Implementing A HIPAA Compliance Program

(Note: State law may be stricter than federal law)

Follow These Instructions:

1. Watch the tutorial DVD first. It covers these steps.
2. Determine who is going to be the companies **Security Risk Officer**.
3. Perform a **Security Risk Analysis**. Covered Entities (CE) are mandated by federal law to perform a Security Risk Analysis first. Refer to the file named **HIPAA 101** in the HIPAA Compliance Program. This file can be found in the **HIPAA Program CD** under the **HIPAA Security Risk Analysis** (SRA) File. The purpose of an SRA is to detect potential HIPAA liabilities and what can be done by the entity to correct and prevent these liabilities from turning into breaches of electronic **Protected Health Information** (ePHI).
4. Review the requirements of the **Security Standards Matrix** on page 10 of the HIPAA 101 document.
5. Be sure that you have a written policy and procedure for the Administrative, Physical and Technical Safeguards listed in the HIPAA 101 file. This can be done by copying the regulation number (i.e. 164.310(b)) and then pasting it into the search bar of the HIPAA policies and procedures file in Word. All files that contain a reference to a particular CFR number.
6. Read each **Policy #** in the **HIPAA Compliance Program** and make any necessary changes to the **policies and procedures**. Be sure to change the field where it says “Covered Entity” or something similar.
7. Perform a Security Risk Analysis as necessary but at least once per year.
8. Be sure all files are encrypted. If a laptop computer or other device is lost or stolen and the files are encrypted you are not required to file a breach notification with the DHHS. (IT people will know how to do this)
9. Address any violations and disciplinary action within 30 days in writing.

Remember, the government requires:

A Culture Of Compliance