

Case Study: Medical Center Hospital, Odessa, TX

Secure, Auditable & Standardized Control over Vendor Access

Medical Center Hospital Overview

Medical Center Hospital (MCH) is a 376 bed facility located in Odessa, Texas serving more than 50,000 patients annually. Like other healthcare institutions, MCH has a lean IT staff tasked with supporting over 200 applications from more than 75 distinct software vendors. These vendors routinely require remote access for maintenance, patches, troubleshooting and upgrades.

The Vendor Network Access Challenge

Vendors were accessing MCH's secure network with a combination of methodologies including modems, VPN accounts, desktop sharing, pcAnywhere, vendor proprietary solutions and site to site networks. This array of methodologies created a constant strain on MCH's IT staff to build and maintain these vendor connectivity solutions. Additionally, collecting and maintaining audit information required by HIPAA was impossible.

The SecureLink Enterprise VSN Solution

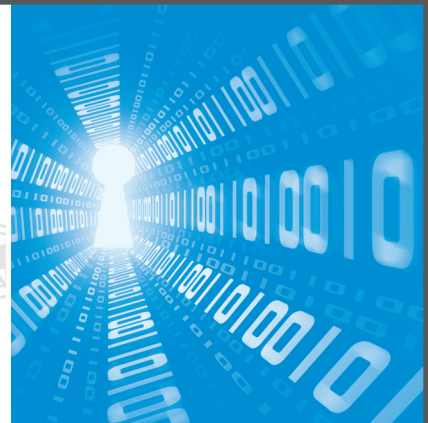
One of MCH's vendors recently standardized on the SecureLink Virtual Support Network for the service of all its clients. Recognizing the power and simplicity of SecureLink VSN, MCH contacted Enexity about an enterprise version of SecureLink VSN that could be used to enable remote access for its remaining vendors. MCH worked with Enexity to design and deploy SecureLink Enterprise VSN, the first product specifically designed to enable unified vendor remote access to secure networks.

SecureLink Enterprise VSN is easy to deploy and maintain, has strict security controls and detailed audits of all vendor activity. SecureLink Enterprise VSN is also extremely vendor-friendly providing all the essential tools support technicians need with easy browser-based access.

Medical Center Hospital's Success with SecureLink Enterprise VSN

Shortly after implementing *SecureLink Enterprise VSN*, Medical Center Hospital saw a tremendous reduction in the IT staff's involvement with managing vendor access to their networks. Their initial concerns that vendors would be reluctant to shift access methods were also quickly alleviated. Kay Warner, Computer Security Officer at Medical Center Hospital stated, "Our vendors have been quick to accept and utilize SecureLink Enterprise VSN. Even our most inflexible vendors recognize *SecureLink Enterprise VSN* as a far superior solution to their entrenched and outdated support methodologies."

Kay Warner concluded, "Medical Center Hospital now has a standardized method for controlling vendor access and comprehensive, historic audit trails of all vendor activity. It takes a load off of our IT staff, allows us to get better support and delivers fully on the HIPAA requirement to know who is accessing our system and what they're doing while on it. Somebody should have thought of this long before now!"



"HIPAA says you have to know who is on your system and what they're doing while they're on; SecureLink Enterprise VSN does exactly that!"

-Kay Warner, Computer Security Officer, Medical Center Hospital, Odessa, TX

ENEXITY

1301 S. Capital of Texas Hwy
Suite A-130
Austin, TX 78746
866-ENEXITY (363-9489)
www.enexity.com
info@enexity.com