The Right Rx for Upgrading Today's Hospitals

How Device Servers Modernize Health Care Information Systems

CORPORATE HEADQUARTERS
167 Technology Drive
Irvine, CA 92618

Tel: 800.422.7055
sales@lantronix.com
www.lantronix.com

EUROPEAN HEADQUARTERS
Tel: +31 (0) 76.52.36.74.4
EMEA@lantronix.com

ASIA / PACIFIC HEADQUARTERS
Tel: +852 3428.2338
asiapacific_sales@lantronix.com

JAPAN HEADQUARTERS
Tel: +81 3.6277.8802
japan_sales@lantronix.com

Contents

Introduction

The American health care system has recently received a great deal of attention as the U.S. government attempts to overhaul America's costly and outdated health care infrastructure. When you consider the United States spends over $2 trillion on health care annually, which will continue to steadily rise with a rapidly aging U.S. population and a growing number of underinsured or uninsured, few would argue that health care reform, on some level, is necessary.

One key way to drive costs out of the health care system is by computerizing or "modernizing" the sector's medical records system, which is a key part of President Obama's health care reform proposal. As stated in the Obama Administration's Fiscal 2010 Budget:

*"**Computerizing America's Health Records in Five Years**. The current, paper-based medical records system that relies on patients' memory and reporting of their medical history is prone to error, time-consuming, costly, and wasteful. With rigorous privacy standards in place to protect sensitive medical record, we will embark on an effort to computerize all Americans' health records in five years. This effort will help prevent medical errors, and improve health care quality, and is a necessary step in starting to modernize the American health care system and reduce health care costs."*

To help drive the adoption of Electronic Health Records (EHRs), which is expected to save billions of dollars and reduce medical errors, the American Recovery and Reinvestment Act (ARRA) of 2009 is providing more than $17 billion to the health care industry. ARRA also offers doctors and hospitals financial incentives for participation in the national Health Information Technology (HIT) network of shared patient data, which is designed to streamline medical care in addition to reducing costs.

HIT standards will enable a nationwide electronic exchange of medical information. However, hospitals, clinics, doctors' offices and other health care facilities still need to consider a host of factors, such as data security, technical issues, and a shortage of qualified IT professionals, when fully implementing EHRs and a HIT-compliant network.

The Department of Health and Human Services (HHS) is currently developing standards, implementation specifications, and certification criteria for EHR and HIT networks to meet the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of (ARRA). The HITECH Act relates directly to the need for a nationwide adoption of EHR and HIT technologies. The federal agency is also taking Health Insurance Portability and Accountability Act (HIPAA), ARRA, Medicare and Medical EHR incentive programs into consideration.

On January 13, 2010, HHS released the Interim Final Rule, which is the first step toward adoption of proposed standards, implementation specifications, and certification criteria for EHR and HIT.

Although not ratified, minimum requirements have been established that center on the collection of patient health data, a safe and secure national network infrastructure, and technologies that allow EHRs and associated patient data to be indecipherable to unauthorized individuals when transmitted over a national wired or wireless network or any other health care provider's network.

Lantronix has offered network enablement solutions for medical devices for more than twenty years. As a result, many of the Lantronix device servers have been customized to meet the stringent requirements of the health care industry.

This paper shows how device server technology can be used to remotely access laboratory and bedside equipment and Electronic Medical Records (EMR) to help health care providers make timely diagnosis and treatment decisions. Device servers offer remote access either wired or wirelessly using safe and secure means of transmitting patient health data over a hospital's network.

Identifying the Challenges

If medical devices that contain valuable patient data could be easily accessed over an IP-based network, it would significantly improve coordination of patient care by enabling doctors to diagnose and establish a course of treatment much faster, and saving the limited time of health care professionals. Associated benefits would include a significant cost reduction, and network access to all medical devices via a HIT-compliant network.

However, there are several key challenges in the health care sector that must be addressed.

- Security – Selecting a Secure Device Server
- HIPAA Concerns about Wireless Communications
- Serial-Based Medical Equipment
- Lack of Qualified IT Professionals

Security

Since most treatment decisions are based on medical tests, doctors want remote and immediate access to laboratory results to assist them in a more timely diagnosis. Nurses also want remote access to bedside equipment from the nurse's station to quickly access patient care requirements.

As the need to enable network connectivity to laboratory and bedside monitoring/analysis equipment grows, one of the biggest concerns raised by health care providers is how to safely and securely collect and upload the volumes of test and lab results to EHRs when making treatment decisions.

Firstly, device servers must be secure to comply with ARRA and HIPAA requirements. The role of device servers is to transfer stored data electronically from a medical device to another entity. When selecting a device server, primary security features should include user/password functionality and stringent encryption.

When logging into a device server, a user name and password will ensure that an authorized person is accessing the medical device. Device servers should have the ability to create a local database of authenticated user names and passwords for all users logging into the device server. Remote authentication should also be an option.

LDAP, Kerberos, and Radius are computer servers that store user names and passwords of authenticated users. A user logs into the device server, which forwards the login credentials to the remote authentication server, which confirms user permission.

Encryption is simply the translation of data into a secret code, and it is considered the most effective way to ensure data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Modern encryption is achieved using algorithms with a "key" to encrypt text or other data into digital nonsense and then decrypt or restore the information to its original form. There are two main types of encryption: asymmetric (also known as public-key encryption) and symmetric. There are also many methods for encrypting data based on these two types of encryption. One of the most commonly used is AES.

- Advanced Encryption Standard (AES) also known as Rijndael: It can use 128-, 192- or 256-bits to encrypt and decrypt data in blocks of 128-bits. As of 2004, there have been no successful attacks against AES.

There are also protocols that use authentication and encryption methods. In many cases, they use the AES algorithm for encryption. SSH and SSL are most often used.

- Secure Sockets Layer (SSL): Certificate-based internet security used to encrypt data between a browser and a server.

- Secure Shell (SSH): Uses public-key cryptography to create an encrypted tunnel, and is typically used to log into a remote device and execute commands.

Wireless encryption is constructed a little differently:

- Wired Equivalent Privacy (WEP) -- an encryption algorithm built to secure 802.11 wireless networks. Uses an RC4 stream cipher with 40 or 104 keys. This protocol is vulnerable to hacking and is therefore not HIPAA compliant.

- Wi-Fi Protected Access (WPA): Uses a pre-shared key (PSK) and is designed as a fix for the vulnerability issue with WEP using Temporal Key Integrity Protocol (TKIP) encryption with 64-bit message integrity. It is fully compliant with HIPAA requirements.

- WPA2/802.11i – aka Robust Secure Network (RSN): Takes advantage of AES level encryption. This protocol along with enterprise wireless security methods that utilize Extensible Authentication Protocol (EAP) such as EAP-TLS, EAP-TTLS, PEAP and LEAP (Cisco) provides a scalable authentication and wirelessly security framework for development in hospitals. It is fully compliant with HIPAA requirements.

HIPAA Concerns about Wireless Communications

HIPAA governs health care providers, health plans, etc., to maintain appropriate protection of patient health records. This includes both paper and electronic data records. The HIPAA security and protection controls were updated in 2003 to address concerns of transmitting patient health records electronically.

Wireless networks, based on the International Electrical and Electronics Engineers (IEEE) 802.11 standard, transmits data over radio frequencies, which means that any wireless device that communicates on the same radio frequency can also receive transmissions not necessarily destined for it.

The WEP protocol was the first attempt to protect and encrypt wireless data. However, it was soon discovered that WEP was flawed and easily cracked with rudimentary hacking tools. As a result, WEP was not HIPAA compliant,

therefore, it could not be considered safe enough to protect the transmission of patient records. This unfortunately soured the health care industry on wireless communications for a time.

The availability of 802.11i standard from IEEE and the WPA2 Specification and Certification from the WiFi Alliance provides a foundation for securing wireless networks and offering safeguards that are fully compliant with HIPAA requirements.

Serial-Based Medical Equipment

The health care industry fully acknowledges the requirement of obtaining patient records and laboratory-related data electronically; however, the challenge comes when much of the medical equipment containing patient test, monitoring, and laboratory data is not accessible from an Ethernet or Wi-Fi network.

Most of today's equipment only provides a serial port for communications, which requires a personal computer (PC) or laptop computer to be connected directly to the device's serial communications port in order to access patient data. This problem occurs in doctor's offices, clinics, medical laboratories, as well as pharmaceutical and hospital environments.

Here is a list of medical equipment often supplied with only a serial port:

- Blood pressure monitors
- Patient monitoring systems
- Blood chemistry analyzers
- Glucose analyzers
- CAT scanning equipment
- Prescription barcode scanners
- Ventilators
- EKGs
- X-ray equipment
- Breathalyzers
- Anesthesia monitors
- Vital sign machines

Lack of IT Resources

In a recent article in the Rural Health Voices – News and Opinion from the National Rural Health Association, Dr. David Blumenthal, National Coordinator for Health Information Technology, U.S. Department of Health & Human

Services, announced a need for 50,000 qualified health IT workers nationwide to assist hospitals and health care providers in sharing electronic patient health data.

Currently, doctors, nurses and hospital staff are forced to learn how to use EHRs and implement HIT system practices in order to take advantage of ARRA incentives.

Wireless Protocols

Wireless communications protocols are available in a variety of flavors including Wireless Fidelity (Wi-Fi), Bluetooth, Radio Frequency (RF), and ZigBee, all targeted at specific applications. Wireless communications have allowed us to access data and information from almost any remote location without being directly connected to the data source. The health care industry was one of the first commercial adopters to take advantage of wireless technology, particularly Wi-Fi AKA Wireless Local Area Network (WLAN).

Wi-Fi Technology

Wi-Fi was the best available solution when the health care industry first began to adopt wireless technology. In addition to consumer market approval, it also enjoyed a good support infrastructure that included plenty of supplier competition and product availability. Wi-Fi is based on the IEEE 802.11 standard and is promoted by the nonprofit Wi-Fi Alliance, which certifies wireless products in an effort to promote the best of the technology.

The first widely supported version of Wi-Fi was the 802.11b standard (2.4-GHz band), which supports 11 channels. Since then, other standards -- 802.11a, 802.11g, and 802.11n have followed with beefier specifications, including higher data rates and throughout.

802.11 Standards	Year of Release	Frequency (GHz)	Data Rate (Mbit)	Throughput (Mbit)	Indoor Range (m)	Outdoor Range (m)
a	1999	5	54	23	35	120
b	1999	2.4	11	4.3	38	140
g	2003	2.4	54	19	38	140
n	2009	2.4	72.2	30	70	250
n	2009	5	150	130	70	250

Table 1. 802.11 a/b/g/n comparison

The health care industry favors 802.11a due to the less congested 5-GHz frequency. It also offers a direct migration path to 802.11n, which offers a higher data rate and throughput, along with an extended range.

Wireless Benefits for Medical Applications

In the health care sector, there are many opportunities to employ wireless access. As an example, in hospitals, "crash carts" are used to transport medical equipment to and from patient and operating rooms. Equipment may also be transferred alongside the patient's bed as the patient is wheeled from one location to another. If this equipment is wirelessly enabled by a device server, the data collected by the medical device can always be accessible from anywhere in the hospital.

Doctors and nurses can also take advantage of wireless handheld devices like portable digital assistants (PDAs) to access medical devices during their rounds in hospitals or at office visits in their own practice. This allows patient data to be immediately uploaded to the patient's EHR instead of being logged into a paper chart folder to be later entered into a computer.

Also, the use of computer-based physician order entry (CPOE) and bar-code scanning for medications is expected to expand over the next few years and wireless communications networks are essential to their success. Wireless technology can also assist doctors in outpatient clinics and portable screening labs by giving them access to high-resolution images like magnetic resonance imaging (MRI), ultrasound, and computed tomography, from remote laboratories and hospitals. The fastest way to wirelessly enable these types of medical devices is by using wireless device servers.

In a real-world example, an academic medical center installed an IEEE 802.11 WLAN in all patient-care areas. Using hand-held PDAs and PCs mounted on mobile carts, patient care teams can now wirelessly access electronic medical records as they conduct rounds and perform patient care.

Physicians, nurses, and therapists use mobile technology to check test results, order medications and tests, and document patient care and visits while they are with the patient, instead of returning to a central station to view and enter the information after interacting with the patient. Mobile access to data saves time every day for all types of clinicians and makes innovative new software applications such as CPOE possible, which in turn reduces errors when ordering medication and other critical services.

Device Server Technology

Available in both external and internal (embedded) versions, device servers are used to provide a secure means of transmitting patient health data over a hospital's network. While health care providers typically require an external solution, medical device manufacturers prefer an embedded solution that can be integrated into their product design.

External Device Servers

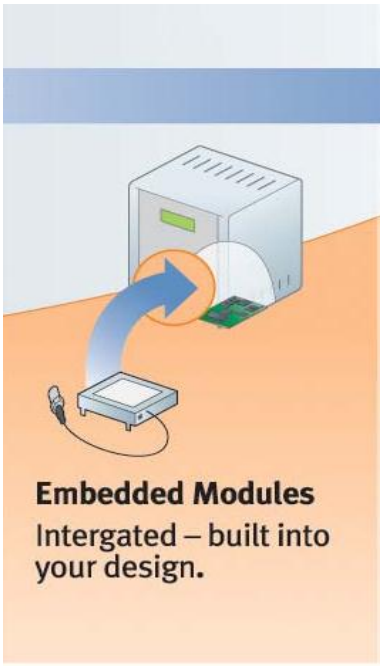
External device servers with multiple serial ports are well-suited in medical applications. Hospital Intensive Care Units (ICU) can take advantage of multi-port device servers to consolidate bedside patient monitoring devices and to securely transmit patient data back to the hospital's data center. The data is then processed by the clinical information system (CIS), which is made available to remote care providers to monitor patient conditions in real-time. Remote care providers can then alert the onsite ICU team of any immediately required patient treatment.

Neonatal Intensive Care Units (NICU) can also find device servers instrumental in caring for new infants. NICU teams are aggressively seeking productivity and efficiency gains as a result of continued nursing shortages. Device servers aggregate all infant monitoring equipment and send the data to one consolidated location. The NICU team is now able to perform their duties more efficiently, which results in improved patient care. Care providers striving to offer the best possible patient care are well served by external device servers that optimize time and resources even in times of personnel shortages.

External device servers typically consist of 1 to 48 serial ports and one 10/100Base-T Ethernet port.
The serial ports are available in a variety of physical interfaces -- RJ-45, RS-232, RS-485, RS-422, DB-9 male, DB9 female, DB25 male, and DB25 female -- to offer the end customer and medical device manufacturer a choice in cabling. However, the serial interface is not a big concern since the device server manufacturer should also offer cabling adaptors to support any medical device. A power adaptor or power cable should also be supplied to support 110-230 volt circuitry. At a minimum, the units should support baud rates from 300 to 230K, along with RS-232, RS-485, and RS-422 serial interfaces.

Internal or Embedded Device Servers

Embedded device servers are installed internally in medical devices by the original equipment manufacturer (OEM). This enables the medical device manufacturer to network-enable their products prior to shipping to the end customer.



Devices such as cardiac-output, heart-assist, continuous-dialysis, and glucose analyzers can all be network-enabled using embedded device servers, enabling health care providers to transmit patient data right out-the-box over their IT networks. Embedded device servers also apply to manufacturers of alert messaging systems used by first-responders, municipalities and onsite health care facilities at college campuses. These manufacturers offer both wired and wireless applications like that of college campuses where emergency text messages can be sent to sign boards strategically placed throughout the campus. The campus health staff can also send messages to the sign boards from anywhere on the campus using a hand-held messaging device, embedded with a wireless device server.

Typically, embedded device servers offer several different I/O interfaces including RS-232, RS-485, i2c, and SPI for communicating to the medical device's microprocessor. Other options include configurable GPIOs, a variety of pin headers and form factors. Baud rates from 300 to 921K are typically supported. Device server manufacturers should also provide a software developer's kit (SDK), including a Linux development environment, to allow developers to easily create value-added applications.

Selecting the Right Device Server Manufacturer

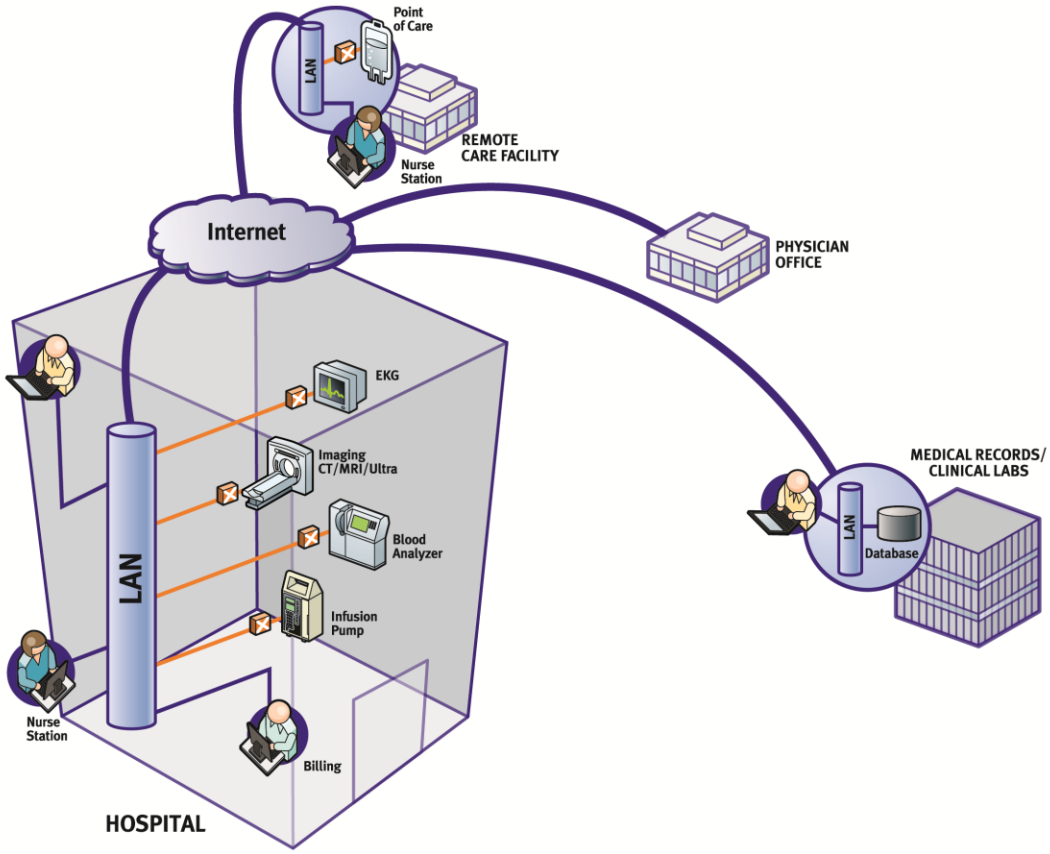
The first step toward choosing the right device server for your application is ensuring that you have the right supplier. First ask the basic questions: How long has the company been in business, how many clients does the company serve, how many devices in their product portfolio are network enabled, and how fast is the company growing. Once you have the answers to the basics, here are five ways to help ensure that a manufacturer is a good fit for your company:

- Customer-Centric philosophy: First and foremost, examine how your potential supplier does business. Does the company understand your application, the market you serve, and your requirements?

- Continued Market Focus: Is the manufacturer a leader in the industry? Be sure the manufacturer will be able to support your existing medical devices during their lifecycles, and develop new solutions as your requirements grow and change in the health care industry.
- Experience Developing Market Solutions: The combination of serial devices, protocols, security requirements, network topology, and market regulations is virtually unlimited. Factors such as cost and operation environment also determine the type of device server solution best suited for a particular market. Look for a vendor that has the engineering resources and experience with both wired and wireless solutions.
- Dedicated to Device Networking: Is device networking the manufacturer's core business? Consider where their R&D, support and market focus will be today and in the future. Selecting a vendor that is dedicated to device networking will result in continued support, active R&D investment and technology improvement.
- Technical Support: To ensure that you obtain the highest value for your device networking investment, choose a vendor that backs up its products with a knowledgeable and reputable technical support staff, and offers a variety of technical support options. Is tech support fee-based or included? Does the manufacturer have field application engineers (FAEs)? Does the company offer training, maintenance, and a warranty?

Device Server Solutions from Lantronix

Lantronix offers a wide selection of external and embedded device servers designed to support the health care industry and allow medical Original Equipment Manufacturers (OEMs) to quickly add network connectivity.



External Device Servers

EDS8PS and EDS16PS

Hybrid Ethernet Terminal and Multiport Device Servers

Key Features:

- Ethernet multiport configuration
- Curved edges on the top of the unit to allow for spillage runoff
- An edge overhang to protect the serial ports from spillage
- No power toggle to prevent accidental power loss to the unit
- Security available via SSH, SSL, AES encryption, username/password protection, IP filtering
- Meets the European Union's Restriction of Hazardous Substances (RoHS) Directive

EDS4100

4-Port Enterprise Device Server

Key Features:

- Four-port configuration
- No power toggle to prevent accidental power loss to the unit
- Security available via SSH, SSL, AES encryption, username/password protection, IP filtering
- Flexible power options including Power over Ethernet (PoE)
- Built-in web server
- RoHS-compliant

UDS1100 and UDS2100

External Device Server

Key Features:

- Available in one or two port models
- Serial-to-Ethernet connectivity for devices with RS-232/422/485 serial interfaces
- No power toggle to prevent accidental power loss to the unit
- Security available via AES encryption and password protection
- RoHS-compliant

WiBox

Wireless Device Server

Key Features:

- Dual-port configuration
- No power toggle to prevent accidental power loss to the unit
- Security available via AES Encryption - 128-256-bit Rijndael AES Encryption, NIST AES FIPS-197 CERT#120
- Wireless security available via WPA - PSK w/ TKIP encryption, WPA2/802.11i - PSK w/ AES-CCMP encryption
- Built-in web server
- 802.11b/g wireless interface
- RoHS-compliant

A custom battery-powered version of the WiBox™ is integrated into the LifeScan OneTouch® DataLink® Unit.

Embedded Device Servers

DeviceLinx Embedded Networking Modules

Key features:

- Integrated solutions that deliver production-ready hardware and software
- Serial to Ethernet networking, together with a host of interfaces
- Robust secure communications including 256-bit AES encryption and SSL/SSH networking
- RoHS-compliant

Conclusion

It is a challenging yet exciting time for the health care industry. Strong government initiatives and financial support will transform the industry by insuring all patient health records will be available electronically to health care providers and patients via a nationally shared health care network. The best electronic and networking technology will soon be implemented which will modernize the industry and greatly improve the level of care the heath-care industry can provide. Lantronix is ideally positioned to offer medical industry proven network enablement and remote access solutions for the emerging health-care industry.