Security Policies and Procedures – The Final Hurdle

By Raymond Posa, MBA

10 Maple Street, Suite 301
Middleton, MA 01949
978-646-9091 978-646-9092 fax office@aappm.org www.aappm.org

Security Policies and Procedures – The Final Hurdle

The security requirements of HIPAA do not go into effect until April of 2005, but did you know that there is a HIPAA Catch 22? You should by now already have your policy and procedures policy manual written and your staff educated regarding your policies. You also have to have your Notice of Privacy statements posted and sign off sheets ready for your patients as of April 14, 2003.

What you may not be aware of is the next step in HIPAA compliance; the Security rules. They have been finalized but don't go into effect until April 2005, or do they. Here is the Catch 22. Even thought full Security compliance is not mandatory until April 2005 under the Privacy rule 164.530 – Safeguards, requires you to have physical, technical and administrative security in place. The catch 22 is that in order to be fully compliant with the privacy rules you need to have most of the security rules addressed also.

The best way to address HIPAA compliance is to treat the regulation as a single integrated entity. By keeping your eye on the total picture, you won't have to waste time; effort and money by have to readdress items at a later date. You should have a total integrated HIPAA plan and work it into your daily routine. Make it second nature and compliance will be much less burdensome.

While the privacy requirements lend themselves well to boilerplate policies and procedures requiring only minor adjustments for your practice; Security will be a horse of a different color. The security requirements are so specific to your practice that writing policies and procedures to address security issues in your practice will require much more thought and effort and we should start addressing these new requirements now.

With privacy, most offices only had to take their existing way of doing business and put it in written, print up their NPP, display it in the waiting room, post it on your web site and hand them out to the patients; done. Security on the other hand will require much more. Security is going to get into areas that most practices have never though of and don't even have a foundation to work off. Security will deal with the physical facility, the computer system, computer user procedures and practice contingency plans among others.

While many have accomplished the privacy portion of HIPAA with out conducting a Gap analysis; with the security portion a Gap analysis will be essential for the following reason: Privacy compliance required little or no expenditures in order to be compliant, security however may require investing quite a bit of money in software, hardware and facilities upgrades. By conducting a Gap analysis you can identify areas needing attention and then work out a long term plan to address these issues. The key here is that you are pro active. You have identified and are working toward mitigating the problem areas. That being said, if there is a breach in your security you are still responsible. The difference is in the amount of your liability. If you have identified problem areas and have a plan to address them you are in much better position than being caught with a security breech and you have no idea that there was a problem and no plan in place to address it. Again we come back to our favorite HIPAA buzz word MITIGATION. HIPAA is all about making reasonable efforts to reduce the risk of having PHI falling into the wrong hands.

The requirements for compliance under the Security provisions of HIPAA, unlike Privacy which many practices took a cookie cutter approach to will be so individualized that it is unlikely that you will be able to meet the requirements with anything less than a well thought out, highly individualized policy and procedures manual. Some of the areas that must be addressed are data backups, intrusion detections / prevention and access control to data.

Data Backups

Have you ever thought about a parachute? It's a nice invention. Could you image having to wear one all the time? It would be cumbersome and awkward, but could you image not having one when jumping from an airplane. Computer backup systems are the same way. They can be a nuisance and a bit of a bother, but like a parachute when you need one nothing else will do.

I have seen so many cases over the years where clients blindly put tapes into their backup units, assume they work and the next day switch tapes and just go about their business. As a matter of sound business practice you need to test and verify your backups to make sure that they are actually backing up your data properly and the information is without errors.

Under HIPAA security rules, not only are you required to perform regular backups but you are also required to test and verify that the backup was successful but you must also have a procedure to make sure you can restore the data and you must also have a provision to make sure you keep a copy safe and off site.

Conventional tape backups are fairly easy to use but making sure that they are meeting the contingency requirements of HIPAA can be a laborious effort for your staff and may even be beyond what the staff can do themselves.

To every HIPPA problem there seems to be a HIPAA solution. Actually, this solution has been around for several years but is now finding a new niche in the medical field, especially in small offices. It is web based backup services. There are many companies offering this service. The way they work is as follows; special client backup software is installed on your computer. This software runs a batch every night just like a tape would. The backup client takes your backup and compresses and 428-bit encrypts its. It then sends it to a remote server, where it is received and processed. The remote server opens the files and verifies the data against a known copy in your folder. The server then recovers a file from you backup to insure its integrity. The remote server now puts together a report with all of the vital information about your backup and E-mails you a report. Every morning you have an E-mail confirming that your backup has taken place, was successful and is fully restorable.

These services address several points of concern in HIPAA security compliance. They provide a safe, hands off approach to backing up your data, they keep your data safe and off-site, they provide you with documentation that you are meeting and exceeding the HIPAA mandates, and they relieve your staff of the responsibility of performing the backups themselves.

Anti-Virus Software and Operating system patches.

Anti-Virus software is so essential in today's computer environment, so much so that I tell clients to not even bother running their PC's if they are not running up to date virus software. Why, because viruses are so prolific that in a very short time you WILL get one. Anti-virus vendor watchdog groups are reporting that new virus activity was up 17.5 percent over the past six months, and viruses are getting more sophisticated, with more sophisticated targeting.

Just to demonstrate this fact for my clients, my anti-virus program has an audible alert option that I can switch on for demonstration purposes; it goes off every time a virus attempts to enter my system. When activated, it will beep every 5 to 10 seconds all day every day, that's how bad things are.

Some users believe it won't happen to them or they can't afford the software or the update subscriptions. My response is, you can't afford not to have it. The cost of repairing a system after being infected will cost much more than even the most expensive anti-virus software; plus you can't even put a monetary value on the cost of lost data. I consider the money paid for anti-virus software to be part of the operating expense of a computer, just like electricity is.

Under HIPAA security requirements you are required to safeguard your systems from outside intrusion and failing to do so is a violation. Virus attacks and outside hacks are considered “common knowledge” and you are responsible to implement procedures to prevent intrusions. Just installing anti-virus software is not enough. You must configure it so that it will quarantine the virus and /or delete it. You need to also make sure the virus patterns that the manufacture provides are up to date.

Once you have your anti-virus software installed and configured and getting its updates, your done, right? Wrong. There is another key component that must also be done; that is updating your operating system. You should be checking for Windows updates on a daily basis. In Windows 98 and later, Windows has a scheduler feature whereby Windows will automatically go to the Microsoft update site and find any new critical updates and download them for you. It will then have a little pop up alert letting you know that the updates are downloaded and ready to be installed.

This is important because many viruses are written to exploit vulnerabilities in Windows. Even though you have anti-virus software if you have critical holes in Windows you are still subject to getting a virus. The anti-virus software also depends upon the Operating system being secure.

Firewalls

In addition to anti-virus software to keep out malicious software attacks, Firewalls keep out direct intrusions as well as blocking some virus exploits. The Firewall is one of the most overlooked pieces of security. Firewalls are designed to prevent unauthorized access to your computers from the web.

The broadband explosion has provided Internet users with a better, faster solution than the traditional dial-up connections we've been used to over the years. That's the good news. The bad news is; broadband connections have some drawbacks, the most serious of which is the fact that they are "always on." A connection that never shuts off is a hacker's dream. Hackers like "always-on" connections like DSL, cable modems and T1 lines because they're always there and they're predictable. This isn't to say that broadband connections are bad. Quite the contrary. Broadband is a great technology. Users just need to make sure they're using the appropriate level of protection that a firewall solution can offer.

Without a firewall in place hackers can access your PHI and either use it for their own purposes or disseminate it to the world at large. Firewalls are a great way to protect your practice’s computers from intruders. They're designed to defend against attack by implementing a series of rules that permit, or deny, traffic to pass between your network and the Internet. Based on the way these rules are set, the inbound and outbound flow of information maybe extremely tight or very relaxed. The trick is to maintain a balance between your practice’s need for security and your employees' need to get their work done without interference.

Firewalls are absolutely necessary and are not very expensive. I would strongly suggest having the firewall installed by an expert. While anyone can take it out of the box and plug it in. The trick is to configure it properly or it becomes a useless piece of hardware sitting on your network not protecting you and only providing you a false sense of security until your network is compromised.

Access Control Using Biometrics

Biometrics are any security device that uses unique physical attributes of the user to identify themselves. There are currently face scanners, palm scanners, retina scanners and finger print scanners on the market today. For our purposes I will contain this discussion to finger print scanners. The finger print scanners are the least expensive of the biometric devices yet still offer outstanding security.

The way the fingerprint biometric systems work is as follows. The scanners come bundled with security software that acts as an overlay on your desktop. The software intercepts the log in procedure and requires a fingerprint input in order to proceed. The software also has a registration process that scans each person’s fingerprints and digitally records the fingerprints as an algorithm, so it never keeps a "picture" of your actual fingerprint. The scanning software then works in conjunction with the Windows operating system security and allows you to assign rights and permissions to each user. It is really a fascinating piece of technology.

Under the security rules of HIPAA which become mandatory in April of 2005, you are required to secure all your computers by the following means:

1) Each user has their own unique login name and password of a minimum of 6 characters.
2) No users shall know or use another person's password.
3) The passwords must be changed at least every 90 days.
4) The passwords must have the proper access level assigned to them based upon the persons job function.

The reality of the situation is that if you use complex passwords and change them frequently, people will forget them; then the system administrator has to recreate the users account and setup a new password. Worse yet, if they can't remember the password, they will write them on a sticky note and put them where they can find it easily, like on the screen. Also in a small office, people are close and share information and they will share their passwords. By using the fingerprint scanners you eliminate all of that and actually make logging in fast and easy. The person just touches the fingerprint scanner and in about a second they are logged in. It takes no thought, just press and go. The scanner's software knows who it is that is logging in and gives them the rights and permissions that they are supposed to have. You can't lose your password, you can't forget it, and you can't give it to someone else.

Access Control to discarded PHI - Office Shredders

One of the most overlooked security flaws in a practice is the waste paper basket. If your office is not currently using a shredder then please by all means at the end of the day take a look through your waste paper basket, especially at the front desk. You may find an abundance of PHI in there. You may think that this is a bit paranoid; to go through the trash, or who wants my trash anyway. Case in point, in Philadelphia there was a crew that was working with insiders in an HMO and they were sending patient PHI out the door in the trash. Their accomplices would then go through the trash and remove the PHI. Their next step was to take the papers back to an apartment that was set up with some very elaborate devices for making forged credit cards and documents. This crew would then open charge cards, make mortgages and even purchase automobiles all with the forged documents.

The bottom line is that the HMO is going to see serious liability on this because they have an obligation to have policies and procedures in place to prevent this kind of activity.

The Final Step – Keeping It All Together

The most effective way to keep track of your HIPPA data is with the use of a HIPAA tracking tool. There are many good one on the market. One of the better ones that I have used is ComplyAssistant, available through www.njhipaa.com. It provides a through review of your practice through every section of the HIPAA regulation. It will produce Gap analysis reports, year to year trending reports, mitigations action plans, work flow plans, incident tracking and graph reports showing all of your results. In the final phase of HIPPA you will find that an electronic HIPAA compliance tracking tool will be worth its weight in gold.

I recommend that every doctor and HIPAA compliance officer spend an hour at the government HIPAA web site (http://www.cms.hhs.gov/hipaa/) this will give you answers right from the horse's mouth. We also encourage the use of open forums such as www.njhipaa.com www.footzine.com or www.aappm.com to get answers to your questions from qualified experts, remember your question are probably the same questions on the minds of your colleagues, so please ask. The single biggest thing to remember about HIPAA is that it is real and enforcement and penalties begin April 2005.

By Raymond F. Posa, MBA, Technology Advisor to the American Academy of Podiatric Practice Management (AAPPM), President, R. Francis Associates. Any questions on the items or services mentioned in this article or comments can be addressed to Mr. Posa by E-mail: Rposa@Rfrancis.com