Securing the connected hospital: making strides in patient care

By Paul Williams

10 Aug 2016

The internet of things (IoT) and pervasive connectivity are changing the risk profile of hospitals, but simultaneously present improved productivity and patient care opportunities.

Completely digital process

In the hospital of the future, patients will be tagged and tracked from admission to discharge. Healthcare professionals will have access to all patient histories and treatment records on mobile and smart devices, patients may have personal online portals containing their treatment records, medication and medical advice, biometric identification may be used to bypass lengthy form completions and provide personal information in the case of an emergency, and wearable devices will notify nurses and doctors of the slightest changes in a patient's vital signs instantly.

South African hospitals are already coming closer to this scenario, with private healthcare facilities digitising records, issuing doctors with mobile devices for patient information on the move, and IoT-enabled medical devices and patient monitors already in use.

Secure ecosystem

These advances bring new risks to the fore: hackers could access and misuse confidential patient information or shut down hospital systems, while ransomware could render patient records useless.

By integrating all connected systems – from devices, to patient admission and management, to connected medical equipment and doctors' rooms – into a secure ecosystem, hospitals are able to protect patient information and secure their internal systems, which reduces risks such as fines, lawsuits and reputational damage.

This layer of security also allows for improved operational efficiency, cost management, risk analysis and customer experience. By implementing highly secure digital patient management systems, hospitals can confidently use the same verified patient data across admissions, X-rays, lab tests and more, so reducing the number of times patients must fill in forms and ultimately improving patient experience.

In addition, secure triangulated wi-fi networks, RFID tagging and scanners, hospitals can control pharmaceuticals from prescription to final dose, ensuring patient compliance, patient tracking, health record tracking, reducing the risk of errors and curbing losses and misuse of scheduled drugs.

Secure GPS trackers can be harnessed to monitor the whereabouts of infants and other patients. Secure patient intranets or apps could allow hospitals to issue comprehensive medical information to patients, improving their treatment compliance and recovery.

Thanks to advanced medical management tools and IoT devices, paper is becoming obsolete in the digital hospital. But next-generation hospital systems and networks must be effectively secured and controlled, with advanced user authentication, a centralised security architecture, next generation network security solutions such as internal segmentation firewalls, web application protection, data leakage prevention, database protection and secure wi-fi.

ABOUT PAUL WILLIAMS

Paul Williams is the country manager SADC for Fortinet.
- Securing the connected hospital: making strides in patient care - 10 Aug 2016

View my profile and articles...