

# Mobile Computing for Hospitals: Transition Problems

Warren Adis

Hagan School of Business  
Iona College, New Rochelle, NY 10801  
(845) 352-7132 wadis@iona.edu

## ABSTRACT

*Mobile communication devices have an untapped potential to increase the quality of healthcare services. These devices can become the backbone for a new level of hospital service. This would include improved communications among medical and support staff, and increased patient monitoring using a whole new generation of RFIDs. Yet, problems come with the introduction of new technology, some anticipated, some not. This paper develops several hospital scenarios depicting possible problem areas in the conceptualizing, planning and design of future mobile networks.*

Key words: mobile networks, RFID, middleware, hospitals.

## INTRODUCTION

It is easy to imagine a sophisticated hospital environment that has adopted mobile technology. This would include the incorporation of mobile Personal Digital Assistants (PDAs) for staff as well as the use of miniaturized mobile patient monitoring devices, somewhat similar to radio frequency identification devices (RFIDs). These monitoring tags act as transceivers, forwarding medical readings to the nurses' central station, and in turn receiving and storing medical and diagnostic updates. The new technologies have the potential to improve resource management and logistics, through more accurate and timely information concerning patients, staff, and equipment (Evanshwick, Swan, and Smith, 1995). These mobile communications devices can then become the basis for overall Quality of Service (QoS) network computing. It is management's challenge to provide QoS computing that translates to QoS patient care (Adis, 2003). Our experience with new technological platforms has shown that the successful transition will be challenged by unexpected and unplanned problems in management, technology and patient care. Mobile computing only adds value to the degree that it improves patient care, management support, and the overall work environment.

New technological platforms obviously have strengths and weaknesses, and it is the job of management to optimize the strengths and constrain the weaknesses. Therefore in each phase of adoption, management must analyze the maturity of the technology, patient care implications, and workplace impact on medical staff. One of the best ways to come to grips with these issues is to conceptualize these tradeoffs through analyzing various common hospital scenarios (Bardram and Christensen, 2004). The remainder of this paper looks at possible pitfalls in various next generation scenarios, analyzing them from three perspectives: patient care, management, and the technical issues.

## TECHNICAL AND MANAGEMENT TRADEOFFS

The introduction of a new technology is an exercise in managing tradeoffs. With mobile computing in a hospital environment the tradeoffs become serious. Due to the mission critical nature, a hospital environment can not manage tradeoffs on a binary basis of all or nothing, but must manage more incrementally. The management philosophy is to choose systems and procedures to maximize the capabilities of the new technology and minimize the risk of unexpected problems (Banavar, 2000).

For instance, in order to gain mobility on the hospital floor, management must be willing to trade a fast, full featured desktop PC for the significantly slower and less robust mobile client. Since management must mandate tasks like encryption and compression to protect sensitive data, the mobile client's speed will be further decreased.

Additional tradeoffs include accepting a less stable and somewhat immature model of client server computing, lacking in some respects the characteristics of solid hardwired communications. This is because the mobile model has to accept the possibilities of lightweight clients and the limited functionality of servers. These mobile client/servers may have a short broadcast range and the inability to handle sophisticated audio and video communications. The lightweight features of these devices include batteries as a power source, antennas rather than high speed Cat 5 wiring, limited storage capacity for programs, less memory for caching documents, and a slower CPU. Furthermore, mobile middleware operating systems, unlike traditional middleware, have to handle frequent communications faults occurring within the hospital work environment. Events, such as radio interference generated from hospital equipment, interrupted work sessions, and the movement of patients, medical staff and equipment from one transmission zone to another, can play havoc with the request-response found in traditional middleware.

Mobile middleware designers have already begun implementing such services as network diagnostics, fault management and reconnection services. For lightweight nodes, middleware now provides improved compensatory services such as data compression (Capra and Mascolo, 2001).

In addition to the technical tradeoffs, there are also management tradeoffs. One such tradeoff is that the medical and administrative staff will have to adapt to miniaturized PDA type equipment. There are also a range of less visible though more critical issues such as theft of patient data, which usually becomes evident well after the initial crime. In a mobile environment, broadcast transmissions are more vulnerable to hackers within range of the signal and therefore data encryption and user authentication are essential middleware services (Morton and Bukhres, 1997).

If this future environment fully incorporates mobile devices for communications, patient monitoring, and delivery of medical information, then an equipment failure can have serious consequences. Tradeoffs in providing patient care are simply not acceptable. Therefore a secure QoS technical environment anticipates potential problems and devises methods to protect the healthcare environment. At no point can the mobile environment deteriorate to the point where the quality and integrity of transmission and security adversely affect patient care. Management must be aware that the critical components in mobile computing are fault tolerant systems, with 'intelligent' self-monitoring middleware (MosquitoNet, 2003). Management thinking also needs to address workflow issues that take advantage of the new mobile environment, while introducing safeguards to guarantee QoS (Campbell, 1997), (Rohrer, 2003).

## **HOSPITAL SCENARIOS**

The following descriptive scenarios show how the new mobile technology will impact common patient-driven events that occur in a hospital. These focus on a complex and fast changing environment, where any number of things can go wrong. This approach analyzes the managerial and technical issues needed for planning, designing, and implementing a QoS patient care. This step is the basis for developing a methodology for incorporating a new technology platform.

### *Scenario 1: Emergency Room*

A family brings an aging relative to the ER. The staff enter the patient registration data into one of the many mobile laptops found in Admissions. In addition to the patient demographics, the staff input the temporary room assignment and name of attending physician. The data now resides on the healthcare data server and the patient accounting server.

In addition, the staff provide the patient with an electronic bracelet, an updated equivalent of the traditional plastic wrist bracelet. This bracelet device is similar to an inexpensive memory stick and contains 256 MB of data storage, and a transceiver for transmitting / receiving information. Besides name and demographics, the electronic bracelet contains information for the attending physician, and has storage capacity for medical diagnosis and treatment plans.

After the patient examination, the doctor orders appropriate medication and schedules an initial treatment as well as further tests for the patient. She enters all of this into her mobile PDA and the data is then transmitted to the healthcare server, which records the information and schedules tests and treatments. The patient information is then forwarded by the mobile network to laptops in the assigned medical sections, including the pharmacy. In addition, the healthcare server broadcasts certain essential medical information to the patient's electronic bracelet, to be stored there for future use.

*Scenario 1 Analysis: Emergency Room*

The weakest link in the hospital mobile network is the electronic bracelet. Two areas in particular are likely to cause problems – faults in data transmission and inadequate bracelet recycling. Such equipment failures are much more likely to be found with the inexpensive bracelet rather than the more sophisticated laptops and PDAs assigned to staff.

From management's perspective both failures are equally serious, since they potentially jeopardize the patient's wellbeing. Taking first the hardware failure, management can devise a series of preemptive workarounds. Additional diagnostic software can be used to regularly 'ping' all transceivers on the network, asking them to identify themselves and transmit their critical data. For instance the system can ping a patient's bracelet, and use the transmitted patient data to perform an electronic comparison of the medication and treatment files with the same data on the health care server. The comparison would match patient data on the server against the data in the electronic bracelets, to ensure that both have the same file sizes and time/date stamps. The ping is a reliable indicator that the message has been received, and the response is a quick check that the data on the bracelet matches the data on the health care server. With any discrepancy the network alerts the nurses, and the bracelet is swapped with a new one.

The recycling issue is in reality a work flow problem. Just as the bracelet has to be antiseptically cleaned, so does the previous patient data have to be electronically purged, and then tested twice. The first time after the machine is physically cleaned and purged, it is tested both for transmission characteristics and empty data directories. Finally after loading the new patient's demographic and medical data, newly created files are sent to the nurse's workstation for a visual inspection. After this point, the health care server routinely requests a read-out of data found on the bracelet for an electronic comparison of the medication and treatment files on the bracelet with those in the health care server. If there are specific critical health care issues, the server regularly sends a copy of critical bracelet data to the attending physician for review and confirmation. This would be the electronic equivalent of checking the patient's medical chart.

*Scenario 2: Test Results*

The patient has taken a series of tests to determine his condition. One of the tests shows an irregular cardiogram reading. The healthcare server downloads a high priority message to the attending physician, as well as downloading the results to her PDA. The heart specialist on call is also alerted and sent the results.

Through messaging back and forth the two doctors decide to meet in one of the conference rooms to discuss the problem. Collaboration is the core of any improved healthcare logistics (Goldberg, 1997). Workflow is improved because the chief participants can use appropriate collaboration software to schedule meetings and services. Messaging confirms the time and place to meet and resolve patient care issues. In this instance the doctors choose a meeting room which has a white board with mobile client capabilities. This visual aid is a useful tool in their discussion. During the meeting, they beam the cardiogram results found on their PDAs to an electronic white board. In this way they can both see and discuss the cardiogram. The middleware supports collaboration software for scheduling and overall workflow. It also supports and manages the necessary data formatting by tracking the features found in each mobile device (Mohan, 2000). For instance, it knows the limited functionality of the doctor's PDA, particularly the small size display panel. Therefore the system middleware modifies the cardiogram's medical data to more easily display on the PDA. When the cardiogram data is shown on a large electronic white board, the middleware modifies the data set to take advantage of the large screen format. This is possible because the middleware's object repository contains the interface and characteristics of each client.

From this collaboration, they decide that the medication needs to be changed, further tests taken, and additional treatments given. They immediately alert the patient's nurses. Both physicians use their PDA to update the system with the changes. Additionally the attending physician decides she wants to discuss the results with the patient. Since the patient's electronic bracelet acts as a global positioning locator (GPL), he can easily be found, whether he is in his temporary room, a new room or in any of the medical sections of the hospital. The GPL feature is integral to providing optimum communications by discovering the location of the mobile clients, and having the middleware change their broadcast zone as they travel.

*Scenario 2 Analysis: Test Results*

When data is moved to a PDA it can lose critical information, since the system is not sophisticated enough to choose which data to drop. In addition when the data is displayed on the whiteboard, there is usually a lack of clarity caused by a display system with insufficient resolution. Furthermore, physicians are used to having the test results in hand, where they can see and physically compare different charts at the same time, rather than having to page through the data on screen. When speaking to their colleagues in diagnostics units who read EKG's, sonogram, and CAT scans, they are likely to meet with even more vociferous objections. One can imagine for example, that x-rays would not translate well to the display screen, and make it difficult for physicians to interpret anomalies. For them, nothing compares to seeing the actual results rather than an electronic facsimile. Management can respond with plans to upgrade to more high definition display systems, with built in magnification.

*Scenario 3: Medication*

Later on in the day the nurse's PDA alerts her that it is time to give the patient his medication. This medication comes from the newly altered treatment plan which the doctors have recently prescribed. The patient name, room number, medication and dosage appear on the nurse's PDA screen. When the nurse picks up the patient's medication and holds it next to her PDA, the information on the electronic tag on the medication is automatically matched against the data on her PDA for accuracy. On returning to the room, the data on the patient's electronic bracelet is also matched against the electronic medication tag. If there is any discrepancy the PDA immediately notifies the nurse, and sends a message to the attending physician. In addition the nurse's PDA automatically sends a message to the healthcare server for error tracking and rectification. Assuming in this instance that there are no discrepancies, the nurse administers the medication, and enters into her PDA the transaction completion codes (time /date and health care provider) that signify that the medication has been administered. Once the medical transaction has been completed, the PDA forwards one segment of the data to the healthcare server that is monitoring the progress of the patient, and a second segment to the accounting program that is maintaining the patient's medical bill. The accounting program also contains a database for managing medical inventory, which is similarly updated based on resources used by the staff.

*Scenario 3 Analysis: Medication*

A key problem area is medical error, whether it is the incorrect labeling of medication or a mismatch between medication and patient. The hospital must have multiple precautions in place, to ensure the correct medication and dosage are administered to the patient (Doug, 2002). The tracking of medical errors is an important component of improved patient care, without which errors are rarely discovered, and even less frequently recorded. In the current manual system it is almost impossible to track manual errors, except those that cause immediate harm to the patient. With the new system, management has for the first time a methodology for tracking patient care. Yet there may still be healthcare issues. For instance it is certainly possible that the medical staff, when rushed, do not follow all of the steps outlined in the Medication Scenario. One answer is to develop a detailed workflow database. Management can easily implement a workflow database to track the administration of medication, from the moment the PDA signals the nurse, till the time that the medication is matched against the patient's bracelet, and finally the time when the nurse enters her medication completion codes into her PDA. Needless to say, there will be some staff members who will be quite vocal about "Big Brother" monitoring their activities, which could be a future area for grievances.

In addition, this tracking of errors gives further insight into workflow issues and potential weaknesses in the delivery of patient care. Similarly the accuracy and timeliness of patient billing is improved. Suggested procedures to improve workflow are as follows:

- Recycling medication rfid tags, similar to the steps used for patient's electronic bracelets
- An electronic audit of each batch of medications to make sure that the tags in the current batch match the medications produced in this batch
- Clerical scanning to match the contents on the label with the data broadcast by the medical tag.

Another potential problem for medication delivery is when power failures result in hospital-wide computer shutdowns. A situation such as this would mandate that the medication tags be battery driven so that power failures are not an issue. To ensure record keeping, the laptop needs to keep a log of activity, so when power is restored to the system it will update the server with any transactions that have been missed due to the outage.

#### *Scenario 4: Mobile Monitoring*

The patient has several mobile monitoring devices attached to him. Some of the devices are composite in that they perform more than one task. For instance, a device can monitor pulse and temperature at the same time, and then transmit the data to a central monitoring station. These miniaturized devices save the patient from feeling that he is wrapped in wires, and in general make him feel more comfortable. If the patient is in transit from one area to another for treatments, the mobile devices can still alert the medical staff of a problem while he is being moved in his wheelchair or trolley bed. As the patient approaches the service department, his electronic bracelet uploads his medical chart on to their monitoring workstation. If the assigned treatment doesn't match the patient, the staff member's PDA sounds an alarm, and the event is recorded on the health care server.

#### *Scenario 4 Analysis: Mobile Monitoring*

The technical staff must regularly complete an environment scan, pinpointing areas where there are poor or no communications because of physical barriers or equipment interference. For instance the scan may determine poor signal reception in the elevators, or in areas using high voltage equipment. The staff can then resolve these communication faults by adding additional transceivers, modifying equipment, and changing transmission bandwidth.

Furthermore as mobile equipment becomes dated, there may arise certain incompatibilities when mixing newer and older technologies. These issues can be resolved through the adoption of communication and interface standards for the mobile equipment as well as for the middleware. Yet there is always the possibility of incompatible equipment or random interference causing a communication fault. In this instance the network can add mobile alarms to the patient's bed and to the ambulatory trolley. These mobile alarms have their own transceiver with an audio/visual alert. The server pings these devices at a much higher rate, for instance 1 per minute. As soon as the device stops receiving pings from the server, it is programmed to turn on the alert, informing staff of the situation. This would help safeguard the patient since if the network loses contact with a critical patient while in transit, the trolley alert signal can notify the medical staff to take additional remedial precautions.

#### *Scenario 5: Visitors*

Each visitor is given an electronic tag that transmits a radio frequency ID. This tag serves as a geographic locator, and thereby informs the security staff of visitors in prohibited areas. The staff also have electronic tags or PDAs to show their location throughout the hospital, which helps in marshaling resources in case of an emergency. In addition to the GPL function, the signals emitted by electronic tags serve as code for opening electronic doors in secure areas. The hospital uses this function to secure prohibited areas from unauthorized access.

Tags can also be used for communication between the nurse's station and visitors in patients' rooms. For example, if visitors need to be reminded that their time allocation is up, or if there are other visitors who are waiting to see the patient, then the electronic tag can be activated to produce a warning beep.

#### *Scenario 5 Analysis: Visitors*

In practice the RFID performs exactly as specified - the difficulty is with the ingenuity of authorized and unauthorized visitors. Visitors have been known to keep their tags for future visits, and to enter unauthorized areas by leaving their tags behind and piggybacking through doors opened by the medical staff. To safeguard against trespass, theft, and malicious damage, management can modify how e-tags are used. For instance, management could take the step to embed e-tags into equipment and supplies, so that the resources have a built in RFID trigger for monitoring against theft (Ryan, 2002). A possible problem is that thieves can find and remove the e-tags on equipment, and thereby eliminate the deterrent value. Management can counter this by gluing the e-tags in inaccessible places to raise the bar to theft.

Concerning trespass, management can introduce motion monitoring devices that issue an e-tag challenge and wait for a transceiver response. For example if a motion detector issues a challenge to a potential intruder, and then does not receive an e-tag transmission, showing an appropriate authorization, it sounds an alarm and notifies the server of

the problem. Similarly at all hospital entrances, there are transceivers whose sole purpose is to monitor the traffic. These devices sound an alert if visitor e-tags or tagged equipment is taken from the hospital.

One drawback to this approach is that hospital staff may be concerned that the motion detector devices are intrusive and infringe on their privacy in the workplace, such as monitoring when they come and go, and whom they meet during breaks. In this case management will have to explain that the monitoring system only records exceptions to the rules, that is, unauthorized activity. The staff may still have concerns that management can at anytime record individual movements if it so chooses and thereby have a complete mapping of the movements, meetings, and whereabouts of the staff. This is an area which does not have any easy answers, and will have to be negotiated case by case.

### *Scenario 6: Patient Privacy and Information Security*

The patient expects information confidentiality, and the hospital is mandated to provide system security. Hospitals, like other institutions, face the threat of hackers attempting to infiltrate their network, causing damage and loss of confidential information. Mobile transmissions, with a broadcast range of hundreds of meters, potentially open up a new set of trapdoors for hackers. It makes sense for hackers to mount an attack through the unsophisticated e-tag, the weakest link in the communication chain. First and second generation e-tags have little or no encryption and the transceiver transmits on a simple command. Hackers could mimic the characteristics of an e-tag, and probe the back doors to the system for further weaknesses.

### *Scenario 6 Analysis*

The adoption of hardware and software security standards helps protect the mobile system from hackers. An example of this would be PDAs which have enough processing power and memory to be able to meet industry level encryption standards. Within a generation the e-tag transceiver will have computer chips that provide an adequate level of encryption. Furthermore, management can be quite proactive in employing security consultants to update the hospital's long range technical plan, and alert them to trapdoors in the system. The middleware can monitor the activity of e-tags and other devices looking for unusual or inconsistent transmission patterns, based on time of day, location, and type of service. It would act like a firewall, alerting staff and requesting permission to shut down rogue devices.

To create a more difficult environment for hackers the middleware has to continually monitor, filter, and update privilege levels on the network by changing codes and passwords of the electronic devices (Birman, 1996).

## **TECHNICAL ISSUES**

### *Middleware*

The more electronic tags, bracelets, PDAs, and devices with RFIDs that exist, the greater the resource requirements on the mobile system and middleware. In addition, the more tasks that the middleware has to perform, from tracking patients to opening doors, the greater the potential stress on the system. The design must be robust and have the ability to scale as new tasks and components are added. In order to safeguard against future incompatibilities, the hospital must use accepted industry standards for RFIDs, interface, and communications protocols. This ensures that the mobile system is able to perform an increasing number of tasks, and can scale to accept the new devices.

Table 1 describes the five critical management areas of this next generation of mobile middleware. These management areas have to handle traditional client server tasks, as well as the mobile services. In particular, the mobile middleware will perform non-stop monitoring and testing of the communications structure, and where necessary provide the compensatory services and enhancements needed for the e-tags, transceivers, PDAs, and other lightweight devices. Similarly, the middleware will use back-up equipment and fault tolerant service to secure the potentially permeable communications. To better understand the overall management services, the middleware can be divided into these five categories:

- Accounting Management
- Configuration Management

- Fault Management
- Performance Management
- Security Management

Table 1 describes these services in detail starting with Accounting Management, whose task is to track mobile devices and their characteristics. By knowing the device characteristics it can provide the necessary compensatory services to ensure appropriately formatted and secure transmissions. It also has the task of matching data found on the healthcare server against data stored on the patient’s bracelet. Configuration Management oversees the autodiscovery of devices and handles their plug and play compatibility, thus supporting network design optimization. Fault Management monitors network reliability and alerts the system to any communication interruption. Whenever possible this area automatically activates backup transceivers to remedy the problem. In addition to monitoring, Performance Management collects network statistics for planned upgrades and changes. Its second task is to balance network load by scheduling non critical data transfers to off peak times. Lastly, Security Management monitors and logs network activity by ID, time, and location. It also tracks login violations. It is easy to see that the tasks performed in these five middleware management areas are critical to the infrastructure of a sophisticated communications environment.

**Next Generation Wireless**

With the release of 802.11N specifications for the next generation wireless standard, some of these hospital scenarios are achievable in the near future. Table 2 provides a comparison between the current generation 802.11G and the proposed 802.11N (Wilson, 2004). This new industry standard shows how fast mobile technologies are changing, and underscores the rapid timeframe for management and technical planning.

Table 2 shows the established Wi-Fi 802.11G protocol and some of its most important features. Its speed, distance and relative security make it a very strong choice for today’s wireless network. By comparison 802.11N makes significant advances in bandwidth, distance and imperviousness to interference. Its security is strengthened with advanced encryption and the QoS is enhanced by using prioritized streaming of audio and video data. Overall, these features have the potential for replacing much of the wired infrastructure of the hospital environment.

**CONCLUSIONS**

It is just a matter of time before hospital management begins to take advantage of wireless technology. The mobile network scenarios depicted in this paper spell out patient care, management and technical problems that a hospital may face. The paper uses QoS guidelines for managing the hospital’s transition. Table 3 summarizes this approach to planning and design by using the three categories of QoS Patient Care, QoS Management, and QoS Technical services.

<b>Accounting Management</b>	
<ul style="list-style-type: none"> <li>• Electronic data distribution</li> <li>• Inventory tracking</li> <li>• Data comparison</li> <li>• Compensatory Services</li> </ul>	<ul style="list-style-type: none"> <li>• Update e-tags, PDAs, and electronic bracelet</li> <li>• Tracking of mobile device and e-tags</li> <li>• Matching patient data on bracelet against health server</li> <li>• Providing encryption, bandwidth adjustments, and formatting services for mobile devices</li> </ul>
<b>Configuration Management</b>	
<ul style="list-style-type: none"> <li>• Autodiscovery/mapping</li> <li>• Plug and play configuration</li> <li>• Change tracking</li> <li>• Network design optimization</li> </ul>	<ul style="list-style-type: none"> <li>• Locating mobile devices during sign-on</li> <li>• Incorporating new hardware and software</li> <li>• Monitoring change in the network</li> <li>• Planning for performance upgrades</li> </ul>
<b>Fault Management</b>	
<ul style="list-style-type: none"> <li>• Alarm notification</li> </ul>	<ul style="list-style-type: none"> <li>• Alerting staff and control hardware of faults</li> </ul>

<ul style="list-style-type: none"> <li>Alarm correction</li> <li>Disaster recovery</li> <li>Remote node reconfiguration</li> </ul>	<ul style="list-style-type: none"> <li>Switching bandwidth and services to remedy problems</li> <li>Logging activities, switching to redundant equipment</li> <li>Upgrading and modifying mobile devices</li> </ul>
<b>Performance Management</b>	
<ul style="list-style-type: none"> <li>Capacity planning</li> <li>Event scheduling</li> <li>Protocol analysis</li> <li>Remote monitoring</li> <li>Trouble ticketing</li> </ul>	<ul style="list-style-type: none"> <li>Tracking bandwidth and throughput</li> <li>Balancing communication loads of scheduled transmissions</li> <li>Sniffing for errors and faults</li> <li>Pinging network equipment for failure</li> <li>Resolving network problems and replacing mobile nodes</li> </ul>
<b>Security Management</b>	
<ul style="list-style-type: none"> <li>Data backup</li> <li>Off hour access logging</li> <li>Password usage tracking</li> <li>Violation logging</li> <li>Firewall filtering services</li> </ul>	<ul style="list-style-type: none"> <li>Securing data and configuration information</li> <li>Monitoring device sign-on by time and location</li> <li>Monitoring device signatures and logins</li> <li>Logging mobile violations</li> <li>Creating DMZ for screening against foreign activity</li> </ul>

Table 1: Mobile Middleware Services.

<b>Protocols</b>	Wi-Fi 802.11	802.11N
<b>Speed</b>	54 Mb/sec	200 Mb/sec
<b>Distance</b>	100 m	250 m
<b>Bandwidth</b>	2.4 GHz	5.6 GHz
<b>Audio-Video Streaming</b>	No	Yes, QoS Prioritizing
<b>Security</b>	Subset of Advanced Encryption Standard	Advanced Encryption Standard

Table 2: Wireless Protocols.

These three categories were chosen to emphasize the multiple perspectives needed in the planning and design process. QoS Patient Care focuses directly on the well-being of the patient. It has a broad impact range, from the delivery of health services to the protection of confidential health information. The QoS Management category deals with administrative issues such as policy/standards, timely billing and scheduling. It also involves the organizational dimension of workflow and collaboration. Finally the QoS Technical category addresses system issues of performance monitoring, upgrades, and security.

Overall, these three QoS categories are the foundation for conceptualizing the planning, design, and management of hospital environments. These categories can equally well serve as the benchmark for evaluating or gauging the success of the transition to new technology (Killijian, 2001).

<b>QoS Patient Care</b>	<b>QoS Management</b>	<b>QoS Technical</b>
Quality Delivery of Care	Collaboration	24/7 Mobile Computing
Privacy	Security Procedures	Middleware Security Services

Informed Participation Integrated Patient Monitoring	Policy / Standards Supervised care Timely Billing	Performance Monitoring System Scaling / Upgrades
Safety Checks for Medications and Procedures	Scheduling and Workflow	Training Problem Resolution

Table 3: Planning and Design Issues.

Hospitals, like most business environments, will be making the transition to the next generation of wireless computing in the near future. If Table 3's guidelines are read broadly, then the criteria are spelled out for successful implementation in most settings. The reason for this is that the QoS wireless concepts are equally valid for the implementation of business solutions across many different business sectors. The QoS wireless techniques and guidelines are in fact driven by the needs and expectations of its business stakeholders.

## REFERENCES

- Adis, W. (2003). Quality of Service Middleware, Industrial Management & Data Systems (IMDS), Vol. 103 No. 1, Emerald, MOB UP Limited.
- Ancona, M. et al. (2000). Mobile Computing in a Hospital: the WARD-IN-HAND Project, Proceedings of the 2000 ACM Symposium on Applied Computing, Como, Italy, pp. 554 - 556.
- Banavar, G. et al., (2000). Challenges: an Application Model for Pervasive Computing, Proceeding of MobiCom2000, August, pp. 266-274.
- Bardram, J. and Christensen, H. Middleware for Pervasive Healthcare, [www.cs.arizona.edu/mmc/24%20Bardram.pdf](http://www.cs.arizona.edu/mmc/24%20Bardram.pdf).
- Birman, K. (1996). Building Secure and Reliable Network Applications, Manning Publications, Greenwich, CT.
- Brewin, B. (2003). Improved Care and Privacy Protection are major goals, COMPUTERWORLD, June 05, 2003.
- Campbell, A. (1997). Mobicore: QoS-aware Middleware for Mobile Multimedia Communications, Proceeding of IFIP 7th International Conference on High Performance Networking, April 1997.
- Capra, L., Emmerich, W., and Mascolo, C. (2001). Middleware for Mobile Computing: Awareness vs. Transparency, Proceedings of the 8th Workshop on Hot Topics in Operating Systems, Schloss-Elmau, Germany, May 2001, pp. 142.
- Coulson, G. et al. (2002). The Design of a Configurable and Reconfigurable Middleware Platform, Distributed Computing, Vol. 15, Number 2, April 2002, pp. 109-126.
- Doug P. (2002). Medication match application assures correct drugs are administered to the correct patients, [http://www.symbol.com/news/pr\\_health\\_hospital.html](http://www.symbol.com/news/pr_health_hospital.html).
- Esler, M. et al. (1999). Next Century Challenges: Data-Centric Networking for Invisible Computing, Proceeding of MobiCom'99, August 1999, pp. 256-262.
- Evanshwick, C., Swan, J., and Smith, P. (1995). Hospital Services and Organizational Theory, [http://depts.washington.edu/chmr/public/p0011/p0011\\_executivesummary.pdf](http://depts.washington.edu/chmr/public/p0011/p0011_executivesummary.pdf).
- Finkenzeller, K. (2003). The RFID Handbook, John Wiley & Sons, NY.
- Goldberg, A. (1997). Virtual Teams, Virtual Projects = Real Learning, Proceedings of the 1997 ACM Symposium on Applied Computing, San Jose, California, pp. 1.

- Killijian, M. et al. (2001). Towards Group Communication for Mobile Participants, Proceedings of Principles of Mobile Computing (POMC). Newport, Rhode Island, pp. 75–82.
- Mohan, C. et al. (2000). Evolution of Groupware for Business Applications: A Database Perspective on Lotus Domino/Notes, Proceeding of the 26th VLDB Conference, September 2000, pp. 684–687.
- Morton, S. and Bukhres, O. (1997). Utilizing Mobile Computing in the Wishard Memorial Hospital Ambulatory Service, Proceedings of the 1997 ACM Symposium on Applied Computing, San Jose, California, pp. 287 - 294.
- Morton, S. and Bukhres, O. (1997). Mobile Computing in Military Ambulatory Care, The 10th IEEE Symposium on Computer-Based Medical Systems (CBMS'97).
- MosquitoNet (2003). The Mobile Computing Group at Stanford University, <http://mosquitonet.stanford.edu/index.html>.
- Object Management Group. (2000). Fault Tolerant CORBA (adopted specification), OMG Technical Committee, March 2000.
- Rohrer, C. (2003). Mobile Computing Improves Patient Care, Integrated Solutions, November 2003, [http://www.integratedsolutionsmag.com/Articles/2003\\_11/031107.htm](http://www.integratedsolutionsmag.com/Articles/2003_11/031107.htm).
- Ryan, C. et al. (2002). Evaluating Policies and Mechanisms for Supporting Embedded, Real-Time Applications with CORBA 3.0, Proceeding of the IEEE Real-Time Technology and Applications Symposium, June 2000.
- Want, R. and Russell, D. (2000). Ubiquitous Electronic Tagging, IEEE Distributed Systems Online, Vol. 1 No. 2, September 2000.
- Wilson, James M. (2004) The Next Generation of Wireless LAN Emerges with 802.11n, <http://www.intel.com/technology/magazine/communications/wi08041.pdf>