



register online @ www.networkingplus.co.uk to receive your free monthly copy

NHS networks



Doctors and other medical staff have much to gain from using portable information devices – but such hardware will be of little use without a reliable wireless network to provide the required connectivity

Carry on wirelessly Doctor!

The NHS is under constant pressure to save money whilst improving services. If you require flexibility and mobility in a hospital then there's only one suitable prescription: a wireless network. But careful treatment is required, warns NICK BOOTH



In his account of life as a junior hospital doctor, *Trust Me I'm a Junior Doctor*, Max Pemberton gave an insider's account of the unreported problems that the NHS suffers from. While official NHS studies always identify the need for improved communication, flexibility, scalability, and security in hospital ICT systems, Pemberton identified other areas of working life that needed improvement. Among the issues he complains of are the impossibility of reading anything written by a senior consultant, equipment going AWOL, the frequent loss of vital X-rays, and general communications breakdowns.

Thankfully, all these technical problems can be addressed by a skillful insertion of a Wi-Fi network.

Despite the budget cuts, the NHS is expected to increase its efficiency through greater fluidity of information, with the IT fitting around the way hospital staff work. That means automation of patient records and constant availability of information to staff as they move around. Wi-Fi is a tremendous benefit to the NHS, which has massive organisational and information needs, a transient and mobile workforce, an even more transient clientele (the patients), and impossibly high standards of security and hygiene to maintain.

But although Wi-Fi can be a potent productivity tool if installed correctly, it can also be a big white elephant if the network manager doesn't tackle the many ominous challenges that can occur.

Plan for success

The first logistical challenge is in planning. This is where NHS managers find themselves hidebound by regulations that aren't found in the private sector, according to Graeme Woodcock, Motorola Solutions' Healthcare manager EMEA. He says that in the health sector, IT investments must go through the official government tender process and it's often the cheapest wireless infrastructure system that gets the nod. But the lowest purchase price doesn't mean it'll provide the best environment for the organisation, warns Woodcock.

Even with the tender process "simplifying" matters, making the business case for a WLAN in the public

sector can be extremely challenging, adds Adam Conway, product management VP at Aerohive. "It's hard to determine how much kit you'll need, let alone what it will cost. In most cases, it's more than just the cost of the access points – it's a controller and management platform too."

Making incorrect estimations can be costly. You can mitigate such costing disasters by choosing a vendor that offers free, no-obligation Wi-Fi planning tools. When you're deeper into the tender process, it's a good idea to ask wireless network vendors to list all the components you will need. This will give a bottom line comparison of your technology options and help you avoid hidden pricing elements, such as paying for feature-by-feature licensing.



Creating a seamless wireless network in Aberdeen Royal Infirmary meant dealing with a wide variety of building materials, including Cumberland block, sandstone, and even granite

But network managers need to keep an eye on the future. "Budget pressures are forcing the NHS to take a short term view and neglect their future-proofing responsibilities," says Woodcock. He says that the IT managers are partly to blame as they only demand today's functionality without taking into consideration any potential upcoming needs. You may want data today, but if you plan in advance for voice, critical security, or location services, you can save a lot of money, he advises.

As a result of this short-sightedness, many find that they are held back by an inflexible wireless infrastructure when

they get further down the line. "It makes the upgrading process logistically difficult and very costly," says Woodcock.

Warding off problems

Hospitals can provide particularly challenging environments for wireless network deployments. For instance, when service provider Capita installed a 1,400 user WLAN in Aberdeen Royal Infirmary for NHS Grampian, the hospital building materials proved to be a major concern. They ranged from 'wafer thin' pre-fab walls through to Cumberland block, sandstone, timber

frames, and even granite. Installers therefore needed to plan for varying degrees of permeability.

There's also the issue of what happens when room usage changes. "If a ward becomes an office, or vice versa, you need a system that you can get up and running quickly, because you can't afford to keep a ward closed for too long," says Paul Allen, network manager at NHS Grampian. He says that this is where the thoroughness that goes into planning and surveying the network will pay off.

But it's a sizeable investment, both in terms of time and money. With the typical hospital campus being spread out over a huge area, employing an engineer to map out every inch of every corridor, ward and office in the entire hospital would take days or even weeks. Meru Networks, however, claims it can automate the planning process, making the mapping of the network the work of hours, rather than days. It does this through a network management system that allows the network manager to integrate an architectural blueprint of the hospital building.

However, others believe that his kind of tool just can't replace an on-site assessment. Ben Wilson, the UK country manager for networking equipment vendor Xirrus, says: "The only way to get a complete coverage report is by conducting a thorough survey." By which he means going out and slogging around the entire campus on foot with a clipboard and some measuring instruments.

The other key choice, which also has a direct bearing on the planning phase of the WLAN, is what network topology is best for the given situation.



Taking control

Meru has developed software that unifies all the separate single cells of a network into one large virtual cell. It says that the benefit of this is a network that promises to be less prone to drop out – a big problem for those walking between cells who could be midway through some work that a disruption will destroy. For example, hospitals use COWs (computers on wheels) connected by Wi-Fi that doctors and nurses trundle around the wards to allow professionals to access instant data, such as patient details, X-rays, and drug information. And with more portable devices, like PDAs and smartphones, being used by medical staff, it's a problem that's only likely to get worse.

An alternative to this is a network where the intelligence is distributed. Xirus' Wilson recommends that network managers should avoid any system with a centralised controller unit and dumb access points – especially in a hospital where the geographical spread means that each point on the network will be even further away from the centralised control than in normal office networks. He says that Wi-Fi networks that have centralised control are more likely to be subject to delay, since every communication by a network access point with every mobile device has to be relayed back to the central controller. This not only causes latency on the network but creates a processing bottleneck at the controller.

By giving each network access control unit its own intelligence, Xirus claims it has massively sped-up Wi-Fi communications with latencies of below 40 milliseconds.

But speed is not the only attraction. By giving the access points more processing power, the company claims it can pack in more broadcasting capacity in each one. The difference, according to Wilson, is that less devices need to be cabled-up to provide the same amount of coverage.

"At Alder Hey, we only had to install 200 access points. The alternative proposal involved the installation of a thousand access points," he says. "So we saved on 800 cable runs and 800 fewer devices have to be taken care of by the network manager." However, the trade-off for this is that each of these access points is more expensive than centralised-intelligence alternatives.

Protecting your assets

Installation and management costs aside, security is one of the biggest concerns in a hospital environment. And the problem here is that security is often obstructive to end users. But the protection of confidential patient data is of paramount importance to the healthcare sector. "When data is transmitted through a wireless network, management must be 100 per cent confident that that data remains secure," says Motorola's Woodcock. "There are no shortcuts to wireless security and all possible routes to attack must be considered and covered."

Motorola's *AirDefense* kit aims to secure the provider's wireless airspace by eliminating rogue devices. It does this by continuously monitoring hospitals' wireless networks and looking for unauthorised access points, improper configurations, malicious hacking attempts, and network performance degradation.

But this should be achievable without off-putting strict and counter productive security systems getting in the way of work, says Andy Cooper, HP's networking and wireless technical consultant. Unlike other applications, Wi-Fi security protocols are transparent to the end-user through client pre-configuration. Utilising 802.1X and WPA2, client data is authenticated and encrypted across the air. Different access rights can be granted, depending on who the user is. Separate SSIDs can create multiple logical networks. For instance, doctors and nurses can be given a clinical 'network' and the requisite high level of access to get at patient data, while support staff could be restricted to hospital administrative information, and patients to internet access only.

Security doesn't have to just cover the data, it's also possible to leverage wireless networks to secure physical assets too. At Bristol North Hospital, HP has installed a tracking system so that Wi-Fi can be used to locate equipment. It's common in hospitals for staff to spend hours phoning around

"Budget pressures are forcing the NHS to take a short term view and neglect their future-proofing responsibilities"

*Graeme Woodcock,
Healthcare manager EMEA,
Motorola Solutions*



NHS Newham cuts costs with controller-less wireless system

With a patient base of 330,000 patients, NHS Newham in London needed to improve its quality of service, modernise, and offer better support to its workforce.

“The mobilisation of our healthcare professionals ensures patients have access to the right expertise on-demand,” explains Charles McNair, director of Resources at NHS Newham. “It is our job to ensure staff can access and update a patient’s records, or schedule a medical procedure, from any location, both securely and in real-time.” This all had to be done within a limited budget, putting pressure on to drive down both the capital and operational costs of the system.

With staff roaming between sites, it was important that the IT network at each location could provide seamless connectivity along with easy maintenance. Authentication has to be fast, with easy access to data without impacting on Patient Identifiable Data (PID) security regulations.

Newham’s IT partners, Swiftpath and Networks First, assessed wireless vendors and then chose Aerohive Networks. The deployment saw a wireless LAN installed at NHS Newham’s headquarters and two of its polyclinics in the borough. The solution will also be rolled out to the remaining 20 sites as business demands dictate.

Paul Wrench, ICT network administrator at NHS Newham, led the procurement process and reckons that Aerohive stood “head and shoulders” above the competitors, primarily because of its controller-less system. “The architecture, intuitive access points, and central administration platform demonstrates this technology is designed

simply to work, and doesn’t require tweaking or reconfiguration,” he says.

Removing the need for controllers at each site had both financial and operational benefits. “It simply wasn’t viable for us to deploy a controller and redundant controller at each site; nor, due to the critical nature of a healthcare environment, were we able to consider centralising controllers,” adds Wrench. Minimising the onsite infrastructure also helped to reduce the number of points of failure in the network.

NHS Newham has benefited from a wireless network that doesn’t require “tweaking or reconfiguration”



the wards in an attempt to locate, for example, an urgently needed blood infusion pump. Using the new system, vital equipment can be located on screen immediately and a porter dispatched to collect it.

The prognosis is clear. Wireless networks have a lot to offer and in these financially challenging times, hospitals owe it to themselves to carefully invest in future-proof Wi-Fi technology to obtain a healthy outcome. ■