Trustwave®

HIPAA Compliance Readiness Service

BE PREPARED

Trustwave provides a suite of customizable solutions to help healthcare organizations achieve smart compliance and smart security

Empowered Decision Making

Healthcare providers are pulled from all sides by incentives to embrace electronic health record systems and also to share records across plans and providers. At the same time, healthcare providers must comply with the Security, Privacy and Breach Notification Rules under the Health Information Portability and Accountability Act (HIPAA).

Compliance frameworks and incentive programs alone should not be the only guide for businesses to make good security decisions. Trustwave recommends smart decision making - requiring risk-centered attention aided by a HIPAA Compliance Readiness Service.

A Trustwave HIPAA Compliance Readiness Service is a structured and detailed evaluation of the posture of an organization as compared to the requirements of the HIPAA Security, Privacy and Breach Notification Rules.

Compliance and Risk Motivations

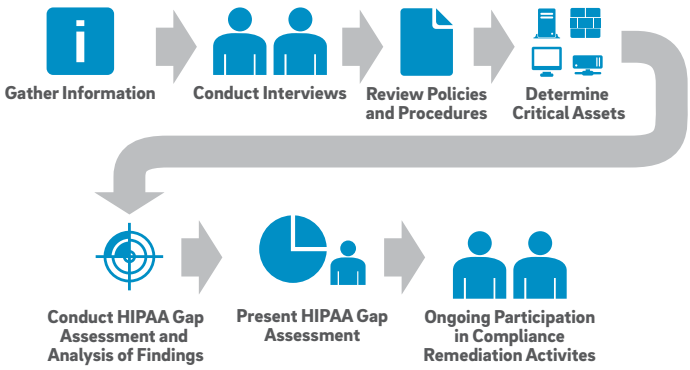
The Department of Health and Human Services (HHS) and the Office of Civil Rights (OCR) are the governing authorities responsible for HIPAA compliance. Interconnected, are the patients whose information and privacy is the subject of HIPAA safeguards. Consequently, businesses and healthcare organizations that handle protected health information are confronted with two risks—risk of audit and risk of breach.

Risk of Audit

As of yet, there is no safe harbor. There is no certification or compliance validation recognized by HHS or the OCR that will give you a pass on a HIPAA complaint. What is available is *preparation*. A Trustwave HIPAA Compliance Readiness Service, with comprehensive reporting and audit preparation services, creates defensible space in the worst case scenario of a HIPAA complaint, investigation or audit.

Risk of Breach

There are consequences to a breach of information. In parallel to fines levied for HIPAA non-compliance, businesses and healthcare organizations risk reputational damage and additional fines and penalties, for entities and individuals, tied to the nature and extent of a breach of PHI. A Trustwave HIPAA Compliance Readiness Service will help you gain an understanding of present breach risks and provide you with guidance for prioritized remediation activities to mitigate the risk of breaching information.



Trustwave HIPAA Compliance Readiness Service

Allied Relationship Project Plan

Our consultants are positioned to perform a collaborative examination of your environment for successes and remediation activities to achieve HIPAA compliance. Trustwave consultants require, and will foster, cooperative input from your personnel. As assessors, not auditors, collaboration with your teams promotes knowledge sharing for information gathering, but also enables your staff to learn from our security professionals.

Objective

The intent of the assessment is to discover all gaps in your current written policies and procedures, 'de facto' processes and your security architecture with respect to HIPAA standards. The HIPAA Compliance Readiness Service address the full spectrum of HIPAA compliance gaps so that specific risks can be categorized, quantified and considered for remediation or acceptance.

Methodology

Trustwave consultants will evaluate the clients' existing compliance posture in reference to the HIPAA standards through interviews and documentation review. Interviews and documentation will be reviewed and evaluated against all aspects of the HIPAA standard which are divided into three main areas—Security, Privacy and Breach Notification Rules.

Actions

Gather Information—Requested at the start of the engagement such as data flow diagrams, existing security policies, inventory of hardware, software and applications as well as network maps and organization charts.

Conduct Interviews— Organized to complete information gathering and to identify information protection requirements.

Review Policies—Examine written policies, 'de facto' practices and gain an understanding of business processes and the PHI environment.

Determine Critical Assets—Define critical business processes, assets and security management processes in place.

Comprehensive HIPAA Gap Assessment—Documentation of all HIPAA gaps discovered during the engagement, reference gaps to HIPAA requirement definitions, and categorize gaps by key activity.

Analysis of Findings—Prioritized list of critical findings, risk ranking of all findings, dashboard overview to assess overall HIPAA compliance posture.

Present HIPAA Gap Assessment—Preparation and delivery of a report that identifies all policy gaps, how they relate to critical HIPAA regulatory issues, and specific actionable recommendations are documented to close those gaps. The report will be written in easy to understand language avoiding unnecessary technical jargon and is designed for all levels of technical and non-technical management.

Post-Reporting Activities—Customized remediation roadmap, phased approach to align with HIPAA guidelines, security program framework, on-going participation with remediation status meetings.

Trustwave®

For more information: www.trustwave.com