SecureTrust
a Trustwave division

Service Description

Health Insurance Portability and Accountability Act

Policy Service

Contents

HIPAA Policy Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Health Insurance Portability and Accountability Act (HIPAA) Policy Service (the "**Service**") is designed to assist and guide organizations in developing a HIPAA compliance policy.

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 & Risk Services

The Global Compliance and Risk Services (GCRS) team and services consist of, among others, the following key elements:

Security Consultant – A Trustwave Security Consultant acts as the primary resource for Client and is responsible for scheduling and conducting 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 Policy Template – A template of baseline policies to assist Client in its development of information security policy to address relevant requirements of HIPAA.

HIPAA Policy Service – Consulting services aimed at providing assistance and guidance for customization of the HIPAA Policy Template.

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's Security Consultant will gather information about Client's operating environment via emails and calls using the HIPAA Policy Template as a guide. Client staff will provide SecureTrust with the current set of internal procedural steps.

Phase II: Draft Creation

SecureTrust will work with Client to create a comprehensive set of policies. Documentation will be created in conjunction with Client to reflect the specific environment and procedures of Client's operating environment.

Phase III: Policy Review and Modification

SecureTrust will review draft documentation with Client staff to help ensure security and compliance objectives are addressed.

Phase IV: Policy Finalization and Implementation

SecureTrust will provide Client the final policy documentation in an editable format as the final deliverable of the Service. SecureTrust will conduct a closeout meeting with Client.

SECURETRUST RESPONSIBILITIES

- Establish contact and remain available for communication 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 and resource requirements.
- Schedule and conduct kickoff, periodic status, and closeout meetings.

CLIENT RESPONSIBILITIES

- Establish contact and remain available for communication 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 Client environment information, and configuration requirements.
- Inform SecureTrust of all Client 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 the Service activities.
- Participate in and understand materials explained during calls, meetings, interviews, discussions, facilities inspection, and controls analysis.
- Client acknowledges:
    - All security and feature upgrades for SecureTrust Portal software will be included in major version release upgrades.

- The Service consists of remote consulting activities.
- The Service start and end dates will be determined during the kickoff call.
- 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.
- If the Service will be provided over multiple years, the Service includes updating the existing policies to include new policies or changes as required by changes in the HIPAA security standards. After the first year, SecureTrust will repeat the same steps as described in this Service Description base on any changes within Client's environment identified to SecureTrust by Client. These changes may require the adjustment of existing policies and procedures, which may include technological changes such as newly deployed systems or devices, system configuration changes, firewall policy changes, adjustments to roles, responsibilities, and internal processes, and updates to compliance requirements.
- SecureTrust will not offer any legal guidance or counseling. The provision of 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.