Implementation of a Comprehensive EMR System in the Secure Corporate Environment

By

Chris Urban

Lewis University

April 2011

(This page has been intentionally left blank)

TABLE OF CONTENT

ABSTRACT

In today's business world, home care organizations are facing increasingly more complex challenges. To meet these challenges, there is need to automate the business with a home care software system that can quickly and easily perform scheduling, administrative, and clinical tasks, be configured to fit the policies and procedures and rapidly scale up to meet growing demand or handle new lines of business. At the same time, the solution has to be intuitive to learn and easy to use.

This project presents an implementation of a new EMR (electronic medical record) integrated system to serve multiple functions for Advocate Home Health Services and to fulfill goals of increased efficiencies, streamlined process improvement, reduction of operating costs, increase of patient data security, and maximized reimbursement. Several areas of Information Systems will be involved or touched by this project, starting with huge involvement of Network and Security and ending up with software and hardware deployment. I'll also show importance of business continuity and disaster recovery planning.

CHAPTER ONE

INTRODUCTION

1.1 Purpose and Scope

Advocate Healthcare is one of nation's top 10 health systems and is the largest integrated healthcare system in the state. It is a collection of hospitals, medical groups, home health services and network outpatient centers. Advocate Home Health division, where I work, is a big part of overall system. We have a comprehensive range of home care professionals, products, and services that provide a seamless transition from hospital to home. [1] As much as being part of home health, we are also integrated with Advocate's Information System. Information Systems supports the Mission, Values, and Philosophy of Advocate Health Care by deploying information technology as an integral part of the strategic and tactical plans of Advocate Health Care. It provides leading edge technology that positions Advocate Health Care as a nationally recognized, faith-based system, with the best service and health outcomes in Chicagoland. It is the aim of Information Systems to improve patient safety and enhance clinical outcomes through the provision of clinical information and technology that is all inclusive, available anytime, anywhere, securely, and appropriately. Also, Information System's goal is to maintain implemented Security Program and Administrative System that provides Advocate Health Care with the ability to protect and monitor Protected Health

Information (PHI) from Unauthorized Access or Use In Accordance With HIPAA, HHS Regulations and Industry Best Practices. [2]

To meet business goals and stay in accordance with Advocate's mission and policies we will be implementing Allscripts Homecare. It is an industry-leading system designed to improve clinical quality of care, financial performance, and operational control. It provides business, clinical, and scheduling functionality for multiple lines of business. Home health, hospice, and private duty are combined seamlessly in one integrated home care software system. This system incorporates a three-tier architecture that distributes processing between clients, servers, and a central database. This three-tier architecture is perfect for our multi-location business with hundreds of users. This system uses Microsoft SQL as a database management system for its superb performance, scalability, low cost of ownership, and easy access to data. Automatic database backups help ensure data safety and integrity. The system supports most common Windows-based laptops. Field devices can be remotely synchronized with the home office system. Synchronization uploads all field data to the home office database and automatically updates the data in field devices, based on any changes made to the central files since the last synchronization. Remote users can communicate with the main office system via any TCP/IP connection. The system implements blowfish encryption and uses the same 128-bit data keys for security as the CIA, FBI, and other U.S. government agencies making data virtually hacker-proof. All data from field to home office, from clients to servers are fully encrypted to maximize patient privacy.

Access to data, functions, screens, and records is password-protected and set by the system administrator. [4]

The system that is presented and documented will be used according to Advocate's security policies. The policy we will start with establishes standards and guidelines for new system implementations in support of Information Security Policies and Procedures and assures that adequate security measures are included at the time of system implementation. Another important policy that we'll follow guarantees to our new system a secure environment with the establishment of sufficient and reasonable measures to control access to the resources. Working with our Security group, we will ensure technical security measures to guard against unauthorized access to our electronically protected health information that is being transmitted over the electronic communications network. As such, we will continually assess potential risks and vulnerabilities to protected health information in our possession, and maintain appropriate technical security mechanisms to guard against unauthorized access. [3] Our new system will be placed on Advocate's own dark fiber network. The Metropolitan Area Network which Advocate is part of contains wired as well as wireless networks. It uses Fiber Distributed Data Interface (FDDI) which provides a 100 Mbit/s optical standard for data transmission. In addition to covering large geographical areas it supports thousands of users. To implement new system on the network is a complex process and requires involvement of many departments.

This paper is organized as follows. Chapter 2 will present an overview of Allscripts System. In Chapter 3, the focus will be on hardware and software used for implementation of the new system. Chapter 4 will concentrate on the environment, where the system will be placed. Conclusion will be presented in Chapter 5.

CHAPTER TWO

OVERVIEW OF ALLSCRIPTS HOMECARE SYSTEM

2.1 Three-tier Architecture

The Allscripts system that will be implemented incorporates three-tier architecture which distributes processing between clients, servers and central database. Please, see Figure 1 for Three-Tier Architecture.

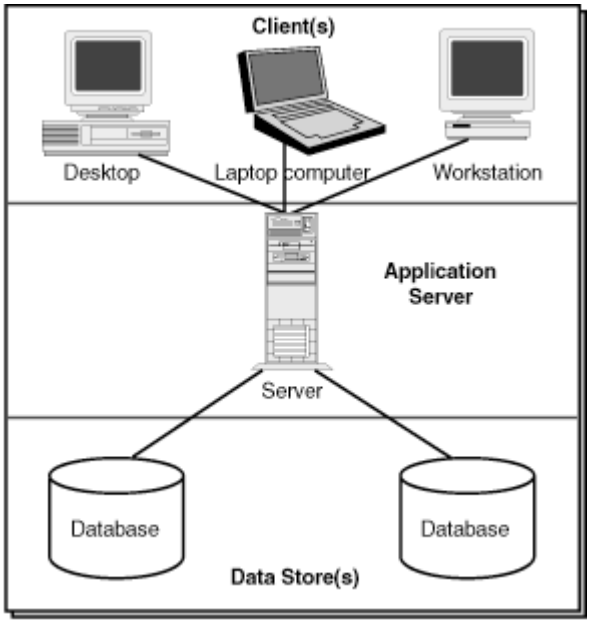

Figure 1. Three-Tier Architecture

In Tier 1, the client contains the presentation logic, including simple control and user input validation. This application is also known as a thin client. Tier 2 the middle tier, is also known as the application server, which provides the business processes logic and the data access. In tier 3, the data server provides the business data. Thanks to the advantages that this architecture brings, three-tier architecture is very popular in many systems. In this type of architecture, it is easier to modify or replace any tier without affecting the other tiers. By separating the application and database functionality system can have better load balancing. Also, adequate security policies can be enforced within the server tiers without interrupting work for clients. [5]

2.2 Hardware and Software Requirements

To begin the search for hardware and software we started with requirements recommended by the vendor – Allscripts. It includes information about the environment for a new system as well as hardware and software that should be used. Here is the list of the requirements:

Network Requirements:

- TCP/IP network
- Broadband Internet access (at least 1.5MB/s)
- Minimum 100BaseT switched network topology. Gigabit connection between servers in multi-server configurations

- Application Server must have a durable Internet connection with a static IP address with adequate bandwidth to remote connections to accommodate the number of simultaneous connections and the nature of tasks being performed. [7]
- Minimum 56K per user with low latency is required (50ms or less is recommended)

General Server Requirements / Configuration:

Allscripts Homecare requires dedicated servers. No other applications should be installed (beyond standard server maintenance applications such as virus protection, monitoring, security, etc.) on the Allscripts Homecare servers.

Allscripts Homecare configurations need to include the following servers:

- Application Server – business logic and data access layers, batch processing
- Database Server – Database access
- Integration Server – Physician Portal – Web portal that gives physicians real-time access to inpatient electronic health record (EHR) software and other information from anywhere using the Web. [6]

Additional Application Server Requirements:

The following items must be installed on the Allscripts Homecare Application Server.

- A static IP address
- Microsoft MSMQ
- Microsoft IIS

- .NET Framework 3.5
- Allscripts Remote Access Software (Secure Link)

Hard Drive Configuration:

The following are recommendation for hard drive speeds on all servers.

- Hard Drive: 15000 RPM

Application Server:

- Dual processor, minimum Pentium IV class (2.5GHz+ recommended) workstations
- Minimum 4GB RAM
- Two 146GB 15000 RPM SCSI Drives RAID 1 (Software Partition)

Database Server:

- Dual processor, minimum Pentium IV class (2.5GHz+ recommended) workstations
- Minimum 4GB RAM
- Two 146GB 15000 RPM SCSI Drives RAID 1 (Software Partition)
- Four 146GB15000 RPM SCSI Drives RAID 10 (Data Partition)

SQL Server Requirements:

Allscripts Homecare uses Microsoft SQL Server for data storage.

SQL Server Options:

- Microsoft SQL Server 2005 Standard or Enterprise, 32 bit or 64 bit
- Appropriate SQL licensing – server license plus CAL for every host or field users, or per processor license (unlimited CALs)

Workstation Requirements:

- Minimum Pentium IV class (2.5GHz+ recommended) workstations with minimum 2GB of RAM.
- Operating system options

  Windows XP Professional

  Windows Vista Business

  Windows 7 Professional
- 1024 X 768 minimum screen resolution (17" or above monitors are recommended for ease of viewing screens)
- Minimum available hard drive space of 4GB
- Internet Explorer 7 minimum
- .NET Framework 2.0 or higher
- JavaScript and cookies must be enabled
- Recommend ActiveX be enabled for Internet Explorer
- 7200 RPM or faster hard drive recommended

Field Device (Laptop/Tablet) Requirements:

- Minimum Pentium IV class (2.5GHz+ recommended) workstations with minimum 2GB of RAM.
- Operating system options

  Windows XP Professional Standard or Tablet

  Windows Vista Business Standard or Tablet

  Windows 7 Professional
- 1024 X 768 minimum screen resolution
- Minimum available hard drive space of 4GB
- .NET Framework 2.0 or higher
- 5400 RPM or 7200 RPM hard drive recommended
- Remote access for synchronization to Allscripts Homecare application server via TCP/IP (i.e. client supplied VPN, RAS, or network modem)
- Touch screen is strongly recommended for signature capture & ease of use

2.3 Encryption

To make sure that we are compliant with HIPAA Regulations we had to choose our new system according to them. Type of encryption used by Allscripts was one of the decision points. That information is critical for the data transfers that would be going on between clinicians, office stuff, IT department and the system's database. We learned that our new system implements Blowfish encryption and uses 128-bit data keys for security.

Blowfish is a keyed, symmetric cryptographic block cipher. Blowfish's security has been extensively tested and proven. [8] As a public domain cipher, Blowfish has been subjected to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. This should be great news to anybody using it. Blowfish is a 16-round Feistel cipher and uses large key-dependent S-boxes. The diagram below – Figure2 shows the action of Blowfish. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries. The F function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output. Since Blowfish is a Feistel network, it can be inverted simply by XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order. Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern. The secret key is then XORed with the P-entries in order. A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P1 and P2. The ciphertext is then encrypted again with the new subkeys, and P3 and P4 are replaced by the new ciphertext. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4KB of data is processed. [8]

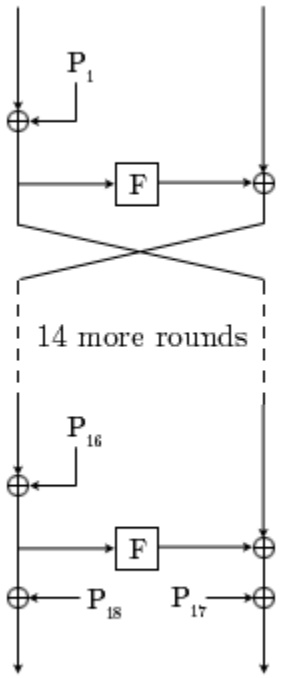

Figure 2. How Blowfish works

Blowfish is one of the fastest block ciphers in widespread use, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers. [8] The relative strength of the encryption algorithm is based on key length. Bruce Schneier, creator of the Blowfish encryption algorithm, has calculated that according to what is called of quantum mechanics today, that the entire energy output of the sun is insufficient to break a 197-bit key. The most common key lengths used by today's web browsers are "40-bit" and "128-bit." As a comparison, a 40-bit key can be "cracked" within a few hours by an average personal computer. [9] However, a 128-bit key would take about one billion strong computers, each capable of trying one billion keys per second. In other words, it would take millions of years to try every possible combination of bits in a 128-bit key. In

the presented example, the 128-bit encryption is not just three times stronger than 40-bit encryption; it is 309,485,009,821,345,068,724,781,056 times stronger what should make users of the encryption pretty happy with that result. Our project will use 128 bit encryption and based on an example above, I think that will give us strong security for our new system.

2.4 Summary

Allscripts identified certain needs for specific hardware and software to be used for the new system implementation. HIPAA data encryption standards require health care providers like Advocate Healthcare, who transmit, store or access protected health information in electronic format to achieve a certain level of data encryption. In Chapter 3 I will provide recommendations that meet these requirements.[9]

CHAPTER THREE

DEPLOYMENT SUMMARY – HARDWARE & SOFTWARE

3.1 Field devices

To meet the vendor's Field Device requirements, Lenovo ThinkPad X201 Tablet has been chosen as a device to serve our clinicians as their input tool. This particular tablet is a thin, light weight and reliable convertible tablet laptop that offers pen, finger and keyboard input options required by mobile professionals who need quick access To electronic data while working outdoors or indoors. It is supplied in latest panel technology for a superior pen and finger touch experience. Here is a list with some details why this is right choice for us:

- 3.57 lbs starting weight
- Up to 8 hrs battery life
- Wide Viewing Angle Panel technology for on-the-go presentations and computing.
- Multiple wireless connectivity options—WiMAX, GPS and Wireless WAN" (7)

Hardware experts like the durability of this unit. The X201 Tablet is designed from the inside out to withstand the rigors of life outside the office:

- Designed to pass 8 rigorous MilSpec tests

(physical shock, thermal shock, altitude, dust, vibration, humidity, heat and cold)

- Shock-mounted hard drive protection with Active Protection System

- Spill-resistant keyboards

- Magnesium alloy or carbon-glass fiber top and bottom covers

It is comfortable and easy to use. It was designed to be comfortable and easy to use whether user is sitting, standing, or walking or whether user is using the pen, finger, or the keyboard. It is perfect for our clinicians because it provides a lightweight, durable and reliable tool to automate their lives and help transition toward fully electronic medical records. The ThinkPad X201 Tablet also provides industry-leading wireless technology for sharing and transferring patient records to central hospital servers and the advanced security options to ensure protection and privacy of those confidential records. [10] Just to confirm that the right move was done choosing Lenovo product we confirmed with the resources that Lenovo is one of the lead laptop providers and they use the latest technologies in their products. Since 2005, the ThinkPad range has been manufactured and marketed by Lenovo, which purchased the IBM personal computer division. Known for their reliability, quality, durability, and performance, ThinkPads are popular with businesses, corporations, and schools; the ThinkPad has been used in space including being the only laptops certified for use on the International Space Station.[11]

3.2 Back-office devices

As far as a workstation choice for our system, there will be upgrade to company's existing computers and HP products will be used. HP has a perfect line of workstations that might be used for our project. HP Compaq dc7900 Business PC uses Energy efficient technologies, leading remote manageability solutions, and there is three flexible form factors designed to fit our specific business needs. The HP Compaq dc7900 PC is the stable platform that can lower the cost of ownership. [12] HP Compaq Business Desktop dc7900 series is HP's most stable and secure business PC with professional innovations such as energy efficient technologies and leading remote manageability solutions. [13] Here is some hardware specifications that will be installed on the HP Compaq Business Desktop dc7900 Small Form Factor sold to us: - Processor - Core 2 Duo E8500 / 3.16 GHz, RAM 3 GB, HDD 2 x 160 GB, DVD±RW (±R DL) / DVD- RAM, Gigabit Ethernet, Windows7 Professional.

3.3 Servers

For server hardware, there was a search for system which would help to improve cost-effectiveness with high performance, simplify management and serviceability and manage risk with resilient architecture and virtualized environment. The one that was chosen for our project was IBM System x3650 M3. Our attention was caught with energy-efficient design which supports more cores and memory and data capacity in a

scalable 2U package that is easy to service and manage. With more computing power per watt and the Intel Xeon processors, costs could be reduced while maintaining speed and availability. What was impressive about the x3650 M3 was that it offers a flexible, scalable design and simple upgrade path to 16 HDDs or SSDs, and 192 GB of memory. It also was equipped with comprehensive systems management tools such as advanced diagnostics, a cable management arm and the ability to control resources from a single point. Below is a list of the features that we find important to adapt for the new system:

- Power optimized performance that leverages the speed of new Intel processors with more capacity and memory.
- Innovative, energy smart 2U design to help lower operational costs.
- Energy efficient design with UDIMMs, 40 W processing and UEFI BIOS.
- Better service ability with a highly scalable, flexible design that is easy to deploy, integrate, service and manage.
- Easier risk management with resilient architecture.

Here is hardware summary that can be used successfully when implementing the new system:

- Up to two 3.46 GHz six core Intel Xeon 5600 series processors, up to 1333 MHz memory access speed.
- Up to 192 GB RDIMMs or 48 GB UDIMMs high performance, new generation DDR-3 memory.

- Internal storage flexibility with up to sixteen 2.5" hot-swap SAS/SATA HDDs or SSDs.
- Low 675 W design and up to 94% efficient power supplies, six cooling fan modules, new UEFI BIOS, altimeter monitored by Integrated Management Module and IBM Systems Director Active Energy Manager.
- NEBS 1/ETSI equivalent compliance for both AC and DC power supplies.
- VMware ESXi embedded hypervisor support with optional 2 GB USB key for virtualization [14]

The IBM hardware that was chosen will be good fit for us. It comes in a, 2U rack which comes with the hardware provides expandability and high performance in a dense form factor. As far as processors go, high-performance, energy-efficient six-core Intel Xeon 5600 series processors improve productivity through higher processing performance, reduce cost with outstanding performance per watt, maximize multithreaded applications for faster concurrent execution and large cache size, which yields faster transaction processing. Fast 1333 MHz, DDR-3 RDIMM memory with 18 DIMM slots support 2 GB, 4 GB, 8 GB or 16 GB DDR-3 RDIMMs with 18 slots which is perfect for memory scalability and ideal for compute-intensive, general-business applications and virtualized environments. It has the ability to transfer I/O data at eight times the speed of the memory cell it contains, enabling faster bus speeds and higher peak throughput than previous-generation memory. The system supports the VMware ESXi embedded hypervisor and it’s designed to optimize virtualization performance. It also comes with IBM Systems Director which is a comprehensive systems management platform that helps to increase uptime, reduce costs and improve productivity via advanced server

management capabilities. It also provides IBM Systems Director Active Energy Manager which helps to provide advanced power notification and control, monitor power consumption, achieve lower heat output and decrease cooling costs. IBM Calibrated Vectored Cooling helps to maintain a healthy system by keeping internal components cool. Snoop filters on Intel core chipset improve application efficiency to boost processor performance. IBM Integrated Management Module (IMM) increases server availability by continuously monitoring the system and notifying of potential system failures or changes. [15]

As a backup solution for our servers, Symantec NetBackup software has been chosen. It provides the ability to protect completely and store efficiently. It is data recovery program with comprehensive data protection for virtual environments like the one at Advocate. Software for data recovery enables more efficient backups and faster restores of virtual environments through deep hypervisor integration.

3.4 System's Virtualization

Having all the hardware in place allowed us to introduce virtualization to our existing environment. We had a chance to create an automated system built on VMware

virtualization platform. When we researched different system options and got familiar with the “virtualization world”, it made sense to put our new system on a virtual platform. It allowed us to run multiple virtual machines on a single physical system, with each virtual machine sharing the resources of the one physical system. How does it work? The VMware virtualization platform that we chose is built on a business-ready architecture. It uses software to transform hardware resources including the CPU, RAM, hard disk and network controller to create a fully functional virtual machine that can run its own operating system and applications just like a normal computer. Each virtual machine contains a complete system, eliminating potential conflicts. VMware virtualization works by inserting a thin layer of software directly on the computer hardware or on a host operating system. This contains a virtual machine monitor that allocates hardware resources dynamically and transparently. Multiple operating systems run concurrently on a single physical machine and share hardware resources with each other. By encapsulating an entire machine, including CPU, memory, operating system, and network devices, a virtual machine is completely compatible with all standard operating systems, applications, and device drivers. [16] We looked for a stable virtualization provider and we agreed on using VMware. They are the world's leading desktop and datacenter virtualization provider. By implementing VMware, we maximized our hardware and software investments with our servers, network, storage, operating systems, and applications. [17]

Another important piece to our new development was disaster recovery planning. Traditional disaster recovery solutions are often very costly and complex and can’t meet

the recovery objectives even after doubling hardware and cost. Testing them can be a nightmare because the steps are tedious and the documentation is hard to keep up-to-date. In case of disaster, VMware allows us to recover to any machine, not just specific duplicate hardware, reducing hardware costs and maintenance budget and lowering the complexity of maintaining a backup site. It gives us confidence that we can recover from disasters rapidly, ensure reliable disaster recovery, reduce the cost of disaster recovery and automate disaster recovery. Traditional disaster recovery plans require many manual, complex steps to allocate recovery resources, perform bare metal recovery, recover data and validate that systems are ready for use. VMware virtualization simplifies this environment. Hardware configuration, firmware, operating system install, application install become data stored in just a few files on disk. To protect these files, only good backup is needed or replication software. These files can then be recovered to any hardware without requiring any changes, because virtual machines are hardware-independent. Outdated recovery plans are often difficult to test, difficult to keep up-to-date, and depend on exact execution of complex, manual processes. In a virtualized environment, testing is simpler because it can be executed with non-disruptive tests using existing resources. Hardware independence eliminates the complexity of maintaining the recovery site by eliminating failures due to hardware differences. [18]

3.5 Security, Monitoring and Recovery Software

After research and numerous consultations, our technical advisors decided to use Computrace from Absolute Software as a solution for security of our remote devices. LoJack, which is another name for the product is a computer theft recovery service with remote device and data security features. If the portable device is stolen or missing, there is possibility to remotely block access to it and the personal data it contains. If the protected computer is stolen, the Recovery Team uses latest technology to track it, and then works in parallel with local law enforcement to get it back. [19] There are two ways to protect important data. Data Delete function can be used to erase personal information and sensitive files remotely. Provider also can prevent access to the computer by freezing it remotely. Any attempt to use it displays a message from owner onscreen. Geolocation is a nice tool that can track computers on an online map. It uses GPS or Wi-Fi to map owner's laptop's current and past locations. The technology behind Absolute Software's products is the Computrace Agent, a small software client that is embedded into the BIOS firmware of most computers at the factory. The Agent in the computer maintains daily contact with the Absolute Monitoring Center. If owner reports the stolen computer, Agent contact will increase to every 15 minutes. Increased contact allows provider to obtain specific details like the physical location of the computer, any activity that has occurred post-theft, and other important data that will aid vendor in working with local law enforcement to catch the thief and return the property to owner. [20] Regardless of recovery status, owner still can remotely delete data to remove some or all of the information stored on the portable device so that it doesn't fall into the wrong hands. This could include files and applications containing personal photos, internet bookmarks, browser cookies, financial information, and stored passwords. If the

computer has been stolen, user must complete a couple of steps: Report the theft to local law enforcement as soon as possible and report the theft to the vendor and complete the theft report. [21] To recover stolen computers, Recovery Team tracks the computer via its internet connection. When the user connects to the internet with stolen computer, the vendor begins to collect information on the user which can help lead the police to the location of the computer.

There are two main types of information they use that can help to assist the police. The Internet Protocol (IP) Address of the computer registers with their Monitoring Center each time the computer connects to the internet. This information can be useful in determining the location of the computer. The process also uses forensic information which can be gathered from the stolen computer through the use of patented Forensic Tools which are downloaded to the computer once it is reported as stolen. [22]

3.6 Remote connections – VPN

As I mentioned before, our clinicians will use tablets to connect and synch information to our network. To help them to manage the connections and do it in secure manner, we'll be using the Cisco VPN client. Cisco VPNs help securely connect offices, remote users, and business partners. VPNs have become the primary solution for remote connectivity for organizations of all sizes, using affordable, third-party Internet access. Cisco VPN solutions provide exceptional security through encryption and authentication

technologies that protect data in transit from unauthorized access and attacks. A Cisco VPN helps users:

- Use highly secure communications, with access rights tailored to individual users
- Quickly add new sites or users, without significantly expanding your existing infrastructure
- Improve productivity by extending corporate networks, applications, and collaboration tools
- Reduce communications costs while increasing flexibility [23]

A Cisco client will be very helpful for our organization to accomplish what we looking for because Remote access VPNs provided by them extend almost any data, voice, or video application to the remote desktop, emulating the main office desktop. With their VPN, user can provide highly secure, customizable remote access to anyone, anytime, anywhere, with almost any device. Cisco remote access VPNs:

- Create a remote user experience that emulates working on the main office desktop
- Deliver VPN access safely and easily to a wide range of users and devices
- Support a wide range of connectivity options, endpoints, and platforms to meet your dynamic remote access needs [23]

It’s very easy to make the VPN experience simpler and more secure with the enhanced remote access technology of Cisco AnyConnect Secure Mobility Client. This software builds on prior Cisco AnyConnect VPN Client offerings to improve the always-on VPN experience across more laptop and smartphone-based mobile devices. As mobile

workers roam to different locations, with always-on and intelligent VPN, the Cisco AnyConnect client can:

- Automatically select the optimal network access point
- Adapt its tunneling protocol to the most efficient method

Cisco AnyConnect is the first VPN solution to use the Datagram Transport Layer Security (DTLS) protocol. The DTLS protocol provides communications privacy for datagram protocols. This protocol allows applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery which is very important in medical business where sensitive information is being transferred all the time. DTLS helps provide an optimized connection for latency-sensitive traffic, such as voice over IP (VoIP) and TCP-based application access. [24] The Client helps enable built-in web security and malware threat defense as part of the Cisco AnyConnect Secure Mobility solution. Users can now have a choice in supplementing employee access to corporate resources from advanced mobile devices and different locations with a consistent, context-aware security policy which is very important in today's world.

Establishing encrypted VPN tunnels with the Cisco VPN Client provides highly secure remote connectivity for the mobile employees. It is very important that their IPSecurity (IPsec) -based VPN client is compatible with all Cisco equipment. [25] The Cisco client can be preconfigured for mass deployments. It is very important with multiple devices.

It requires little user intervention for initial logins, which makes it very easy to use for clinicians. It also supports Cisco Easy VPN capabilities by decreasing network security policy configuration at the remote location

The Cisco VPN Client supports practically any OS platform. This project uses Windows XP/ Windows 7 devices, but it is good to know that the provider has wide experience with all platforms for troubleshooting.

CHAPTER FOUR

INSTALLATION ENVIRONMENT

4.1 Network Overview

Advocate owns a dark fiber network. It is a privately operated optical fiber network that is run directly by its operator (Advocate) over dark fiber leased or purchased from another supplier, rather than by purchasing bandwidth or leased line capacity. Dark fiber networks may be used for private networking, or as Internet access or Internet infrastructure networking. Dark fiber networks may be point-to-point, point-to-multipoint, or use self-healing ring or mesh topologies. [26] The type that is owned and managed by Advocate is fully meshed network for high redundancy. Our network operates using the latest optical protocols using wavelength division multiplexing to add capacity where needed, and to provide an upgrade path between technologies without removing the network from service. We are part of a metropolitan area network (MAN) which is a large computer network that services large part of Chicagoland area. Our MAN interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet. A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be

owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks. [27] We use Fiber Distributed Data Interface (FDDI) which provides a 100 Mbit/s optical standard for data transmission in a local area network . It can extend in range up to 200 kilometers (124 miles). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber. [28]

There are several advantages in using FDDI:

- FDDI supports real-time allocation of network bandwidth. - This allows you to use a wide array of different types of traffic.
- FDDI has a dual ring that is fault-tolerant. The benefit here is that if a station on the ring fails or if the cable becomes damaged, the dual ring is automatically doubled back onto itself into a single ring.
- The FDDI compensates for wiring failures. The stations wrap within themselves when the wiring fails.
- Optical bypass switches are used that can help prevent ring segmentation. The failed stations are eliminated from the ring. It is important because ssubsequent failures will cause additional ring segmentation. [29]

4.2 Security Approach – Policies

Advocate Health Care maintains many policies related to system security. This section describes those policies that directly affect implementation of the new system.

Data Security Access Control Policy establishes that Information Systems provides a secure environment for Information System's managed computerized assets with the establishment of sufficient and reasonable measures to control access to these resources. It is important for any devices connected on our network. This policy ensures that whenever practical, users manage their own security. For the major systems that cross functional boundaries, the Information Systems performs the day-to-day activities. Information Systems and Internal Audit perform periodic reviews to ensure that security practices are appropriate. Access to each system is controlled by individual passwords. Random computer generated passwords are supplied to local security administrators by Information Systems for this purpose. Whenever possible, applications are purchased and designed to allow the users to change their own passwords periodically. On those systems that have no such capabilities, passwords are changed at least on a semi-annual basis. Applications are designed and modified to limit the users to access only that information covered by their job function. Access control measures prevent unauthorized users from gaining access to communication networks and legitimate users from accessing unauthorized resources. Also, unauthorized local access is prevented, and remote access is controlled so that individuals desiring access are identified as authorized. [30]

Another very important policy is the one that covers Information Security for New System Implementations. This policy establishes standards and guidelines for new system implementations in support of Information Security Policies and Procedures and assures that adequate security measures are included at the time of system implementation. These standards apply to all new system implementations planned and controlled by the Advocate Health Care. An evaluation of new product security features must be part of the software selection phase to assure that adequate security is inherent in all new purchased applications. Security Administration personnel is assigned to the selection team to review the security portion of new systems. Among the features that should be included are:

- user-id field of at least six characters and a password field of eight alpha-numeric characters in length.
- The ability to automatically change passwords on a periodic basis.
- The ability to create users with different levels of access.
- The ability to log and report security violations as well as security changes.
- An encrypted password file or the ability to secure files by other means.
- The ability to have the system automatically time-out a terminal after a period of time has elapsed with no terminal activity.

All implementation plans must include security tasks to assure that policies and standards are being adhered to, and that any necessary procedures are in place at the time production information is first loaded into the system, irrespective of production

dates. Security Administration personnel should be assigned to the implementation team for an orderly creation of security procedures. Security Administration needs to have final approval as to the makeup of user-ids and passwords on all security systems including operating systems, networks and applications. Security Administration personnel review new systems for access control requirements and apply applicable standards consistent with system capabilities and good security practices. Security Administration personnel will supply passwords to those applications that have no automated user password change capabilities. Security defaults such as password expiration, previous password usage, and terminal time-outs are implemented where ever applicable to provide enhanced security. Security Administration department also reviews new systems requirements as well as user practices to determine a convenient and effective standard for each system. Non-associates are authorized by the project leader for access to only the resources required and removed immediately when their participation in the project is completed. All non-associates, such as consultants and vendors, who have access to Advocate's system resources, must be identified to Security Administration. Included must be a listing of resources or privileges required and a projected date when their access can be removed. Access is removed upon completion of project tasks. Approved temporary access can be granted for follow-up work on an access by access basis. Confidential information must be processed and stored in a manner that is accessible only to those individuals specifically authorized to access it. Data owners must be consulted before implementation to define which information is confidential and review the distribution of that information. [31]

Another important policy is called the Business to Client VPN Policy. All our remote users will be directly affected by this policy. It explains how Approved Advocate Health Care employees and authorized third parties (customers, vendors, etc) may utilize the benefits of Virtual Private Networks (VPNs), which are a user managed service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. VPN capabilities and provided through Advocate Remote Connection (ARC). Policy shows clearly that approval for VPN access is granted to specific individuals on a case-by-case basis. Requests for VPN access must include a written justification that details the reasons why VPN access is needed. Vendors, Independent Consultants, and Independent Contractors requesting VPN access must also sign a confidentiality form. It is the responsibility of the employee or vendor with VPN privileges to ensure that unauthorized users are not allowed to access Advocate Health Care internal networks. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system. VPN gateways are set up and managed by Advocate Health Care network security team. All computers connected to Advocate Health Care internal networks via VPN or any other technology must use current anti-virus software. The approving management must inform Advocate Health Care's Security Administration Team immediately of the termination of any employee that they approved access for. Account activity is also closely monitored by the security team. [32]

With the support of our remote users and portable devices, we have to make sure that we are compliant with Advocate's security policies. We have to pay special attention to

remote connection rules. With the high amount of remote users, it is very easy to miss something what might be very costly down the road if rules are not followed properly. To make sure that the goal will be achieved, our organization has been preparing segmented control structure with our IT Director on the top and several associates with specific assignments reporting directly to him.

4.3 HIPAA Regulations

When there is a talk about security policies, HIPAA Regulations cannot be forgotten. This section discusses the nature of HIPAA and its importance.

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. As the industry has implemented these standards, and increased the use of electronic data interchange, the nation's health care system became increasingly effective and efficient. [33]

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical

safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information. [34]

Health information technology as we can see at Advocate Healthcare involves the exchange of health information in an electronic environment. Widespread use of health IT within the health care industry improves quality of health care, prevent medical errors, reduce health care costs, increase administrative efficiencies, decrease paperwork, and expand access to affordable health care. It is very important that the privacy and security of electronic health information is ensured as this information is maintained and transmitted electronically. [35]

An important component of Advocate's approach to HIPAA is a policy called "Confidentiality and Privacy of Protected Health Information". Its purpose is to provide guidelines for maintaining confidentiality and privacy of patient information. It is very clear that all disclosure from and access to Protected Health Information (PHI) should be carried out in accordance with legal, accrediting, and regulatory agency requirements. Incidental disclosures that may occur due to the communication that must take place when caring for a patient and for any treatment, payment and health care operations process is permitted as long as reasonable precautions are in place to reduce the likelihood of an inappropriate disclosure taking place. Breach of patient confidentiality and privacy may result in disciplinary action, up to and including termination. There are some general guidelines regarding public identification of patients. Any communication tool that contains name and diagnosis together may not

be displayed in or visible from any public area. The patient's name on the chart should not to be visible to persons not involved in patient care. When seeking information about patients through phone communications, the staff needs to give name only or leave a message providing telephone number. Staff's title, location, and purpose of call cannot be identified. An important part from IT standpoint is confidentiality of computers and fax machines. Computer screens should be logged off when unattended. Computers in-use should fade out so information cannot be seen by patient/visitors. Computer passwords cannot be shared. Fax machines cannot be left unattended with patient information left uncollected or in view of unauthorized individuals. [36] Our clinicians must be very careful when they will deal with remote devices and patient records. That's why following HIPAA rules becomes very important for records security. To help with these challenges our Organization invests a lot of resources into adequate hardware, fully encrypted integrated EMR system and security software.

CHAPTER FIVE

CONCLUSION

This paper has presented an implementation of a new EMR integrated system. This system will serve multiple functions for our business. It will help the organization to achieve goals to increase efficiencies, streamline process improvement, minimize operating costs, increase patient data security and maximize reimbursement. Certainly, the implementation of the plan described in this paper will introduce many challenges to our organization. The users, management, implementation team and vendors must be working together to achieve a success. The Field Technology team as well as Network and Security teams will be very busy to make sure that all aspects of the new system will be in total synch with existing environment. Even though it requires a lot of sacrifices from many individuals and departments it is worth it to have one single integrated home health system. Systems like this can produce many benefits. Comprehensive EMR system of this kind includes many business, clinical, and scheduling functionalities for multiple lines of business combined seamlessly in one integrated software package. It also meets new and emerging standards and requirements in healthcare industry including PPS, Medicaid, HIPAA transaction standards, ICD-9-CM code sets, CPT codes, entry of standard HCPCS codes, and requirements for password-protected electronic signatures. This can only translate in wide range of benefits in the future for the healthcare providers as well as their customers.

REFERENCES

1. Advocate Home Health Services Info. Retrieved January 22, 2011 from http://www.advocatehealth.com/body.cfm?id=57
2. Advocate Policies Info. Retrieved January 22, 2011 from http://advocateonline.advocatehealth.com/page.cfm?id=6314&fuseaction=pnp.listsearchresults
3. Advocate Security Awareness Info. Retrieved January 22, 2011 from http://advocateonline.advocatehealth.com/page.cfm?id=10233
4. Allscripts Solutions Information. Retrieved January 22, 2011 from http://allscripts.com/en.html
5. Three-tier architecture information. Retrieved on March 21, 2011 from http://www.linuxjournal.com/article/3508
6. Hardware requirements. Retrieved on February 19, 2011 from https://c.na0.content.force.com/servlet/servlet.FileDownload?file=00P00000007hRey
7. Hardware requirements. Retrieved on February 19, 2011 from https://www.misyshealthcare.com/Client+Support/Misys+Homecare/Documentation/Users+Guides.htm
8. Blowfish Encryption. Retrieved on March 3, 2011 from http://www.splashdata.com/splashid/blowfish.htm
9. Blowfish Encryption 128 Bit . Retrieved on March 3, 2011 from http://www.firstbackup.com/Product/Features/blowfish.asp
10. Lenovo Tablet Info. Retrieved on February 19, 2011 from http://www.lenovo.com/shop/americas/content/pdf/notebooks/ThinkPad/X-Series%20Tablet/X201t%20ThinkPad%20Tablet%20Datasheet.pdf
11. ThinkPad Info. Retrieved on February 19, 2011 from http://en.wikipedia.org/wiki/ThinkPad
12. HP Desktop Info. Retrieved on February 19, 2011 from http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01570344
13. HP Business Desktop Info. Retrieved on February 19, 2011 from http://www.pcwb.co.uk/catalogue/item/A0470209

14. Server Hardware. Retrieved on March 3, 2011 from http://www-03.ibm.com/systems/x/hardware/rack/x3650m3/index.html

15. Hardware details. Retrieved on March 3, 2011 from http://www-03.ibm.com/systems/x/hardware/rack/x3650m3/features.html

16. Virtualization Overview. Retrieved on March 3, 2011 from http://www.vmware.com/virtualization/what-is-virtualization.html

17. VMware Info. Retrieved on March 3, 2011 from http://www.vmware.com/virtualization/why-choose-vmware.html

18. Disaster Recovery. Retrieved on March 3, 2011 from http://www.vmware.com/solutions/continuity/disasterrecovery.html

19. LoJack for Laptops. Retrieved on February 19, 2011 from http://www.absolute.com/en/lojackforlaptops/features.aspx

20. Absolute Software Technology. Retrieved on February 19, 2011 from http://www.absolute.com/en/lojackforlaptops/technology.aspx

21. FAQ for LoJack. Retrieved on February 19, 2011 from http://www.absolute.com/en/support/consumer/faqs/stolen.aspx

22. Recovery Process. Retrieved on February 19, 2011 from http://www.absolute.com/Shared/FAQs/ABT-RS-FAQ-E.sflb.ashx

23. CiscoVPN. Retrieved on February 22, 2011 from.http://www.cisco.com/en/US/products/ps5743/Products_Sub_Category_Home.html?POSITION=SEM&COUNTRY_SITE=us&CAMPAIGN=HN&CREATIVE=Security+-+Tier+1_VPN&REFERRING_SITE=Google&KEYWORD=vpn+client_B|mkwid_sSdy9LRsh_5211189638_432txu7stz1v01134&gclid=CPPbzrbAn6cCFYgh3wodGC9cdw

24. Cisco Anyconnect. Retrieved on February 22, 2011 from http://www.cisco.com/en/US/products/ps10884/index.html

25. VPN Encryption. Retrieved on February 22, 2011 from http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html

26. Dark Fiber Network. Retrieved on February 22, 2011 from http://en.wikipedia.org/wiki/Dark_fibre_network

27. MAN. Retrieved on February 22, 2011 from http://en.wikipedia.org/wiki/Metropolitan_area_network

28. FDDI. Retrieved on February 22, 2011 from http://en.wikipedia.org/wiki/FDDI

29. FDDI Advantages. Retrieved on February 22, 2011 from http://www.ustudy.in/node/703

30. Data Security Access Control Policy. Retrieved on March 21, 2011 from http://advocateonline.advocatehealth.com/page.cfm?id=6314&fuseaction=pnp.viewPolicy&polref=2069&ei=p
31. Information Security for New System Implementations Policy. Retrieved on March 21, 2011 from http://advocateonline.advocatehealth.com/page.cfm?id=6314&fuseaction=pnp.viewPolicy&polref=2071&ei=p
32. Business to Client VPN Policy. Retrieved on March 21, 2011 from http://advocateonline.advocatehealth.com/page.cfm?id=6314&fuseaction=pnp.viewPolicy&polref=6561&ei=p
33. HIPAA Information. Retrieved on March 21, 2011 from https://www.cms.gov/hipaageninfo/
34. HIPAA Privacy Rules. Retrieved on March 21, 2011 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
35. Health information technology Information. Retrieved on March 21, 2011 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html
36. Confidentiality and Privacy of Protected Health Information Policy. Retrieved on March 21, 2011 from http://advocateonline.advocatehealth.com/page.cfm?id=6314&fuseaction=pnp.viewPolicy&polref=5850&ei=p