

Improve security and reduce costs with an accurate risk assessment

















Identifying potential security threats that put your patients' data and organization at risk requires a thorough HIPAA security risk analysis. Our HIPAA Security Assessment is an in-depth appraisal of your organization's adherence to existing policies and industry best practices. After identifying any areas of weakness, we'll develop countermeasures in three areas – people, process, and technology – for HIPAA Security Rule requirements.

- > Understand gaps in regulatory compliance requirements
- > Identify weaknesses in existing policies, procedures, and standards
- > Determine weaknesses in access controls, user provisioning, configuration management, vulnerability management processes, and incident handling processes
- > Review of network, operating system, application, and endpoint security measures

Business Value

- Cost effective compliance
- Completion of Meaningful Use requirements
- Prioritized and recommendations for remediation
- Remediation validation and policy creation

Zones HIPAA Security and Compliance Audit

Steps	Professional Package	Enterprise Package
Automated Security Scanning: Commercial scanning tools used to identify potential vulnerabilities		
Management Process: Review security management processes in place to protect confidential data		
Facilities Management: Review the facilities and physical security process to protect confidential data		
Network Architecture Review: Review network security design and identify weaknesses		
Security Policy Review: Review HIPAA security policies for accuracy, completeness, and best practices		
Report Development and Interpretation: Analyze results and develop a remediation plan to meet security requirements		
Remediation Validation: Perform mini-assessment after six months to validate remediation steps have been implemented		
Policy Creation: Create or modify up to five policies to meet gaps in the security procedures		

How the Process Works

You'll receive comparative information and baselines against industry standard protection practices in addition to the HIPAA mandated review items in the Security Rule. A complete assessment, as required under HIPAA risk assessment specifications, includes interviews with personnel, system analysis, policy and procedure review, and remediation suggestions.

- > Assess the current state of security
- > Develop a comprehensive HIPAA security policy and authorization levels
- > Review all relevant security documentation and interview staff
- > Perform vulnerability scanning over a VPN connection or locally
- > Evaluate current practices
- > Recommendations report to close gaps in security practices