July 7, 2010

Part 5 HIPAA Security FAQ's

OK, the last in the series of HIPAA Privacy and HIPAA Security FAQ's.

Part 5. Here we go. Are You HIPAA Compliant? You should know by now. This series has definitely given you an indepth education on HIPAA Privacy and HIPAA Security. If there is still something you do not understand, please ASK. My goal is to help each of you become legally compliant, HIPAA and Medicare. I want to make it quick, simple and easy for you to get it done and then focus on taking care of the folks.

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 is required for data backup and storage?

If reasonable and appropriate, you must create a retrievable, exact copy of the EPHI, when needed, before movement of the equipment.

What are considered technical safeguards?

The Security Rule defines technical safeguards as the technology and the policy and procedures for its use that protect EPHI and control access to it.

What implementation specifications are associated with the Access Control standard?

1) Unique User Identification (Required)

2) Emergency Access Procedure (Required)

3) Automatic Logoff (Addressable)

4) Encryption and Decryption (Addressable)

Am I required to have a unique user identification specified for each user of my computer system?

Yes, it is required. You MUST assign a unique name and/or number for identifying and tacking user identity. This will enable you to hold users accountable for functions performed on information systems with EPHI when logged into those systems

Am I required to establish emergency access procedures?

Yes, it is required. You MUST establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency. Determine what types of information will be needed during times of emergency. If you determine that you have everything you need to care for a patient (I.e. paper "treatment" cards etc.) that is what you document as your emergency access procedure.

Am I required to have automatic logoff that terminates a session after a predetermined time of inactivity?

No, it is addressable. If it is a reasonable and appropriate safeguard then you must implement procedures that terminate an electronic session after a predetermined time of inactivity. This protects EPHI when the uses leaves their workstation unattended.

Is encryption required of electronically protected health information?

No, it is addressable. **But, the new Breach Notification Interim Final Rule states:**

"Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information."

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

What does it mean to protect the integrity of protected health information?

What this means is that you must be sure that the integrity of the EPHI is not improperly modified without detection until disposed when be transmitted electronically. Check with your IT professionals, software vendors, business associates and trading partners for their capability of insuring your data is not modified and if it is, it will be detected and you will be notified.

What is the penalty for not complying with the HIPAA Security Rule?

HIPAA provides for civil and criminal penalties for failing to comply with security rule. How the penalties are enforced and the degree to which they are enforced is based on the actions of a covered entity took as soon as they became aware of violations involving the security rule. This means that we have to make a good faith effort to adhere to requirements in the security rule. The consequences for criminal violations of the HIPAA Security Rule may include fines of up to $250,000 and imprisonment.

What is the most important thing I should do to start protecting electronic protected health information?

Assess, Assess, Assess…..

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