June 29, 2010

Part 4 of HIPAA Security FAQ's continued

Part 4..... Almost done with all of the Security FAQ's. Again, I want you to know everything about HIPAA so please, if you have any questions, ASK. My goal is to help each of you become legally compliant, HIPAA and Medicare. I want to make it simple and easy for you and you take care of the folks. Again, there is nothing more important in your practice than taking care of the patients and spreading the word of chiropractic.

Security is part of the HIPAA Standards that is much less known than HIPAA Privacy, but not less important. The most important thing in HIPAA Security is assessing your risk of a breach and doing everything you can to stop it before it happens.

When reading these FAQ's, remember the difference between "Required" and "Addressable". "Required" means you must implement the standard and "Addressable" means you have reviewed it, decided if you are at risk or not, and implemented any necessary policies or procedures to mitigate the risk.

Edie Hofmann
ICCOM
International Center for Chiropractic Office Managers

www.ICCOM.org

Call Edie at: 313.330.0199 or CLICK to email Edie

What are the implementation specifications of Facility Access Controls?

1) Contingency Operations (addressable)

2) Facility Security Plan (addressable)

3) Access Control and Validation Procedures (addressable)

4) Maintenance Records (addressable)

What does Contingency Operations mean?

This means how are you protecting EPHI during or immediately following a disaster. If you have a disaster, and data needs to be restored, how is security and appropriate access being protected and maintained? Do you need a guard at the door? Do you need to tell your staff only the doctors are to report? Can all staff report to help with the restoration? You must write a policy and procedure for that situation if it is reasonable and appropriate.

What does facility security plan mean?

If appropriate and reasonable you must have procedures to safeguard the facility and keep it secure from unauthorized individuals at all times. Such has locked doors, surveillance cameras, alarms, etc.

What does "workstation use" mean?

A workstation is defined as an electronic computing devise (laptop, desktop etc). If appropriate and reasonable you must have written 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 surrounds of the specific workstation that can access EPHI. One policy may be that no one can "surf the net" while on any computer that has EPHI on it or no one can be on the computer if not scheduled to work at that time.

Do workstations apply to the workstation I use at home?

If you have a computer at home or a laptop that you carry back and forth that has EHPI on it, it is considered the same as any workstation in the office and must be protected.

What are the implementation specifications for Device and Media Controls?

1) Disposal (Required)

2) Media Re-se (Required)

3) Accountability (Addressable)

4) Data Backup and Storage (Addressable)

What is my main concern with disposing of electronic media?

When disposing of any electronic media that contains EPHI you must

make sure it is unusable and/or inaccessible. One way to dispose of electronic media is a degaussing whereby a strong magnetic field is applied to fully erase the data. If you do not have access to degaussing equipment, another way to dispose of the electronic media is to physically damage it beyond repair, making the data inaccessible.

What does "media re-use" mean?

It means re-using the electronic media by moving it to another location, selling it or giving it away. If you choose to re-use the media, you must remove all EPHI previously stored on the media to prevent unauthorized access to the information. You are to maintain a written record of all movement of electronic media if reasonable and appropriate.

to be continued....

Have you looked at the checklist yet? Are you compliant? Find out for yourself.

HIPAA Privacy Checklist

HIPAA Security Checklist

If you find that you are not compliant. Please purchase my manuals and start the process with the most easy to implement strategies on the market today!
http://www.iccom.org/index_files/ICCOMProducts.html

==========

ATTENTION DOCTORS

I am asked all the time, "Will you tell me A-Z what I need to do to be sure I am compliant?"

First, if you do not have fully customized manuals specific to your office then you need to purchase my manuals. NOW!

The customization includes your clinic information, the officials' contact information, etc as mandated by the HIPAA Laws/HHS, and all the policies and procedures you much follow to be compliant. I do all the customization for you. It is ALL done and the only thing left for you to do is to have your compliance official read the material and implement all the policies and procedures, as well as, conduct staff training. After that is done, if you are ever audited, believe me they will ask for all the documentation I have stated above, your staff will be able to immediately locate the manuals and the documentation and can then attest that they have been trained on the information. All of which are required by law.

==========

Please visit my website to learn more about HIPAA Privacy and HIPAA Security rules and more and ORDER my manuals if you do not have them.

http://www.iccom.org/index_files/ICCOMProducts.html

email me with any questions you may have: (click here to email me)

A Leader in Chiropractic Office Management and Compliance Training