

## Wireless Solutions in Healthcare: Expanding 'Point of Care' Practices and Services in Hospitals

The U.S. healthcare industry is presently undergoing a significant shift in its approach and use of next-generation information processing technologies that will put more emphasis on secure and reliable wireless networks as a means to improve patient relationships, provide more 'point-of-care' access to critical information, and reduce the possibility of medical errors.

At the center of this shift are 802.11 wireless technologies (WiFi) which are being used by an increasing number of hospitals across the country to extend current wired systems and provide remote access to critical patient data by doctors, nurses and clinicians within a hospital environment. Wireless networks are also being used by healthcare providers to review and input information directly at a patient's bedside, provide secure point-of-care access to patient information, and offer collaborative links to other healthcare providers within a hospital environment.

These same systems are being used to provide public wireless access to hospital patients, hospital visitors, contractors, and suppliers, and to provide a managed wireless pipeline to the Internet without jeopardizing sensitive hospital records and files. Wireless networks can also be used to provide a way for patients to take a proactive role in the medical process by reviewing personal records and information at bedside, validating drug interaction data, and consider treatment options – all in real-time with the assistance of a qualified healthcare provider.<sup>1</sup>

There are a number of factors fueling the adoption of secure and reliable 802.11 wireless technologies in the \$1.5 trillion healthcare industry. These include:

- An increasing demand by doctors, nurses and other healthcare providers to improve the quality and efficiency of patient care and to extend critical information links directly and immediately to the patient. These efforts range from improved front office data collection and information 'triage' operations to the use of collaborative wireless networks and wireless voice-over-IP (VoIP) systems within operating rooms and critical patient care areas of a hospital;
- A strong effort to extend current *wired* hospital information systems to healthcare personnel anywhere within a hospital environment through the use of wireless computers-on-wheels (COWs), wireless-enabled handheld and notebook PCs, and other wireless-enabled devices. The idea is to improve relationships with patients and reduce the possibility of errors by deploying wireless tools that enable doctors and nurses to input critical data on the spot and offer immediate and reliable access to patient information and records;
- The development of a new breed of wireless controllers and intuitive wireless access points (APs) that can be used to quickly and effectively deploy 802.11 wireless solutions throughout a hospital, and can easily be configured to control and manage the use of that wireless network by authorized personnel;

---

<sup>1</sup> WIRELESS IN HEALTHCARE © 2004, The FocalPoint Group, LLC ([www.thefpgroup.com](http://www.thefpgroup.com))

- A rising demand for wireless networks and management infrastructures that are 'future-proof' in terms of scalability and can keep pace with the evolving information systems demands of most healthcare organizations;
- The need for wireless solutions that can seamlessly and cost-effectively integrate with existing back-end infrastructure and security processes and procedures;
- Advances in wireless controller technology that offer such features as seamless mobility across hospital networks and subnets, role-based access control and policy enforcement, real-time monitoring and intrusion detection, and enterprise-level IPSec data encryption and protection;
- Improved bandwidth management, Quality of Service (QoS), and multi-level access control that allow hospitals to securely manage wireless users within a specific RF environment and control access to sensitive and non-sensitive information.

### **Selecting a Wireless Healthcare Solution**

Hospital administrators share many of the same basic concerns as traditional enterprise users when it comes to evaluating and selecting a controller as the hub of a wireless network. These concerns include reliability, ease of use, security and scalability. However, hospitals are especially focused on such issues as access control, user management, and user permissions in evaluating and selecting the right wireless controller solution because they routinely deal with highly-sensitive medical information and are under constant scrutiny by government agencies due to HIPAA regulations<sup>2</sup>. Bandwidth management, and the ability to dynamically 'throttle' and adjust user bandwidth, is also a concern given the wide range of information and graphics-heavy content that may flow through a hospital wireless network environment.

Healthcare providers have other concerns when it comes to selecting and implementing the most effective wireless solution. At Palmetto Health, a not-for-profit healthcare collaborative in South Carolina, for example, administrators wanted a system that could provide strong security to comply with current and evolving HIPAA privacy regulations, but also wanted a system that would provide consistent and uncompromising wireless coverage throughout each of the group's three hospitals. The Palmetto staff also looked for a solution that could support existing clinical applications that allow nurses to create and access patient records and files from any one of the 1,300 beds in the hospital collaborative.

The Palmetto Health wireless solution presently consists of a Bluesocket® BlueSecure™ 2100 and BlueSecure 5000 Controller, and more than 400 Cisco Systems, Inc. wireless access points installed throughout the three hospitals in the Palmetto Health group.

Selecting a wireless solution that can be easily integrated and is compatible with existing hospital administrative and clinical systems is also an important issue in healthcare. When Winchester Hospital, a 200-bed community facility located just outside Boston, MA, started investigating wireless network solutions, a primary objective was to find a network that would be able to easily extend an existing desk-bound patient assessment system out to nurses and physicians anywhere within the hospital. The hospital worked with a local systems integrator to install a wireless network that is secured and managed by a BlueSecure 2100 Controller.

Winchester Hospital is now looking at expanding the use of its wireless network and clinical documentation system from simple patient assessments to real-time electronic medication

---

<sup>2</sup> The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

tracking and a Bedside Medication Verification (BMV) system that will make use of scanners and coded patient wrist bands.

### **Deploying a Wireless Healthcare Solution**

While most healthcare organizations would like to include a test or pilot phase as part of its wireless plan, this is not always possible given the intense level of activities common to most hospitals, as well as the limited IT resources of many smaller healthcare organizations and groups. As a result, many wireless deployments occur virtually overnight and are immediately put into service to support day-to-day hospital operations. It is for this reason that it is important to select a wireless solution that is easily installed, configured, launched and incorporated into a hospital's existing network infrastructure.

One of the best ways to ensure compatibility with existing networks and provide simple and secure access is to deploy wireless controllers that offer connection via an IPSec virtual private network (VPN) and provide LDAP authentication for user log in. The controller should be able to handle all of the data encryption requirements, provide *on-the-fly* multi-level authentication, and manage the flow and prioritization of wireless traffic.

Making the system easy to use from an end-user perspective is also an important issue in healthcare wireless IT, since the end-user mix in a typical hospital is so diverse and primarily focused on patient care as opposed to technology issues. Many hospitals include initial and continuing education and training programs as part of their wireless launch and deployment initiatives. These programs usually include some level of classroom training in the most effective use of a wireless network, and are supplemented with frequent 'refresher' courses that bring healthcare providers up to speed on the latest internal network policy changes and available applications.

### **Expanding and Enhancing a Healthcare Wireless Solution**

While the most obvious benefit of a wireless network within a healthcare environment is rapid 'point-of-care' access to critical patient information, hospitals also rely on wireless solutions as a framework for the introduction of additional technologies and services. One of these technologies is voice over IP (VoIP) communications, which allows doctors, nurses and others to talk and consult with one another through the hospital's 802.11 wireless networks. A number of hospitals are using wireless client devices such as the Vocera Communications, Inc. WiFi communications badge to provide a hands-free audio bridge to healthcare workers anywhere within a wireless network. VoIP telephone systems are also being used by hospitals across the country with great success and at a substantial cost savings.

Hospitals are also making use of the robust user access and authentication capabilities built into controllers, like those in the Bluesocket BlueSecure series, to launch public-access wireless systems and establish secure wireless 'hotspots' that can be used by hospital patients, visitors and suppliers. The wireless controllers manage and restrict access among these users, prevent unauthorized access to sensitive areas of the network, and provide a reliable route directly out to the Internet. Most of these systems are presently positioned as a no-cost benefit to enhance patient relations, but can also easily be configured as a *pay-as-you-go* option to provide additional revenue for hospitals and other healthcare organizations.

### **Summary: A Positive Prognosis for Wireless in Healthcare**

Hospitals and other healthcare organizations have been reluctant to aggressively adopt wireless solutions, primarily because of concerns for security, reliability and compatibility with existing medical applications. However, these concerns are quickly mitigated with the introduction of a newer generation of wireless controllers that are specifically designed for open systems

interoperability, secure access throughout a network and sub-networks (as demonstrated by Bluesocket's patent-pending Secure Mobility® technology), flexible role-based access control and policy enforcement, strong data encryption intrusion detection capabilities, and scalable bandwidth management. Hospitals are also attracted to wireless because of its ability to act as a communications backbone for other evolving technologies, such as VoIP and radio frequency ID (RFID) tagging systems.

However, there are distinct differences between generic wireless gateways, or switches, and true full-featured wireless controllers. Some of the major differences center on the security, management and scalability of these systems, as well as their ability to seamlessly integrate with existing wired and wireless networks and provide a reliable platform for current and future medical applications. All of these issues should be considered as hospitals investigate and evaluate wireless alternatives and look for technology that can deliver a cost-effective and capable solution.

---

The 'Wireless Solutions in Healthcare: Expanding 'Point of Care' Practices and Services in Hospitals' BluePaper was produced by *Shoreline Research* for Bluesocket, Inc., a leader in providing secure and reliable wireless solutions for healthcare and other enterprise-class applications. The company's **BlueSecure™** Controllers (BSC 400, 1100, 2100 and 5000) are presently installed in hospitals and Fortune 1000 companies worldwide. Hospitals that presently rely on BlueSecure solutions include Mount Carmel Health, one of the largest healthcare systems in the state of Ohio; and Winchester Hospital, an award-winning medical facility located just outside Boston.

All BlueSecure Controllers feature Bluesocket's **Secure Mobility®** technology for wireless data and voice applications, and provide reliable, policy-based WLAN security and management tools that can be easily deployed within any organization. This technology is designed to work with Bluesocket's **BlueView™ Management System**, which provides centralized configuration and maintenance, policy-management, and monitoring capabilities for BlueSecure Controllers and wireless access points (APs).

BlueSecure networks can be enhanced with the addition of the company's **BlueSecure Intrusion Protection System™ (IPS)**, available in both centralized and non-centralized versions. The IPS monitors activities within a wireless network and can protect that network against accidental or deliberate security breaches and the introduction of rogue devices. The system will also alert network administrators to potential WLAN threats and automatically block or disable unauthorized devices and non-authenticated users. The **BlueSecure Centralized IPS™** is a complete wireless intrusion detection and prevention system, consisting of centralized phased array 802.11a/b/g RF sensor and management software built-into the BlueView Management System.

To complete the wireless network picture, Bluesocket also offers its **BlueSecure Access Point 1500**, which is a next-generation "thin" AP that works in conjunction with BlueSecure Controllers for enterprise wireless LAN (WLAN) deployments. The BlueSecure Access Point 1500 features dual radios supporting 802.11 a/b/g technologies with fixed omni-directional antennas.

For more information regarding Bluesocket's complete WLAN solution suite, visit the company's Website: [www.bluesocket.com](http://www.bluesocket.com).



Shoreline Research