6 Steps to Avoid HIPAA Fines

The most common mistake a practice makes in trying to become compliant with HIPAA is thinking that a risk analysis is enough or that a set of policies in a three ringed binder is sufficient.

The set of HIPAA rules put forth by the government are complex and in-depth, and need to all be addressed. What does that look like? Something like this: a risk analysis (the discovery of deficiencies that a practice has with relation to the HIPAA Privacy and Security Rule), risk management (the remediation of the deficient items), policies and procedures addressing each section of the Privacy and Security Rule), vendor management (making sure proper Business Associate Agreements and assurances that the Business Associate is complying with the HIPAA Security Rule are in place), and finally that the staff has attested to each privacy and security policy and they have taken a HIPAA 101 training course and successfully attest they understand the basics of HIPAA.

The best way to avoid being fined by an auditor is to show due diligence. What is that? It is making a good faith effort in complying with the rules, documenting all findings, and being able to show anyone your compliance plan and efforts.

The 6 Steps:

1. You must have a risk analysis that audits you for administrative risk (policies and procedures), technical risk (how are you safeguarding the access to and protection of ePHI that resides on your systems), and physical risk (assessing how you are protecting the data within the four walls of your site or sites.
2. You must remediate (fix) all deficiencies that were found during the risk analysis and document what you did to resolve the deficiency.
3. You must have policies and procedures covering all aspects of HIPAA Privacy and Security and HITECH (breach notification).
4. You must educate your staff with training and track their attestation that they understand all the new policies and procedures you have put into place to safeguard protected health information.

5. You must identify your business associates and make sure you have up to date BA agreements in place. If possible get assurances the BA you share data with is complying with the HIPAA Security Rule.
6. Finally you need to create a culture of compliance that everyone takes HIPAA and safeguarding ePHI to a different level of protection.