

## **Service Description**

Health Insurance Portability and Accountability Act  
Policy and Procedure Service

# Contents

<b>HIPAA – Policy and Procedure Service .....</b>	<b>3</b>
Service Description .....	3
Base Service Features .....	3
SecureTrust Portal.....	3
Global Compliance & Risk Services .....	3
Delivery and Implementation.....	4
Project Initiation .....	4
Phase I: Data Gathering .....	4
Phase II: Draft Creation .....	4
Phase III: Review and Modification .....	4
Phase IV: Finalization and Implementation .....	4
SECURETRUST RESPONSIBILITIES .....	4
CLIENT RESPONSIBILITIES.....	4

# HIPAA – Policy and Procedure Service

SecureTrust™ is a division of Trustwave Holdings, Inc.

## SERVICE DESCRIPTION

SecureTrust's Health Insurance Portability and Accountability Act (HIPAA) Policy and Procedure Service (PPS) is a professional service. SecureTrust's PPS is designed to assist and guide organizations in development of policy and procedures in compliance with the HIPAA.

## BASE SERVICE FEATURES

SecureTrust's PPS 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 & Risk Services**

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

**Security Consultant** – An information security consultant is the primary resource for the fulfillment of the service.

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

**SecureTrust Compliance Review Board (CRB)** – The CRB serves as an escalation point for requirement interpretation or complicated compliance questions, providing consistency and continuity across SecureTrust assessments. The CRB is the final point of escalation for issue resolution regarding compliance status against requirement interpretation or the review of a compensating control.

**HIPAA Policy Template** – A template of baseline policies to assist Client in its development of information security policy and procedures to address relevant requirements of the HIPAA.

**HIPAA PPS Consulting** – Consulting assistance and guidance for modification of the HIPAA Policy Template. SecureTrust will provide consulting services to assist Client in the development of policy and procedures using the SecureTrust HIPAA Policy Template.

## 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: Data Gathering

SecureTrust's security consultant will gather information in order to gain an understanding of Client's operating environment. This information will be gathered during calls, and the template will serve as the framework of the policy and procedure documents. 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 and procedures. Documentation will be created in conjunction with Client to reflect the specific environment and procedures of the Client operating environment.

### Phase III: Review and Modification

SecureTrust will review draft documentation with Client staff to help ensure security and compliance objectives are addressed. Any necessary additions or modifications will be made to the draft at this time.

### Phase IV: Finalization and Implementation

SecureTrust will work with Client to finalize policy and procedures documentation for implementation. 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 and resource requirements.
- Schedule and conduct kickoff, periodic status and closeout meetings.

## 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 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 consulting activities in relation to the client environment.
- 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 engagement consists of remote consulting activities.
  - The assessment period 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 assessment.
  - SecureTrust will perform the service in the English language.
  - If the multi-year service is selected, the service includes updating the existing policies to include new policies or changes as required by security standards. Subsequent years will utilize the same methodology and Client shall identify any changes within the environment. 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 as well as adjustments to roles, responsibilities and internal processes, and updated compliance requirements.
  - SecureTrust will not offer any legal guidance or counseling. The provision of the HIPAA PPS 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 service is dependent on Client's provision of accurate information and access to Client systems and resources to SecureTrust.