SecureTrust™
a Trustwave® division

SecureTrust™ HIPAA Gap Assessment

PRIORITIZE YOUR EFFORTS IN SAFEGUARDING PHI

SecureTrust helps healthcare organizations safeguard protected health information, achieve compliance and maintain security.

A SecureTrust Health Insurance Portability and Accountability Act (HIPAA) Gap Assessment is a structured and detailed evaluation of your HIPAA compliance program. A gap assessment is a good first step, and a useful periodic activity to assess overall compliance, help identify areas where you are not compliant yet and help identify gaps for safeguards already meant to be in place.

A gap assessment is not a requirement. More specifically, a gap assessment is not intended to meet the HIPAA risk analysis requirement. That's because a gap assessment does not cover all possible risk to the confidentiality, integrity and availability of electronic protected health information (ePHI). Please see our HIPAA Risk Assessment data sheet for more information. A gap Assessment can help healthcare organizations confirm whether implementation specifications have been met. A SecureTrust HIPAA Gap Assessment will evaluate your compliance program to identify gaps in safeguards and provide prioritized remediation guidance.

Compliance Enforcement

HHS OCR

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is the governing authority responsible for HIPAA compliance enforcement. The OCR conducts investigations based on complaints of potential HIPAA violations. Failures of non-compliance investigated by the OCR typically result in a financial settlement paid to the OCR plus an agreement to implement corrective action plans. And, the worst cases result in civil monetary penalties when the violation is egregious or there is a failure to correct a known issue.

Self-Enforcement

Safeguarding protected health Information is patient care. Interconnected to requirements and enforcement, are the patients whose information and privacy is the subject of HIPAA rules. And, short of an audit or a comprehensive risk analysis, it may be hard to know whether your organization has legitimately implemented safeguards. A SecureTrust Gap Assessment helps you avoid complaints and your proactive self-enforcement helps create defensible space in the case of an investigation or audit.

Businesses and Healthcare Organizations Handling PHI are Confronted with Risk of Audit and Breach

All organizations should seek to avoid an audit or breach by preparing for the worst case scenarios.

Risk of Audit

There is no such thing as a HIPAA certification. You must assess, control and harden your systems to safeguard protected health information. And, in parallel, your policies and documentation must be sufficient to answer to an investigation or audit by the HHS OCR. Periodic assessment of your HIPAA compliance program is useful to maintain your implementation ahead of a HIPAA complaint or audit. SecureTrust helps you prepare with comprehensive evaluation, prioritized remediation, reporting and audit preparation.

Risk of Breach

There are long term consequences of a PHI breach for patients. There is an irreparable impact to the patient when static information, like a name and social security number, has been exposed because those identifiers are not intended to change and may remain exposed for repeated misuse.

And, there are costs to the business. There is the cost of incident response, forensic investigation and breach containment. There is the cost of notifying patients, the regulatory authority and in some cases the media that a breach has occurred. There are expenses for credit monitoring and breach protection according to the number of records affected. There are costs of HIPAA audit preparation. And, of course, healthcare organizations risk reputational damage tied to the nature and extent of a breach. A SecureTrust HIPAA Gap Assessment will help identify lapses in compliance and provide you with prioritized guidance for remediation activities to mitigate the risk of a breach.

SecureTrust HIPAA Gap Assessment

Objective

The intent of the assessment is to discover gaps in your written policies and procedures, 'de facto' processes and your current compliance program. SecureTrust consultants require, and will foster, cooperation from your personnel. As assessors, not auditors, collaboration with your team promotes knowledge sharing for your staff to learn from our security professionals.

Methodology

SecureTrust consultants will evaluate your compliance posture relative to HIPAA standards through interviews, observation and documentation review. The assessment may be limited to certain business process or may encompass the enterprise. And, the subject of evaluation may be a subset of HIPAA controls or all aspects of the HIPAA Rules.

Activities

Information Gathering: Request, at the start of the engagement, for information such as network and data flow diagrams, existing security policies, inventory of hardware, software and applications as well as organization charts.

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

Determine Critical Assets: Establish what are the critical business processes, assets and security management processes in place.

Interviews and Observations: Discussion based interview sessions with individuals responsible for HIPAA controls to complete information gathering and consider whether controls operate as designed and intended. Assessor gathers facts and objective evidence to draw conclusions whether HIPAA controls and implementation specifications are indeed operationally effective.

Analysis of Findings: Assessment of overall HIPAA compliance posture including a prioritized list of critical findings as well as detailed risk ranking of all findings.

HIPAA Gap Assessment Report: Preparation and delivery of a HIPAA Gap assessment detailing lapses in compliance, how identified issues relate to critical HIPAA regulatory issues and specific actionable recommendations to close those gaps. The report will be written in plain English avoiding unnecessary technical jargon and will be built for all levels of technical and non-technical management.

Post Reporting Activities: Ongoing consultant participation for internal remediation status meetings.

SecureTrust is available to assist covered entities and business associates of all sizes determine to what extent they are compliant with specific elements of the HIPAA requirements and implementation specifications.

SecureTrust™
a Trustwave® division

For more information: www.securetrust.com