

HIPAA Security and Compliance Audit

Our HIPAA information security audit is an in-depth appraisal of an organization's adherence to existing policies and industry best practices, and identification of areas of weakness that need to be addressed to meet business needs and/or regulatory and compliance requirements. We will assess existing weaknesses and develop countermeasures in three areas — people, process and technology — for HIPAA Security Rule requirements.

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

Our cost-effective approach to security and compliance makes it affordable for any size healthcare organization to be in compliance — without cutting any corners. Our comprehensive HIPAA Security assessment service offers an approach based on assessing physical and logical security, and company practices for securing confidential data.

How the process works:

- 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
- Deliver a recommendations report to close gaps in security practices

Key value propositions include:

- Quickly validate problems and resolution, and prioritize vulnerabilities
- Automated testing provides recommendations for remediation
- Discover key weaknesses, policies and procedures
- Categorize missing controls
- Review network, operating system, application and end-point security measures
- Develop key remediation recommendations















BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge transfer

FEATURES & BENEFITS

- Understand gaps in regulatory compliance requirements
- Understand 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 end-point security measures
- Development of key remediation recommendations

HIPAA Security and Compliance Audit Steps

Steps	Professional Package	Enterprise Package
Automated Security Scanning: Commercial scanning tools used to identify potential technical vulnerabilities.		
Management Processes: 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 6 months to validate remediation steps have been implemented.		
Policy Creation: Create or modify up to 5 policies to meet gaps in the security procedures.		

Ready To Get Started?

Contact us at **888-282-0696** or **sales@aurorait.com** to learn how Aurora Security Services can help you accomplish your specific business and IT security goals. Explore further by visiting our website at: **www.aurorait.com**