTOCOLS BARRIERS

The emergence of wireless technology at the user level is attributed to the publicity of the Bluetooth protocol. About 5 years ago, this protocol was publicised by vendors such as IBM and Microsoft. However, since then other protocols such as those by the IEEE have emerged in the market. Current trend appears to be a move towards the use of non-proprietary protocols such as the IEEE 802.11 series [24, 27, 28]. Due to the variety of protocols available, organisations find it difficult to choose a protocol suit that would meet the needs of all the organisations' applications. This has resulted in confusion. This appears to be a barrier.

[29] points out that there is a lack of benchmarking statistics in the area of performance of protocols. While there have been implementations of wireless mobile technology within the health care system, much of the research conducted into wireless implementations have been descriptive in nature and describes the advantages of using the wireless system using single qualitative opinions [30-32]. Therefore, it appears that there is an overall lack of quantitative data collection to prove the claimed wireless advantages. This has resulted in lack of confidence in using such a technology in a healthcare setting. This is seen as a barrier.

While the hardware devices are useful in the total picture of wireless technology, they need to communicate and a set of agreed upon rules for communication is used to ensure uniformity and device neutrality. These set of rules are called protocols. An area of controversy within the literature and the IT industry is the support for wireless protocols [29] as multiple vendors provide multiple protocols. For instance, to communicate using wireless technology different sets of protocols are available such as Bluetooth and IEEE. On one hand the hardware manufacturers are imbedding support for as many wireless protocols as possible, allowing for integration of new and existing wireless systems in order to maintain healthcare applications developed so far. On the other hand, support for multiple non-standard wireless protocols increases hardware prices and encourages non-compliance with standards. This is seen as a barrier to the uptake of wireless technology in healthcare industries.

COST BARRIER

There are competing views within the literature as to whether wireless systems are worth the cost of development and implementation [33, 34]. Few studies have expressed concerns regarding the viability of wireless technology because of the unjustified benefits. It appears that these feelings stem from the fact that most studies have looked into the cost advantages of new wireless systems with existing systems from a technical point of view and compared the technical cost factors alone. However, studies that have investigated a number of other intangible factors indicate that wireless implementation may provide enormous benefits such as quality of healthcare services to wider community. What appears to be a major barrier is the cost of installation of the new system when a working wired system is already available and the lack of immediate return on the investment.

For the majority of research into wireless implementations, wireless technology is portrayed as the next revolution in hospital care [28, 35, 36]. "Wireless" would seem to indicate that there is no need for wires, but wireless systems need to connect to the main wired infrastructure at some point. This has been indicated in our opening paragraphs. The age of the available physical infrastructure may become a barrier when buildings classified under the 'historical structures' are considered for wireless implementation, as any work on the infrastructure needs permission from relevant authorities. Therefore, cost issues become a concern to organisations because the existing physical infrastructure needs to be maintained as it is or needs

to be upgraded to accommodate various wireless access points.

Return on investment is what businesses are aiming for when investing in a system. This area has also been covered extensively within the literature, and most seem to highlight the reduced occurrence and therefore cost of recovery from medical inaccuracies [36, 37]. Studies have explored the issues of savings from billing errors and any associated legal costs [36, 37]. Cost appears to be a major barrier to the wireless uptake in healthcare.

USER INTERFACE

User interfaces are identified as a crucial link between wireless devices and end users and the issue of user interfaces is emerging in the literature due to the significance associated with the cognitive ability of users in understanding various interaction techniques using these interfaces. While user interface design is an established research area for wired systems, research in the area of interfaces associated with wireless technology is improving in the recent years. Surprisingly, hospital wireless information systems research is not at the forefront of mobile interface design despite the fact there are many wireless healthcare devices already available in the market place such as blood pressure monitors [38, 39]. One reason may be due to the special conditions under which the wireless systems are being utilised in healthcare and the sensitivity of these devices and the information packets passed through these devices. An emerging area of interest is voice recognition for medical command transcription as this may avoid transcription errors and delay in transcribing manual records from source to a computer based records [38]. While traditional computing has evolved in the past three years with various software applications to recognise voice samples, the wireless technology is still struggling due to the hardware limitations of the wireless devices. Further, due to the sensitivity of the patient information, there is some form of reluctance by physicians to adopt this concept. This appears to be a major barrier for the uptake of wireless technology in healthcare. While the voice recognition will mimic data entry operations, a problem that is being investigated is the elimination of background voices and unauthorised command entries so as to arrive at accurate translation of voice commands into data fields. It is hoped that research into speaker recognition will help to eliminate commands from unauthorised personnel and background voices, by authenticating the users voice, and determining the users authority [38]. It is widely accepted that the choice of mobile devices is an important consideration for wireless implementation and this choice is dictated by the ease of use provided by the interface. This appears to be a barrier because healthcare industry is reluctant to commit on a type of device due to the infant stages of development in this area [36, 40].

COVERAGE

Coverage is not only a technical wireless issue, but also an issue within the hospital setting. By nature, mobile devices may be used to roam around and it is important that connection to the network is retained so that collected data is not lost and information is accessible when and where it is needed. Previous studies provide details of wireless coverage in healthcare settings [36, 41].

Of particular interest to a healthcare setting is the range of the Wireless Local Area Network (WLAN) because of the scale and dispersion of physical buildings [27, 42]. This has lead to research into how range can be maximised through optimising bandwidth and signal strength in a healthcare setting [43]. [44] suggests that wireless range should be limited for security reasons because by having a wider range for wireless devices, the geographical area for network hacking is increased, making these attempts more difficult to monitor and prohibit. It appears that Baylor's theory is purely hypothetical and there is no concrete evidence available to support such a theory. Further, current wireless devices are capable of handling Wireless Encryption Protocols (WEP) and the adverse effect arising out of hacking can be minimised. While studies have compared the wireless range available for various wireless technologies, there appears to be no conclusive agreement as to the security issues associated with the wireless coverage [45]. Issues associated with wireless range appear to a major barrier in the uptake of wireless technology in healthcare settings.

The issues of unexpected problems in connection due to coverage have been studied in prior research [41]. These connection losses are not only inconvenient, but may also risk data access to ensure patient well being by not having important patient data available when it is required for the administration of medication. Prior studies attribute these problems to network range, lead walls and wireless interference [27]. Furthermore, it appears that fundamental problems in coverage may result in denial of service when patient information is most needed. In certain cases, denial of service can result in legal prosecution and healthcare industries are aware of this issue. This has resulted in a barrier adversely influencing the uptake of wireless technology in healthcare settings.

In the past two years, research studies focus particularly on the load-testing of WLAN's [46] and whether implementations are capable of handling the

wireless needs of the hospital environment. Prior studies into interference have covered aspects of technical issues and is of particular concern to hospitals due to the importance of medical data integrity [47] and disruption of sensitive medical equipment, which could put patient's lives at risk. Due to the importance of medical data for health, billing and medical reasons, data integrity needs to be ensured. Interference from walls [45], other RF equipment and coverage holes may diminish or corrupt data integrity leading to losses in patient health data, billing revenue, and legal recovery costs [41]. These are potential barriers to the uptake of wireless technology in healthcare settings.

In terms of radio interference, there exist two dominant competing views within wireless hospital literature; one suggests that interference with medical equipment is non-existent [47], and the other portrays interference as life threatening [36, 48, 49]. According to the first group of literature "Wi-Fi-enabled handhelds or laptops generate about 5 percent of the radiofrequency power that cellular or PCS phones emit". Medical treatment and diagnostic equipment manufacturers have even gone as far as embedding wireless systems into their equipment [47]. However studies have investigated the issues of interference with sensitive equipment and have deployed measures such as frequency modulation to attempt to remove this interference. Interference has been noted ranging from pace maker disruption which, are possibly life threatening to wheel chair malfunctions [50]. These equipment malfunctions have been put down to the lack of medical device immunity to Radiofrequencies (RF) and the increased number of RF emitting devices such as mobile phones and mobile computers. Standards for medical equipment immunity were established in 1993, and these standards must be tightened to allow for increased number and power of RF and their close proximity to sensitive equipment. These conflicting outcomes from prior studies demonstrate that there exists competing views on the issues of interference in the hospital setting, ranging from total acceptance to the banning of wireless technology neither of which seems appropriate [51], resulting in perceived barriers.

SECURITY

Security appears to be a major barrier to the uptake of wireless technology in many areas, including healthcare. The management of security issues in a hospital is an established area, but is challenged through the introduction of wireless technology. Research has been undertaken to specifically lay down foundations for wireless security management [44]. The main concerns for security management within a hospital setting are confidentiality of billing and medical information [19, 41, 51] and privacy of patient information [19, 41]. Of particular concern to the protection of private and confidential information is the monitoring of network accesses [43] and the tracking of mobile devices [47].

Security threats in wireless environment can range from passively eavesdropping into others' message to actively stealing user's data [52]. In a radio frequency operated mobile commerce, it is possible to listen to one's communication with minimum difficulty. This has an impact on healthcare because of the concern about data and voice messages from unauthorised access. On the other end of the problem is the inherent security risk involved in transferring information over the networks. This problem consists of two components: *identification integrity*, and *message integrity*. The identification integrity refers to the signature elements found in the messages in order to establish where the message is originating. The message integrity refers to details to establish that the message is received as sent and no third party has attempted to open, modify or alter the contents. According to [53], these two items appear to cause a lot of concern to both sender and receiver. While the sender risks theft or misuse of their personnel information such as account and bank details, the receiver (a healthcare provider) risks repudiation of the transaction and resultant non-payment.

In addition to the above two, additional security concerns in wireless technology arise due to the new development in technology itself [53]. The mobile technology is envisaged in such a way that the services offered will eventually warrant payment for the type of services offered. This is already emerging in the domain of mobile telephones. For instance, when mobile telephone users access other network carriers, a special charge is levied on the users. Therefore, it is safe to assume that there will not be any "free services" in the future. The technology is developing in such a way that the payment for such services will be through some form of "smart cards". The details stored in the smart cards need to be transmitted via the networks for validation and verification in order to determine service levels. If these networks are not fully secure, there are possibilities for security breaches to happen.

One major security breach that can happen in wireless networks is when the user details are transformed from one mobile network to another [54]. When this transformation occurs, any encrypted data needs to be decrypted for transparency. In wireless technology, when mobile devices make requests to web pages of a network server, a four-stage process is followed. First, the requests arise from the originating Wireless

Transport Security Layer (WTSL) protocol. Second, the requests are translated at the originating Wireless Application Protocol (WAP) gateway. Third, they are sent to the standard Session Security Layer (SSL) protocol of the destination network. Fourth, the translated information reaches the Hyper Text Transfer Protocol (HTTP) modules in the new network in order for the requests to be processed. In the process of translating one protocol to another, the data is decrypted and then re-encrypted. This process is commonly known as the "WAP Gap". If an attacker is able to have access to the mobile network at this point, then simply capturing the data when it is decrypted can compromise the security of the session.

Data in the Mobile environment is secured using encryption technology. According to [55], it has already been proven that the technology is vulnerable to attacks. Hackers have broken some of the existing algorithms for encryption. So, there is nothing like a complete security. Further, there is no international regulatory framework available to fix certain security related problems. For example, in the current climate, no individual organisation or government can guarantee security to consumers. When the security breach appears in an international transaction, no one country will be able to assume responsibility to prosecute the vandals. While these problems have been recognised and solutions are being proposed, organisations tend to loose consumer confidence. This will potentially impact organisation's revenue.

Trust is central to any commercial transaction and more so in the case of healthcare [56]. Trust is normally generated through relationships between transacting parties, familiarity with procedures, or redress mechanisms. In the case of healthcare, the need for creating the trust in the consumer assumes extreme importance because of its virtual nature. It hinges on assuring consumers and associated businesses that their use of network services is secure and reliable, that their transactions are safe, that they will be able to verify important information about transactions and transacting parties such as origin, receipt and integrity of information, and identification of parties dealt with. Therefore the challenge is not to make mobile Commerce fool proof but to make the system reliable enough so that the value greatly exceeds the risk.

Any new development in technology in today's consumer minds creates both curiosity as well as reluctance. The informality and lack of overall control creates the perception that the Internet is inherently insecure [57]. This inherent perception can trigger business risks and technological risks [10]. Business risks involve products and services, inadequate legal provisions, reliability of trading partners, behaviour of staff and demise of Internet service provider. Technological risks involve hacker attacks, computer viruses, data interception and misrepresentation call all arise. To achieve satisfactory levels of trust, organisations have to think about managing both business and technological risks. Currently healthcare relies mostly on knowledge-based trust that is useful for Business-to-Business commerce [56]. However, there is a big surge in the identification-based trust to satisfy consumer concerns about their transaction details. In addition, current architectures for mobile communications do not provide full security measures in terms of transaction integrity. Some of the models envisaged for mobile communication are based on smart cards oriented approach and hence the issue of transaction security needs greater examination in healthcare.

WORKFORCE ISSUES

The impact of changing work practices due to the advancement of the information technology is a major concern in many organisations, including healthcare organisations. The changing work practices include an increased reliance on computing technology and a move towards a more flexible workforce [58]. While the increased reliance on computing leads to technical errors that may go unnoticed by healthcare operators at the time of capturing patient data, the move towards a more flexible workforce may introduce health related issues. While these two major issues are only concerns at the moment, they may become a major barrier for the uptake of the mobile devices in the healthcare because only a selected few people may be offered training due to cost implications. According to [58], the huge expansion of the use of IT would further result in information overload, causing increases in working time, leading to problems in scheduling the available workforce and work coordination. In the healthcare industry, when these problems are applied to the existing workforce, it would result in a shortage of manpower with the right levels of training. This will adversely impact the healthcare industry resulting in some form of barrier.

CONCLUSION

This paper provided some barriers to the uptake of wireless technology in a healthcare domain. While these barriers appear to be dominating the industry in the current time, a number of solutions are also emerging to address these barriers. In recent months healthcare solutions started appearing using handheld devices and these solutions appear to provide promising signs.

REFERENCES

1. Yuan, M.J. and J. Long, *Build database powered mobile applications on the Java platform*. 2002.
2. McConnell, E.A., *Wireless technology: Freedom to roam.* Nursing, 2000. **30**(9): p. HN1-HN4.
3. Simpson, R.L., *Wireless communications: A new frontier in technology.* Nursing Management, 1996. **27**(11): p. 20-21.
4. Wisnicki, H.J., *Wireless networking transforms healthcare: physician's practices better able to handle workflow, increase productivity (The human connection).* Opthalmology Times, 2002. **27**(21): p. 38 - 41.
5. Davis, R., *Pursue front end solutions to revenue problems.* Healthcare Financial Management, 2002. **56**(8): p. 30 - 36.
6. Yacano, F., *Monitoring air quality: handhelds and wireless tools from efficient links.* R & D, 2002. **44**(5): p. 42 - 46.
7. Turisco, F., *Mobile computing is next technology frontier for health providers.* Healthcare Financial Management, 2000. **54**(11): p. 78 - 82.
8. Athey, S. and S. Stern, *The impact of information technology on emergency health care outcomes.* RAND Journal of Economics, 2002. **33**(3): p. 399 - 388.
9. Shah, M., *Grassroots Computing: Palmtops in health care.* The Journal of American Medical Association, 2001. **285**(13): p. 1768 - 1769.
10. Shroeder, S., *Wired for business.* Risk Management, 1999(March): p. 12-22.
11. Stevenson, S., *Mobile computing places data in the palm of the hand: Devices deliver real-time access to information.* Opthalmology Times, 2001. **26**(4): p. 15 - 18.
12. Toms, G.E., *Understanding and facilitating the browsing of electronic text*. International Journal of Human-Computer Studies, 2000. **52**: p. 423-452.
13. Bevan, N., *International standards for HCI and usability.* International Journal of Human-Computer Studies, 2001. **55**: p. 533-552.
14. Atwal, R., *The wireless office: Evolution, Revolution or Bust*. 2001, Gartner Research.
15. Ogando, J., *Plastics with a bluetooth bite.* Design News, 2001. **56**(13): p. 65-66.
16. Martin, M.M.C.-S., *Hospital staff operates anywhere it pleases.* Communications News, 1999. **36**(1): p. 44-45.
17. Anon, *How wireless LAN solves echo problem.* COMP. MED., 1989. **18**(1): p. 1.
18. Turisco, F., *Mobile Technology is Next Technology Frontier for Healthcare Providers.* Healthcare Financial Management, 2000. **54**(11): p. 78-81.
19. Abreu, E., *Doctors with devices -- Wireless technology keeps physicians connected even as they make their rounds.* Industry Standard, The (United States),, 2001. **4**(14): p. 88.
20. Microsoft, C., *Healthcare's Wireless Condition: Expecting.* Wireless Data News, 2002. **10**(21): p. 1.
21. Pappas, C., et al. *A mobile e-health system based on workflow automation tools*. in *Fifteenth IEEE Symposium on Computer-Based Medical Systems.* 2002. Maribor, Slovenia.
22. Segarra, M. and F. Andre, *Framework for dynamic adaptation in wireless environments.* PROC CONF TECHNOL OBJ ORIENTED LANG SYST TOOLS, 2000: p. 336-347.
23. Ratib, O., et al., *Use of personal digital assistants for retrieval of medical images and data on high-resolution flat panel displays.* RADIOGRAPHICS, 2003. **23**(1): p. 267-272.
24. Tachakra, K.B.R.S.H.I.S., *Applications of medical wireless LAN systems (MedLAN).* International Journal of Medical Marketing, 2002. **2**(2): p. 136-142.

25. Taft, D.K., *Sun builds out Java tool sets.* eWeek, 2001. **19**(13): p. 12.
26. Imielinski, T. and B.R. Badrinath, *Mobile Wireless Computing.* Communications of the ACM, 1994. **37**(10): p. 18-31.
27. Cole, R.J., *Filling a hospital's wireless Rx*. Communications News, 1995. **32**(5): p. 20.
28. Sealander, B., *A real head-turner.* Communications News, 1999. **36**(8): p. 52-54.
29. Sullivan, J., *Test sets evaluate wireless performance parameters.* Microwaves & RF, 1997. **36**(3): p. 158.
30. Larkin, M., *Can handheld computers improve the quality of care?* The Lancet, 2001. **358**(9291): p. 1438.
31. McConnell, E.A., *The freedom to roam.* Nursing Management, 1999. **30**(4): p. 51,54.
32. Mendez-Wilson, D., *Doctors get healthy dose of wireless.* Wireless Week, 2001. **7**(11): p. 44-48+.
33. Clark, E., *The wireless ward.* LAN (United States), 1995. **10**(13): p. 143-146.
34. Rege, O., *Winning with wireless solutions.* Pharmaceutical Executive, 2002. **22**(8): p. 10.
35. GE, M.S.G., *Wireless Is a the Heart of New Hospital.* Wireless News, 2002.
36. Niekerk, C.V., *Wireless Technology to Improve Patient Care.* Africa News Service, 2002.
37. Phillips, B.I.C., *WIRELESS LANS: IMPROVING THE WAY WE RECEIVE HEALTH CARE.* Wireless Data News, 1998. **6**(11): p. 1.
38. Ancona , M., et al. *Mobile computing in a hospital: the WARD-IN-HAND project*. in *Proceedings of the 2000 ACM symposium on Applied computing*. 2002. Como, Italy: ACM Press.
39. Holzman, T.G., *Computer-human interface solutions for emergency medical care.* Interactions, 1999. **6**(3): p. 13-24.
40. Mills, K., *A busy hospital is making huge time savings using Ipaq Pocket PC's to access patient data on the run*, in *The Australian*. 2003. p. 356.
41. Bissell, M., *Point-of-care testing at the millennium.* Critical Care Nursing Quarterly, 2001. **24**(1): p. 39-43.
42. Cornell, C.I., *CORNELL OFFERS LOW-COST WIRELESS EMERGENCY RESPONSE.* Tele - Service News, 2002. **14**(12).
43. Cox, J., *Wireless net challenges hospital IT group.* Network World, 2003. **20**(11): p. 17-18.
44. Baylor, H.C.S., *Healthcare system goes wireless.* Communications News, 2002. **39**(9): p. 40.
45. Blum, J., J. Kramer, and K. Johnson, *The palm as a real-time wide-area data-access device.* JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION, 2001: p. 52-56.
46. Milsom, S., *U.K. MOBILE PHONE NETWORK CHOOSES LOADRUNNER.* Computer Protocols, 2000. **13**(10): p. 1.
47. Phillips, B.I., *Wireless Curing Hospital's Connectivity, Cost Problems*, in *Wireless Data News.* 2003. p. 1.
48. Lin, J.C., *Health aspects of wireless communication: a real and present wireless danger.* ACM SIGMOBILE Mobile Computing and Communications Review, 2000. **4**(1): p. 17-18.
49. Hemeon, W.R., *Warning: HDTV and telemetry on a collision course.* Nursing Management, 1998. **29**(9): p. 81.
50. Bassen, H.I., *Radiofrequency interference with medical devices - A technical information statement*, in *IEEE ENGINEERING IN MEDICINE AND BIOLOGY MAGAZINE*. 1998. p. 111-114.
51. Simpson, R.L., *Eyeing IT trends and challenges.* Nursing Management, 2002. **33**(12): p. 46-47.

52. Loney, M., *M-Commerce safety fears,* in *IT Week*. 2000. p. 6.
53. Zhang, Y. and W. Lee. *Intursion detection in wireless ad-hoc networks.* in *ACM/IEEE MobiCom*. 2000.
54. Hulme, G., *Services Seeks to Bring e-Business to Small Businesses,* in *Informationweek.com*. 2000. p. 21.
55. Ghosh, A.K., *Security and Privacy for E-Business*. 2001, New York: Wiley.
56. Fink, D., *Developing trust for Electronic Commerce,* in *Internet and Intranet: Security and Management: Risks and Solutions*, L. Janczewski, Editor. 2000, Idea Group Publishing. p. 44-86.
57. Schiller, J., *Mobile Communications*. 2000, New York: Addison-Wesley.
58. Sparks, K., B. Faragher, and C.L. Cooper, *Well-being and Occupational Health in teh 21st Century Workplace.* Journal of the Ocupational and Organisational Psychology, 2001. **74**(4): p. 489-510.