BLUE GOAT CYBER

HIPAA Security Risk Analysis

HIPAA SRA High-Level Objective:

We assist you in meeting the requirement to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Our HIPAA Security Risk Analysis helps you remain in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Rule 45 C.F.R. Section 164.308 (a)(ii)(A) regulation as well to meet the requirement for a security risk analysis (SRA) under the Centers for Medicare and Medicaid Services (CMS) Incentive Programs, Medicare Access and CHIP Reauthorization Act (MACRA) and, Merit-Based Incentive Payments System (MIPS), as applicable.

Steps to Schedule Your HIPAA Security Risk Analysis:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

HIPAA SRA Service Description:

Blue Goat Cyber's HIPAA Security Risk Analysis includes the following activities:

- A Kickoff Meeting with your team (e.g., Security, Privacy, Compliance official, IT, HR, Legal, Facilities) who will be involved with the engagement. The purpose of the meeting is to explain the SRA process, expectations, roles, and timeline.
- Review your existing policies and procedures documentation that correlate to the 49 HIPAA Security Rule regulations.
- Guide your team in identifying and documenting where HIPAA-covered ePHI data exists (e.g., on servers, workstations, portable devices, medical devices, or with Business Associates, etc.) and the security controls in place to protect the data.
- Conduct a Checkpoint Meeting with your team to offer initial feedback regarding the policies and procedures documentation that was provided and review the ePHI inventory that was documented.
- Conduct a Compliance Review Meeting with your team to assess the existing controls in place for each of the Security Rule regulations, determine whether evidence is being maintained to support your organization's compliance with the regulations, assess the organization's preparedness for various natural, man-made and malicious threats, and note the findings (i.e. compliance risks) and recommendations (i.e. corrective actions) to be included in the Security Risk Analysis Report.
- Document the preliminary risk findings and recommendations based on the Compliance Review Meeting discussions and provide this draft information to the your team for review.
- Provide your team an opportunity to send feedback and proposed language changes to the preliminary risk findings and recommendations.
- Deliver a final Security Risk Analysis Report (i.e., one report) which contains the following sections:
  - Overview
  - Executive Summary
  - Assessment Methodology
  - Qualitative Analysis
  - Findings
    - ePHI Inventory
    - Criticality of ePHI Applications
    - Threat Matrix
    - Risk Matrix
    - Site Review
    - Best Security Practices
  - Next Steps
  - Final Thoughts
  - Appendix A – Security Rule Compliance Matrix
  - Appendix B – ePHI Inventory Table
  - Appendix C – Criticality of ePHI Applications Table
  - Appendix D – Threat Matrix Table
  - Appendix E – Policies & Procedures Documentation Compliance Table, if applicable
  - Appendix F – Facility Walk-Through Checklist, if applicable
  - Appendix G – Disclaimer
- Deliver a Risk Management Plan that includes the risk findings and recommendations documented in the SRA Report.
- Deliver a presentation of the significant SRA Report findings and recommendations to the your Executive/IT management, if requested.

BLUE GOAT CYBER

Blue Goat Cyber
PO Box 20310
PMB 45092
Cheyenne, Wyoming 82003-7007

(307) 317-8884
info@bluegoatcyber.com