

HIPAA IT Security Risk Assessment

Hayes uses its HIPAA IT Security Risk Framework methodology to assess your organization's HIPAA compliance and to identify and address potential IT security risks and vulnerabilities.



Problem Statement

- An increase in security breaches across the industry with associated fines, penalties and damage to reputation
- Lack of confidence in the organization by community
- HIPAA IT security program depends on users across the organization (not just IT)
- Additional security and privacy standards
- Missing policies and procedures
- Inconsistent education and awareness
- Increase in mobile technology
- Need to attest for Meaningful Use
- Conforming to the requirements and schedules set forth by the HITECH Act (HIPAA Security Rule requirements)



Business Solution

- Identify areas and processes vulnerable to security breaches
- Develop governance and reporting structure
- Develop HIPAA IT security strategy and plan; identify consistent and frequent reporting structures to leadership
- Review IT security policies and procedures
- Enhance education and awareness programs
- Develop a comprehensive internal and external communication and response plan



Methodology

- Conduct risk assessment utilizing Hayes HIPAA IT Security Framework
- Analyze current state
- Perform operational workflow analysis to understand exchange and location of ePHI/PHI
- Review security and privacy standards compliance
- Provide summary of IT security and privacy status with HIPAA guidelines
- Develop IT security action plan to address risks
- Create appropriate documentation to demonstrate compliance with the HIPAA Security Rule and the Meaningful Use Program
- Create a gap analysis and provide a findings report with an action plan