

Maximizing Physician Productivity Through Secure & Efficient IT Networks

Introduction

Information is becoming digital. In the past few decades, we've seen financial exchanges, business records, music, and videos all make the leap from traditional storage mediums to new digital formats. As the world's information rapidly transitions to one digital format or another, many medical offices, dental practices, laboratories, pharmacies, and other healthcare providers have begun trading their file cabinets for storage servers. By migrating from paper-based patient information to electronic health records, healthcare providers have lowered costs, maximized physician efficiency, gained immediate access to patient records, and dramatically improved patient care.



Electronic information formats allow providers to immediately access pertinent information in patient records, as well as quickly and efficiently share information with hospital emergency rooms, specialists, and other healthcare providers to seamlessly care for patients. For instance, with the Healthcare Information Exchange (HIE) initiative, ongoing efforts to share patient healthcare information across different providers allows secondary providers to immediately obtain a patient's health records which can avoid unnecessary or duplicate treatments, halt the administration of potentially harmful medications, and enable providers to make more informed decisions on patient care.

Security Concerns



Although the immediate benefits of moving towards electronic data are obvious, so are the potential dangers of electronically stored and transferred data. Network worms and viruses threaten the stability of IT systems that store patient records. Worse, phishing, whaling, malicious websites, and specially crafted data mining applications threaten the privacy and confidentiality of patient data. Further, the Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of patient information by entities such as health care clearinghouses, health insurers, and medical service providers. Organizations which cannot adequately demonstrate the capability to safeguard such information from Internet and network threats can be subject to civil penalties of \$100 per violation, up to \$25,000 per year for each requirement violated.

Network Backbone Performance

Network performance is a critical aspect for a hospital or clinic. The ability to quickly access images and patient records is directly dependent on the speed of the network. X-Ray, MRI, and other images typically have very large file sizes and can quickly saturate a network with just a few simultaneous transfers. In larger environments, this can quickly become a problem as slow network performance delays the arrival of critical patient data into doctors' hands.



Continuous Connectivity



Mobility and Network Connectivity go hand in hand in a dynamic healthcare environment where the network users (physicians, administrators, and staff) are mobile and patients are often not. Specifically, wireless network connectivity, achieved through the use of wireless access points, switches, and management systems, allows healthcare providers to stay connected while moving from patient to patient. Hospital and healthcare information systems have also begun leveraging wirelessly networked patient beds, IV pumps, and other monitoring equipment to more accurately dispense care and efficiently monitor supplies.

Failsafe Storage

Proper storage and safeguarding of patient data is one of the most critical components to employing an electronic health records system. Storage systems need to be accessible, available, easily expandable, and reliable. Inefficient storage can inhibit the provider's ability to add new patient records. Inability to properly protect the records from hardware failures and catastrophic data loss puts patient care – and the provider's operations – at risk. Data Storage, data backup, and a disaster recovery plan is one of the center pieces of a sound health care system. Having the proper storage security elements and procedures goes a long way towards HIPAA compliance as data storage is also well regulated by HIPAA.

NETGEAR® Solution

NETGEAR® provides reliable, high-performance, business-class networking products that are designed to meet the needs of healthcare providers. NETGEAR components work together to provide a comprehensive network solution, while sharing common interfaces to simplify configuration and on-going management of the solution.

NETGEAR ProSecure® UTM and STM security appliances employ an array of network and content security technologies to protect the network from a wide range of threats. The UTM works in conjunction with the ProSafe® switches and wireless access points to allow for secure segmentation of the network. This keeps guest traffic separated from patient records and other critical internal infrastructure. ProSafe switches utilize Power over Ethernet (PoE) ports to power devices without the need of power outlets. This allows flexible deployment of ProSafe wireless access points and other PoE devices such as phones and surveillance cameras. ProSafe gigabit switches and wireless N access points ensure that files and other information is transferred at maximum throughput. NETGEAR ReadyNAS® network storage delivers cost-effective and reliable storage capacity for storing and sharing medical records, digital imaging and other data. With embedded backup, off site replication, and cloud-based backup features the system provides extra layers of data protection for disaster recovery. Additionally, the ReadyNAS Remote allows doctors and experts to access centralized data from remote locations securely and easily. Together, the NETGEAR business infrastructure works to help healthcare organizations keep their electronic data and network assets safe and secure. This is a critical step in meeting HIPAA requirements on information security.

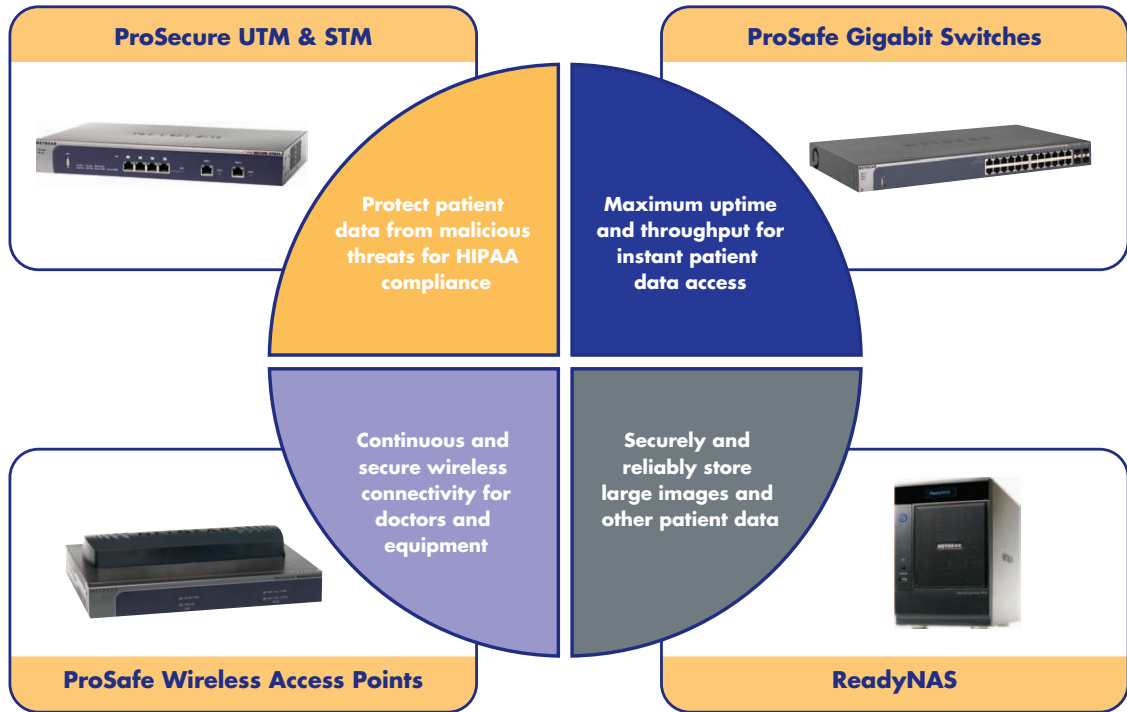


Diagram: NETGEAR Product Solutions for Healthcare

NETGEAR, the NETGEAR logo, Connect with Innovation, ProSafe, ProSecure and ReadyNAS are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2010 NETGEAR, Inc. All rights reserved.