June 16, 2010

Part 3 of HIPAA Security FAQ's continued

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.

What are my responsibilities in protecting health information from malicious software?

Malicious software can be thought of as any program that harms information systems, such as viruses, Trojan horses or worms. Malicious software is frequently brought into your system through email attachments and programs that are downloaded from the Internet. This must be part of the training process regarding their rule in protecting against malicious software.

What is the purpose of the Log-In Monitoring specification?

Security awareness and training should address how users log onto systems and how they are supposed to manage their passwords. If

Edie Hofmann
ICCOM
International Center for Chiropractic Office Managers

www.ICCOM.org

Call Edie at:
313.330.0199
or CLICK to email Edie

reasonable and appropriate you must monitor all log-in attempts and report discrepancies. Talk with your software vendor.

Do I need a procedure for changing passwords on my computer?

It is not required. It is an addressable standard. If it is reasonable and appropriate safeguard you should regularly change your password. In FTC, Identity Theft Prevention Rule, it is required to change passwords on a regularly scheduled routine.

What are security incident procedures?

Basically it is how you and your staff are to respond to, report, and document suspected or known security incidents, harmful effects and outcomes. This would include such things as stolen computers or passwords, corrupt backups, virus attacks, physical break-ins, etc.

The new HITECH rules are very specific concerning these security incidents.

What is the purpose of a Contingency Plan standard?

To establish strategies for recovering access to EPHI should the clinic experience an emergency or other occurrence, such as a power outage, fire, vandalism, natural disaster, etc. that disrupts critical business operations. The goal is to ensure that you can still conduct business and that the EPHI is available when needed.

What are the contingency plan standards?

1) Data Backup Plan (required)

2) Disaster Recovery Plan (required)

3) Emergency Mode Operation Plan (required)

4) Testing and Revision procedures (addressable)

5) Applications and Data Criticality Analysis (addressable)

What is required for data backup plan?

You must have a backup procedure to create and maintain retrievable exact copies of EPHI.

What is required for a disaster recovery plan?

You must have a procedure to restore any loss of data.

What is required of emergency mode operation plan?

You must have procedures to enable continuation of protecting the EPHI while you are in emergency mode. (If the power goes out, your EPHI must continue to be protected)

What is required of testing and revision procedures?

First, it is not required. It is addressable, but if you find that it is a reasonable and appropriate safeguard you must have procedures for period testing and revision of your contingency plans.

What is required of application and data criticality analysis?

Remember, this is not required. It is addressable. If you find that it is a reasonable and appropriate safeguard you must have procedures to identify how important each application software is to patient care or business needs and prioritize for data backup. This will help you better select which application software gets restored first and/or if there is any application software that must be available at all times.

What is meant by physical safeguards?

The Security Rule defines physical safeguards as "physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

What does it mean that facility access controls are addressable?

You must have policies and procedures to limit physical access to your facility or other place the EPHI is housed. Facility is defined as "physical premises and the interior and exterior of a building."

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)

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

==

Please visit my website that further explains the HIPAA Privacy and HIPAA Security rules and more.

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