SecureTrust
a Trustwave division

Service Description

Health Insurance Portability and Accountability Act

Risk Assessment

Contents

HIPAA Risk Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Health Insurance Portability and Accountability Act (HIPAA) Risk Assessment is a professional services engagement. The HIPAA Risk Assessment provides an understanding of assets, vulnerabilities, threats, likelihood of threat events, and impact of threat events on the Protected Health Information (PHI) environment. The risk assessment is meant to assist in accomplishing the HIPAA risk requirement and provide a record of potential risks to the PHI environment. The HIPAA Risk Assessment helps organizations measure risk and plan risk treatment.

SecureTrust's Approach and Methodology

SecureTrust's HIPAA Risk Assessment aligns with the Department of Health and Human Services (HHS) Audit Protocol, Office for Civil Rights (OCR) recommendations for HIPAA audit preparation and industry standards such as National Institute for Standards and Technology (NIST) Special Publications 800-30 R1 and 800-66 R1 and SecureTrust proprietary methodology. The HIPAA Risk Assessment involves various policies, procedures, and practices that will be evaluated by SecureTrust through documentation review, interviews, facilities inspection and controls assessment.

BASE SERVICE FEATURES

SecureTrust's HIPAA Risk Assessment service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal consists of, among other features, a Compliance Manager application to manage the engagement process as well as collect and securely store evidence, documentation, and final deliverables.

Global Compliance and Risk Services (GCRS)

The Global Compliance and Risk Services (GCRS) team consists of, among others, the following key personnel and functions:

Security Consultant – An information security consultant serves as the primary resource for the fulfilment of the service, responsible for performing the risk assessment, reporting and assisting in remediation planning.

Managing Consultant (MC) – An MC provides guidance, project oversight and reports quality assurance to the Security Consultant as well as serves Client as a secondary point of contact for escalations and queries.

HIPAA Risk Assessment – An assessment of threats and vulnerabilities to the confidentiality, integrity and availability of PHI including the likelihood and impact of threat events given existing security controls. A

SecureTrust security consultant works with Client resources to gather information for analysis, enabling SecureTrust to carry out the assessment and produce a report.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate delivery of the service which includes scheduling and conducting the remote kickoff meeting to define and agree to a high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables, resource requirements and escalation procedures.

Phase I: Discovery

SecureTrust will perform discovery of information related to Client's PHI environment and business operations. SecureTrust will work with Client to determine critical assets, examine business processes, and identify security and compliance management processes in place. SecureTrust may request information including, but not limited to:

- HIPAA compliance governance structure and key stakeholders;
- PHI data flow diagram(s) and detailed narratives;
- Inventory of network devices, hardware and software;
- List of applications supporting the PHI environment;
- Network diagrams;
- Organization chart;
- List of security incidents that occurred within the last two years;
- Copies of the reports from any security audits, penetration tests or vulnerability assessments conducted in the last two years; and
- Copies of existing security policies, including but not limited to:
    - Acceptable Use Policy;
    - Ethics Policy; and
    - HR Discipline Policy.

SecureTrust will include consideration of predisposing conditions in Client's environment that will increase or decrease the likelihood of threat events or impact on assets. To determine predisposing conditions and vulnerabilities, SecureTrust will leverage input from previous audits, security assessments, vulnerability scans, penetration tests, code reviews and any other relevant documentation that may be made available.

SecureTrust will begin report deliverable development.

Phase II: Assessment

SecureTrust will interview appropriate personnel within the organization to understand the details of the PHI environment, business operations and identify compliance management processes in place. During the interview sessions, SecureTrust will seek to determine any de facto practices that should be formalized in written policy.

SecureTrust will perform an on-site assessment of Client facility including computer rooms, communications facilities, physical security facilities and systems, and other aspects of the operational environment identified as relevant.

SecureTrust will apply threat scenarios based on agreed sources of risk and determine the likelihood and impact of the known or hypothesized outcomes. From these scenarios, the most critical assets will be assigned a threat profile for integration, and a relative weight with respect to the overall profile.

SecureTrust will identify and assess implementation of safeguards for the PHI environment.

SecureTrust will continue development of the report deliverable.

Phase III: Risk Analysis

SecureTrust will analyze all the information captured to determine risks to critical assets.

The level of risk is calculated based on:

- Likelihood of a threat exploiting a vulnerability; and
- Severity of impact that the exploited vulnerability would have on the system, data and function in terms of loss of confidentiality, integrity or availability.

Phase III: Reporting

SecureTrust will create, prepare and deliver a report to Client documenting all findings and recommendations from the assessment to resolve critical or high risk findings.

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish and maintain contact with Client.
- Establish communication and escalation plans.
- Create a Client account in the SecureTrust Portal.
- Define high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Validate scope of the engagement.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Determine risk assessment results.
- Create, prepare and deliver to Client a final report documenting all findings and recommendations from the assessment.

CLIENT RESPONSIBILITIES

- Establish and maintain contact with SecureTrust.
- Establish communication and escalation plans.
- Agree to high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables and resource requirements.
- Accurately provide all necessary information including key stakeholders, applicable environment information and configuration requirements.
- Inform SecureTrust of all environment maintenance activity and changes that may impact the service.
- Respond to requests from SecureTrust teams when establishing contact and collecting information.

- Accurately provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in assessment activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection and controls analysis.
- Client acknowledges:
    - All security feature updates for SecureTrust Portal software will be included in major version release updates.
    - Personnel from the following departments are generally involved:
        - Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance.
    - The HIPAA Risk Assessment is not intended to take the place of a HIPAA regulatory audit, which can only be performed by the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) or their delegates.
    - The engagement consists of remote and onsite assessment activities.
    - The assessment period start and end dates will be determined during the kickoff call.
    - SecureTrust may request evidence from Client's systems and processes as required to prove compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner.
    - SecureTrust is not responsible for defining systems in scope or whether information provided by Client is accurate.
    - SecureTrust retains the right to reject or accept Client comments based on the facts and circumstances of the service.
    - SecureTrust will perform the service in the English language.
    - SecureTrust will not create or modify Client documentation as part of the HIPAA Risk Assessment.
    - SecureTrust will not provide remediation services as part of the HIPAA Risk Assessment.
    - SecureTrust will not offer any legal guidance or counseling. The provision of the HIPAA Risk Assessment does not guarantee compliance with data privacy regulation. Client is responsible for making all management decisions with regard to its data privacy policies.
    - The quality and accuracy of the services is dependent on Client's provision of accurate information and access to Client systems and resources to SecureTrust.