



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

**Approaching a HIPAA-compliant Health Care
Application**

GCWN Gold Certification

Author: Brian M. Lich
Advisor: Richard Genova

Accepted: January 30th 2006

TABLE OF CONTENTS

ABSTRACT.....	2
1. INTRODUCTION.....	3
2. PRE-IMPLEMENTATION PLANNING AND DESIGN.....	4
A. Functional Specification.....	5
B. Critical Item Identification.....	7
C. Design Analysis.....	12
D. Security Considerations.....	13
3. IMPLEMENTATION.....	14
A. Hardware Installation.....	15
B. Software Installation.....	16
C. Verification of Requirements.....	22
4. POST-IMPLEMENTATION AND MAINTENANCE.....	24
A. Post-Implementation Issues.....	25
B. Staying HIPAA Compliant.....	26
C. Change Management Policy and Procedure.....	30
5. CONCLUSIONS AND RECOMMENDATIONS.....	33

ABSTRACT

HIPAA security regulations are a priority for every information security professional charged with securing technology in a health care environment. In 2005, one organization, referred to as the Dental College, consolidated five legacy patient management systems into one, named axiUm, delivered via Citrix thin client computing technology. This paper will discuss how this organization approached their HIPAA security compliance by using Citrix as the secure medium for transmission of electronic patient health care information (E-PHI). Several questions will be answered in this paper:

- What steps did the Dental College do to make sure they met the HIPAA Security regulation standards?
- How are these standards audited to ensure that the established baseline is maintained?
- What steps could the Dental College do to improve on their existing HIPAA Security policies?
- Why was Citrix chosen as the means of delivering axiUm?
- How did Citrix help to secure E-PHI?

- How was the Microsoft Windows environment configured to ensure secure, reliable patient care?

1. INTRODUCTION

From Cisco Systems to ChoicePoint Incorporated, breaches in data have become a major problem in today's online environment. It is the organization's responsibility to ensure that confidential information is secured.

Due to the overwhelming occurrences of unauthorized disclosure of personal information, the federal government has put into place several rules and regulations that organizations are to follow in order to keep this data safe. In a healthcare environment, the Health Insurance Portability and Accountability Act (HIPAA) is a federal regulation that focuses on keeping patient health information (PHI) confidential. The full set of regulations can be found at the following web site:

<http://tinyurl.com/eyl7k>. Additionally, the National Institute of Standards and Technology has provided a resource guide that may assist in understanding the HIPAA regulations. This guide can be found at the following address: <http://tinyurl.com/9xo8m>.

During the time that the HIPAA regulations were set to go into effect, one institution was implementing a new patient management system. This paper will look at how a dental school in North America, referred to as the Dental College, approached these set of regulations using Citrix as the mechanism for securing PHI. This paper uses a case study approach to look at the planning, implementation, and maintenance of the project.

2. PRE-IMPLEMENTATION PLANNING AND DESIGN

Project planning is the single most important thing to ensure a successful project. In a large project, a good

project plan will touch on many facets of an organization that are otherwise not involved. It is important to ensure that all personnel that are to be affected by the outcome of a project are involved, or at the very least well informed.

This section of the paper will focus on some of the planning issues involved with delivering and securing a patient management system in a way that is both streamlined in terms of administering the technology but also a system that is easy for the user to access and use on a daily basis. Specifically, this section will look at the following planning issues and how they must be integrated into a complete security architecture using Microsoft's Windows environment:

- **Functional Specification** - A functional specification can be defined as a listing of technical requirements given to prospective vendors in order for them to submit a bid for the project.
- **Critical Item Identification** - Critical items are issues identified during the planning phase that must be addressed before the project design can be started.
- **Design Analysis** - It is in this phase of planning where all prospective vendors are considered.
- **Security Specific Considerations** - This section discusses the security issues particular to the axiUm implementation at the Dental College.

A. Functional Specification

In December of 2004, the Dental College chose a patient management application called axiUm, developed by Exan Academic (<http://www.exanacademic.com/>). This functional specification will assume that axiUm is the application replacing our legacy systems and will concentrate on how axiUm is to be delivered and secured to the end user.

This specification is broken down into three parts:

- Networking
- Application delivery
- HIPAA issues

Networking

Because most of the Dental College's desktop computers are still running 10 Megabit network connections, one of the largest obstacles dealt with is networking bottlenecks. Within the dental school proper, the networking hardware (e.g. switches, routers, and so forth) is controlled by a centralized department on campus. In addition to this, there are several remote clinics that are placed throughout the city where the network is managed by two, referred to as Hospital Network A and Hospital Network B, other networking groups instead of the campus. A model of the Dental College's current network is shown in Figure II.1 below.

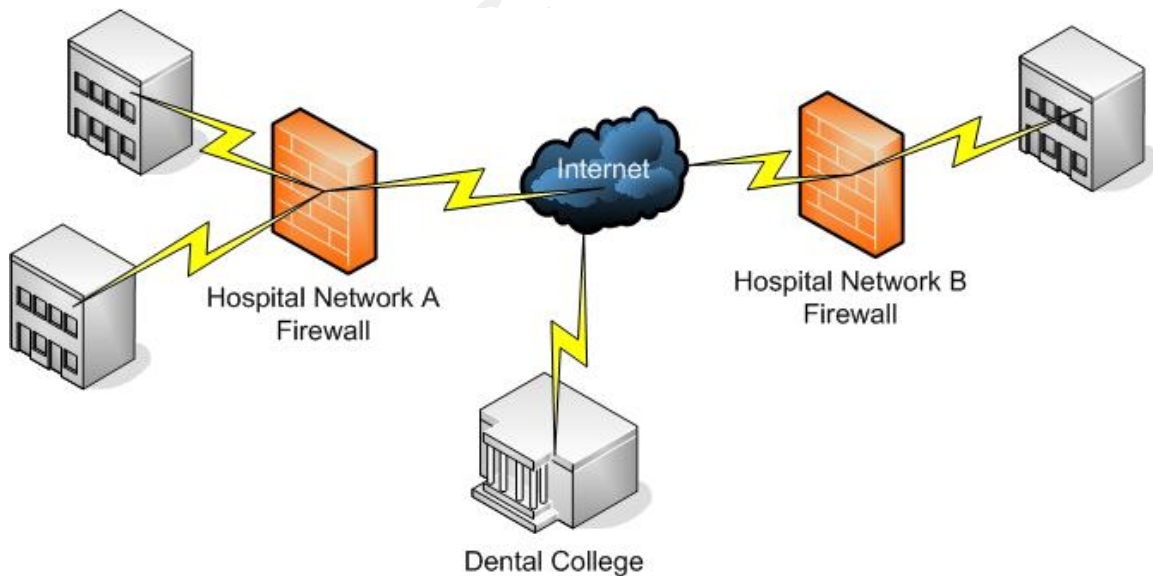


Figure II.1: Dental College Network Diagram

In addition to just being able to communicate back, the data that is sent from this application over the network must also be encrypted. In a Windows environment, this encryption can be achieved via SSL or IPSEC.

Application Delivery

As mentioned in the networking section above, axiUm must be able to traverse across multiple networks in an encrypted manner. Additionally, axiUm must have the ability to be centrally managed so, if an update is released by Exan Academic, deploying this update must be completed in a timely and efficient manner.

If a faculty member is using their computer at work, axiUm must be easily accessible from either a shortcut on their desktop or from the Start Menu. From home, the faculty member must have the ability to connect to the application via a web interface that will run on Windows Server 2003 and Microsoft Internet Information Services 6.0 (IIS). IIS must be secured so the Dental College's patient health information secure. Compared to previous versions of IIS, IIS 6 is much more secure out of the box so additional hardening steps are not necessary in this environment. Some out of the box hardening steps include blocking unnecessary script mappings unless the administrator explicitly turns them on, more secure access control lists to prevent intentional directory transversal attacks, and not installing unnecessary services (e.g. FTP service) by default. However, the data that is transmitted -- generated from axiUm on the faculty's home computer -- must be encrypted. Additionally, the faculty member may opt to install a VPN client and access axiUm from a shortcut on their desktop as well.

HIPAA Issues

Prior to axiUm, the Dental College had five legacy billing systems that were not HIPAA compliant. Upon completion of this project, the goal was to consolidate all of these systems into one HIPAA compliant patient management system.

Several issues needed to be addressed before this project could be considered HIPAA compliant. Two issues addressed in this paper were that of data encryption and auditing of Windows Server 2003 local security policies. Data encryption is important in securing PHI because it will prevent an adversary from sniffing confidential information from the network. Also, the Windows Server 2003 local security policies serve as a way to efficiently manage the security settings enforced on the servers that support this patient management system.

B. Critical Item Identification

Critical items are defined as those issues that must be addressed before a project can be started. In this project, three critical items were identified before the project was started; then, decisions were made on how to properly address these in order to avoid other unexpected issues that may arise during the implementation phase. The three critical items for this project are listed in the following bulleted list and then addressed in the sections that follow:

- **Chair side Patient Care** - Chair side patient care is defined as bringing the electronic chart to the dental chair to ensure top-notch care for the patients of the Dental College.
- **Networking** - As mentioned in the functional specification, the data networking in this project provided many obstacles because not all of the clinics associated with the Dental College were maintained by the same Internet Service Provider.
- **HIPAA** - New federal laws were put into place in April of 2005 to protect electronic patient health information. These rules must be followed when implementing axiUm in order to comply with the new set of regulations.

Chair side Patient Care

As defined above, chair side patient care is where the physician - specifically in this case, the dentist - has access to the patient's electronic chart without leaving the patient. The decision of whether or not to go chair side with axiUm affected many facets of the Dental College in addition to the technology side of the larger operations of the school. For the technology side, many of the issues were related to the network - discussed in the next section - but, apart from the networking, staffing issues had to be considered (i.e. Does the Dental College have enough IT personnel to support a computer at every dental chair?).

While the Dental College was resolving this critical item from a technology perspective, many things were considered. The first consideration was the physical hardware to be installed at each chair. A significant security concern with the student laptops is that they are local administrators. Before deciding on whether or not to introduce this potential threat into the data network, the school also considered buying new desktops for each chair, installing new thin clients, and using older desktop computers acting as thin clients that would serve the application at the dental chair. Eliminating the laptops in the client would increase the endpoint security in the Dental College exponentially since all of these desktops would be managed and secured using industry standard regulations; however, cost was the deciding factor in allowing the use of laptops for chair side requirements.

Networking

Once the decision to go chair side was made, the next critical item to be addressed was the networking. The Dental College is spread over three separate networks - Hospital Network A, the centralized campus network, and

Hospital Network B. Each of the three groups has different policies on what is allowed on their respective networks. For example, Hospital Network A has a strict firewall policy where no unsolicited inbound traffic is allowed; on the other hand, Hospital Network B will allow all traffic between the campus and themselves.

Since the Dental College was built in the early 1900's, data networking was not a concern during its construction. The Dental College asked the campus to perform a site visit and discuss our networking options. The result of this network analysis was an estimated cost of approximately \$220,000 to wire the Dental College for chair side patient care.

Another alternative posed by the campus was using wireless Ethernet technology in each of these clinics. There is currently a wireless initiative on campus that calls for complete wireless coverage regardless of where you are on campus. From a technology perspective, wireless technology as a standard is still very young with a lot of surrounding security issues. Some of these issues are how to place the wireless access points for optimal performance, authentication of wireless clients to control who is allowed on the wireless network, and encryption of the data that is transmitted from the wireless access point to the server. There were several debates over the wireless versus wired question but ultimately it was decided - against the better judgment of the Technology Services group -- that the dental school would go with wireless technology in the dental school wherever wired jacks did not already exist.

Windows XP has a built-in service named Wireless Zero Configuration. This service eases the wireless setup on the client by auto-discovering wireless access points that are beaconing their SSID. Because of its ease of use, the Wireless Zero Configuration was used at the Dental College.

Whereas the wireless networking support is more secure in that the operating system will not let you connect to insecure wireless networks without first warning you, the campus decided on a third-party solution to secure their wireless so we were unable to take advantage of this feature.

HIPAA

There are two interrelated parts to the HIPAA legislation - privacy and security. The HIPAA security regulations went into effect in April of 2005 with the privacy regulations having been implemented the previous year.

The HIPAA privacy regulations cover a wide variety of issues but focuses both on how PHI is accessed by employees of the health-care facility and how this information is released to third parties. The HIPAA privacy regulations go into great detail defining who has access to a patient record. A patient has the right to define exactly who has the ability to look at their patient record, and, under the HIPAA regulations, it is the health-care's responsibility to make sure that this patient information is not given out to somebody who is on the restriction list. The health-care facility must also have policies and procedures to prevent unauthorized access to PHI.

The second part of the HIPAA legislation is the security regulations. Whereas the privacy regulations dealt with how PHI is released (and who this information is released to), the security regulations deal with how this patient information is secured in order to prevent unauthorized disclosure of this information. For the purpose of this paper, only secure access to electronic PHI will be discussed. The HIPAA regulations specifically state that all electronic PHI must be secured as it travels across either an internal or external computer network. In the

event that encryption is not possible, documentation must be produced that clearly states that the data is not encrypted. In the Dental College's case, it was required that all electronic PHI is encrypted and the manner in which the electronic PHI is stored must be secured.

C. Design Analysis

There are several dental school-specific patient management systems available on the market. The Dental College decided to go with axiUm because it was already in 29 other dental schools across North America and Europe. Citrix was chosen as the means to deliver this application over Microsoft Terminal Services because of its built-in load balancing and its ability to transmit all data from the client to the server via a 128-bit SSL connection.

AxiUm requires an Oracle database backend, and the security mechanisms put in place on this server must be effective in protecting the PHI that is stored in the database. These security mechanisms will be explained in the software installation section of this paper.

In addition to the security of the Oracle database, transmitting PHI over a wireless protocol must be done in a secure manner. Generally, the wireless is set up on campus using 802.11b wireless technology. It is secured with Cisco VPN servers that require users to authenticate to the VPN for a routable IP address and use of the wireless network. If authentication does not take place, the user is not allowed on the network. Securing the wireless network in this way allows an additional layer of security, because all data that is sent from the client is encrypted via PPTPv2 or IPSEC protocols depending on the client. A Windows XP VPN connectoid is installed on the client where all of the IPSEC settings (e.g. allowed protocols and IPSEC pre-shared key) are pre-configured.

D. Security Considerations

All of the servers at the Dental College use Windows Server 2003 with Service Pack 1. There are several checklists available as a starting point to aid an administrator in securing these servers. For example, the NSA publishes a detailed summary of suggested best practices for securing Windows Server 2003 (See <http://tinyurl.com/59m2g>). Using the NSA security guide as a model and leveraging the local security policies with an Active Directory group policy object, the Dental College was able to configure a centralized, easy to manage infrastructure. Of course, these best practice guides are only intended as a model and compatibility testing must be proven prior to deployment. A summary of the Dental College's security settings are shown in the Table II.1.

Policy	Setting
Enforce Password History	5
Maximum Password Age	60
Minimum Password Age	2
Minimum Password Length	14
Store Passwords using reversible encryption	Disabled
Account lockout duration	15
Account lockout threshold	3
Reset account lockout counter after	15
Audit account logon events	S, F
Audit account management	S, F
Audit directory service access	S, F
Audit logon events	F
Audit policy change	S, F
Audit privilege use	F
Audit system events	S, F
Guest account status	Disabled
Limit local account use of blank passwords to console logon only	Enabled

Digitally encrypt secure channel data (when possible)	Enabled
Digitally encrypt sign channel data (when possible)	Enabled
Require strong session key	Enabled
Digitally sign communications	Enabled
LAN Manager authentication level	Send NTLMv2 response only
Clear virtual memory pagefile	Enabled
Do not allow anonymous enumeration of SAM account and shares	Enabled

Table II.1: Local security policy settings

3. IMPLEMENTATION

This section regarding the implementation phase of this project explains how security was planned and not bolted on to the deployment of axiUm after the fact. The parts covered in this section are as follows:

- **Hardware Installation** - The first part of this section will explain the hardware used for axiUm. This part is split into two separate parts: the client and server sides.
- **Software Installation** - This part will explain how the Windows Firewall was configured so that axiUm will function in the campus network while still maintaining a level of protection that is suitable for an enterprise environment.
- **Verification of Requirements** - One of the requirements of this project - due to new HIPAA federal regulations regarding electronic patient information -- is that all data must be encrypted from client to server. Whereas Citrix advertises that 128-bit SSL encryption is integrated into the Citrix client, it must be verified that the data is actually encrypted.

A. Hardware Installation

The hardware installation can be split into two parts: the server side and the client side.

The physical installation of the server hardware consists of installing each server into a computer rack and wiring the servers for Ethernet, keyboard, mouse, video, and fibre channel connections. The specifications for the servers used to support axiUm, which are identical in configuration, are as follows:

- Dell PowerEdge 2850 2U servers
- Dual Intel Xeon 3.2 Gigahertz processors
- Six Gigabytes of RAM in the Citrix servers and eight Gigabytes in the Oracle server
- Dell PERC 4Di RAID Controller
- Two 36 Gigabyte hard drives in RAID-1 configuration
- One QLogic 2340 Fibre Channel Host Bus Adapter in the Citrix servers and two host bus adapters -- for storage area network redundancy reasons -- in the Oracle server

For most of the desktops at the Dental College, the existing desktop infrastructure was used. However, the decision to bring the patient management system chair side required that a computer be installed at every chair. For the clinics that did not have a laptop program in place, old desktop computers were salvaged from the campus' surplus warehouse -- or from other departments on campus -- and deployed. For the computers that are used as cashiering stations, a signature pad was also installed so that electronic signatures could be captured for proof of acknowledgement of Dental College's HIPAA privacy policies, informed consent forms, and to sign any contracts negotiated for treatment.

B. Software Installation

Similar to the hardware installation, the software installation for Citrix will also be split into two parts: the server side and the client side.

The server side software installation of this project used to support the axiUm application is pretty straightforward (e.g. Microsoft Office 2003, Adobe Reader, and so forth). This paper will not look into detail on the client applications that are installed on the server; rather, it will focus on the host-based security software that is in place.

The campus does not have many security measures in place in terms of firewall security protecting the University as a whole from an outside intruder. With that said, one big advantage to Windows Server 2003 Service Pack 1 is its built-in firewall, named Windows Firewall. This firewall is identical to the one that is shipped with Microsoft Windows XP Service Pack 2. The Windows Firewall does not have all of the features included as standard features of third-party host-based firewalls such as outbound packet filtering, the ability to open multiple ports with one firewall exception rule, and the comprehensive logging and reporting available on the traffic that is coming to your server. However, the Windows Firewall is sufficient until the campus is able to implement more restrictive policies on Internet packets that are coming from a computer that is located off-campus. Each server in the Dental College has the Windows Firewall enabled with specific firewall exceptions. A list of the firewall exceptions for the Citrix servers (shown in Table III.1) and the Oracle server (shown in Table III.2) are shown in the following tables.

NOTE: For security reasons, the actual IP filter lists have been removed.

Description	Exception	IP Filter List
Veritas BackupExec Remote Agent	TCP 10000	x.x.72.130/255.255.255.255
Citrix ICA Service	TCP 1494	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.143.0/255.255.255.0
Citrix IMA Service	TCP 2512	x.x.72.0/255.255.255.0
Citrix Presentation Server Management Console	TCP 2513	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
Citrix Session Reliability	TCP 2598	x.x.0.0/255.255.255.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.143.0/255.255.255.0
Citrix XTE Service	Xte.exe	x.x.72.0/255.255.255.0
axiUm Messenger UDP Broadcast	UDP 16464	x.x.72.0/255.255.255.0
Citrix XML Publishing Service	TCP 3988	x.x.0.0/255.255.255.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.143.0/255.255.255.0
File and Printer Sharing	TCP 139 TCP 445 UDP 137 UDP 138	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
HTTP (only on Web Interface server)	TCP 80	x.x.0.220/255.255.255.255 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
Intel PDS (Symantec)	UDP 38293	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0

Remote Desktop	TCP 3389	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
RCP Communications	TCP 135	x.x.72.0/255.255.255.0
SAN Storage Processors	TCP 6389	x.x.72.137/255.255.255.255 x.x.72.138/255.255.255.255
Symantec Antivirus RTVScan	TCP 2967	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
Symantec Antivirus RTVScan (Pre-10.x)	UDP 2967	x.x.72.123/255.255.255.255
TCP Port 1059	TCP 1059	x.x.72.0/255.255.255.0
TCP Port 2294	TCP 2294	x.x.72.0/255.255.255.0

Table III.1: Citrix server firewall exception rule list

The Oracle server firewall exception list is shown below in Table III.2:

Description	Exception	IP Filter List
Veritas BackupExec Remote Agent	TCP 10000	x.x.72.130/255.255.255.255
Oracle.exe	Oracle.exe	x.x.0.220/255.255.255.255 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
Oracle TNS Listener	TCP 1521	x.x.0.220/255.255.255.255 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
axiUm Messenger Broadcast	UDP 16464	x.x.72.0/255.255.255.0
File and Printer Sharing	TCP 139 TCP 445 UDP 137 UDP 138	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0

Intel PDS (Symantec)	UDP 38293	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0
Remote Desktop	TCP 3389	x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0 x.x.0.0/255.255.0.0

Table III.2: Oracle server firewall exception rule list

The client-side software installation requirements were much less than on the server because all of the resources run on the server-side. The Citrix ICA client (version 9.15) needed to be installed on each machine.

Additionally, the Windows Firewall is installed on every desktop and laptop in the Dental College environment. A specific entry in the exception list did not have to be created because the client initiates the connection, but it did increase the overall endpoint security on the client.

Access control is crucial to ensure the integrity of the data in any computer network. However, this is even more important in an environment where sensitive information (e.g. patient information including social security numbers, medical histories, and so on) is stored.

Access to the axiUm application is controlled via a layered security approach. The campus has an existing Microsoft Active Directory infrastructure (referred to as ADS) that stores all user accounts and passwords for the entire campus infrastructure. Within ADS, a universal security group, named AXIUM, was created containing all of the user accounts having access to axiUm. If a user authenticated to ADS and is part of AXIUM, the user will see an axiUm icon on their desktop that they can use to launch the application. The desktop icon is placed on the user's desktop by a Citrix application named the Program Neighborhood Agent (PN Agent).

This agent polls the server for published applications and the users who has access to them. When a user logs into a computer, the PN Agent asks the Citrix web farm if the user has access to the application. If the user does have access, an icon is placed on the desktop. This ADS group membership is the first layer of security. Figure III.2 shows the process in which the user authenticates to axiUm if they are a member of AXIUM.

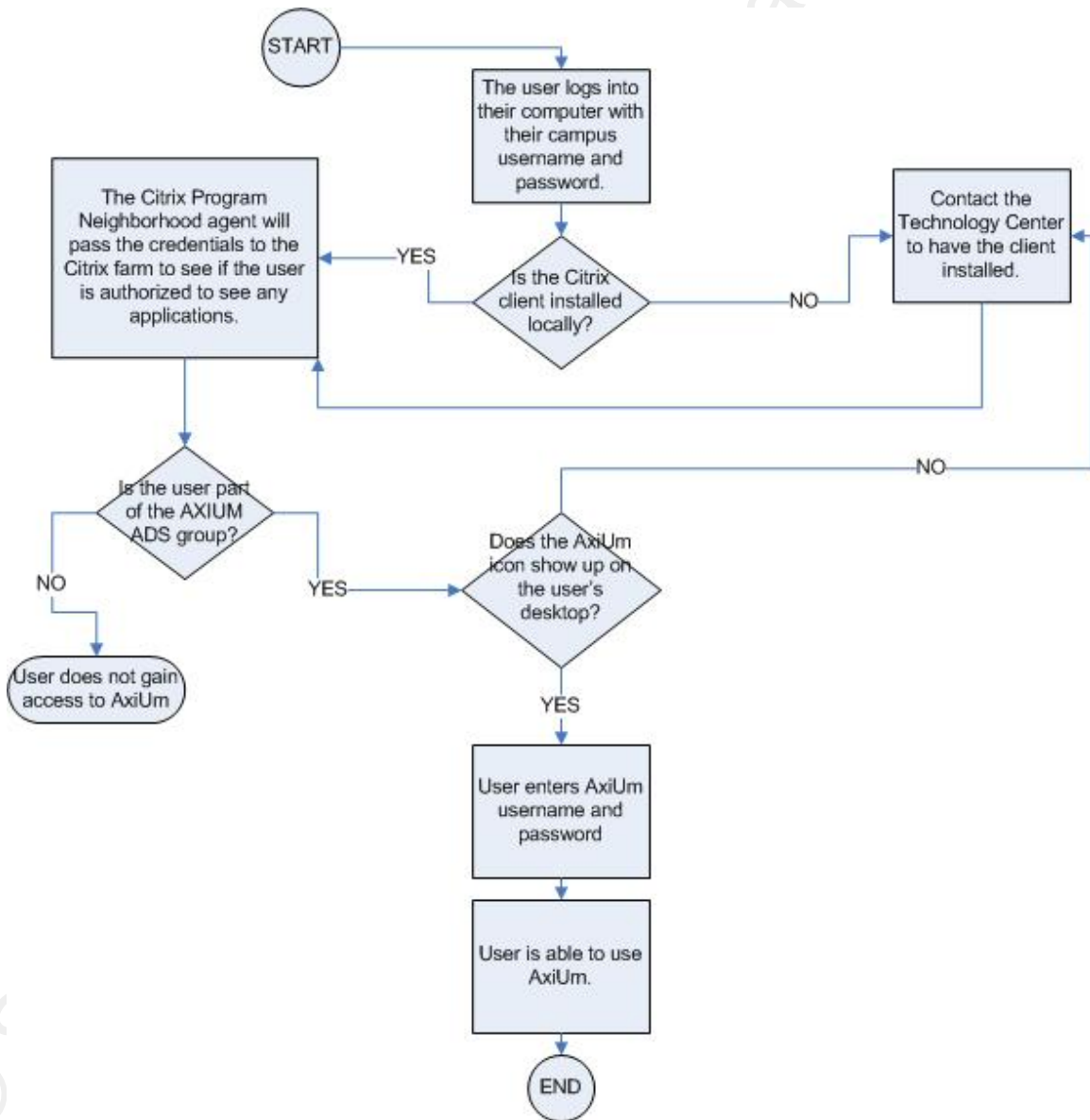


Figure III.2: Citrix PN Agent Process

The second layer of access control security is within the axiUm application itself. A user table is contained within the Oracle database that stores encrypted usernames and passwords used to access the system. So, the user must be in the AXIUM ADS group in order to launch the axiUm application, and once the application is started, the user must supply a username and password to enter the axiUm application. From a network security perspective, requiring two set of credentials has proven extremely effective in reducing the chance of unauthorized access to the system. Currently, the second authentication layer is another password challenge/response system, but there are plans to implement either biometric or smart card authentication in the near future.

C. Verification of Requirements

Before the Dental College went live with axiUm, it was imperative that our critical items were met. From a technology perspective, there were two things that warranted a verification before this project could be put into production:

- Verify that the outside networks - Hospital Network A and Hospital Network B - could communicate back to the web interface server for axiUm authentication.
- Verify that the data is encrypted from client to server.

Communication from the outside networks back to the school's Citrix web farm proved to be easier than expected. Hospital Network A has a firewall but it does not do any outbound filtering - similar to that of the Windows Firewall -- so a request that originated inside of the Hospital Network A network is allowed out without restrictions. However, Hospital Network A has MAC address filtering enabled in order for a computer to get on to the network. Hospital

Network B's network is set up where all communications from the campus network is considered trusted.

The last issue that needed to be addressed before the project could go live was in response to our HIPAA critical item where all data must be encrypted from the client to the servers. To address this issue, a 128-bit Secure Sockets Layer (SSL) certificate was installed on the Citrix Web Interface server. This certificate was purchased through Verisign because the campus Active Directory infrastructure was not set up for a PKI environment. The Web Interface server is used to authenticate all clients to the Citrix web farm. A SSL certificate for a Citrix Web Interface server acts exactly as a SSL certificate on a Internet web server does where the client will negotiate a SSL connection (through a SSL handshake) with the server before any data is transmitted across the network. SSL has proved to be the industry standard in securing web-based communication and works well in a Citrix environment.

In order to make sure the data was actually encrypted over the SSL connection, network packet analysis was done between a client and the Web Interface server. A screenshot of this analysis is shown in Figure III.3:

No.	Time	Source	Destination	Protocol	Info
128	5.367383	.71.94	.72.151	TCP	3304 > 443 [SYN] Seq=0 Ack=0 Win=64512 Len=0 MSS=1460
129	5.367768	.72.151	.71.94	TCP	443 > 3304 [SYN, ACK] Seq=0 Ack=1 Win=64512 Len=0 MSS=1460
130	5.367786	.71.94	.72.151	TCP	3304 > 443 [ACK] Seq=1 Ack=1 Win=64512 [TCP CHECKSUM INCORRECT] Len=0
131	5.368103	.71.94	.72.151	SSLV3	Client Hello
132	5.368991	.72.151	.71.94	SSLV3	Server Hello, Change Cipher Spec, Encrypted Handshake Message
133	5.369333	.71.94	.72.151	SSLV3	change_cipher_spec, Encrypted Handshake Message
134	5.370332	.71.94	.72.151	SSLV3	Application data
135	5.371603	.72.151	.71.94	TCP	443 > 3304 [ACK] Seq=147 Ack=1025 Win=63488 Len=0
134	6.735233	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
155	6.736450	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
156	6.736437	.71.94	.72.151	TCP	3304 > 443 [ACK] Seq=1025 Ack=3007 Win=64512 [TCP CHECKSUM INCORRECT] Len=0
157	6.737689	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
158	6.739590	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
159	6.739615	.71.94	.72.151	TCP	3304 > 443 [ACK] Seq=1025 Ack=8907 Win=64512 [TCP CHECKSUM INCORRECT] Len=0
160	6.740817	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
161	6.742145	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
162	6.742177	.71.94	.72.151	TCP	3304 > 443 [ACK] Seq=1025 Ack=8907 Win=64512 [TCP CHECKSUM INCORRECT] Len=0
163	6.743368	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
164	6.744731	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
165	6.744743	.71.94	.72.151	TCP	3304 > 443 [ACK] Seq=1025 Ack=14747 Win=64512 [TCP CHECKSUM INCORRECT] Len=0
166	6.746024	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
167	6.747907	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
168	6.747920	.71.94	.72.151	TCP	3304 > 443 [ACK] Seq=1025 Ack=14747 Win=64512 [TCP CHECKSUM INCORRECT] Len=0
169	6.749145	.72.151	.71.94	TCP	[TCP segment of a reassembled PDU]
170	6.750437	.72.151	.71.94	SSLV3	Application Data,

Figure III.3: Packet Analysis of Citrix communication

The packets were captured using the open-source Ethereal network analyzer which is a very robust sniffer that is preferred by many networking professionals around the world.

In the above figure, the IP address of the Citrix Web Interface server is x.x.72.151 and the client has the IP address of x.x.71.94. Using Ethereal's analysis, you can see that an encrypted handshake occurred between the client and server with the negotiated protocol being SSLv3. After this handshake has occurred, all communication is encrypted and transmitted over TCP port 443 (SSL).

The Windows Server 2003 servers must be configured to meet HIPAA standards and then must be audited to ensure that these settings are enforced. Enforcing these settings is done via Active Directory group policy objects. The settings are then audited on a regular basis using Shavlik's NetChk Compliance product, which is covered later in the Staying HIPAA Compliant section of this paper.

4. POST-IMPLEMENTATION AND MAINTENANCE

Aside from the inevitable issues that arise after a project is put into production, ongoing maintenance of the project is another essential piece that will ensure that the implementation continues to function efficiently and correctly. The last part of this section will look at the Dental College's Change Management Policy and Procedure. This policy was written for two reasons. First, the new HIPAA regulations require that policies are written to document how a system containing electronic patient information is changed. Secondly, this document serves as an internal change management policy to make sure that changes to the system are communicated to all of the appropriate areas within the Dental College.

A. Post-Implementation Issues

Post-implementation issues are going to happen regardless of the amount of planning that has gone into the project. With proper planning, the number of issues can be minimized.

There were two issues that introduced themselves after the project was put into production: a critical Microsoft Windows Server 2003 Service Pack 1 bug and Citrix client printing.

Since the release of Microsoft Windows NT 4.0, security issues have plagued this version and all operating system versions released after Windows NT 4.0. In response to these continuous security problems, Microsoft started a Trustworthy Computing Initiative where all Microsoft code would be put through a rigorous internal security audit before an operating system or major Microsoft application was released. Because of the scope of the initiative, it took several years for it to start showing up in released Microsoft products. Service Pack 1 of the Windows Server 2003 operating system was the first server operating system to show great strides in the use on this security initiative.

Windows Server 2003 Service Pack 1 was not released until after the project went into production. However, it was decided that all servers should be upgraded to this new version for many reasons. The most notable reason to upgrade was for the integrated Windows Firewall (described in the Software Installation part of this project). Unfortunately, the decision to upgrade to Service Pack 1 did not go through the proper planning process as the rest of the project went through so there were issues with the upgrade. One issue was of a bug introduced with Service Pack 1 that would cause the server to intermittently blue screen leaving the server useless until rebooted. This bug is documented in Microsoft KB article 901150 (<http://support.microsoft.com/?id=901150>). At the time of this writing, a public hotfix was not available for download to correct the problem, so a support call had to be logged with Microsoft in order to receive it. The hotfix

installation was successful until Microsoft security advisory MS05-053 (KB896424) was released. This update was a critical security hotfix issued to in the November, 2005 patch cycle. Unfortunately, this hotfix replaced the private one that was installed from Microsoft so a new call had to be placed to Microsoft Product Support Services. A new private hotfix was installed, Microsoft KB article 907242 (<http://support.microsoft.com/kb/907242/en-us>), and everything has worked fine since the installation.

B. STAYING HIPAA COMPLIANT

Ongoing auditing of HIPAA policies put into place by any organization is a key factor in staying HIPAA compliant. Depending on its size, this can prove to be an enormous task and one whose workload can decrease with the use of third-party utilities. The Dental College chose Shavlik's NetChk Compliance product to help with it.

NetChk Compliance allows the administrator to create a template and use this against a pre-defined set of servers and produce a report of its output. In its current version, NetChk Compliance is an agent-less application that will run against a remote server - or several remote servers at once -- and verify that the Windows Local Security Policy has not changed from what it is supposed to be. In addition to just the Windows Local Security policy settings, it will also monitor the existence and startup type of Windows Services. A third-party utility had to be used for maintaining compliance because Windows 2003 Server does not have an efficient way to monitor the Windows Local Security Policy on several machines at once.

The Dental College runs monthly scans against each of the Citrix and Oracle servers and saves them to an electronically filed report. If a compromise were to

happen, the Technology Services group would be able to easily identify the change and take corrective actions to contain the issue. Two sample reports are shown in the following figures, IV.1 and IV.2.

Scan Policy Compliance Details					Shavlik
					Report Date: 2/17/2006 2:08 PM
Scan Date	Scan By	Version	Policy Name	Machine Group	
2/17/2006 2:03:52 PM		1.1.41			
Machine:				Windows Server 2003, Standard	
Compliance Check	Finding	Operator	Policy	Compliance	
Account Lockout Threshold	3	=	3	✓	
Administrator Account Status	false	=	false	✓	
Alerter Service Status	Disabled	=	Disabled	✓	
Application Management Service Status	Manual	=	Manual	✓	
Audit Account Logon Events	Success\Fail	=	Success\Fail	✓	
Audit Account Management	Success\Fail	=	Success\Fail	✓	
Audit Directory Service Access	Success\Fail	=	Success\Fail	✓	
Audit Logon Events	Fail	=	Fail	✓	

Figure IV.1 NetChk Compliance Detailed Report

The detailed report above is useful for the security administrator who wants to make sure that the Windows Local Security Policy has not changed from the template that was configured within NetChk Compliance. This report will show the administrator every option configured in the template and whether or not this option is compliant (as compared to the NetChk Compliance template).


Scan Detail Executive Summary					Shavlik
					Report Date: 2/17/2006 2:11 PM
Scan Date	Scan By	Version	Policy Name	Machine Group	
2/17/2006 2:03:52 PM		1.1.41			
Compliance		Results			
✓ Compliant Checks	91.67%	110 of 120			
✗ Noncompliant Checks	8.33%	10 of 120			

Figure IV.2 Netchk Compliance Executive Summary

The Executive Summary report (shown in Figure IV.2) is a good report to get an overview of the current state of the entire server infrastructure. It is especially useful for

non-technical executives who want to know the rate of HIPAA-compliance in their organization. This report is presented to the Dental College's administration twice a year and is filed with the HIPAA Security Officer in the event that an external HIPAA audit was ever conducted.

Whereas NetChk Compliance offers some out of the box templates that can be used for HIPAA compliance, the Dental College decided to create a new one. The Dental College template audits every Windows Server 2003 option available within NetChk Compliance. Since this template is very large, Table IV.1 will only highlight a few of them.

Policy	Setting
Maximum Password Age	60
Minimum Password Age	2
Minimum Password Length	14
Account lockout duration	15
Account lockout threshold	3
Automatic Logon	Disabled
File System Status	Allow NTFS Only
Shares Status	Allow Administrative Shares Only
Audit account logon events	S,F
Audit account management	S,F
Audit directory service access	S,F
Audit logon events	F
Audit policy change	S,F
Audit privilege use	F
Audit system events	S,F
Guest account status	Disabled
Limit local account use of blank passwords to console logon only	Enabled
Digitally encrypt secure channel data (when possible)	Enabled

Digitally encrypt sign channel data (when possible)	Enabled
Require strong session key	Enabled
Digitally sign communications	Enabled
LAN Manager authentication level	Send NTLMv2 response only
Clear virtual memory pagefile	Enabled
Do not allow anonymous enumeration of SAM account and shares	Enabled
Telnet Service Status	Not Installed
SMTP Service Status	Not Installed
FTP Publishing Service Status	Not Installed
Messenger Service Status	Disabled

Table IV.1 Excerpt from Dental College's template

The table above is not an exhaustive list; rather, it is only an example of some of the NetChk Compliance options that are available to the security administrator when they are doing the HIPAA compliance scans.

The Dental College was able to leverage the security policies built into Microsoft Windows to stay secure with the reporting capabilities of Shavlik's NetChk Compliance product to greatly reduce the administrative burden for the Dental College's Technology Services group. This burden will continue to lessen as Shavlik Technologies and Microsoft Windows server operating system continue to further develop their products.

C. Change Management Policy and Procedure

The scope of this policy is to ensure that a comprehensive procedure is established to track all system maintenance, in specific regard to the axiUm system implemented throughout the dental school.

Purpose

The purpose of this policy is to establish control and accountability over routine maintenance and changes to systems, including hardware, software and network components, with specific emphasis on the axiUm system. The availability and reliability of systems is largely dependent upon regular updates and maintenance, especially those provided by the vendor supporting the system.

Definition of the term "change/update" in regard to axiUm system:

A "change/update" to the axiUm system will be defined as:

- Any modification in the original application source code
- Any hardware modification (e.g. network servers) that could potentially effect the performance, usability and/or availability of the axiUm system
- Any modification to additional systems (e.g. database server) that interact or otherwise interface with the axiUm system
- Any modifications in the operational processes that govern the store/access/manipulation of information within the system.

Process for implementing changes/updates to axiUm system:

Once a change/update has been determined as necessary, a complete description of the change, as documented using the Dental College application design document, will be completed, reviewed and approved by the following individuals:

- Network Administrator/Senior Security Analyst
- HIPAA Security Officer
- Clinic Systems Manager
- Director of Technology Services
- Associate Dean for Clinical Affairs

- HIPAA Privacy Officer

Note that the design document includes specific sub-sections for system testing, training, project timeline as well as other critical issues that should be addressed when changes to any production system are being considered. Under no circumstances should any change/update be made prior to the completion of this documentation (i.e. a completed and approved design document).

Policy on remote access for implementation changes/updates to axiUm system:

As part of the service/maintenance agreement with Exan Academic (manufacturer of axiUm), authorized Exan individuals will be allowed remote access to the axiUm system installation within the dental school.

As outlined in the above-mentioned policy, remote access will not be *carte blanche*, but rather controlled in such a manner so that the system vendor must first contact the dental school and communicate their intention to remotely access the system. Under no circumstances should this remote access be followed with changes/updates to the axiUm system that has not first been approved via the process outlined above.

System maintenance logs and review:

- All system maintenance as defined in this policy will be recorded in a log and reviewed on a regular basis to ensure policy compliance and applicability.

Additionally, the completed design documents (described above) will serve as maintenance logs. At a minimum interval of six months post-change/update implementation, the associated design documents will be reviewed by the individuals listed above to ensure continued compliance with

all policies/procedures, as well as to serve as general "post-implementation" review to judge impact of said changes/updates on system usability, functionality and reliability.

5. CONCLUSIONS

In conclusion, Citrix provided an application environment that satisfied all of the critical items identified earlier in this paper. To reiterate, the critical items were chair side patient care, networking and HIPAA. Citrix was chosen over Windows Terminal Services for several reasons. Citrix supports built-in software load balancing across the server farm. Windows 2003 Server only supports this through the use of clustering. Secondly, Windows 2003 Server does not provide an equivalent feature to Citrix's Program Neighborhood Agent where icons could be automatically published to the user's desktop. Since ease of use was critical to the Dental College's users, the Program Neighborhood Agent was a necessity.

All of the dental school students have laptops that the Technology Center has no administrative control over. The requirement for secure chair side patient care necessitated the need for Citrix since the application does not physically reside on the computer itself. If a laptop is infected with a virus, the electronic patient information will remain secure because the Citrix client is only a window to the application and not the application itself.

Whereas the networking from the dental school to other Dental College clinics (where the data networking is controlled by an outside party) was not as large of an issue as initially expected, the wireless network presented a challenge in the dental school proper. Citrix helped ease the wireless load because the bandwidth is only a fraction compared to a traditional client server application.

The HIPAA set of regulations require that all electronic patient information from a client to a server be encrypted. Again, Citrix reduced the encryption burden because 128-bit SSL encryption is built into the Citrix client. Using a traditional client server application model, third party encryption software (e.g. IPsec, SSH, TLS, and so on) would have been required. In terms of HIPAA compliance, Shavlik's NetChk Compliance product is used to monitor each server to verify that Windows security is maintained, and was chosen to monitor compliance because Windows security policy reporting lacks the necessary features that the Administration at the Dental College required. They wanted to be given one report showing a snapshot over the overall security of the servers transmitting and storing patient health information, on a monthly basis.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC505: Securing Windows and PowerShell Automation	SEC505 - 201709,	Sep 18, 2017 - Nov 13, 2017	vLive
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	vLive
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced