Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

HIPAA-compliant configuration guidelines for Information Security in a Medical Center environment

The Health Insurance Accountability and Portability Act of 1996 (HIPAA) was passed by Congress and signed into law by President Bill Clinton. This Act mandates that health care providers and other covered entities implement comprehensive privacy of protected health information of patients. HIPAA regulations cover three important areas: information privacy, information security, and standardization of transaction code sets. It should be noted that the rules for the HIPAA Security standards were proposed in August, 1998....

Copyright SANS Institute

Author Retains Full Rights

AD

Robert Happy Grenert
GSEC v1.4b
Practical, Option 1
Original Submission
SANS Gateway Arch - St. Louis, August 4-9, 2002

HIPAA-compliant configuration guidelines for Information Security in a Medical Center environment

Introduction

The Health Insurance Accountability and Portability Act of 1996 (HIPAA) was passed by Congress and signed into law by President Bill Clinton. This Act mandates that health care providers and other covered entities implement comprehensive privacy of protected health information of patients. HIPAA regulations cover three important areas: information privacy, information security, and standardization of transaction code sets. It should be noted that the rules for the HIPAA Security standards were proposed in August, 1998. As of the date of this writing, the final Security rules had not been published in the Federal Register, which is the last step to making them law. The final HIPAA security regulations will become effective two years after the date of their publication in the Federal Register, so the final compliance date has not been set.

In Part 1, this document will deal with the HIPAA requirements for implementation of an assessment and certification process for primary healthcare providers. In Part 2, I will specifically recommend HIPAA-compliant information security guidelines for 7 critical and most common hardware devices that are a part of many medical centers Information System. The configuration guidelines will implement security standards promoted by the InfoSec community, but not specifically Healthcare InfoSec, which has up until now lagged behind the rest of the security community in its requirements and assessments. Because each hospital or medical center has their own unique set of hardware needs and requirements, this document will not address manufacturer specifics, but will give general guidelines to be applied to any particular network. The goal is to use these security configuration guidelines, then to be able to assess their implementation and certify the results. This paper will show that information security is an on-going project and encompasses more than just a few pieces of hardware plugged into a network. Much thought, planning and research must be done in advance to provide maximum security to patient health information but still provide an environment where the medical needs of the patient are not jeopardized by the inability of clinical staff to access digital medical information.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Part 1 – Assessment and Certification Guidelines

The U.S. Department of Health and Human Services (HHS) draft version of the HIPAA Security regulations is the document the healthcare industry is using to make their preparations for security of "protected health information" (PHI). The final rule is expected to change little from the proposed rule. However, as stated at http://www.sans.org/rr/policy/HIPAA_policy.php: "When the final HIPAA security rule is released, necessary changes will then be made to align them with whatever changes are contained in the final rule." [1]

But, this draft rule is really only a summary of what will be expected in the healthcare industry and does not give specifics or standards as to how the regulations should be implemented. For now, we must look to other areas for direction. There are many other sources from government and private industry which reinforce the need for Information Technology Security standards, policies, and practices, as well as stressing the need for securing personal health information.

President George W. Bush's "Critical Infrastructure Protection Board" published a paper in September 2002 entitled *"A National Strategy to Secure Cyberspace"* which is found at: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html [2] In it, one of the Agenda items listed under Level 4, "National Priorities" stated: **"R4-38** The appropriate Federal agencies should consider reviews of the IT security issues related to the implementation of … the **Health Insurance Portability and Accountability Act."**

So besides just HHS being involved implementing HIPAA, and the Office of Civil Rights being involved in enforcing HIPAA regulations and investigating complaints and violations, other "appropriate" Federal agencies will be involved in publishing guidelines on how HIPAA Security should be implemented.

HHS's best indication of what will be required in the final HIPAA Security regulations comes from a reference in an addendum to their "Notice of Proposed Rule Making for the Security and Electronic Signature Standards" (NPRM) published in the Federal Register in 1998. Under the section HIPAA SECURITY MATRIX- mapping, http://aspe.hhs.gov/admnsimp/nprm/sec16.htm, "Certification Requirements" [3], the mapped "Standard" for such requirements refers to footnote "47" - **NIST** "Generally Accepted Principles and Practices for Secure Information Technology Systems" at http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf [4]

This NIST document is THE document which provides us the minimally acceptable standards for information security, and since the NPRM specifically refers to this document, the NIST Principles and Practices are the best indication of what the healthcare industry should be using to secure "Protected Health Information" until the final HIPAA regulations are published.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Specific direction from NIST for the purposes of this paper are found in section 3.4.4 "Implementation Phase", which state:

> **Accreditation.** *System security accreditation is the formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk. It is usually supported by a review of the system, including its management, operational, and technical controls.*

Further, at section 3.4.5 "Operation/Maintenance Phase", under "Audit and Monitoring Techniques" we find this direction:

> Periodic Reaccreditation. Periodically, it is useful to formally reexamine the security of a system from a wider perspective. The analysis, which leads to reaccreditation, should address such questions as: Is the security still sufficient? Are major changes needed? The reaccreditation should address high-level security and management concerns as well as the implementation of the security.

So not only does the NIST document include the requirements for initial accreditation, but it includes periodic reaccreditation, which is also required in the HIPAA Security regulation.

One of the first comprehensive documents which addressed the complete HIPAA Security draft regulations was published in May 2001 by *Association of American Medical Colleges,* at http://www.aamc.org/members/gir/gasp/. Their "Guidelines for Academic Medical Centers on Security and Privacy - *Practical Strategies for Addressing the Health Insurance Portability and Accountability Act"* [5] not only gave us HHS's version of HIPAA Security regulations, but also provided a minimally technical, non-medical "Explanation" of each of the proposed regulations. This paper will specifically address the following requirement, which is the very first of the HIPAA Security regulations:

> **SEC.01 Certification 45 CFR §142.308(a)(1)**
> ***HIPAA Requirement***
> *…(The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.)*
>
> ***AMC Explanation of HIPAA Regulation***
> Certification is the process of determining whether technical security controls are implemented and comply with specified criteria. Each covered entity is required to establish a certification process that demonstrates and documents that its computer systems and networks meet these criteria.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

> Either internal staff or external persons may perform certifications. The process should consider risks identified in the risk assessment process.

The AMC went on to breakdown this regulation even more succinctly:

> *Category I Guidelines - Actions must be taken to address these*
> Implement a certification process to determine the extent to which systems and networks meet established security criteria.

The AMC listed their "*Key Issues"* along with "*Category II Guidelines -Actions should be taken to address these"* and a list of recommendations to be followed to be "HIPAA compliant". While not listed here, these recommendations fall under the category of "Best Practices" which will be addressed in Part 2.

After this lengthy background information on the regulations and what must be done, we can now proceed to the "how to"; applying InfoSec industry "best practices" as configuration guidelines for technical testing to meet certification standards.

Part 2 – Recommended configuration guidelines

The following are 7 of the most common and critical hardware devices that may be part of a medical center Information Systems environment and are of the highest concern and applicability to HIPAA Security regulations for systems certification and accreditation:

- Routers
- Firewalls
- VPN
- Windows-based Web Servers
- Windows-based Mail Servers
- Wireless Access Points
- Modems

The testing of these devices to prevent intrusion and the certification by medical center or hospital management is the key to HIPAA Security compliance. While there are other network devices such as switches, hubs and intrusion detection systems that are critical to network security and need to be a part of an assessment process, the focus of this paper is the above devices which are accessed from the outside world and will be the first targets of attempts at unauthorized access.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Routers

Routers are the first layer of a multiple-layer defense against intrusion and unauthorized access from outside the internal network. A Router provides security by allowing or denying traffic to or from a source or destination IP address and port, as found in the layer 3 IP header. To deny access to the inside by unwanted outside traffic, a Router can act as a packet filter to help protect a Firewall from attack, as well as taking some of the network load off of the Firewall, so that the Firewall does not have to inspect each and every packet that presents itself to the Router.

A Router should be placed on the outside "border" or perimeter of a network and properly configured to routes packets through a network, to drop traffic to unknown destinations, and to block local broadcasts. Routers need to be specifically programmed for this mission for each network they are used on, because factory defaults are not sufficient. This security filtering is accomplished by the use of an Access Control List (ACL) which gives commands or "rules" to the Router in its own internal OS language on what type of traffic to allow or deny, based upon IP address. This filtering can bet setup with "standard" or "extended" ACL commands to also check source and/or destination IP addresses. These extended ACLs can also deny or permit packets based upon packet header information, protocols or port number. Even with all this inspection going on, a Router will not act to "tear down" a packet and inspect it for a dangerous payload. That is the job for a Firewall and will be discussed later.

Again, because each network is different, as well as each brand of Router, only general guidelines and "best practices" can be encouraged here for use of ACLs, although the concepts and capabilities of all Routers should be similar. The concept is to deny what you know you want to deny, allowing only what you know you want to allow, then for good measure, deny everything else. These rules can be set using the standard ACLs, but only work by checking the source IP address. To deny traffic to specific destinations, extended ACLs must be used. An example would be for a network administrator to deny network users from accessing a Peer-to-Peer file sharing network, such as KaZaA, Morpheus, and others, by maintaining a list of IP addresses to be blocked. Default or other improper installation configurations on these P2P programs can open up a network to external access.

Instead of using a commonly-held philosophy of "allow everything unless I specifically deny it", a network should be assessed to determine which ports on a Router will need to be opened, so that ports not in use can be closed. "Deny all but what I specifically allow" would be a "best practice" for the healthcare industry, as it is in the InfoSec community.

Another optional Router configuration is to setup "stateful" packet filtering, which can be done using "reflective" ACLs. In this type of filtering, the Router

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

dynamically generates its own “inbound” ACL in real time, based upon outbound connections that have been specifically permitted. Restrictions put in place on a Router should also deny “spoofed” traffic from “internal” or private addresses that could not possibly be coming from the Internet, as well as multicast traffic or packets from invalid addresses.

While this document is not meant to be an all-inclusive dialogue of Router configurations, the important thing to remember is that in a medical center or hospital environment, the protection of patient information is the key function of Information Systems security. There is nothing about securing a Router that is specific to the healthcare industry. The information being secured in most instances is “protected health information”, but no special Router configuration is required by HIPAA.

Secondarily, access to outside resources for the medical staff must be allowed for research and other patient care purposes. This may mean permitting, or not blocking access to, certain types of web sites that many companies would normally not allow staff access to, or would at least automatically filter the content of. It has been my experience that generic blocking of web sites based on content, such as nudity, is too confining in a clinical environment. Many research and clinical information sites show pictures of human bodies in various states of undress, as well as medical or physical conditions. Generic blocking of access based upon content is therefore too restrictive. However, specific filtering based upon known IP addresses which are used in an ACL to either allow or deny access to these types of web sites is much more appropriate in the medical world.

The actual assessment of Router security can be done by running penetration software such as “Nmap”, “Nessus”, “Enum”, “Netcat” or other such programs. It is advisable to get written permission from medical center or hospital administration before attempting to “hack” into any systems.

There are some final considerations for the secure use of a Router. Audit logs should be enabled and checked for signs of attempted or successful intrusion. The initial configuration of a Router usually requires direct connection in console mode, but after this setup, remote access can be allowed by a Telnet session or web-based interface. Neither of these are secure, especially when a public network is used, so a policy that continues use of the direct-connect console mode, or a “ssh” secure shell interface would be preferred. Of course, the Router and other network equipment must be physically protected from hands-on intrusion.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Firewalls

Firewalls are the second layer of a multiple-layer defense against intrusion and unauthorized access from outside the internal network. A Firewall provides "packet-level" security and inspection and can also allow or deny traffic through specific ports, by ingress or egress filtering, like a Router does.

A properly configured network would have a Firewall placed where the various types of network traffic intersect, i.e.; where internal servers connect to the Internet, where internal servers connect to Web or Mail servers, and where Web or Mail servers connect to the Internet.

While Routers can look at fields in data packets, Firewalls perform this function faster. By using "Network Address Translation" a Firewall can also shield internal network addresses from the outside world. The recommended configuration would have all internal network addresses connecting to the Internet with only one external IP (gateway) address. NAT works to modify the outbound packet changing from internal private address to public NAT'd address.

As with any security configuration, a properly configured Firewall should deny traffic not specifically allowed, but this configuration but must be monitored and tweaked as necessary, so as not to limit legitimate traffic.

In an article for *Healthcare Information Security – Newsletter* in May 2002, CISSP Bob Cartwright writes, "Packet filtering is minimal inspection" [6] He explains that a Firewall should use a set of rules and those rules should act as a filter to allow or deny the traffic. Cartwright lists 5 types of Firewalls and explains the differences:

- Stateful Application Gateway Proxy – tears apart packets and rewrites them, which can be a slow process
- Software or Appliance firewall - An Appliance is more expensive, gives better throughput, and is easier to install
- Packet filtering - Doesn't permit those not listed from incoming or outgoing, is fast, can be complicated, but vulnerable if configured poorly
- Application proxies – Are more secure, more flexible, slower, and use more system resources; and,
- Stateful inspection firewalls – A compromise of secure application proxy and less secure packet filtering, with better speed, but must be configured correctly

The catch to proper configuration is that a Firewall must be opened just enough to allow remote users and legitimate traffic to connect to inside resources. But doing this can allow "black-hats" or other unauthorized users a way inside the network. When accessing Firewall configurations, it is recommended that each

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

setup be tested first, then saved to revert back to in case the configuration is too restrictive.

One type of Firewall not previously mentioned are software based Firewalls. Well-known software-based Firewall applications such as "ZoneAlarm" or "Black Ice Defender" should not be used exclusively on individual servers or workstations in a medical center or hospital environment. Such software firewall on local servers should not take the place of network-based firewalls, but could be used in addition to them.

The security assessment of a Firewall can also be done by running penetration software such as "Nmap", "Nessus", "Enum", "Netcat" or other such programs. Be sure to get written permission first. As always, enable audit logs and check for signs of attempted or successful intrusion.

There is nothing about securing a Firewall that is specific to the healthcare industry. InfoSec "best practices" are recommended, but no special Firewall configuration is required by HIPAA.

VPNs

A "Virtual Private Network" can be used by any remote user to securely access the internal servers at work. Remote users working for a medical center could include Information Systems support staff, transcriptionists, physicians and their staff, and others. A VPN creates a secure "tunnel" through a public network (i.e. the Internet) by using encryption and authentication. A VPN can use a number of different protocols, but the "IPSec" protocol is currently the most secure. However, IPSec is not perfect.

In a Microsoft Windows environment, a software-based VPN would have a specific WinNT, W2K or .NET Server on the inside network configured to allow a VPN connecting through its external internet connection. The remote user would then configure their Windows 2000 or XP system to connect to the VPN via the Internet, providing the IP address of the VPN Server. Proper protocol configuration should include the use of IPSec on both ends.

Alternatively, a hardware-based VPN appliance could be used and configured with appropriate internal and external IP addresses, protocols and user information. The remote user then installs software specific for the appliance and connects via the Internet.

In *Healthcare Information Security – Newsletter* of February 2002, Gerald Nussbaum makes the following recommendations [7]:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Do not use "split-tunneling" while connected to the VPN. If the remote user is connected to both the internal network and the Internet simultaneously, it could allow an unauthorized user to gain internal network access if the remote user's PC is not properly configured or does not have its own personal Firewall.

- A VPN should be used in conjunction with all other security hardware

- Check into "direct peering" from an ISP wherein: "A user connects to the Internet and his packets are directed through a private peering point through to the ISP that connects to the organization's network and vice versa."

The security assessment of a VPN can be done by running password cracking software such as "John the Ripper" or other such programs. Be sure to get written permission first. As always, enable audit logs and check for signs of attempted or successful intrusion.

There is nothing about securing a VPN that is specific to the healthcare industry. InfoSec "best practices" are recommended, but no special VPN configuration is required by HIPAA.

Windows-based Web Servers

These types of web servers are probably the most hacked servers in the world today. While Microsoft has been fairly good about providing "hot fixes", "patches" updates and "Service Packs" to plug discovered holes in web server security, an un-patched web server is not only subject to be attacked and compromised, but can also be used to attack other servers as well.

In the January 2003 issue of "*Advance for Health Information Executives*" author Robert N. Mitchell writes, quoting Jonathan Taylor, enterprise security engineer, at Sutter Health, Sacramento California [8]: "A good security practice is to change the default configurations, change the Web folder location, change the scripts folder location and modify system permissions so that they are not set with default configurations."

A knowledgeable black-hat would know to probe a Windows web server for default user names and could then attempt unauthorized access. Therefore, additionally security measures should include:

- Remove all default users, home directories and configuration, sample files, administration web sites, anonymous logins, null sessions

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Disable all unused Services in Computer Management and install the O/S with minimum services
- Configure "Live Update", install all service packs, hot fixes, and patches
- Install and automatically update anti-virus software
- Use different hard drives or partitions for the O/S, HTML and FTP folders
- Remove or rename guest account and rename administrator account
- Enforce strong passwords complexity and force the password change often
- Disable NetBIOS, remove OS/2 and Posix references from the Registry
- Apply a high security web template and configure it

As an assessment tool, consider testing the initial server configuration by applying a "scoring tool" to benchmark the current or "before" level of security, then apply the security template for an "after" score. Such a security template should also be checked in conjunction with the "SANS/FBI Top 10 Windows Vulnerabilities", found at http://ww.sans.org [9] A free SANS/FBI Top 20 vulnerabilities scan is available at http://www.qualys.com [10]

Because of its age, Windows NT Server should not be considered as a web server of choice. It is recommended that W2K Server or higher (.NET Server) be used, and that any WinNT systems be upgraded or replaced.

As mentioned before, log various events and regularly check audit logs for signs of hacking or intrusion.

Additional security assessment of a web server can be done by running penetration software such as "Nmap", "Nessus", "Enum", "Netcat" or others; password cracking software such as "John the Ripper" or other such programs. Get written permission first, enable audit logs and check for signs of attempted or successful intrusion.

There is nothing about securing a web server that is specific to the healthcare industry. InfoSec "best practices" are recommended, but no special web server configuration is required by HIPAA. However, because medical center web servers now frequently include remote access to patient records, radiology images and other "protected health information", it is vital that these sources of information are secure and reviewed often to apply appropriate updates.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows-based Mail Servers

Because Windows-based Email Servers, such as Microsoft Exchange Server are based on the same O/S as the above web servers, the recommended security configurations are much the same.

In the March 2002 issue of *Healthcare Information Security – Newsletter,* Jahen Moreh lists the 4 most popular methods for securing Email [11]:

- Public Key encryption – such as PGP, which is not widely used, but is one of the most secure methods. Encryption should be easy to use or automatic
- Password-based security– both sender & recipient use same password to encrypt and decrypt, but passwords must be complex and secure
- Web-based security – there is no content in any Email message, only a link to a secure web-site where the recipient logs in to get messages
- Key-server security – recipient gets an encrypted message, then retrieves a key from a server by password and decrypts the message

Additional security assessment of a web server can be done by running penetration software such as "Nmap", "Nessus", "Enum", "Netcat" or others; password cracking software such as "John the Ripper" or other such programs. Get written permission first, enable audit logs and check for signs of attempted or successful intrusion.

Because mail servers are where incoming Email attachments are delivered, anti-virus software must be installed and constantly updated to prevent network infection. Additionally, outgoing Email messages from medical center staff may frequently include "PHI", so it is vital that these servers are secure and reviewed often to apply appropriate updates.

Wireless Access Points

Wireless network communications in a medical center environment can allow clinical staff and physicians, while visiting patients in their rooms or exam rooms, to have instant access to medical records, radiology images, and treatment history on PDA's, wireless PCs or other medical devices. An IS department can also use such devices to have access to servers and user accounts to change or reset passwords or permissions.

In a December 9, 2002 article entitled "Six basic tips for implementing closed networking on a wireless network" by Scott Lowe, MCSE, and publish by Tech Republic http://www.techrepublic.com/article.jhtml?id=r00620021209low02.htm [12] we are given some initial steps for wireless security:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Plan antenna placement – limit the external reach of the signal by placing the WAP in the center of the area to be serviced, away from windows and outside walls

2. Use WEP (Wireless Encryption Protocol) – make sure it is enabled, even though it is not completely secure

3. Change the SSID and disable its broadcast – change the factory defaults and passwords

4. Disable DHCP – use only assigned IP addresses on WAPs and devices connection to them

5. Disable or modify SNMP settings – if supported by the WAP. Change or disable both pubic and private community strings

6. Use access lists – controls based upon MAC address, if supported by the WAP. (This topic is discussed below)

Even with these steps taken, wireless networks are inherently un-secure because of radio signal propagation in all directions, through walls, and even outside buildings. Due to the physical size of most medical center and hospital buildings, "Multiple Access Point Architecture" is required if Wireless access is to be available campus-wide. Most newer Wireless Access Points include WEP to prevent eavesdropping, but WEP has been shown to be vulnerable. WEP can be cracked with publicly available software such as "AirSnort" or "WEPCrack".

Because of this, current generation Wireless communication needs to be made more secure through the use of IPSec or access through a VPN.

In the July 2002 issue of *Healthcare Information Security – Newsletter,* Eddie Schwartz states the need for securing Wireless Access Points [13]:

> The quickest solution to creating wireless access will be to connect wireless access points through to your existing VPN access. Any user can connect to the access point and arrive at the door to the VPN. From there, supporting the device is the same as supporting any remote computer.

Other options for securing WAPs include setting controls based solely on MAC address or SSID, but since MAC addresses may be spoofed, relying on this alone may not be sufficient. You could also disable the SSID on Access Points. Since this prevents them from broadcasting their SSID, they are not as easily located, and they won't respond to anonymous requests for SSID. But neither of these methods is as secure as connecting WAPs through a VPN, based on the current generations of Wireless products. The InfoSec industry can only hope

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

that future versions of 802.xx Wireless will have more security and encryption built-in.

With this amount of security in place, one of the few remaining concerns would be Denial of Service (DoS) attacks by Radio Frequency (RF) interference in the area where the Wireless service is active. While RF interference is possible to manipulate to those who know about this technology, it is expensive to do and not practical to defend against. In a serious situation that could affect patient care, local law enforcement or other experts could use a spectrum analyzer to locate the source of the RF. The source of such a DoS would be traceable if run continuously and so the prospect of on-going RF DoS attacks is not realistic.

Additional security assessment and vulnerability of WAPs can be done by running sniffing software such as "AirSnort" or "WEPCrack" and "War Driving" (or walking) in the area of Wireless service. Get written permission first, enable audit logs and check for signs of attempted or successful intrusion.

Modems

Once the standard for Internet connectivity, modems for the most part have been replaced by high-speed network connections to the Internet for many hospitals and medical centers. However, in 2003 there are still many vendors, insurance companies and government agencies that still have old main frame computer systems that require slow, sometimes very slow modem connections to transmit patient billing information, or to connect to a main frame for direct data input.

Among these entities still requiring modem connections are Blue Cross/Blue Shield, Medicare, and insurance clearinghouses such as NEIC. It is very common for medical center staff to dial-up to a main frame at one of these providers each day and stay connected for most of the day while directly inputting data, as well as batch transmitting bills containing patient data on a daily basis.

The transmission of PHI over common-carrier phone lines, or even the direct data input of PHI will have to cease when HIPAA Security regulations become effective. Modem connections to sources outside the medical center are a major security hole. Dial-up phone connections are not secure and cannot be easily monitored. They bypass network security, firewalls, content filtering programs, and other security measures. It is predicted that the final HIPAA Security regulations will see and end to the common use of modems for DDI and other data transmission.

However, there may be some need for temporary, emergency modem use. In situations where a network T1 or wireless Internet connection is down, emergency dial-up to an ISP could provide temporary connectivity for very important reasons, such as to transfer banks funds to a payroll account on

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

payday. In such cases, a personal firewall such as ZoneAlarm of BlackIce Defender properly configured would be the perfect emergency security measure.

In order for a medical center to get a handle on the current use of modems, there are several things that can be done. The location of all modems must be identified. All modems not needed for an emergency situation such as previously mentioned should be disabled or removed from the PCs. In a large organization this could be a really big project. This project will also undoubtedly run into varying degrees of resistance with staff, some of whom will want to continue to use their modem for FAX transmissions, phone answering, or other uses. Just because there is a stand-alone FAX machine connected to a specific phone line, it doesn't mean that location can be considered safe. Someone working nearby with a modem-equipped PC could easily run a line splitter and dial out on the line.

In a telecom environment where the number and locations of modems and FAX machines is unknown, the technique of "war-dialing" can be used against phone systems to find unsecured modems. Commercially available programs such as Sandstorm's "Phone Sweep" http://www.sandstorm.net/ [14] is a telephone scanner that will dial every phone number in your organization and find computers running CarbonCopy, RAS, pcANYWHERE, and other remote-access programs. These programs sitting on a modem that has its "auto-answer" feature turned on are ripe for unauthorized war dialers to connect to and attempt access. Any modem in use should have its auto-answer feature disabled as a power-on default to prevent unauthorized access.

Other tried and true war dialers such at "Tone Loc" provide a similar service, but without the cost. These same types of programs are used by phone "Phreakers" who run war dialing programs in an attempt to identify modem lines that can lead to allowing them unauthorized access into a computer or network. It is better to run these programs as a defense to identify un-secure modems before Phreakers do.

Many newer telephone systems include a digital phone "switch" which is really a computer that controls the telecom hardware and has a software interface on a PC that allows a PBX administrator to setup and control the phone system. In many of these types of systems there are specific digital and analog phone ports or lines in use, all of which had to be identified and designated properly when the phone system was installed and setup. In this type of environment, the administrator knows exactly where the analog phone lines are, which can cut the time when trying to identify un-secure modems. Controlling who has access to analog lines can prevent unauthorized use of modems. This type of phone switch also allows an administrator to turn off an analog port at any moment, in case an intrusion is suspected.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

There is no single security measure that will provide total security to any medical center information system. Security policies and procedures must be in place, taught and enforced. It is the security hardware that implements security policies by enforcing rules. Proper installation, configuration, use and monitoring of routers, firewalls, VPNs, Windows-based web servers, Windows-based mail servers, wireless access points and modems requires constant vigilance on the part of an IT or IS staff and the ISO. All of these pieces of hardware combined with all other security measures can help provide a secure network.

Before HIPAA-compliant systems security certification can take place, intrusion testing must be run and permission should be obtained to prevent misunderstandings and possible prosecution. Proper HIPAA Security certification will determine whether technical security controls are implemented and comply with. This certification must demonstrate and document that the networks and information systems meet HIPAA Security criteria and must consider and document accepted risks in the final accreditation process.

Lastly, security is a state of mind and an on-going process, not a project with a certain start and completion date.

References:

[1] Sato, Miles M. "HIPAA Security Policy Development: A Collaborative Approach" April 30, 2001 http://www.sans.org/rr/policy/HIPAA_policy.php

[2] *"A National Strategy to Secure Cyberspace"* http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html

[3] "Certification Requirements" - HIPAA SECURITY MATRIX http://aspe.hhs.gov/admnsimp/nprm/sec16.htm

[4] "Generally Accepted Principles and Practices for Secure Information Technology Systems" - NIST http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[5] "Guidelines for Academic Medical Centers on Security and Privacy - *Practical Strategies for Addressing the Health Insurance Portability and Accountability Act"* Association of American Medical Colleges http://www.aamc.org/members/gir/gasp/.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[6] Cartwright, Bob. "Firewall basics – Some points to consider."
Healthcare Information Security–Newsletter. Vol. 2 No. 5 May 2002: 10-11

[7] Nussbaum, Gerald. "Ten tips for tweaking your VPN."
Healthcare Information Security–Newsletter. Vol. 2 No. 2 February 2002: 1, 7-8

[8] Mitchell, Robert N. "How Secure Are Your Systems?"
Advance for Health Information Executives. Vol.7 No.1. January 2003: 30

[9] "SANS/FBI Top 10 Windows Vulnerabilities"
http://ww.sans.org

[10] Free SANS/FBI Top 20 vulnerabilities scan
http://www.qualys.com

[11] Moreh, Jahen. "Comparing the best approaches for securing e-mail systems."
Healthcare Information Security–Newsletter. Vol. 2 No.3. March 2002: 1, 5-7

[12] Lowe, Scott. "Six basic tips for implementing closed networking on a wireless network" Tech Republic. December 9, 2002
http://www.techrepublic.com/article.jhtml?id=r00620021209low02.htm

[13] Schwartz, Eddie. "Securing wireless networks – don't let uncertainty impede progress." *Healthcare Information Security–Newsletter. V*ol. 2 No.7. July 2002: 1, 4-5

[14] "Phone Sweep" Sandstorm. http://www.sandstorm.net/

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced