MEDTEC's Security Site Visit Results (CRISP REC)

Federal Register/Vol. 68, No. 34/Thursday, February 20, 2003/Rules and Regulations

Practice Name:

Doctors Office Address		**Walk Through Observations**
#15. Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a) (1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.	Under the HIPAA Security Rule, you are required to implement policies and proce- dures to prevent, detect, contain, and correct security violations (45 CFR 164.308). Visit the Office for Civil Rights website for more information.
DATE:	**YES / NO**	**Solutions / Coments**
Front Office		
File Cabinets (Locked?)		
Workstation monitors protected and out of view?		
Common equipment monitors		
Admin printer		
Fax Machines		
Passwords Posted		
Patient clipboard receivable		
Desk access		
Locked doors to back room		
Exam Room		
Computer log off after certain amount of time?		
Workstation monitors locked down?		
Waiting room		
Can patients see Admin Computer Screen(s)?		
Access to paper files?		
Access to Exam rooms?		
Doctors office		
Locked doors/ Computers?		

Computer timeout?			
Admin printer?			
Passwords posted?			
Desk Lock?			
Other office Concerns:			
1			
2			
3			
4			
5			
Administrative Safeguards			
Standards: Implementation Specifications (R)=Required, (A)=Address		YES / NO	Solutions / Coments
Security Management Process	Risk Analysis (R)		
	Risk Management (R)		
	Sanction Policy (R)		
	Information System Activity Review (R)		
Assigned Security Responsibility	(R)		
Workforce Security	Authorization and/or Supervision (A)		
	Workforce Clearance Procedure		
	Termination Procedures (A)		
Information Access Management	Isolating Health care Clearinghouse Function (R) Access Authorization (A)		
	Access Establishment and Modification (A)		
Security Awareness and Training	Security Reminders (A)		
	Protection from Malicious Software (A)		
	Log-in Monitoring (A)		
	Password Management (A)		
Security Incident Procedures	Response and Reporting (R)		
Contingency Plan	Data Backup Plan (R)		
	Disaster Recovery Plan (R)		
	Emergency Mode Operation Plan (R)		
	Testing and Revision Procedure (A)		
	Applications and Data Criticality Analysis (A)		

Evaluation	(R)		
Business Associate Contracts and Other Arrangement.	Written Contract or Other Arrangement (R)		
Physical Safeguards			
Facility Access Controls	Contingency Operations (A)		
	Facility Security Plan (A)		
	Access Control and Validation Procedures (A)		
	Maintenance Records (A)		
Workstation Use	(R)		
Workstation Security	(R)		
Device and Media Controls	Disposal (R)		
	Media Re-use (R)		
	Accountability (A)		
	Data Backup and Storage (A)		
Technical Safeguards			
Access Control	Unique User Identification (R)		
	Encryption and Decryption (A)		
	Emergency Access Procedure (R)		
	Automatic Logoff (A)		
Audit Controls	(R)		
Integrity	Mechanism to Authenticate Electronic Protected Health Information (A)		
Person or Entity Authentication	(R)		
Transmission Security	Integrity Controls (A)		
	Encryption (A)		
Site Auditor:	**Date:**		