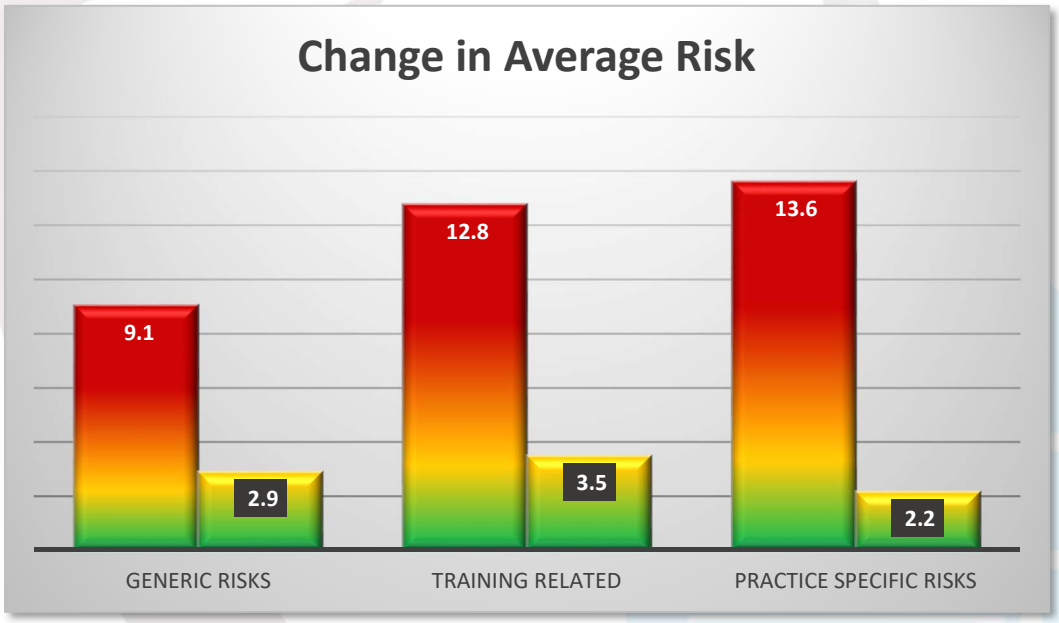
Compunet
HIPAA Security Pros

Risk Assessment Report

Including results from anticipated mitigations and safeguards

Summary of Proposed Mitigation Efforts

Generic Threat Impact reduced by 83%
Training Related Threat Impact reduced by 75%
Practice Specific Threat Impact reduced by 89%



HIPAA Security Risk Assessment

The Security Risk Analysis is a multi-step process that is executed as follows:

Step 1: Site review and assessment
Step 2: Determine and present mitigation safeguards
Step 3: Implement mitigation safeguards
Step 4: Site review and re-assessment
Step 5: Annual audit and assessment of systems and safeguards

The purpose of Step 1 is to identify all systems that contain or process PHI or other protected information, then review and document the security of these systems. This information is used to identify threats, and to determine the likelihood and impact of these threats. In Step 2 the mitigation options and other safeguards will be determined. This list will become the task list for securing the systems. Step 3 is devoted to implementing changes on the various systems that contain PHI. Step 4 is for evaluating the changes and completing the Remediated Risk Analysis. As HIPAA Compliance requires constant vigilance annual audits and assessments should be completed to determine if new risks have been introduced into the system.

The steps of the HIPAA Security Risk Analysis are designed to address elements of each safeguard that makes up the HIPAA Security Standards as defined in the HIPAA Final Security Rule. This Risk Analysis together with the HIPAA Compliance Checklist addresses the following Security Rule Standards:

- Section 164.308 Administrative Safeguards
- Section 164.310 Physical Safeguards
- Section 164.312 Technical Safeguards

Pre-Mitigation Scoring

The results of the Pre-Mitigation Risk Analysis are as follows:

- The Generic Risk Score is 281 for an average risk of 9.1
- The Training Related Risk Score is 179 for an average risk of 12.8
- The Practice Specific Risk Score is 109 for an average risk of 13.6

Impact of Mitigation

Given that the practice uses a Cloud based EMR there is a minimal amount of PHI stored on the local computers. This greatly reduces the impact of threats. If each of the recommended safeguards are implemented the remediated risk scoring would be as follows:

- A Generic Risk Score of 90 for an average risk of 2.9
- A Training Related Risk Score of 179 for an average risk of 3.5
- A Practice Specific Risk Score 13 for an average risk of 2.2

These changes will represent an 83.3% improvement in Generic Risk Score, an 75.0% improvement in Training Related Risk, and an 88.6% improvement in Practice Specific Risk Score. Moreover, the most significant risks to an accidental disclosure or a breach will be substantially diminished.