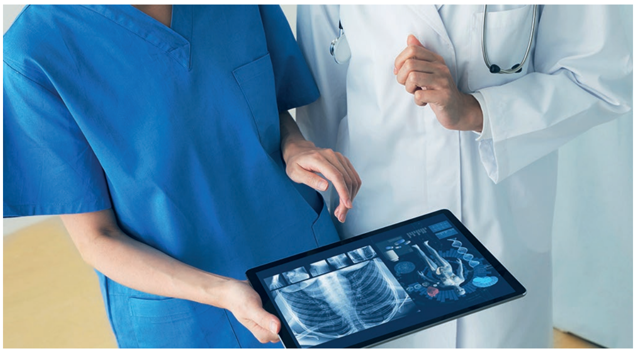
LANCOM Whitepaper

Cloud-managed hospital networks (SDN) for top-level treatment and care

These days, applications and processes are increasingly being digitalized: Growing numbers of users, devices and things (IoT) are networked with one another, which is especially true in the healthcare sector and particularly affects clinics and hospitals. Each individual hospital bed in US hospitals already has more than 10 networked devices in its periphery. An efficient network is the heart of every clinic, and developing and managing it is a highly complex operation. At the same time there are more and more reports about devastating cyber attacks with immense damage to the affected facilities. Conventionally managed networks quickly reach their limits here. Cloud-managed networks, on the other hand, deliver automation and maximum operational reliability. The focus here is no longer just on the hardware and a one-off installation of the infrastructure. In fact, it is more a matter of ensuring that the actual state of the networks and individual components is always transparent and that data traffic is secure. This represents a paradigm shift with considerable opportunities and interesting prospects for hospital operators, who already face enormous cost pressures.

IT – more than just a competitive factor for hospital operators

IT departments in hospitals are under pressure: They have to manage the transition from written to electronic data collection while ensuring the confidentiality of sensitive health and patient data. The issue is nothing less than protecting against the theft of medical data and keeping up efficient clinical processes—which potentially protects the lives of patients. Both must be guaranteed, not only in the interests of the patient but equally to safeguard the business operations of the hospitals. For example, doctors on duty must at all times have quick access to patient files, where previously the paper file might have to be retrieved from a colleague's desk. As a consequence, the permanent availability of the network for mobile devices such as laptops and tablets is not only obligatory, it is critical. With vital signs recorded not only by stationary monitoring devices but also by mobile devices, medical professionals and nursing staff can, in future, be more mobile, flexible, and therefore more efficient. This saves time, and that benefits the patient.



Patient tracking, asset management, and hospital convenience

Using modern network infrastructure in hospitals opens up further fields of application that improve process efficiency and even provide competitive advantages. Wi-Fi infrastructures can be expanded to provide highly efficient real-time location services (RTLS), which can be used to precisely locate medical devices, beds, or even wheelchairs. This eliminates time-consuming searches for missing assets or the purchase of multiple assets, it increases utilization and prevents theft.

Location-based services (LBS) based on Bluetooth technology can be installed to locate and identify patients with dementia or who are disoriented. Patients are given wristbands with an integrated radio module, which gives them adequate freedom of movement and keeps them safe as well.

Today and in the future, processes are increasingly being digitally captured via Wi-Fi—the results of morning ward rounds, findings from the emergency room, asset tracking, patient and visitor navigation, or personal meal requests—almost every move is monitored digitally.

Furthermore, patients have increasingly sophisticated expectations of their stay in hospital: They would like to use their mobile device to surf the Wi-Fi securely from the bedside, or take advantage of the entertainment offerings.

Cloud management is keeping pace with technical progress

As positive as digitalization is, the consequences for the network are far-reaching: The different sections of the hospital and areas of responsibility—medical data transmission, communication, multimedia entertainment, and administration—demand a reliable infrastructure. An increasing number of devices require constant and uninterrupted access to sensitive and / or vital information.

The consequence: The networks have to process more and more data. Legacy networks at hospitals were rarely designed to meet such requirements. Generally these systems are inflexible and cannot be expanded quickly to meet changing needs, which makes them just the opposite of what modern hospitals need: A versatile infrastructure that, rather than being limited by permanently installed components, is flexible and scalable, i.e. quickly adapts to changing requirements.

The changing framework conditions will sooner or later overload conventional network structures and force managers to rethink. To get a grip on the increasing complexity, networks have to be “rethought” and replaced by flexible cloud-managed infrastructures. The following questions play a key role: How can networked services such as the digital documentation of treatments, patient monitoring, or location solutions, etc. for medical devices be made available to doctors and nurses? How do we guarantee not only IT security but also patient data sovereignty at the same time? How do modern services such as Wi-Fi hotspots and entertainment systems contribute to patient satisfaction, and what effect do these investments and changes ultimately have on the total cost of ownership (TCO)? Building this bridge is achieved with cloud-managed (W)LAN concepts and modern SD-WAN solutions for real-time connection of distributed hospital locations, external specialists and rehabilitation centers.

The idea behind it is the automatic installation, monitoring and expansion of networks. Older digital infrastructures that were traditionally management-intensive and static are being transformed into dynamic networks with flexible expansion options. For this purpose, functional levels of the network are decoupled from the hardware in the form of virtual services, i.e. the control plane is separated from the data plane. A software application controls the handling of data packets on the hardware data plane—routers, firewalls, switches or access points. While traditional architectures required changes to the settings on old and new hardware to be configured individually and manually, cloud management enables the central, location-independent design, management and monitoring of networks with just a few clicks of the mouse.

Uncertainty about introducing cloud management

The legal situation is complex, and many have deep concerns about security from cyber threats to patient data when operating new technologies, especially cloud services. However, this is where providers of network infrastructure solutions can score points, create trust and highlight the advantages of solutions made in Europe—thus incorporating the relevant security standards. Particularly noteworthy here is a recently published report from the European Union Agency for Cybersecurity (ENISA) (https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/). Its aim is to provide best practices for cloud security in the healthcare sector, and to identify aspects of security and data protection required for cloud services for the healthcare sector. As the paper clearly shows, cloud solutions give healthcare providers the flexibility they need and allow the fast provision of new services, including "virtual" health and telemedicine. The study presents typical use cases for cloud applications at hospitals, such as the electronic health record, remote support and medical devices, and it discusses 17 security and data-protection measures that guarantee the required cloud security. An online tool for the implementation of the procurement guideline for hospitals and also published by ENISA (https://www.enisa.europa.eu/news/enisa-news/procurement-guidelines-for-cybersecurity-in-hospitals-new-online-tool-for-a-customised-experience) aims to provide procurement managers with comprehensive information in order to align hospital procurement processes with the achievement of legally required cybersecurity goals. In this white paper, it is important to highlight the advantages of European providers and solutions with the corresponding security standards and, in particular, data-protection compliance and trust. It offers pointers helping hospitals to select a trustworthy cloud-service provider with whom they can take appropriate organizational and technical precautions to implement national and European legal standards such as the EU General Data Protection Regulation (GDPR). At this point, we would refer you to a guideline describing how compliance risks can be minimized in company networks. You are welcome to request the document here.

Its relevance was underlined once again by the decision of the European Court of Justice (ECJ) on July 16, 2020. At that time, the court overturned the Privacy Shield, i.e. the data-protection agreement between the European Commission and the USA. The Privacy Shield provided the basis for US companies to process EU citizens' personal data. The court's decision removed the legal basis of this practice almost overnight, and was a clear victory for the protection of EU citizens' personal data. The judgment demonstrates yet again that hospitals should rely on European providers to protect patient data and avoid any data protection-related difficulties.

Cloud-based management of the hospital networks pays off in many ways

In the long term, cloud-managed hospital networks are far more cost-effective and economical than traditional networks, as they offer higher performance and lower maintenance costs, especially since there is almost no need for on-site technicians.

Hospitals therefore benefit from considerable time and cost savings, because SD-WAN and cloud management make day-to-day working for network administrators much easier. The software handles the configuration and the resources that are freed up can be used for planning, monitoring and further development of the networks. The entire infrastructure gains versatility and can be adapted to shifting requirements much faster than before. Bandwidths are adjusted within minutes, services are enabled and stopped online, and the status of the entire network is constantly monitored in real time. Even complex processes such as troubleshooting or rolling out new network segments and services can be completed with a click of the mouse within minutes or at least hours, instead of the days or even weeks that they used to take.

In emergencies: Rapid intervention and automatic prioritization

Networks in healthcare environments have to be extremely reliable—lives depend on it. If a traditional network fails or malfunctions, the effects on clinical processes can be serious. Not only is this expensive, it also poses a serious risk to patient care. Cloud-based infrastructures offer the best possible overview and the option to influence every device and application operating on the network. This is an important building block for managing information security in hospitals thanks to monitoring of the current status of all components such as routers, firewalls, switches, and access points. The IT admin can instantly detect anomalies, expiring licenses, errors or device failures, and can react immediately, usually before users are impacted.

Individual prioritization of different network applications

Especially when there are high traffic volumes, networks have to do more than just support each connected device. They have to be able to differentiate between a patient record being viewed during a routine check-up or whether it is required in the intensive care unit or emergency room. Processes must be prioritized accordingly. Critical processes and devices come first. IT administrators can prioritize the network traffic for urgent and thus time-critical applications, and slow down or even halt transmissions for less urgent applications. In case of doubt, back office or administrative applications need less bandwidth, for example, that the time-critical transfers of medically relevant data.

The promise of cloud-managed hospital networks

Key drivers of digital transformation are the installation, rollout, and management of hospital networks in combination with the latest cloud technology. Cloud technologies ensure that all of the functions for configuration, management, and monitoring can be performed easily, centrally, and from any location via laptop, tablet or smartphone. Be it high-speed Internet access, the high-tech networking of hospital sites via SD-WAN, setting up Wi-Fi profiles, prioritizing time-critical data traffic, or integrating new devices such as routers, firewalls, switches or access points—a modern cloud solution adapts to the needs of the hospital, no matter how big or small. The investments remain manageable and the expenditure can be calculated on a monthly basis.

IT and investment security included – made in Germany

With networks managed from a public cloud, the most essential prerequisites are trust, security, and data protection. This is why there is simply no alternative for hospitals and clinics to choose a provider who is subject to, at the very least, European or, better still, German data protection law and who hosts their services in local data centers in accordance with the GDPR.

Secure investment in the future

Another important consideration is investment security. Many network manufacturers use specialized routers or access points for their cloud-managed network solutions. They only operate via the cloud and are partially tied to individual networks or locations. The concept of “booking-out” the hardware from the cloud management in order to manage it with conventional tools, or to move it from one location to another, is simply not possible. This is a significant limit on flexibility and results in unforeseen additional expense should changes occur. Optimal investment protection comes with network components that operate either autonomously or via the cloud, and which allow adaptation to changed operational requirements at any time.

Hospital-networks-as-a-Service via Managed Service Provider

For small and medium-sized clinics in particular, networks hosted in a public cloud by a service provider (Managed Service Provider, MSP) who specializes in the healthcare sector can be very interesting and economical. They can be booked flexibly and according to your needs on a "pay as you grow" basis. The service you pay for is what you booked, i.e. "pay what you get". Adding new users and devices takes just minutes by defining them in the central administration dashboard and connecting them to the existing network .

Private cloud for high security requirements

For hospitals large enough to be classified as critical infrastructures with extended security requirements, self-hosting models allow the management cloud to be operated at their own data center. The system can even be hosted on its own dedicated hardware, called a private appliance. This allows the cloud-based management system to operate "on premises" on infrastructures that are not shared with any other clients.

Conclusion: Innovation caters for reliable care

Hospital operators are under enormous pressure due to the increasing requirements mentioned above. This pressure is directed straight at their IT departments, because they need to be the trailblazers for a holistic digital strategy that includes medical equipment, IT technology, and data networking. The network plays a key role here. Cloud management is the future of network administration and provides far greater flexibility for any hospital on its way to digitalization and successfully becoming a future-proof hospital.