



HIPAA Security Rule Compliance Workshop for Clinics - \$600/ Clinic

These workshops are designed to provide an educational, cost-effective and interactive environment for understanding the HIPAA Security Rule, HITECH Act and their related compliance and reporting requirements. Attendees will leave with an improved understanding of security requirements, as well as a risk assessment, vendor management tool, draft policies and implementation guidance.

Recommendations:

- The person(s) responsible for information security should attend (typically 1-2 people).
- All security related policies and procedures should be reviewed prior to attendance and current copies should be available during the workshop. (Electronic copies of the documents are preferable. Have them on a laptop, if possible, or a flash drive or CD/DVD would also work.)
- Develop and bring a list of all business associates with which the clinic exchanges patient information (especially electronic information).
- If possible, each clinic should bring one laptop computer to use when creating documents. (A limited number of laptops will be available for use during the workshops.)
- Ask your EHR vendor if they have a SAS70 or other internal controls report and bring it with you, if possible.

Component	Time	Description	Deliverables
General security overview and education	30 minutes	Regulatory requirements, cyber threats, types of controls, compliance vs. security, policy implementation guidelines, etc.	Understanding of security components, risk mitigation categories, and implementation procedures
Risk Matrix Development	2-3 hours	Categorized risk assessment including inherent and residual risks for internal and external threats such as computer operations, technology deployment, data integrity, disaster recovery, physical security, etc.	Current state risk assessment with guidance on updating and maintaining the risk assessment in the future
Lunch break	30 minutes		
Information Security Policy	1-2 hours	Information Security policy and implementation guidelines.	Information Security policy
Vendor Management	1 hour	Vendor management responsibilities and critical items.	Vendor management program and assessment questionnaires
Break	15 minutes		
Security Administration, Training, etc.	30 minutes	Management reporting, training, physical and system access, roles and responsibilities.	Varied – depending on participant needs
Wrap-up	15 minutes	Q&A	