Trustwave®

HIPAA Risk Assessment

PRIORITIZING YOUR EFFORTS IN PROTECTING ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

Perhaps the most important obligation on the road to HIPAA Compliance is to perform a Risk Assessment on the EPHI environments.

Risk Identification

The primary purpose of the Risk Assessment is to help structure secure operations for your organization. Performance of a Trustwave Risk Assessment will help you to gain a comprehensive and accurate understanding of the risks and vulnerabilities to the confidentiality, integrity and availability of protected health information (PHI) in your environment.

Risk Assessment

Trustwave Risk Assessments are comprised of our proprietary methodology combined with industry-accepted assessment methodologies and guidelines. Our assessment will help you identify the risks associated with handling protected health information (PHI), electronic and otherwise. Further, our assessment can be tailored to meet your needs across various non-HIPAA contexts.

The Trustwave Risk Assessment supports multiple business initiatives:

- Assessment of Information Security Programs
- Identification of threats facing PHI and the supporting electronic PHI infrastructure
- Development of a Risk Management Program
- Compliance with HIPAA Security Rule
- Prioritization of security program efforts

Risk Management

Trustwave Risk Management solutions address multifaceted risks to your organization. We aid and prepare you in mitigating the risk of audit by the Office of Civil Rights (OCR). Further, we can assist you in adequately addressing your security posture, more holistically, for the risk of breaching information, regardless of a HIPAA complaint or investigation.

Analysis of the Risk Assessment can be immediately applied as a basis for an informed investment in Risk Management solutions for the people, processes and technologies utilized in your in your organization.

The identification and qualification of risk is a primary step in developing a formal, ongoing Risk Management Program, which could provide a structured approach to ongoing evaluations. The HIPAA Security Rule provides the business with latitude to apply safeguards to sensitive data with discretion. Accordingly, a Risk Assessment and analysis are the first steps in the HIPAA Security Rule compliance process as well as the first steps in building a secure organization.

Expert Intelligence

Trustwave Compliance and Risk consultants will help guide you. In tandem with your staff, our team will facilitate an iterative process of discovery, assessment, and remediation. With over 100 experienced consultants in every corner of the globe, we can match you with the perfect consultant for your engagement.

Trustwave compliance-related methodologies have been refined after delivering thousands of compliance and security standards assessments. Our methodology adapts to a wide range of data types, threat sources, operating environments, control objectives, and implementation specifications.

Trustwave HIPAA Risk Assessment

Assessment Project Plan

We begin with the end in mind—achieving successful HIPAA compliance—but it all starts with a plan. The Risk Assessment project begins with information exchange meetings to discuss the details of the project, including timeframes, resources, and critical milestones. Prior to, and during the information exchange meetings, Trustwave will request current, complete, and accurate details of your relevant environment to appropriately inform the Risk Assessment. Trustwave will work with your point of contact to develop the project plan.

Risk Formulation Methodology

The Trustwave Risk Assessment approach combines Trustwave proprietary methodology with guidance from various industry accepted assessment methodologies including ISO 2700X, OCTAVE and, OCR recommended, NIST 800-30 series.

Risk Formulation Strategy

+ Discovery of your electronic PHI environment
  - *Stakeholders, assets, networks, devices and define PHI dataflow*
+ Discovery of your business operations
  - *Policy, procedures, technology, business requirements for electronic PHI infrastructure*
+ Threat Assessment
  - *Events, actors, intent, capability, likelihood and impact*
+ Discovery of Predisposing Conditions and Vulnerabilities
  - *Conditions that increase likelihood of threat events or increase impact on assets*

= RISK FORMULATION

Assessment Delivery

Trustwave will work with you to identify and prioritize environments to be assessed and many of these activities will be conducted in parallel. The assessment activities can be conducted by a combination of methods including on-site interviews, phone conference, web conference, email, and direct phone communication as well as research and discovery conducted independently by Trustwave.

Findings Summary

The output of the Risk Assessment is delivery of findings via a Risk Assessment Report. The findings summary is a structured report designed to prioritize mitigation activities into categories with unique or parallel workflows.

Findings include:

- Discoveryof PHI in your environment
- Overarching Risk Assessment results—prioritizing major gaps in policy, process, and procedure
- Security Control Coverage—high level review of controls and major compliance gaps
- Strengths and best practices identification
- HIPAA compliance recommendations—risk mitigation and best practice plans for the security life cycle incorporating OCR guidance

Trustwave®

For more information: www.trustwave.com