Understanding a Risk Assessment

To be able to protect patient information one must always understand the risks to the information. A HIPAA Risk Assessment will help you answer these particular questions:

1. Where is patient information stored, accessed, developed or modified?
2. What are threats to this information?
3. Just how much potential are these threats?
4. Exactly what is the impact for these threats?
5. What additional safety measures can be implemented to protect the information?

How do you identify how you are protecting patient important information along with your weaknesses? The HIPAA Security Rule and Meaningful Use requirements require all companies to execute a HIPAA Risk Assessment. Let's look at a simple concept of a Risk Assessment.

Step 1 – determine where patient information is stored (EMR, PACS system, email, etc)
Step 2 – determine threats to patient important information (employee loses a laptop with patient information, fire destroys your EMR, a patient is sent another patient's test results, etc.)
Step 3 – Assess how you are currently protecting patient important information (backing up your EMR on a nightly basis, using secure email to send patient information, using anti-virus to protect your systems from viruses, etc.)
Step 4 – Identify your risk for each of the hazards that were identified in Step 2. You determine your risk by looking at how likely something is to happen and the impact if it does happen.
Step 5 – Determine additional protections to minimize the risk.

Hopefully you have a better understanding of the HIPAA Risk Management process and the benefits of performing a HIPAA Risk Assessment. Risk Assessments should be performed once a year (or at most once every two years) or when major changes to systems occur.

Please feel free to give CAM HIPAA Solutions a call for any questions that you may have.

6627 Valjean Ave.
Van Nuys, CA 91406

Phone: +888-959-0220
Fax: +818-356-7187

Email: info@camhipaasolutions.com
Website: www.camhipaasolutions.com