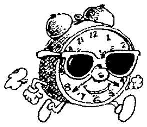
HIPAA Security Readiness Scorecard



The clock is running. What is your readiness?

Key: ✓ = Done • = In Progress

Task	Should Be	Status
Designate a security officer or manager	✓	
Communicate the security officer designation to the workforce	✓	
Appoint a HIPAA project manager	✓	
Appoint a cross-functional HIPAA project steering committee	✓	
Establish HIPAA subcommittees: Transactions and Code Sets, Privacy, & Security	✓	
Conduct a HIPAA readiness assessment	✓	
Inventory all:		
• Policies and procedures for privacy and security	✓	
• Information systems and the criticality/sensitivity of the information processed	✓	
• Business associates with whom protected health information (PHI) is shared	✓	
• Bio-medical equipment that stores PHI	✓	
• Employees with dial-in/remote access to patient information systems	✓	
• Vendors with dial-in/remote access to patient information systems	✓	
Solicit HIPAA readiness plans from information systems vendors	✓	
Develop a HIPAA compliance plan, budget and reporting system	✓	
Conduct HIPAA awareness sessions for the workforce	✓	
Create new policies, procedures and forms as identified in the readiness assessment including incident response	•	
Further develop and confirm corporate risk profile	•	
Conduct a risk analysis based upon the findings of the readiness assessment	•	
Develop or update contingency and disaster recovery plans	•	
Establish a facility security plan for safeguarding patient information	•	
Implement destruction procedures for confidential trash and media containing PHI	•	
Adopt backup, storage and retention procedures for all media containing PHI	•	
Create guideline on workstation use and location		
Establish a formal configuration/change control process *(includes anti-virus updates)*		
Review access controls and consider creating a role-based model		
Automate the process of notifying IT of terminations (*to remove accounts in a timely fashion*) and transfers (*to ensure minimum necessary access*)		
Establish formal security and privacy training program (*document training*)	•	
Implement HIPAA language for chain of trust agreements *(BAC for Privacy)*		
Determine actions or items to be audited, adopt audit trail retention policy, and establish and conduct audit trail monitoring process	•	
Define minimum security standards for information systems that process or store PHI	•	
Conduct a vulnerability scan on information systems that process or store PHI		
Certify information systems that process or store PHI		
Conduct a network intrusion test		
Test incident response		
Review information security program		
Test contingency and disaster recovery plans		

HIPAA is not just an IT issue.
HIPAA compliance will require a "Team Effort"

John Parmigiani
National Director, HIPAA Compliance Services
CTG HealthCare Solutions
410-750-2497
john.parmigiani@ctghs.com