Global Information Assurance Certification Paper

HIPAA Security for Small Health-Care Practices: Evaluating Computer Vendor Proposals

Miriam Ferguson
February 6, 2005
GSEC Practical Assignment Version 1.4C
Option 1 – Research Topics in Information Security

Abstract

The new Security Rule section of HIPAA has small health-care practices scrambling to decide how to comply with this ruling by April 21, 2006. Typically, small practices depend on their computer vendors to take care of their technology requirements because small practices do not usually have the expertise to handle technology on their own. Some small practices turn to venders for new computer systems because the practice has outdated equipment.

This study is a guide to educate small practices how to evaluate computer-system proposals from vendors in order to comply with HIPAA. This guide outlines the HIPPA Security Rule and raises issues and questions so that a practice can put together a Request for Proposal (RFP) to send to vendors that adequately prepares the practice to evaluate the vendor's security practices.

Introduction

Two years ago, I assisted in purchasing a new electronic patient information (EPI) system and electronic medical records (EMR) for the organization where I work prior to the publication of the new security rules. This effort led to consulting with a small ophthalmology group in rural South Carolina regarding the purchase of a new patient-information computer system. Eventually, they plan to implement EMR as well, but the driving force behind the purchase of a new computer system will be the practice management piece. I quickly realized through my own experience and from reviewing the computer proposals for the ophthalmology group that health-care computer vendors rarely think about security for the computer systems they sell. Many small health providers make assumptions that the system they are buying is HIPAA compliant and is properly secured. I will address how a small health care organization should evaluate computer vendor proposals for HIPAA compliance.

In 1996, Congress passed the Health Information Portability and Accountability Act which consists of five parts or titles. Title II of HIPAA addresses Administration Simplification which covers 3 areas. The first area addresses the protection of Personnel Health Information (PHI) with the Privacy Rule. Area 2 addresses Transaction and Code Set Standards which affects electronic transmission of health-care claims to insurance companies, Medicare and Medicaid. And last, but not least, area 3 covers The Security Rule which will regulate how electronic PHI (EPHI) is used, transmitted, and maintained. Health-care facilities must be in compliance with The Security Rule by April 21, 2005. However, small practices have until April 21, 2006, to implement the Security Rule (The SANS…18) (U.S. Dept…8334).

The HIPAA Security Rule is broken into three major areas: administrative safeguards, physical safeguards, and technical safeguards. These three major areas are then broken into 18 more specific standards. Twelve of these standards have implementation specification that describes how a standard should be implemented, and the remaining six standards do not have implementation specifications. The 36 implementation specifications are broken into two types: required and addressable. Required means you have no leeway in how the standard is implemented; they must be implemented as described (The SANS…3-4). With addressable standards, the health-care provider has three options on how to implement the specification: “implement an addressable specification if reasonable and appropriate, implement an alternative security measure to accomplish the purposes of the standard, or implement nothing if the specification is not reasonable and appropriate and the standard can still be met” (The SANS…4). The health-care provider should use gap analysis to determine how their health-care practice is currently meeting the HIPAA security rule. The gap analysis is used as “the implementation requirements for the mandated risk analysis” (The SANS…49). Through risk analysis, a health-care

practice will determine the potential threats to their EPHI, determine the vulnerabilities of the system the EPHI resides on, and determine how to keep the EPHI safe. At this point, the practice will have to weigh the potential cost for their EPHI being compromised to the cost of safe guarding the EPHI (The SANS…35).

The HIPAA Security Rule is meant to be vague so each practice can determine their implementation specifications without being locked in to a specific product, vendor, or system. Therefore, the computer vendors that a practice may consider can be vague as well about how HIPAA security is implemented with their system. Generally, when you ask a vendor if their system is HIPAA compliant, the vender replies "Yes, we have to be compliant." Compliancy is not that straightforward. Ultimately, the security officer at the practice is responsible for the HIPAA compliancy and not the vendor. The first step in evaluating vendor proposals for a new computer system is to read the HIPAA regulations. HIPAA regulation can be found on the Internet at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf. Small practices should check the WEDI web site for the Small Practice Security Implementation White Paper at (http://wedi.org/cmsUploads/ pdfUpload/WhitePaper/pub/2004-04-20SmallPractice.pdf). Another thorough but basic resource is the HIPAA Security Implementation by SANS Press. Not only does this resource describe what the HIPAA security rules are and how to implement these standards based on your practices gap and risk analysis, but it lists other excellent resources to help a person understand HIPAA. This paper describes the basic nuts and bolts for the small health practice to evaluate vendor proposals for HIPAA compliance.

Once you are familiar with the HIPAA security rule and its requirements, you can develop a "Request for Proposal" (RFP). The RFP should include application specific questions related to the needs of your practice and questions related to implementing the HIPAA security rule. This paper will outline the HIPAA security rule standards and will suggest how a computer vendor should address this standard for a small practice. This is not meant to be an all inclusive list but a starting point for discussion with the vendor. Each practice will have to decide how it is going to address each HIPAA security standard.

Administrative Safeguards

Standard: Security Management Process

Implementation Specification: Risk Analysis (R)
"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the covered entity" (U.S. Dept…8380).

A computer vendor can assist you in determining your risk after a system is

installed. However, a vendor will probably not offer any assistance. Therefore, ask the vendor during your review process if they can assist you with risk analysis. Although a vendor may agree to assist a practice in evaluating the risk of the computer system, proceed with caution. The vendor is evaluating their computer system and may not be forthright in detecting security holes in their system.

Implementation Specification: Risk Management (R)
"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level" (U.S. Dept...8380).

Risk management involves two standards. First, it involves managing the risk for the practice to an acceptable level and then maintaining an acceptable amount of risk. Since new threats to computer security are developed all the time, this standard will always be a moving target that will constantly have to be addressed (WEDI…7-8).

A computer vendor can assist a small practice by continually evaluating new products to help reduce a practice's risk to security breaches. One of the most common ways to reduce a systems security risk is by applying patches to computers, servers, and routers. Patches reduce the possibility of a virus, worm, or Trojan taking advantage of a software glitch that could bring down a computer system. Microsoft, HP, Dell, and other computer vendors have information on their web sites about securing your computer system with patches (Microsoft step 4) (Hewlett Packard step 2) (Dell step 2). Sometimes patches can cause your software to stop functioning properly. Therefore, you should have a second group of non-production servers and computers (commonly called a sandbox) to test patches before they are applied in a live environment. For a small health care practice, this is not financially feasible and the practice will probably not have the expertise to set up a sandbox for implementing patch trials. A computer vendor should have a sandbox set up to evaluate the various patches for all of the products they sell. In a timely manner, the vendor should either send you the patches to apply or post the approved patches on their Web site. This way you know that the patches that are applied to your computer system will not cause problems with your EPM and/or EMR software products.

Implementation Specification: Sanction Policy (R)
"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity" (U.S. Dept...8380).

A computer vendor will not write policies for a practice regarding how to discipline employees who violate the HIPAA security rules regarding EPHI. However, a vendor should help you set up audit trails to help you monitor when and if EPHI on your computer system has been comprised and who was involved. This information will help you assess whether the practice's

employees are following the rule set forth in your policies and procedures in regard to EPHI.

A vendor should explain how it sanctions its workforce members and what recourse the practice has if an employee of the computer vendor you select violates your policies regarding EPHI on your system.

Implementation Specification: Information System Activity Review (R)
"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports" (U.S. Dept...8380).

Ask the vendor how its system audit logs are set up, how reports are accessed (if there are any reports to access), and how security incidents are tracked. The practice should be able to audit and generate reports on the EPM and EMR software to see if personnel are accessing some part of the program that they should not have rights to. Find out if the reports are generated automatically, how often are they generated, if the reports are easy to read, and how easy is it to use the information to evaluate the computer system. Ask to speak with other practices that are using this system and find out if the reports are useful. At a minimum, confidential EPHI should be audited (WEDI…8). In addition, all devices (routers, servers, firewalls, and other hardware) on the network should be audited in order to determine if someone is trying to hack your system. Ask the vendor about audit capabilities for all hardware on your system and how the audit works.

Standard: Assigned Security Responsibility

"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity" (U.S. Dept...8380).

A computer vendor cannot be your security officer. A person within your practice needs to be selected and held accountable for the HIPAA security rule. This person may be a physician, officer manager, or another health-care professional. Identify the security official who is responsible for the development and implementation of the policies and procedures for your practice and have them work closely with the computer vendor (WEDI…9).

Standard: Workforce Security

Implementation Specification: Authorization and/or Supervision (A)
"Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI is appropriate or in locations where it might be accessed" (U.S. Dept...8380).

The vendor should have the ability to give employees access to only the software elements that are required for the employee to accomplish job responsibilities and deny access to all other elements of the software. For example, the person collecting money from patients should not have the ability to delete charges and payments because this access provides a mechanism for employee theft.

In addition, the vendor needs to assure that their engineers do not open holes in the server or the computer system in general that could compromise the network. For example, if the VPN (virtual private network) software is on the server in a shared folder so you can install the software on various computers, make sure that only the system administrator has rights to that folder. The best practice is not to share the VPN folder--period. Engineers try to make their lives easier and inadvertently open your system to hackers and disgruntled employees. Find out from the vendor how they educate their personnel in security issues. Does the vendor even address security with employees? Does the vendor have policies for the staff to follow to ensure your system stays secure? How do they make sure those policies are followed and what happens when the policies are not followed?

Implementation Specification: Workforce Clearance Procedure (A)
"Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate" (U.S. Dept...8380).

A vendor cannot help you with this standard. This implementation requires policies regarding who you hire and what access you give them to your system. However, a vendor should address how their potential employees are screened.

Implementation Specification: Termination Procedures (A)
"Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by the Security rule" (U.S. Dept...8380).

Again, a vendor can not help you with this standard. Termination procedures require you to define in policies and procedures how you terminate an employee to insure your network is not compromised by employees after they leave your employment. But the vendor should tell you how they protect the information it has about your system that could allow a former employee of the vendor to gain access to your system. A former, angry employee of the vendor could do significant damage your system. How does the vendor try to protect your system against this risk?

Standard: Information Access Management

Implementation Specification: Isolating Health care Clearinghouse Function (R)
"If a health care clearinghouse is part of a larger organization, the clearing house

must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization" (U.S. Dept...8380).

This standard will not apply to a small health practice.

Implementation Specification: Access Authorization (A)
"Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism (U.S. Dept...8380)."
AND
Implementation Specification: Access Establishment and Modification (A)
"Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process" (U.S. Dept...8380).

These standard involve documenting the roles of each employee, and if the employee role changes, then documentation is made regarding that change. In addition, the practice has to document how access is established and modified. Audit logs can assist with monitoring this standard, an issue which your computer vendor should address (WEDI…11-12) Also, the vendor should address how a user is authenticated. Are passwords, tokens, or a combination of passwords and tokens used to authenticate the user? If passwords are used, how does the vendor ensure that the passwords meet industry standards for secure passwords? Passwords should contain letters, numbers, and symbols. They should never contain an actual word and should be changed every 30 days (Bradley step 2). How often is the password required to change? How does the vendor keep the user from using the same password over and over? The practice will base their policies and procedures for this standard on the way the vendor handles authorization. It has been my experience that some computer vendors set up generic passwords for the workforce and never try to apply any password security. In fact, some vendors use non-secure passwords for modems, switches, routers, firewalls, servers, and software. Typically, they use the same password for every practice they set up. So, if you have the same computer system as your neighbor down the street, chances are you have all the information you need to get into their system and vice versa. Ask the vendor if they use unique passwords for each system they set up. Specify in your agreement with a vendor that they will share all log-in information with you for their system and that you have the right to change and monitor all passwords to adhere to industry standards for secure passwords.

Standard: Security Awareness and Training

Implementation Specification: Security Reminders (A)
"Periodic security updates" (U.S. Dept...8380).

Ask the vendor if they have a way to send a "message of the day" to each user that logs into the computer system. Security reminders could be sent to each user daily, weekly, or monthly.

Implementation Specification: Protection from Malicious Software (A)
"Procedures for guarding against, detecting, and reporting malicious software (U.S. Dept...8380).

At a minimum, vendors should include virus protection in their proposal. If not, the vendor should be questioned about the reason virus protection was not included. Contracts with most vendors include a clause that the practice is responsible for preventing viruses, and the vendor will charge extra to fix any system infected with a virus. The virus software should be centrally managed so that virus logs can be viewed easily. In addition, the software should be set up to alert the security officer when a virus has been detected (WEDI…14).

Policies should be implemented that require all employees to get approval from the security officer before any software is loaded. Viruses can be introduced when downloading or installing non-approved software. In addition, ask the vendor how they secure their workstations. I have seen work stations set up that give each authenticated user administrative rights to his or her workstation. Two elements can be used to prevent unauthorized installation of software on workstations. First, you can set up the computers with user rights that don't allow the user to install programs and you can use group policy editor and security templates to secure the workstation even further. Microsoft's article 307882 at http://support.microsoft.com/default.aspx?scid=kb;en-us;307882&sd=tech describes how to use group policy editor to define local computer policies for Windows XP. Local policies can also be defined for Windows 2000. Microsoft's article 313434 at http://support.microsoft.com/default.aspx?scid=kb;en-us;313434&sd=tech describes how to define security templates for Windows 2000. Second, use a program to control access to the Internet. By controlling where an employee can surf, you reduce the risk of malicious software being downloaded onto your computer system. The cost should far exceed the time, cost, and energy of cleaning computers of malicious software. Require the vendor to lock down your computers as mentioned in the first element. The vendor will not freely set your computers up this way. Most vendors do not offer a means to control Internet use. Therefore, you will probably have to research these products on your own.

Firewalls can also help protect you against malicious software from coming from outside your system (The SANS…159). There are various types of firewalls so become familiar with the different type of firewalls. If the vendor does not recommend a firewall, question the vendor about why a firewall is not in their proposal. For those that do propose a firewall, ask the vendor why they are recommending a certain type of firewall. Ask the vendor, how the firewall will be setup and what connections will be allowed through the firewall. A firewall that

is not configured properly is useless.

Implementation Specification: Log-in Monitoring (A)
"Log-in Monitoring" (U.S. Dept...8380).

Ask the vendor how log-in attempts are monitored. Does the system lock out a user after three failed attempts to log on? Will the system notify the security officer when someone has been locked out because he or she exceeded the maximum number of log-in attempts? (WEDI…14) It has been my experience that vendors do not routinely set up this feature although it can easily be setup in Window's systems. In addition, Unix/Linux systems also have the means to monitor log-in attempts (The SANS…159). If the vendor does not routinely set up this feature, then require that it be done.

Implementation Specification: Password Management (A)
"Procedures for creating, changing, and safeguarding passwords" (U.S. Dept...8380).

As mentioned earlier, passwords can be managed by the computer system. A security template can be loaded on the domain server to manage your passwords. A vendor should implement this standard with no problem. The only element that you cannot totally control is users sharing their passwords. However, you can educate users and put policies in place to regulate this type of abuse.

I have found that password security for the individual software programs that a vendor sells leaves a lot to be desired. In one situation, the EMR passwords have to be managed by an administrator. No rules can be applied to guarantee that the password meets the standards for a secure password. The system administrator has to change and enter every password for each user. With the practice-management software, users can change their own passwords but no rules can be set up to control what passwords are entered. They could use cat as their password. In this situation, you can not adequately control passwords for the vendor software, but you can set adequate policies to authenticate users to the domain server.

How the vendor manages passwords will determine the procedures the practice will use to create and change passwords. So, ask the vendor how it suggests you manage passwords for your practice. In addition, ask the vendor how it manages passwords they use to gain access to your system. The vendor should abide by the same password policies as your practice adheres to.

Standard: Security Incident Procedures

Implementation Specification: Response and Reporting (R)
"Identify and respond to suspected or known security incidents: mitigate, to the

extent practicable, harmful effects of security incidents that are known to the covered entity: and document security incidents and their outcomes" (U.S. Dept...8380).

Ask the vendor if they have a way to determine if the computer system has been compromised? Other than virus protection, audit logs and monitoring the servers and monitoring other hardware for performance, a vendor will probably not offer any other solutions that will be adequate for a small practice. However, if the vendor recommends some type of Intrusion Detection/Prevention System, be aware that unless you monitor and manage the system constantly, then it is of no use and is probably overkill for a small practice. Ask the vendor if it monitors your system for security incidents. Ask if the vendor can assist you in securing your system if an incident occurs or if it can they help you contain the threat. Ask the vendor if it can help you recover from an incident (The SANS…162-164). How the vendor responds to these questions will determine how this specification is handled.

Standard: Contingency Plan

Implementation Specification: Data Backup Plan (R)
"Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI" (U.S. Dept...8380).

Does the vendor offer automatic backups? What is its response time for backup failures? Does it offer offsite backup services? At a minimum, the vendor should provide automatic backup services that will verify the backup (WEDI…17). In addition, vendors should be able to tell you how to rotate tapes, how often to clean the tape drive, and how to store your tapes.

Recently, I have seen one vendor that will be offering offsite backups for a very reasonable cost. However, it is contracting with a company that specializes in offsite storage. Therefore, you need a business agreement with that third party as well as with the vendor. Another computer system I looked at offers to set up another computer off site so your information can be backed up to that computer. If one computer fails, the other one is available to run your practice with until the other computer is fixed. This set up was also offered for a reasonable price.

Implementation Specification: Disaster Recovery Plan (R)
"Establish (and implement as needed) procedures to restore any loss of data" (U.S. Dept...8380).

As part of a disaster recovery plan, you are supposed to use a "warmsite" to test your data recovery abilities. Also, this facility would be available to you to set up your system in case of a disaster (Veritas Hotsites, Warmsites, and Coldsites). For a price, you can use the equipment in this facility to run your business until

your system can be operational again. Ask the vendor if it has such a service. If not ask how long it will take to get you up and running if a disaster occurs. Ask the vendor what are its procedures in recovering from a disaster. Small practices may not be able to afford a "warmsite" and will probably be dependent on the vendor to help them recover from a disaster because the practice will not have the expertise or resources to handle disaster recovery on their own.

Implementation Specification: Emergency Mode Operation Plan (R)
"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode" (U.S. Dept...8380).

Unless the vendor can offer a "warmsite," then there is nothing it can do to help you with this item except get you back up and running as quickly as possible. It will be up to the practice to figure out how they will operate until the computer system is running again.

Implementation Specification: Testing and Revision Procedure (A)
"Implement procedures for periodic testing and revision of contingency plans" (U.S. Dept...8380).

Again, if your vendor can provide a "warmsite," you can test your procedures. If not, the vendor will probably not be able to help you with this specification.

Implementation Specification: Applications and Data Criticality Analysis (A)
"Assess the relative criticality of specific applications and data in support of other contingency plan components" (U.S. Dept...8380).

If you are using EPM and EMR software, you need to work out a plan for restoring these two systems. It may be that you would need the EMR software up first because it will contain life-saving information for patients (WEDI…18). Ask the vendor how you can prioritize the recovery of these two systems. Your vendor may not give you an option as to which product will be restored first.

Standard: Evaluation

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting security of electronic PHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart" (U.S. Dept...8380).

Changes will occur all the time in the computer industry. You may add new hardware or software that can change the elements that you have just laid out (WEDI…19) In addition, threats change constantly. If changes occur that your

vendor is involved with, then work with them to address any new security issues. Ask the vendor if it offers a service to analyze your system for security risk.

Standard: Business Associate Contracts and Other Arrangement

Implementation Specification: Written Contract or Other Arrangement (R)
"Document the satisfactory assurances required through a written contract or other arrangement with the business associate that meets the applicable requirements" (U.S. Dept...8380).

You will need a Business Associate Contract with your vendor and any third party businesses associated with the vendor that have access to your EPHI (for example, an off-site backup site that has contracted with your computer vendor). If the third party does not have access to the electronics PHI, you do not have to worry about this business contract. Make sure you develop the business contract so you can specify the elements that are addressed in this paper. For instance, there should be a statement that holds the vendor responsible for the actions of their employees or former employees.

Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: Contingency Operations (A)
"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in an event of an emergency" (U.S. Dept...8380).

For this specification, you have to make sure the vendor can get in touch with someone from the practice to coordinate the disaster recovery plan. This specification outlines who and how people have access to EPHI during a disaster.

Implementation Specification: Facility Security Plan (A)
"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft" (U.S. Dept...8380).

It is not hard for small practices to know who should be in their facility, so elaborate security systems are not needed. A general security system should be adequate for the overall building security. However, the actual computer system may need to be secured within the building. Since small practices have limited space, talk with your vendor about a rack system that can be locked if the system has to be located in an open room.

Also, make sure that the vendor can identify the employees that it sends to work on your system. Know who is coming and how you can identify them.

Implementation Specification: Access Control and Validation Procedures (A)
"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision" (U.S. Dept...8380).

As far as controlling access to the practice physically, this should be straightforward for a small practice and will not need assistance from the vendor. However, ask the vendor how you can identify its workers.

Implementation Specification: Maintenance Records (A)
"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example hardware, walls, doors, and locks)" (U.S. Dept...8380).

Vendors can not assist a practice with this specification.

Standard: Workstation Use

"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI" (U.S. Dept...8380).

As mentioned earlier, a vendor can help a practice lockdown a computer using user rights and security templates. Make sure that only approved employees have access to CD burners, mass storage devices, PDAs, and other such devices. These devices could be used to take patient health information out of the practice. In addition, e-mail can be used to transmit patient information out of the practice and needs to be monitored (The SANS…184-185). Ask the vendor how they secure their servers, desktops, laptops, PDAs, and other equipment containing EPHI. Vendors should lock down workstations so the provider does not have to rely on employees following the practice's policies. In other words, with certain software settings, the practice can control most of the workstation-use issues that the practice should implement. For example, a workstation can be set up so the end-user can not load software without approval. This safeguard will make the practice policies and procedures easier to document and enforce.

Standard: Workstation Security

"Implement physical safeguards for all workstations that access electronic PHI, to restrict access to unauthorized users" (U.S. Dept...8380).

This standard involves technical and physical safeguards. All equipment, including routers, switches, and firewalls, must be secured physically as well as technically. A vendor can definitely help you technically secure your system. However, it may not offer any means to physically secure your system. The practice may have to look to other resources for locks and other physical security items.

Technically speaking, you should ask the vendor how it prevents unauthorized access into its system for modems, routers, switches, wireless connections, servers, workstations, and any other equipment that may be used for EPHI. The practice should become familiar with the basics of securing workstations by using resources such as HIPAA Security Implementation by SANS Press and "The Twenty Most Critical Internet Security Vulnerabilities" by The SANS Institute at http://www.sans.org/top20/. There is no reason a vendor could not implement basic workstation security for a practice.

Being familiar with basic specifications for hardware security can help a practice determine if the vendor is using current industry standards. One vendor I am familiar with has a habit of connecting modems directly into your computer systems, thus leaving a back door for hackers. At a minimum, a remote power switch should be connected to the modems to assist the security officer in turning off the modems when they are not in use. "Banyan Vines Checklist" published at http://csrc.nist.gov/fasp/FASPDocs/inoutput-control/USAIDTechSafeBSPI3.html lists items to evaluate in order to check for remote access security such as turning off modems when not in use, using a firewall to mediate modem access, removing default passwords on the modem, and removing modems on workstations that have dial up access. This specification requires highly trained security expertise to evaluate thoroughly. A practice should consider consulting a computer security expert to truly evaluate this specification.

Standard: Device and Media Control

Implementation Specification: Disposal (R)
"Implement policies and procedures to address the final disposition of electronic PHI , and/or the hardware or electronic media on which it is stored" (U.S. Dept...8380).

If you are considering an agreement with a vendor to maintain your hardware, ask the vendor how it disposes of any EPHI on hardware that is removed from your practice. Ask the vendor if the hardware can be cleansed before the device leaves your practice and if it can provide documentation stating that the device was cleansed of any EPHI.

Implementation Specification: Implementation Specification: Media Re-use (R)

"Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use" (U.S. Dept...8380).

Ask the vendor how they recommend you destroy your backup tapes and any other media that contains EPHI.

Implementation Specification: Accountability (A)
"Maintain a record of the movements of hardware and electronic media and any person responsible therefore" (U.S. Dept...8380).

Your vendor really can not help you with this specification unless it has included an inventory mechanism in it proposal. However, a small practice really does need an elaborate inventory system.

Implementation Specification: Data Backup and Storage (A)
"Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment" (U.S. Dept...8380).

Again, ask the vendor if it has an automated off-site backup option. Otherwise, ask the vendor how data is backed up and verified.

Technical Safeguards

Standard: Access Control

Implementation Specification: Unique User Identification (R)
"Assign a unique name and/or number for identifying and tracking user identity" (U.S. Dept...8380)*."*

Earlier, password management was discussed and how passwords should be managed. This is only part of the equation for unique user identification. There can be multiple log-ins for a computer system. For example, a person may have a log-in for Windows and another log-in for the EPM and/or EMR software. For Windows, you can determine what type of user name and password combination to use based on Windows specifications which should meet any basic HIPAA requirements. However, the vendor will control how user identification is setup for its software. So ask the vendor how user identification is setup for its software. One vendor I am familiar with only allows you to use numbers and letters up to six characters for the user name and password. In addition, the system administrator has to manage all passwords. This is definitely not the most optimal way to implement unique user identification, but it may be adequate for a small practice.

Implementation Specification: Emergency Access (R)
"Establish (and implement as needed) procedures for obtaining necessary

electronic PHI during an emergency" (U.S. Dept...8380).

As mentioned earlier, a small practice will be very dependent on a vendor to assist it during an emergency. Ask the vendor how quickly it can assist the practice in case of an emergency and how the vendor can assist the practice in this situation. Based on the vendor's comments, the practice can establish and implement its procedures.

Implementation Specification: Automatic Logoff (A)
"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity" (U.S. Dept...8380).

There are actually several ways that this standard can be addressed. There are software settings inside Windows and Citrix that will log the user off after 10 or 15 minutes (whatever you specify) of inactivity. A password screensaver can be set up to take effect after 10 or 15 minutes of inactivity. The bottom line is the vendor should have a solution for this standard and should be required to setup the computer system to adhere to this specification.

Implementation Specification: Encryption and Decryption (A)
"Implement a mechanism to encrypt and decrypt electronic PHI" (U.S. Dept...8380).

If a messaging system is proposed by the vendor, ask them if messages that contain EPHI can be sent across the Internet. If so, then how will the vendor address this issue? Will the information be encrypted? Any communication with the outside world will have to be encrypted if it contains EPHI. Ask the vendor to address how encryption is handled for all EPHI exiting your private system and entering the public domain. User credentials should also be encrypted in the vendor set up.

Standard: Audit Controls

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI" (U.S. Dept...8380).

Earlier discussions have touched on the subject of audit controls. Vendors definitely should have a means to implement this standard.

Standard: Integrity

"Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information (A)
Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner" (U.S. Dept...8380).

At a minimum, vendors should recommend using servers that use RAID and error correcting (ECC) memory to help ensure data integrity (The SANS…218)

Standard: Person or Entity Authentication

"Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed" (U.S. Dept...8380).

Vendors can use a "single-factor authentication" which uses one proof of identification or a "multi-factor authentication" mechanism which uses more than one proof of identification (The SANS…219). Vendors I am familiar with only offer a "single-factor authentication system." A "multiple-factor authentication" system is best, but a single-factor system will probably be adequate for a small practice. If the vendor only uses a single-factor system, then ask if it is working on a multi-factor system for authentication.

Standard: Transmission Security

Implementation Specification: Integrity Controls (A)
"Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposal of" (U.S. Dept...8380).

Ask the vendor what means is used to transmit EPHI to ensure the data is not altered until the information is destroyed. There are numerous integrity controls that can be used to meet this specification. Make sure the vendor is using well-known controls such as Public Key Infrastructure, Cyclic Redundancy Checks, Hashing functions or blocking ciphers (The SANS…226). A practice should be skeptical of a vendor that is not using a well-known integrity control.

Implementation Specification: Encryption (A)
"Implement a mechanism to encrypt electronic PHI whenever deemed appropriate" (U.S. Dept...8380).

Ask the vendor how they encrypt data sent to insurance companies and other transactions that involve EPHI over a public network such as the Internet. As with integrity controls, vendors should use well known encryption methods such as Advance Encryption Standard, 3 DES, blowfish, and IPSec (The SANS…226). If the vendor is not using a recognized encryption process, ask it why.

Ask the vendor what access controls they recommend to keep your data safe if your practice accesses the Internet. At a minimum, this should include a firewall and virus protection. There other options that could be considered like desktop firewalls.

Conclusion

A small health-care practice will probably not have the expertise to thoroughly evaluate a computer system for HIPAA compliance. However, the practice can help protect itself when purchasing a new computer system by becoming familiar with the basics of HIPAA regulations. Based on this knowledge, a RFP can be developed to get detailed information from the vendor in order to adequately evaluate a vendor's computer system for HIPAA compliance. Between the answers the vendor gives to the questions related to HIPAA and answers related to how the vendor's software functions, the practice can make an informed decision as to which vendor to choose. While a practice may choose a vendor that has software that will meet its operational needs more than it meets the HIPPA requirements, a practice should use the HIPAA regulations to encourage the vendor to secure its system as required by HIPAA. If the vendor does not secure its system, the practice will have to address HIPAA through another avenue.

The vendor's response to the RFP should be used in the contract with the vendor to specify the vendor's responsibilities. In addition, a business contract needs to outline the vendor's responsibilities in keeping the practice's EPHI protected as outlined in the practice's policies and procedures

Ultimately, security should come first and not as an afterthought. Securing a system after it has been installed is more costly and time-consuming than planning for security up front. The practice will have to decide how security will be handled and at what cost. Most vendors entered the health-care business before security was required by HIPAA. Vendors have to rethink how their systems will function in the world of HIPAA. In my opinion vendors have to make sure their systems are as secure as possible because many practices are depending on the vendors for this service, especially small practices.

References

"Banyan Vines Checklist." National Institute of Standards and Technology. CRSC.NIST.com. http://csrc.nist.gov/fasp/FASPDocs/inoutput-control/USAIDTechSafeBSPI3.html (22Jan. 2005).

Bradley, Tony. "Microsoft Windows Security 101." Netsecurity.com. 2005. Primedia Corporation. http://netsecurity.about.com/cs/windowsxp/a/aa100903.htm (29 Dec. 2004).

"How to Define Security Templates in the Security Templates Snap-in in Windows 2000." Microsoft.com. 15 July 2004. Microsoft Corporation. http://support.microsoft.com/default.aspx?scid=kb;en-us;313434&sd=tech (29 Dec. 2004).

"How to Use Group Policy Editor to Manage Local Computer Policy in Windows XP." Microsoft.com. 15 July 2004. Microsoft Corporation. http://support.microsoft.com/default.aspx?scid=kb;en-us;307882&sd=tech (29 Dec. 2004).

The SANS Institute. HIPAA Security Implementation 2nd ed. United States: SANS Press, 2004.

"Small Practice Security Implementation White Paper." WEDI/SNIP – Security and Privacy Workgroup. 20 April 2004. Workgroup for Electronic Interchange. http://wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/2004-04-20SmallPractice.pdf (29 Dec. 2004).

"Steps to Protect Your PC." HP.com. 2004. Hewlett-Packard Corporation. http://h20239.www2.hp.com/techcenter/security/Protect_PC.htm (29 Dec. 2004).

"The Technology of Disaster." Veritas.com. 3 October 2003. Veritas Corporation. http://www.veritas.com/van/articles/3943.jsp (29 Dec. 2004).

"The Twenty Most Critical Internet Security Vulnerabilities." SANS.org. 8 October 2004. Ver. 5. The SANS Institute. http://www.sans.org/top20/ (22 Jan. 2005).

"Tools You Need to Secure Your PC." Dell.com. 1999-2005. Dell Corporation. http://support.dell.com/support/topics/global.aspx/support/security/security_1 (29 Dec. 2004).

U.S. Department of Health and Human Services. Health Insurance Reform: Security Standards; Final Rule: 45 CFR Parts 160,162, and 164. Washington: U.S. GPO, 2003. http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (29

Dec. 2004)

"What are Viruses, Worms, and Torjan Horses?" Microsoft.com. 9 March 2004. Microsoft Corporation. http://www.microsoft.com/athome/security/viruses/virus101.mspx (29 Dec. 2004).