SecureTrust™
a Trustwave® division

SecureTrust™ HIPAA Risk Assessment

IDENTIFY RISKS TO THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF EPHI

BENEFITS

Defend against common failures resulting in enforcement actions, corrective action plans, settlements or civil monetary penalties. Common failures include:

- Failure to conduct an accurate and thorough assessment of potential risks to the confidentiality integrity and availability of ePHI
- Failure to implement policies and procedures sufficient to manage risks to a reasonable and appropriate level
- Failure to implement a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate
- Failure to implement security measures sufficient to reduce risk and vulnerabilities to a reasonable and appropriate level
- Failure to implement procedures to perform technical and non-technical evaluations in response to environmental changes affecting the security of ePHI
- Failure to obtain written business associate agreements

The first, and perhaps most important, obligation on the road to HIPAA compliance is to perform a risk analysis.

Electronic protected health information (ePHI) is subject to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. And, any entity that creates, maintains or transmits ePHI is bound by HIPAA requirements to identify and implement safeguards to secure ePHI.

A risk analysis is the first step to securing ePHI because the results must be used to identify the appropriate safeguards for implementation. Every organization subject to HIPAA has to determine the appropriate way to achieve compliance, by considering the organization's specific risks. For that reason, a risk analysis is the foundation of a HIPAA security program. In other words, you can't say what safeguards are appropriate without assessing your specific risks.

A SecureTrust HIPAA Risk Assessment will help you gain an accurate understanding of the threats, vulnerabilities and risks to the security of ePHI. This allows your organization to implement reasonable and appropriate security measures according to the size, complexity and capabilities of your organization. And, in turn, your organization will be positioned to protect against reasonably anticipated threats and vulnerabilities.

SecureTrust HIPAA Risk Assessment

Components and Requirements

To conduct a legitimate risk analysis, your organization must evaluate scenarios and risk factors using a documented and repeatable procedure to assign a defensible risk level. HIPAA mandates that this risk analysis process be set in policy and that the policy should be guided by thorough written procedural documents.

How it works

The Security Rule requires entities to evaluate the risk to the security of e-PHI and implement reasonable and appropriate measures to protect against reasonably anticipated threats or vulnerabilities. The scope of the assessment should depend on the potential risks to all ePHI regardless of format or where it is in your environment.

The assessment will seek to collect data and identify the various locations, systems and processes where ePHI is created, maintained or transmitted. An asset inventory is created to determine which information systems, media, devices, applications, servers, networks and processes will be examined.

Vulnerability review will include consideration of both technical and non-technical flaws and weaknesses in systems design and implementation that could be intentionally or accidentally exploited and result in a security incident or breach.

Multiple types of information systems and operational threats may exist and may be grouped into categories such as natural, human and environmental. Threat assessment includes all potential threats for a person or thing to intentionally or accidentally exploit or trigger a specific vulnerability.

Risk assessment includes consideration of the effectiveness of controls and security measures for example encryption, security testing and monitoring, vulnerability management and patch management.

The fundamental objective of risk assessment is to determine the likelihood and impact of a risk event. The risk assessment will determine the likelihood that a threat will produce or exploit a vulnerability as well as the potential impact of the incident. Risk levels are assigned for threat and vulnerability combinations to consider risk treatment or acceptance.

The assessment must be conducted in a complete and thorough manner. Documentation and reporting of the risk assessment activities will result in sufficient detail to demonstrate that the assessment was indeed carried out in a complete and through manner.

Frequency for risk assessment is not prescribed. Entities must make sure risks are identified and addressed as part of normal business operations. Entities should review, update and reperform risk assessment processes on a periodic basis at least annually and in response to significant change. An intended benefit of the risk assessment is knowledge sharing so your team can repeat the assessment and conduct periodic reviews on your own.

SecureTrust consultants will guide you and help you stand up your risk assessment process. We will work with you to conduct a comprehensive risk assessment to help you identify, document and analyze the threats and vulnerabilities that could impact the confidentiality, integrity or availability of ePHI.

What You Get

The assessment will result in a report detailing how well your organization is able to address risk. The report will include an executive summary of high risk findings and overarching risk assessment results as well as detailed findings for policy, processes and procedures to secure ePHI. The output will include risk mitigation and best practice recommendations to consider risk treatment or acceptance.

What's Next?

After the risk analysis organizations must manage and treat the security risks identified, meet the general requirements of the HIPAA Security Rule and determine which implementation specifications are addressable. The HIPAA Security Rule provides organizations latitude to apply safeguards to ePHI. This discretion allows entities to develop and customize their risk management processes and determine risk treatments that are sufficient, feasible and effective for each covered entities specific needs. SecureTrust is available to support you with consultation for the design, implementation and the ongoing management and treatment activities to adequately address your risks.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com