WHITEPAPER

Architecting for HIPAA on Twilio

OVERVIEW

- Customer Requirements for All Products
- HIPAA Eligible Products and Services

Introduction

This document is intended for Twilio customers that have a Business Associate Agreement (BAA) in place with Twilio, or intend to enter into a BAA with Twilio. This document provides specific guidelines on how customers can use Twilio to develop HIPAA compliant applications and workflows. Twilio believes that security and compliance is a shared responsibility between Twilio and the customer. There are aspects of HIPAA controls that Twilio has put in place for all of our customers' data. There are additional safeguards that customers seeking HIPAA compliance will require, and it is Twilio's responsibility to provide the services and tools necessary to configure for the additional requirements. It is the customer's responsibility to ensure that their applications and workflows built on Twilio utilize these tools to architect a solution that supports HIPAA compliance. Throughout this document, we have indicated whether each Twilio feature is required for HIPAA compliance or recommended for additional security, as well as highlight use cases that customers should avoid at this time. There are also sections that call out special considerations that customers should take note of under certain circumstances.

Customers that enter into a BAA with Twilio will need to specify which of their Twilio Projects and Subaccounts are designated HIPAA (per the BAA) for all existing and future Projects and Subaccounts created with Twilio. They may use any Twilio products and services under the designated HIPAA Projects and Subaccounts, but workflows that potentially contain PHI can only be built using HIPAA Eligible Products and Services. Designated HIPAA Projects and Subaccounts cannot be used to process, store, or transmit PHI using Twilio products and services that are not HIPAA eligible. Customers that wish to add new Projects and Subaccounts will need to contact their Twilio Account Representative or contact Support.

We understand that customers rely on Twilio's products and services to power their applications and various critical communications workflows. As such, we will not deprecate any HIPAA eligible products and services without at least 180 days notice to our customers. Any notice of deprecation will be posted as an update to this document.

Customer Requirements for All Products

This section outlines the set of required and recommended best practices for building a HIPAA compliant workflow on Twilio, regardless of which products and services are being used.

Security and Compliance

Twilio provides various capabilities for customers to enhance the level of security when building using Twilio's APIs. This section identifies the requirements for building HIPAA compliant workflows, as well as recommended best practices for optimal security.

Required for HIPAA

Encrypted Communication

Twilio supports encryption to protect communications between Twilio and your web application. Customers building HIPAA compliant workflows are required to use HTTPS for making requests to Twilio as well as in configuring Twilio's requests to be made to the customer. Note: Twilio cannot currently handle self signed certificates.

Signed Webhook Requests

Customers building HIPAA compliant workflows are required to ensure that the requests to your web application are indeed coming from Twilio, and not a malicious third party. To allow this level of security, Twilio cryptographically signs its requests, and it is the responsibility of the customer to verify that the signature is valid.

Recommended for HIPAA

HTTP Authentication

Twilio supports HTTP Basic and Digest Authentication. This allows the customer to password protect the TwiML URLs on your web server so that only the customer and Twilio can access them. Customers building HIPAA compliant workflows are encouraged to use either tiers of authentication when possible.

Static Proxy

Static Proxy routes all Voice, SMS TwiML requests and Taskrouter webhooks from Twilio to the customer's servers via a static set of server addresses. This provides customers with a predictable set of IP addresses that can be added to a firewall or security device. Customers building HIPAA compliant workflows are encouraged to leverage this option when possible.

Public Key Client Validation

Public Key Client Validation provides a mechanism that lets Twilio and the customer know that they are talking to the intended services and the requests have not been tampered with. This is accomplished by introducing public / private keys to secure the communication between Twilio and the customer. Customers building HIPAA compliant workflows are encouraged to leverage this option when possible.

Developer Tools — Runtime

Runtime is a collection of tools and services available through the Twilio Console to make developers more efficient throughout the development lifecycle — from building, deploying, operating, and scaling solutions. Some of these capabilities access and store PHI when used to develop HIPAA compliant workflows and thus require appropriate HIPAA controls to be in place. It is the responsibility of the customer to ensure that only the tools indicated as Eligible for HIPAA be used when developing a workflow with PHI. Twilio will continue to enhance our ability to support HIPAA compliance while using these tools and update this document accordingly.

Eligible for HIPAA

Debugger

Debugger contains a detailed log of activity within your application. This log can help customers dive deeper and understand which Twilio resources were impacted (and by whom). Depending on the customer use case, Debugger may expose PHI to users of Twilio's Console. It is the responsibility of the customer to ensure that any of its employees with access to the Twilio Console have the right access credentials and training for handling PHI.

API Explorer

The API Explorer provides a way to access the full range of REST API requests through the browser. Through various API calls, PHI can be accessed and downloaded by users of Twilio's Console. Depending on the use case, API Explorer may expose PHI to users of Twilio's Console. It is the responsibility of the customer to ensure that any of its employees with access to the Twilio Console have the right access credentials and training for handling PHI.

Special Considerations for HIPAA

Assets / Private Assets

Assets can be used to upload and host static files that support web, voice, and messaging applications. In order to build a HIPAA compliant workflow, customers may not upload any files that contain PHI to Assets or Private Assets. Customers can still use Assets or Private Assets to store non-PHI files in support of HIPAA compliant workflows.

TwiML Bin

TwiML Bins are a serverless solution that provides Twilio-hosted instructions to our customer's Twilio applications. They are a useful way to prototype and explore Twilio's capabilities without needing to set up your own web server to respond to requests. When using TwiML Bins for HIPAA compliant workflow, the customer should not include any PHI in any text body of the TwiMLs stored on TwiML Bin. TwiML Bin (without PHI) can still be used to develop HIPAA compliant workflows.

NOT ELIGIBLE FOR HIPAA

- **Studio:** Twilio Studio is a visual interface to design, deploy, and scale customer communications. Customers can build and run stateful workflows and access context variables with rich multi-channel visual modeling tools for creating IVRs, chatbots, and more. Studio should not be used to build solutions requiring HIPAA compliance, as Twilio has not yet undergone HIPAA remediation work for the PHI that would be processed, stored, or transmitted as a result of using Studio.

- **Sync:** Twilio Sync is a state synchronization service, offering two-way real-time communication between browsers, mobiles, and the cloud. Sync should not be used to develop HIPAA compliant workflows at this time, even if the communication channels being used are HIPAA eligible.

- **Functions:** Twilio Functions is a serverless environment which empowers developers to quickly and easily create production-grade, event-driven Twilio applications that scale with their businesses. Functions should not be used to develop HIPAA compliant solutions at this time, even if the communication channels being used are HIPAA eligible.

HIPAA Eligible Products and Services

This section outlines the product-specific requirements, recommended best practices, and special considerations for building a HIPAA compliant workflow on Twilio.

Programmable Video

Programmable Video provides the building blocks and flexibility to build and scale a reliable, high quality video experience using WebRTC and our suite of SDKs. Group Rooms are covered by Twilio's BAA, and unless specifically referenced below, all additional Group Room features listed under HIPAA Eligible Products and Services are HIPAA eligible.

Required for HIPAA

HTTP Auth for Accessing Media Recordings

For building a HIPAA-compliant workflow using media recordings, customers are required to enforce HTTP basic auth using Twilio account's AccountSid and Authentication token when making the initial request to access the URL to the media (via GET API). The returned URL can be configured to remain available for up to 1 hour, but Twilio does not enforce authentication on the URL. Customers are required to ensure that this URL (which enables access to the media recording) is kept secured from unauthorized access.

Special Considerations for HIPAA

DataTrack API

DataTrack is an API for publishing real-time data among Room Participants to enable customers to build shared whiteboarding, collaboration features, augmented reality apps, and more. When building HIPAA compliant workflows using DataTracks, it is the customer's responsibility to understand the role of any third party application / API being used in conjunction with DataTracks and obtain a BAA if necessary. This includes Twilio's Programmable Chat API, which is not yet covered under Twilio's BAA, and thus cannot be used for HIPAA compliant workflows.

Programmable Voice and SIP

Twilio's Programmable Voice allows customers to build applications that make, receive, and intelligently control voice calls with one API. Twilio Elastic SIP Trunking delivers global PSTN connectivity that enables businesses to increase communications agility, reduce costs and deliver uniform global services. Twilio's Programmable Voice SIP Interface instantly enables businesses to augment their VoIP infrastructure / SIP endpoints with Programmability.

Unless specifically referenced below, all Programmable Voice and SIP capabilities listed under HIPAA Eligible Products and Services are HIPAA eligible. Features that require special considerations for HIPAA are outlined below, as well as features that are commonly used with voice and SIP that are not yet HIPAA eligible. Only Voice traffic to/from US area codes are considered HIPAA eligible at this time.

Required for HIPAA

HTTP Auth for Accessing Recordings

By default, Twilio's recording URLs are public and do not require authentication (the URLs are quite long and difficult to guess). However, for building a HIPAA-compliant workflow using recordings, customers are required to enforce HTTP basic auth to access media using the account's AccountSid and Authentication token. This information can be found in the voice settings page in the console.

Basic SIP Security

When exposing a SIP application to the public internet, customers should take special care to secure your applications against unauthorized access. For building a HIPAA-compliant workflow, customers are required to enforce SIP Security Best Practices.

Secure Traffic for SIP Interface

Twilio's SIP Interface allows voice traffic to interact between customers' existing VoIP infrastructure and their TwiML Application built using Twilio's Programmable Voice. When connecting the existing VoIP infrastructure with Twilio's Programmable Voice via SIP Interface, customers must use one of two options to secure the traffic between Twilio and the customer's SIP infrastructure, which would otherwise be over the public internet. SRTP Support for SIP Interface can be used, or alternatively Twilio Interconnect can be used to establish a secure connection.

Secure Elastic SIP Trunking

Elastic SIP Trunking enables customers to instantly scale their existing VoIP infrastructure to send/receive voice traffic via SIP to/from the PSTN. When using Twilio's Elastic SIP Trunking for HIPAA compliant workflows, Secure Trunking must be used to enable Secure Real-time Protocol (SRTP) to encrypt media and Transport Layer Security (TLS) to encrypt signaling. Alternatively, Twilio Interconnect can be used to secure the traffic between the customer's SIP endpoint and Twilio, which would otherwise be over the public internet.

Special Considerations for HIPAA

Twilio Phone Numbers for Voice

Twilio considers telecommunications providers as conduits per HIPAA guidelines, thus we do not require a BAA from these providers. Twilio will still make attempts to secure the traffic to/from the providers when feasible to maximize the security of PHI in transit. When customers need Twilio Phone Numbers to support inbound calling workflows, we can attempt to ensure that calls terminate with providers with whom Twilio has established a private connection. We do this by assigning Twilio Phone Numbers from providers that meet this requirement. Twilio currently does not support this capability through the Twilio Console, but customers can contact their account representative to make this request.

For customers that already have Twilio Phone Number(s) assigned, the existing numbers may be from providers with whom we do not have a privatized connection. We are currently unable to retroactively change the provider of existing numbers, but we are continuing to add more private connections with our US number providers. This does not mean that the customer's solution built on existing phone numbers is not HIPAA compliant. This is added security that Twilio is choosing to support on a go-forward basis, and it is a standard that we believe is above and beyond what other telecommunication platforms offer.

Call Recordings

By default, all Programmable Voice Recordings are encrypted at rest while stored in Twilio's cloud storage. For additional security, we recommend that customers building HIPAA-compliant workflows use Voice Recording Encryption, which encrypts the recordings with your public key as soon as the call ends, while the recording is within the Twilio infrastructure, and before it is in cloud storage. The recording remains in this encrypted state until you retrieve it, ensuring that the recording can only be accessed by you, the holder of the corresponding private key.

Recording Transcription

Recording Transcription offered directly through Twilio's API is eligible for HIPAA workflows. However, any transcription service via Add-ons from Marketplace are not HIPAA eligible at this time.

Media Streams

When using Media Streams, it is the responsibility of the customer to ensure that the recipient / destination of the media is HIPAA compliant. If the media is streamed to a third party application, it is the responsibility of the customer to ensure that a BAA is obtained from the third party vendor.

NOT ELIGIBLE FOR HIPAA

This section outlines features that are commonly used in conjunction with Twilio's Programmable Voice and SIP products that are not yet HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not yet HIPAA eligible.

- **Third-party Add-on via Marketplace:** Third-party APIs accessed through the Twilio Marketplace are not HIPAA eligible at this time. Even if the customer is able to obtain a BAA with the third party vendor, the Twilio Marketplace has not undergone HIPAA eligibility work.

- **Autopilot**: Integration with Autopilot for interactive voice response (IVR) workflows are not HIPAA eligible at this time. IVR workflow without Autopilot are still eligible for HIPAA.

Programmable SMS

Twilio's Programmable SMS APIs allow customers to send and receive text messages over the carrier network to any phone, anywhere in the world. Unless specifically referenced below, all Programmable SMS capabilities listed under HIPAA Eligible Products and Services are HIPAA eligible. Features that require special considerations for HIPAA are outlined below, as well as features that are commonly used with SMS that are not yet HIPAA eligible. Only SMS traffic to/from US area codes are considered HIPAA eligible at this time.

Required for HIPAA

No specific configuration requirements are necessary for use of Twilio's HIPAA eligible SMS APIs. Please be sure to refer back to Security Requirements for All Products at the beginning of this document.

Special Considerations for HIPAA

Messaging Geographic Permissions

Twilio provides our users with the ability to send outbound SMS messages globally, but HIPAA eligible traffic is limited to/from US area codes. Since no special request form is required to send global messaging, we recommend you visit our Messaging Geographic Permissions page in Console to preview the list of countries in which your project allows messaging content to and from.

NOT ELIGIBLE FOR HIPAA

This section outlines features that are commonly used in conjunction with Twilio's Programmable SMS products that are not yet HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not yet HIPAA eligible.

- MMS: MMS enables exchange of attachments and picture messages between mobile phones over the carrier network without requiring a separate mobile app. This capability cannot be used in conjunction with Programmable SMS for workflows requiring HIPAA compliance at this time.

- Marketplace Add-ons: Third-party APIs accessed through the Twilio Marketplace are not HIPAA eligible at this time. Even if the customer is able to obtain a BAA with the third party vendor, the Twilio Marketplace has not undergone HIPAA eligibility work.

- Autopilot (also known as SMS Bots): Integration with Autopilot for bot-enabled SMS workflows are not HIPAA eligible at this time. Customers may choose to integrate Twilio's SMS APIs with a third party bot / AI solution of their choice; however, it is the customer's responsibility to ensure that the third party application is used in a HIPAA compliant manner.

- Channels: Channels lets you send and receive messages on multiple platforms with the Programmable SMS API that you already use. Whatsapp, Facebook Messenger, and LINE cannot be used in conjunction with Programmable SMS for workflows requiring HIPAA compliance at this time.

CHANGE LOG

3/20/2020	Added Programmable Voice / SIP and Programmable SMS
3/10/2020	Added clarification on customer requirements for Programmable Video
2/27/2020	Initial release