June 7, 2010

Part 2 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.

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 three categories that the security standards are divided into?

1) Administrative safeguards: Assignment or delegation of security responsibility to an individual and the training requirements, as well as, written policies and procedures to manage the selection, development, implementation and maintenance of the security measures to protect EPHI.

2) Physical safeguards: The mechanisms required to protect electronic systems, the equipment and the data from threats, environmental hazards and unauthorized intrusion. This includes restricting access to EPHI and retaining off site backups.

3) Technical safeguards: Primarily the automated processes used to protect data and control access to the data, i.e. passwords, encryption and decryption

What are the implementation specifications in the Security Management Process?

1) Risk Analysis (required)

2) Risk Management (required)

3) Sanction Policy (required)

4) Information System Activity Review (required)

What is the importance of Risk Analysis and Risk Management?

This activity forms the foundation upon which an entity's necessary security activities are built. The results from the initial risk analysis and then the written risk management processes will become the baseline for your ongoing security process.

What is system vulnerability?

A system vulnerability is a flaw or weakness in a system, due to its design, installation, lack of policies and procedures, or some other cause. Any of these weaknesses, whether intentional or accidental, could potentially result in a breach or inappropriate use or disclosure of electronic PHI. Some vulnerabilities may be caused by ineffective policies regarding user or log on IDs and passwords, holes or weaknesses in some of the software tools, or flaws in the operating system, application or inadequate access controls.

What is the importance of a Sanction Policy?

Appropriate sanctions must be in place so that workforce members understand the consequences of failing to comply with your security policies and procedures to deter noncompliance.

What is the importance of an information system activity review?

This initial and on-going audits of activity within your system enables covered entities to determine if any EPHI is used or disclosed in an inappropriate manner. It is a tracking of everything that is done on your computer. These should be in the form of audit logs, access reports and/or incident tracking reports.

What is the purpose of assigning security responsibility /Security

Official?

The purpose of this standard is to identify who will be operationally responsible for assuring that the covered entity complies with the Security Rule. Covered entities should be aware that this is comparable to the Privacy Rule standard that requires all covered entities to designate a Privacy Official. The Security Official and the Privacy Official can be the same person, but are not required to be.

What does workforce security cover?

1) Authorization and supervision of the workforce (addressable)

2) Workforce clearance procedures (addressable)

3) Termination Procedures (addressable)

How do I determine what level of access is required for each person in the clinic?

First of all, because this is an addressable standard, you must determine if it is reasonable to have different levels of access. Most of the time in smaller clinics this is not necessary. You need only document that it was reviewed and you decided everyone needed complete access. There may be some clinics that access is granted for billing, data entry, patient healthcare information (treatment records) or accounting purpose that may require difference access because the clinic may have departments or larger staff. You will have to work with your software vender to determine what activity levels are available.

Is workforce clearance procedures required?

It is not required to have in place, but it is required that you have reviewed (addressed) your current procedures to determine if these procedures should be altered based on your particular clinic size as stated above.

What should I look for in putting together termination procedures?

Basically, it is what you do when a staff member is fired or resigns from their position. This is an addressable standard. Your computer system needs new passwords immediately, your doors need new locks if they had a key, if you have electronic access, change the access code. This is minimal protection for PHI and/or EPHI.

How do I ensure access is restricted within my clinic?

This should be part of the reports or audits you can run from your computer system. Talk with your software vendor. Daily reports should show every activity that was conducted on your computer software that day.

What must be included in security awareness and training?

1) Security Reminders (addressable)

2) Protection from Malicious Software (addressable)

3) Log-In Monitoring (addressable)

4) Password Management (addressable)

What is meant by "security reminders"?

Where this is a reasonable and appropriate safeguard, you must implement periodic security updates. Check your virus protection. Etc. This needs to be on a specific schedule and written on some type of a calendar. Could be paper or electronic and part of your process.

To be continued…..

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

HIPAA Privacy Checklist

HIPAA Security Checklist

==========

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