



Case Study: Medical Center Hospital

Overview

Medical Center Hospital (MCH) is a 376 bed facility located in Odessa, Texas serving more than 50,000 patients annually. It is the only full-service hospital in Ector county and serves as the regional referral hospital for the 17 surrounding counties of the Permian Basin – an area of about 250 square miles. Like other healthcare institutions, MCH has a lean IT staff tasked with supporting over 1,400 employees in nearly 50 separate departments using 200 different applications from 75 distinct software vendors. Each of these vendors routinely require remote access for maintenance, patches, troubleshooting and software upgrades. In addition to supporting the ongoing operation of the hospital, the MCH IT staff must also manage remote software vendor support connections. And, they have to manage it in a way that won't compromise security.

The Challenge: Organizing Vendor Network Access

Vendors were going through MCH's network to support their applications with a wide range of methodologies including modems, VPN accounts, desktop sharing, pcAnywhere, vendor proprietary solutions, and site-to-site networking. These connection types were typically defined by the vendor – whatever they had used with other customers. This variation in connection types created two significant problems for MCH: First, the variety of remote access connections created an overly complex environment that forced the MCH IT staff to become heavily involved in administering and managing each connection. Additionally, without a standard way of managing remote access, the situation only got more complex as applications, vendors, and support technicians were added to the mix. Second, there was no common method of tracking and reporting on remote support sessions. If they had the capability at all, audit and reporting differed between connection types and applications. It was impossible to implement a uniform security policy with respect to vendor support access, making HIPAA compliance (with respect to remote support) also very difficult to determine.

Healthcare organizations and other regulated industries are also challenged with opposing priorities when application uptime is critical, but the methods to attain it are at odds with security and privacy regulations.

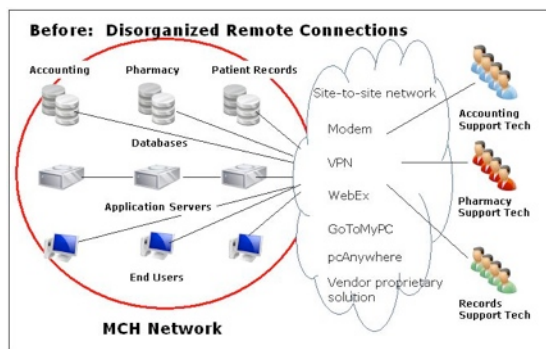
Challenge #1: Time Critical Support

Application interconnectivity and reliability are essential for keeping patient data flowing between departments to ensure good health care and efficient operation. Application failure, data corruption or even slow performance are potentially life threatening and unacceptable for hospitals trying to maintain high standards of care. A single application outage affects multiple hospital departments – the organization using the application and the others that need the data. With a small IT staff managing as many as 200 unique software applications, MCH must rely on software vendors to provide rapid fixes to any problems. This means that, in addition to the typical job of supporting on-site systems and users, the IT staff also must enable remote access by software vendors supporting the hospital's applications. The trick is to provide access for remote support without

consuming too much of IT staff time, and not compromise the security of patient data in the process.

Challenge #2: Data Security

HIPAA requirements have placed healthcare providers in an increasingly controlled environment and have put pressure on hospital IT staff to implement well defined security policies and systems. With civil penalties in the tens of thousands of dollars and potential criminal penalties for employees, directors, and officers of covered entities, keeping patient data secure is a clear priority. And, it's not enough to claim to keep the data secure. Systems need to pass rigorous audits in order to prove HIPAA compliance.



The Solution: SecureLink Enterprise remote support network

MCH needed to find a way to standardize remote software vendor support access to reduce the complexity and enable implementation of a robust security policy. Several of MCH's software vendors recently standardized on SecureLink remote support network to provide remote support for their clients. (Software vendors have a management problem very much like MCH. Instead of managing a wide variety of inbound connections however, the software vendor must deal with connecting to a big range of different customer environments.) Recognizing the power and simplicity of SecureLink, MCH contacted SecureLink about an enterprise version of the product that could be used to manage remote access for all of its vendors.

MCH worked with SecureLink to design and deploy the enterprise version of the product, the first system specifically designed to enable unified vendor remote access to secure networks.

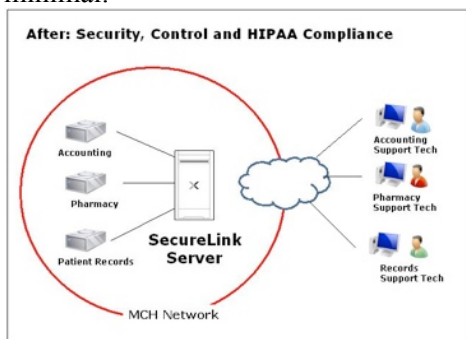
SecureLink Enterprise standardizes remote support access with a system that allows MCH IT staff to easily manage the variety and number of remote support connections needed to keep applications up and running and the hospital operating effectively. Standardization also enables a uniform security policy for remote support access. SecureLink provides:

- **Complexity Reduction** – Supports a wide variety and large number of remote connectivity scenarios without adding management overhead. Vendors may connect to any permitted network service on any operating system.
- **Individual Accountability** – Rather than issuing a generic VPN account to a vendor & allowing multiple technicians to share it, SecureLink Enterprise makes it easy to issue accounts to individual technicians, ensuring accountability and compliance.

- **Dual Factor Authentication** – Each session user is authenticated using a unique, dual-factor authentication that does not require key fobs. Each account is tied to that person's corporate e-mail (ex: vendorname.com). Every time that user wants to connect, they must supply a valid login, and then must supply the key that's automatically e-mailed to that corporate e-mail account. This ensures the technician is who they claim to be, and still employed by the vendor without the need to maintain massive lists of vendor technicians.
- **Granular Permission Control** – MCH can grant access to different network resources for individual vendors at a very granular level. For example, Vendor A may only require read-only access to a single log file on a Windows server, while Vendor B requires access to a database port and telnet on a Unix server.
- **Access Scheduling** – MCH is able to make access available on different terms for different vendors. For example, Vendor A's access must be manually approved by MCH's IT staff, while Vendor B can connect at any time and Vendor C may connect Monday – Friday from 8 – 5 and Saturday from 9 – noon.
- **Real-time connection notifications** – Individuals or groups can choose to be e-mailed each time a specific vendor connects.
- **High Definition Audit** – All vendor activity is captured at the individual user level at a high level of detail, including reason for connecting, support ticket number, access times, data transfers, services accessed, files transferred, commands entered and more.
- **Built-in Tools** – Vendors can be enabled with handy built-in tools, including desktop sharing file transfer and more.
- **Flexibility and Scalability** – Users and applications can be added easily and support technicians have the tools required to effectively perform remote support.
- **Reduced Cost** – Fewer MCH IT staff resources are required for providing and supporting remote access.

SecureLink provides control, security and audit capability while simultaneously providing the tools technicians need to deliver timely and effective remote support. SecureLink operates on a dedicated server located within MCH's secure network. Login access to the SecureLink server is only available to authorized vendor support personnel authenticated to the MCH network. Within the SecureLink application, support technicians are segmented by different user groups that in turn have access privileges to designated systems on an as needed basis.

Using a simple, browser based interface, the MCH staff was able to strictly define system access for each vendor – server, port, application, files, services, date, time and more. Once a vendor's access account was set up, the IT staff involvement in administering support connections was minimal.



Medical Center Hospital's Success with SecureLink Enterprise

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

- **Vendor Acceptance** – MCH's vendors were quick to accept an on-demand, browser-based access to their systems, as it reduced their complexity and improved their efficiency.
- **Reduced Cost** –MCH IT staff resources required for providing and supporting remote access to software vendors was dramatically decreased.
- **Improved Security** – Insecure and un-auditable vendor access methods, such as modems, shared VPN accounts and desktop sharing were eliminated, improving security levels.
- **Improved Service Levels / Uptime** – Vendors have been more responsive and effective at diagnosing and repairing issues and managing ongoing upgrades and maintenance.
- **Compliance** – MCH can confidently produce a detailed report of who has accessed what at any time.

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!"

