Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Mitigating the risks posed by wireless devices in the healthcare industry

Healthcare organisations are reaping value from the ability to use wireless devices but it is essential to ensure Wi-Fi and networks are secure to avoid security risks, according to Wavelink.

Paul Craven, Health Practice lead, Wavelink, said, “Wireless networks have now reached speeds where it makes sense to rely on them for healthcare applications. Untethering healthcare providers from wired devices lets them provide a better quality of service and cuts down on the time spent on administrative tasks. This means frontline providers can spend more time with patients and less time on paperwork, for example.”

Some healthcare facilities are encouraging employees, including professionals like doctors and nurses, to bring their own devices (BYOD). Others have mandated which wireless medical devices should be used or have brought in reliable, high-quality tools designed for their environment, such as the Spectralink PIVOT, to communicate on the job. And in some organisations, different departments within the hospital make different decisions regarding which devices to adopt. All of these different situations can lead to chaos and increase the risk of security breaches.

Paul Craven said, “Technology decision-makers in healthcare organisations must use risk management techniques and thoroughly test each device that will be deployed on the Wi-Fi network. If any of the devices cannot meet minimal security requirements, they need to be identified and rectified.”

There are three key considerations for healthcare organisations looking to implement wireless medical devices:

1. **Confidentiality**. Since medical devices can access patient information, it is essential to ensure confidentiality. This means ensuring unauthorised people cannot access patient data via BYOD devices or other wireless devices.

2. **Interference**. Wireless networks can be subject to interference from a myriad of other devices and networks. It is essential to thoroughly test the network and ensure potential sources of interference are removed or mitigated. This is particularly true when it comes to lifesaving wireless devices where interference can have catastrophic consequences.

Managing interference also includes considering the other devices that may come into the hospital. This can include guest devices on the facility’s network as well as devices using public networks such as those used by patients or visitors.

3. **Policy**. Healthcare organisations need to understand and comply with federal, state and local policies regarding the use of wireless medical devices. This includes everything from federal privacy legislation to state government regulations on the use of Wi-Fi-enabled devices that can interfere with wired medical equipment.

Paul Craven said, “Healthcare organisations should consider using industry-specific mobile devices that are easier to manage for healthcare applications and provide better performance and security as well as a wireless network that delivers a better patient experience coupled with uninterrupted connectivity.”

About Wavelink
Wavelink specialises in the supply, marketing and support of a range of leading edge Enterprise Mobility and UC Solutions. Wavelink distributes a range of products from Spectralink, Fortinet, Extreme Networks, COBS, Digium, Polycom and Purple WiFi. For more information please contact Wavelink on 1300 147 000.