



NetAUDIT™ Security Assessment for HIPAA Security Rule

Meet HIPAA security requirements with a comprehensive assessment of security controls

Thorough assessment affords least impact to the organization for compliance

With over fifty-four unique security provisions within the HIPAA Security Rule (45 CFR Parts 160, 162, 164), many organizations are concerned about how to demonstrate compliance with the least amount of impact to the organization.

HIPAA attempts to answer this concern by placing requirements for assessment into the Rule:

Sec. 164.308 Administrative Safeguards

A covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information held by the entity.

Where is electronic protected health information stored and how does it move

through your organization? What risks and foreseeable threats exist today to your information, systems, and facilities? Where are your weaknesses, vulnerabilities, and misconfigurations?

How much security is enough?

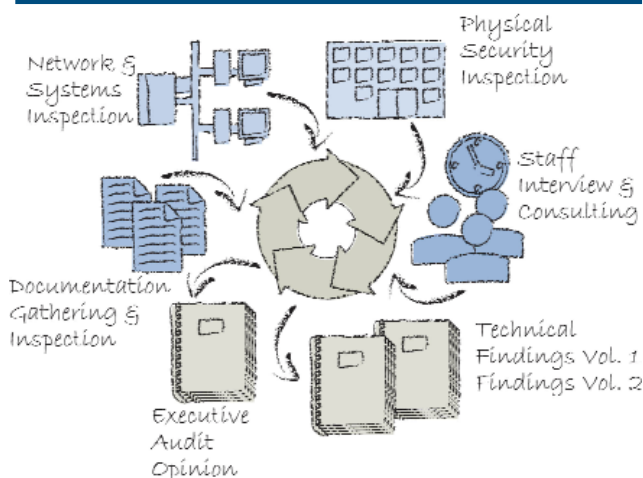
There are twenty-two provisions of the Security Rule that covered entities must consider for implementation in addition to the twenty required provisions. Documentation must exist indicating whether the provision was considered reasonable and appropriate and was implemented, whether it was implemented through an alternate solution, or whether it was not implemented at all and why.

How much security is enough for your organization? What is reasonable and appropriate? What proof do you have to support your decisions?

Benefits

- Meet audit requirement of the HIPAA Security Rule Sec. 164.308(a)(1)(ii)
- Lower IT cost by allocating security resources to preventative efforts rather than post-event remediation
- Provide a reasonable basis on which to rely on the company's security measures for the confidentiality, integrity, and availability of its information and systems
- Help management develop, maintain, and improve existing security controls
- Gain added credibility with customers, board, investors, partners, and creditors
- Demonstrate due-diligence in an organization's efforts to manage risk and liability inherent in its security posture
- Acquire detailed documentation for use in budget and remediation planning

Figure 1: Spohn deploys proven people, processes, and tools that make NetAUDIT the highest quality service for HIPAA Security Rule assessment and compliance



Comprehensive NetAUDIT assessment meets compliance needs and provides valuable information and support

Spohn's NetAUDIT HIPAA Security Assessment results in identifying gaps in compliance with the Rule, identifies weaknesses, vulnerabilities and misconfigurations, and provides the documentation and recommendations necessary to determine reasonable improvements.

NetAUDIT provides the unbiased analysis and documentation of your security measures and delivers the detailed information you need to design, plan, and implement improvements.

On-site Assessment – Inspects the state of your administrative, physical, and technical security policies, plans, procedures, systems, and networks

Risk Assessment – Identifies assets, potential threats, and operational risks

Internal & External Vulnerability Assessment – Identifies technical weaknesses and vulnerabilities

Gap Analysis – Identifies areas of compliance and non-compliance to the Security Rule provisions and is used for planning of any remediation efforts and proof of due-diligence

Remedy Recommendation – Documents reasonable and appropriate recommendations to support your

rationale in designing and implementing any Required and Addressable safeguards

Skilled and experienced in HIPAA compliance and security assessment

Spohn deploys skilled security consultants and tools to assess your organization’s security controls within a process specifically designed for HIPAA Security Rule compliance. The result is an in-depth documented compliance assessment and recommendation. Findings are reviewed in detail with your staff.

Offset the cost of compliance with outsourced efficiency

An investment is required to acquire the security expertise, planning, implementation processes and tools to accurately and thoroughly audit for compliance. NetAUDIT offsets the total cost of periodic auditing through lower cost on-demand services.

Features

- Risk analysis
- System life cycle review
- Organizational review
- Audit backup procedures
- Review BCP/DRP plan
- Review policy
- External vulnerability assessment
- Internal vulnerability assessment
- MBSA vulnerability assessment
- Assess firewall, router, and telecommunications
- Assess virus scanner
- Inspect and photograph physical infrastructure
- Physical security audit
- Assess network topology and access including WAP/WEP
- Phone (War-Dialer) assessment
- Risk management assessment
- Assess security management practices
- Operations security assessment

NetAUDIT HIPAA Security Assessment is a member of a suite of security services for regulatory compliance and corporate due-diligence.

For further information please contact our corporate office at 512.685.1000

Figure 2: NetAUDIT adds value by providing in-depth analysis and recommendations



Gap Analysis of administrative, physical, technical, and organizational security controls including policy, plans, procedures, and documentation
Includes on-site briefings with executive and technical staff to review findings and recommendations



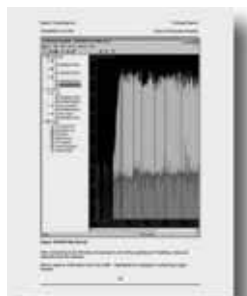
Technical Findings & Vendor Neutral Recommendations with CD-ROM database of data



In-depth Password and User Access Inspection plus 27 other major assessment tasks



Physical security controls are assessed and photographed



Wireless Security (If Present) and LAN network component configuration assessment