



HIPAA SECURITY RISK ASSESSMENT

Requirements of Security Risk Assessment (SRA)



ADMINISTRATIVE REVIEW

Examine policies and procedures to identify any deficiencies related to documented processes for protecting sensitive information and systems. Analysis of human resources, information technology, and other administrative processes.



PHYSICAL REVIEW

Examine physical security as it relates to the protection of sensitive information and systems. Includes facility walkthrough to identify vulnerabilities that could pose a risk for a data breach.



TECHNICAL REVIEW

Examine technical controls and systems in place for protection of electronic sensitive information. Review of antivirus, spam filtering, content filtering, firewalls, encryption tools, and Information systems.



Annual SRA: Required for HIPAA Compliance and Promoting Interoperability Reporting

- Review existing security of PHI
- Identify threats and vulnerabilities
- Assess risks for likelihood and impact
- Mitigate security risks
- Monitor results
- Repeat annually

ENFORCED BY THE OFFICE OF CIVIL RIGHTS PUNISHABLE BY LAW