SecureTrust
a Trustwave division

Service Description

Health Insurance Portability and Accountability Act

Gap Assessment

Contents

HIPAA Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Health Insurance Portability and Accountability Act (HIPAA) Gap Assessment (the "**Service**") provides education and guidance for design and implementation of HIPAA safeguards and identification of supporting organizational policy, procedures, and practices relevant to HIPAA.

The Service aligns with the Department of Health and Human Services' (HHS) Audit Protocol and the Office for Civil Rights' (OCR) recommendations for HIPAA audit preparation. SecureTrust evaluates Client's policies, procedures, and practices through documentation review, interviews, facilities inspection, and controls analysis.

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 is Client's primary resource during the Service and is responsible for conducting the assessment, evaluating compliance, and producing the report.

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 Gap Assessment – An assessment to identify gaps and prioritize areas that may require remediation, to achieve compliance with the HIPAA Security Rule, Privacy Rule, and Breach Notification Rule. SecureTrust will provide a final report detailing the results of the HIPAA Gap Assessment.

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 and Client will work to gather and analyze information related to Client's Protected Health Information (PHI) and business operations. SecureTrust and Client will work 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;
- Applications supporting the PHI environment;
- Network diagrams;
- Organization chart;
- List of security incidents that occurred within the last two years;
- Copies of reports from any security audits, penetration tests, or vulnerability assessments conducted in the last two years; and
- Copies of existing security policies, such as:
    - Acceptable Use Policy;
    - Ethics Policy; and
    - HR Discipline Policy

Phase II: HIPAA Gap Assessment

SecureTrust will test and review Client's environment in accordance with the HHS Audit Protocol.

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

SecureTrust may 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 analyze the results of the Service activities to understand the current environment, define the HIPAA compliance posture, and create a high-level action plan aimed at resolving potential critical and high-risk observations.

Phase III: Reporting

SecureTrust will develop a HIPAA Gap Assessment Report document which will list areas of non-compliance pertaining to Client's PHI environment. The HIPAA Gap Assessment Report includes details of non-compliant observations and recommends specific changes that may be required to bring Client's PHI environment into compliance with the HIPAA.

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

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 milestones dates, key steps, estimates for duration, deliverables, and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.
- Respond to Client action items in Compliance Manager within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Provide Client with information on observations that may require remediation, at SecureTrust's election.
- Produce a draft HIPAA Gap Assessment Report.
- Deliver to Client a final HIPAA Gap 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.
- Accurately respond to requests from SecureTrust teams when establishing contact and collecting information.
- Provide complete and accurate details of the relevant environment and other business operations information.
- Make available resources capable of participating in Service activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection, and controls analysis.
- Client acknowledges:
    - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
    - Client's personnel from the following departments may 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 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 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 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 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.