SAMPLE RISK ASSESSMENT QUESTIONAIRE

Control Category		Answer	General Comments	Further Explanation
Directions: For each control category question, please select either "yes" or "no" in the **Answer** column. ANSWER ALL QUESTIONS BASED ON YOUR ENVIRONMENT. The **General Comments** column is provided for any additional comments the assessor would like to provide. This area can be used for personal tracking purposes and/ or providing further detail; however, filling in this column is not a requirement. The **Further Explanation** column is there to provide the assessor with further information and detail on what is being asked in each question.				
1	**Information Security Policies**			
1.1	Does the organization have Information Security Policies defined and documented?	No		Information security policies are the backbone of any information security program.
1.2	Are all HIPAA required policies and procedures defined from a HIPAA compliance perspective?	No		Policies and procedures that are created to meet HIPAA requirements.
1.2.A	Do policies/ procedures cover the following areas:			
	Risk Management	No		The risk management policy should map to the organizational security policies.
	Sanctions	No		The sanction policy should outline the ramifications of not following the information security policies.
	Termination	No	No documentation in place, but the password for "EHR" and Windows is deactivated immediately when someone is terminated.	The termination policy should outline the appropriate actions to be taken when a termination or separation occurs.
	Mobile Media and Device Security	No	The two physician's place procedure notes on flash drive to be uploaded to the system. CD's are used for mailing out medical records and are password protected.	The mobile media and device policy should define what is devices are allowed and the acceptable use of both mobile media (flash drives, CD/ DVDs) and mobile devices (smart phones).
	Information System Access	No	Physical access is restricted by locked communications closet, and the practice manager's office is locked. Electronic access is controlled via user names passwords, and encryption	The information security access policy should define the rules necessary to maintain an adequate level of security to protect PHI and other sensitive data from unauthorized access.
	Security Training and Awareness	No		Security awareness training ensures users are aware of threats against systems and information within the organization.
	Anti-Malware	No	Symantec end point protection and MX logic Internet proxy server are used.	The anti-malware policy should define a standard regarding the installation, use, and maintenance of anti-malware software.

SAMPLE RISK ASSESSMENT QUESTIONAIRE

Passwords	No	All users have their own their own user name and password.	The password policy should establish a standard for creating and maintaining passwords.
Security Incidents	No		The security incident policy is to ensure that computer security incidents are reviewed and processed.
Data Backup and Storage	No	Full server backup performed daily via Symantec's backup exec software and agents with a 15 business day tape rotation. Back-ups are data stored off site in secure location.	The data backup and storage policy provides for the continuity, restoration and recovery of critical data and systems.
Disaster Recovery	No		The disaster recovery policy should outline the proper methods for disaster recovery planning, preparedness, management and mitigation of IT systems and services.
Third Parties and Business Associates	No		The BA policy should define the requirements needed to establish a relationship with a third party in compliance with the provisions of HIPAA.
Workstation Acceptable Use	No	Workstations are to be used only for business purposes. Downloads and software installation allowed without management permission. Internet access is control by proxy server.	The acceptable use policy should define what behaviors and actions are permitted when using the organization's workstation and network.
Disposal	No	Hard drives are destroyed with hammers; paper documents are shredded.	The disposal policy should define how to securely destroy sensitive data both physically and electronically.
Media Re-use	No		The media re-use policy is related to the disposal policy, and may be incorporated into it.
Unique User IDs	No		The unique user ID policy should require that all individuals with access to sensitive information have a unique login ID.
Person/ Entity Authentication	No		The person or entity authentication policy should define how persons or entities that access ePHI are authenticated to the network.
PHI Security (ePHI)	No	Employees are only given rights to the parts of the system needed to do their job. Integrity ensured by SQL server maintenance plans and backup processes described above. Primary database server has redundant power and drive systems with power protection and lightning protection.	The policy on PHI security focuses on confidentiality, integrity, and availability of electronic protected health information.
PHI Transmission Protection (email)	No	Informal policy is that no PHI is allowed to be emailed	Refers to whenever PHI is being exchanged over the internet (e.g., email).