United bristol healthcare trust

Business

Improving patient care with secure wireless systems for UBHT..

. United Bristol Healthcare Trust (UBHT) has been installing small, closely confined wireless systems since 2003 to provide specific services for clinicians on the wards and to overcome the challenges of providing temporary connectivity between different buildings. The Trust’s objective, however, has always been to implement wireless solutions on a much greater scale throughout its nine hospitals – but only once a robust, scaleable security infrastructure had been implemented. Working with Red-M and security specialist Peapod is providing the Trust with the way forward in wireless. A challenging environment Employing some 7, 000 staff across nine different hospitals, United Bristol Healthcare NHS Trust (UBHT) is one of the largest acute trusts in the country as well as being a major teaching and research centre for the South West. In 2005, the Trust had over 110, 000 inpatient and day case admissions.

Dave Oatway is the Trust’s Computer Services Manager responsible for all operational IT services including support for 4, 000 users and the introduction of new technologies and applications to meet clinical needs. His involvement with wireless dates back to 2003 when a number of small pilot systems were installed to overcome specific problems. In common with many other Trusts, UBHT is spread across several buildings and staff are quite frequently relocated from one building to another, often on a temporary basis. Located in the centre of Bristol adds to the challenge of providing connectivity, as to run traditional cables across, for example, a busy road is expensive and disruptive. Thus, one of the Trust’s first wireless installations was a temporary system providing connectivity for a small group of people who had relocated to a different building.

Another installation saw wireless being used within a ward to enable hematologists to use laptops – equipped with a barcode scanner – to scan patients' wristbands to check blood groups prior to treatment. With this type of application, data is available immediately on the server, avoiding any problems of lag time, for any member of staff or department that has a role in the care of that patient. Seeking a long-term solution for wireless security As part of the Trust's implementation of the National Programme for IT, there is a commitment to utilize wireless throughout all the hospitals when clinical need justifies the use of the technology. UBHT has been working with IT security specialists, Peapod, for a decade. Early in 2005, Dave Oatway turned to Peapod for advice on identifying a robust approach to wireless which would offer guaranteed security and a foundation upon which wireless installations could be rolled out. Peapod introduced him to Red-M, who provided a demonstration of their proposed system and carried out a survey of the UBHT site, providing a report on what they had found and his comments are highlighted on the front.

The system proposed by Red-M was designed to provide the Trust with a ' starter solution' which could be quickly and easily expanded as the number of wireless installations increased and budget became available. In May 2005, Red-M installed a desktop server and two probes; the remaining eighteen probes were installed by the Trust's own staff. Red-M's CounterMeasures software, which prevents unauthorisedconversations, was also installed. Wireless now and in the future Since the Red-M solution was implemented, Dave Oatway and his team have been able to detect when and where people are using wireless equipment and devices, as well as being able to automatically stop any unauthorized attempts to attach to the network. In addition, the system provides details – presented as graphs – of hot spots linked to the time of day, which will enable the Trust to identify and plan for future wireless installations. The Trust's growing number of wireless systems, which are viewed as being complementary to traditional cabling solutions, are predominantly being used in ward environments and in a theatre suite to provide a fast and efficient way of entering and retrieving patient data.

Wireless telephone and the use of wireless to remotely monitor seriously patients on the wards if there are insufficient beds in the Intensive Care Unit are also being considered. A number of significant national projects are also being progressed, including PACS, a digital archiving and retrieval system for x-rays. With the plan to roll out this major new system on wireless, combined with the need to meet government timelines for this service, the need for a robust infrastructure and stringent security is of paramount importance. Dave Oatway is enthusiastic about the benefits and exciting applications that wireless can deliver within a hospital environment, but is keen to stress that patient data confidentiality can only be assured with the installation of a robust infrastructure, such as that recommended by Peapod and delivered by Red-M. “ With cabling there are obviously clearly defined boundaries and it is much easier to limit the risk of unauthorised access. At Bristol, we have thousands of people walking around our buildings every single day.

Although the vast majority will be law-abiding, we have to protect against threats that we don’t even know are out there. The Red-M solution enables us to do this.”