High Level HIPAA Compliance Risk Review

© Emagined Security, all rights reserved.

Overview

High Level HIPAA Compliance Risk Review includes a High Level analysis of an organization's HIPAA compliance in the following areas. This service enables clients to quickly determine if their HIPAA compliance is vulnerable to basic level exploits without going through an in-depth review. At the end of the review, a compliance risk level is assigned to each so they can determine if a full review / penetration testing is warranted.

Benefits

Do you know if you are ready for a HIPAA audit? Do you know if your organization is secure? Do you have Patient Identifiable Information (PII) floating around you network unsecured? Do you know how what fines may be levied on your organization if you don't meet security compliance requirements?

A High Level HIPAA Compliance Risk Review can help prevent huge fines by finding High Level discrepancies before a breach or an audit occurs. Emagined Security's High Level HIPAA Compliance Risk Review is designed for you to quick determine if your organization has applied at least the basic level protection to protect your Patient Identifiable Information (PII).

Description of Service

Emagined Security's High Level HIPAA Compliance Risk Review focuses on performing very high level reviews so you don't have to spend a fortune figuring out how good or bad your situation may be. At the end of the engagement, a basic level risk level report will be provided along with associated raw test results so the company can determine the best approach moving forward. The High Level HIPAA Program Assessment provides a quick analysis of the effectiveness of your organization's security and privacy controls based upon HIPAA requirements through phone interviews. The categories that we assess include:

- **164.306 Security Standards** covers the general areas of (a) General Requirements, (b) Flexibility of Approach, (c) Standards, (d) Implementation Specifications, and (e) Maintenance.
- **164.308 Administrative Safeguards** including (1) Security Management Process, (2) Assigned Security Responsibility, (3) Workforce Security, (4) Information Access Management, (5) Security Awareness and Training, (6) Security Incident Procedures, (7) Contingency Plan, and (8) Evaluation.
- **164.310 Physical Safeguards** including Facility Access Controls and Facility Access Media.
- **164.312 Technical Safeguards** including Access Control, Encryption and Decryption, Operations

© Emagined Security, all rights reserved

Management, Integrity - Change Management, Laptops / Desktops, Mobile Devices, Removable Media, Developing Secure Applications, Web Applications, Vulnerability Management, Testing Security Controls, Person or Entity Authentication, and Transmission Security.

- **164.314 Organizational Requirements** including Business Associates Management, Business Associate Contracts, Other Arrangements, and Group Health Plans.

The **External Vulnerability Scans** performs a limited external vulnerability scan of up to 10 IP addresses against the organization Internet architecture (i.e., firewalls, DNS servers, routers, hubs, load balancers, and supporting systems). By attempting to gain access to the systems on the Demilitarized Zone (DMZ), Emagined Security will attempt to identify risks associated with the current security configuration.

The **Internal Vulnerability Scans** performs a limited internal vulnerability scan of up to 20 IP addresses against the organization internal network. By attempting to gain access to the systems inside the network, Emagined Security will attempt to identify risks associated with the internal current security configuration.

Sales agents will need to either purchase or rent a sensor from Emagined Security for use at the customer site. The sales agent will be responsible for delivery, pick-up, shipping charges and onsite configuration, if required.

At the end of the review, a compliance risk level will be assigned to each section of the review and a basic level risk level report will be provided along with associated raw scan results so the company can determine the best approach moving forward.

© Emagined Security, all rights reserved