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 (the "**Service**") aims to improve Client's understanding of the assets, vulnerabilities, threats, likelihood of threat events, and impact of threat events on its Protected Health Information (PHI) environment. The Service helps provide a record of potential risks to the PHI environment, measure such risks, and plan risk mitigation.

SecureTrust evaluates Client's policies, procedures, and practices through documentation review, interviews, facilities inspection, and controls analysis based on SecureTrust's thorough understanding of the Department of Health and Human Services (HHS) Audit Protocol, Office for Civil Rights (OCR) recommendations for HIPAA audit preparation, industry standards such as National Institute for Standards and Technology (NIST) Special Publications 800-30 R1 and 800-66 R1, and using SecureTrust's proprietary methodology.

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between SecureTrust and Client.

BASE SERVICE FEATURES

The Service includes the following standard features:

SecureTrust Portal

The SecureTrust Portal features consist of, among others, 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 – A Security Consultant serves as the primary resource for the fulfilment of the Service, responsible for conducting the assessment, reporting and consulting activities.

Managing Consultant (MC) – An MC provides guidance, project oversight, and report quality assurance to the Security Consultant and serves as Client's 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.

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team will initiate the Service by scheduling and conducting a 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: Information Gathering

SecureTrust will gather 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 already 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 may consider conditions in Client's environment that will increase or decrease the likelihood of threat events or impact on assets. To identify any such conditions or related vulnerabilities, SecureTrust may review previous audits, security assessments, vulnerability scans, penetration tests, code reviews, or any other relevant documentation made available.

Phase II: HIPAA Risk Assessment

SecureTrust will interview appropriate Client personnel to understand the details of the PHI environment and Client's business operations and to identify compliance management processes already in place.

During the interview sessions, SecureTrust may identify and recommend that de facto practices should be formalized in written policy.

SecureTrust will perform an assessment of Client's facility including computer rooms, communications facilities, physical security facilities and systems, and other aspects of the PHI environment.

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

The level of risk is calculated by comparing:

- The likelihood of a threat exploiting a vulnerability; and
- The severity of impact that the exploited vulnerability would have on confidentiality, integrity, or availability of the system and data.

Phase III: Reporting

SecureTrust will develop a HIPAA Risk Assessment Report documenting observations and recommendations, including the levels of risk assigned to risks to the PHI environment.

SecureTrust will send a draft HIPAA Risk Assessment Report to Client for review. Client may comment and suggest changes to the draft report with supporting documentation. The SecureTrust QA team will review and finalize the report. SecureTrust retains final authority regarding the contents of the final HIPAA Risk Assessment Report.

SecureTrust will provide, as the final deliverable for the Service the HIPAA Risk Assessment Report which will include:

- Documentation of risks identified by SecureTrust
- Recommendations for mitigating such risks

SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communications from 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 the agreed scope environment with regard to HIPAA standards.
- Create and respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Identify to Client certain observations that may require remediation.
- Provide Client with a draft HIPAA Risk Assessment Report for review and comment.
- Deliver to Client the final HIPAA Risk Assessment Report documenting observations and recommendations from the Service.

CLIENT RESPONSIBILITIES

- Establish contact and remain available for communications from 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 the Service 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.
    - Client's personnel from the following departments will typically need to be involved:
        - Security Governance, Information Technology, Enterprise Risk Management, Legal and Compliance, Procurement, Internal Audit, Human Resources, Facilities, Complaints, and Finance.
    - The Service is not a replacement for 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 Service may consist of remote and onsite assessment activities.
    - The Service 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 for determining 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's documentation as part of the Service.
    - SecureTrust will not provide remediation services as part of the Service.
    - SecureTrust will not offer any legal guidance or counseling. The Service does not guarantee compliance with data privacy regulatory requirements or any other regulatory requirements. Client is responsible for making all management decisions with regard to its data privacy policies.
    - The quality and accuracy of the Service is dependent on Client's provision of accurate information and access to Client's systems and resources to SecureTrust.