Version: 1.1
Updated: 04.27.23

Architecting for HIPAA on Twilio

Contents

Introduction

This document is intended for Twilio customers that have a Business Associate Addendum (BAA) in place with Twilio, or intend to enter into a BAA with Twilio for use of the HIPAA Eligible Services, as defined in the BAA. For a complete list of these services, see the HIPAA Eligible Services page. This document provides specific guidelines on how customers can use the HIPAA Eligible Services 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.

Please note this document may be updated from time to time. 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. Any defined term used, but not defined herein, shall have the meaning ascribed to it in the BAA and Documentation (as defined in the Agreement).

Designation of HIPAA accounts

Customers looking to build HIPAA compliant workflows on Twilio will need to purchase a Twilio Editions package that contains HIPAA Accounts in order to designate their Projects and Subaccounts as HIPAA Project(s) (as defined in the BAA). Customers that enter into a BAA with Twilio will need to specify which of their Twilio Projects and Subaccounts are designated as HIPAA Projects (including HIPAA Subaccounts) requiring HIPAA eligibility (per the BAA) for all existing 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 Services.

If a project (Master Account) is designated as a HIPAA Project at the signing of a BAA, then any future Subaccounts created in that Project will also be automatically designated as HIPAA Subaccounts. Any Subaccounts that existed prior to the signing of the BAA, unless specified in the BAA, will not automatically be designated as HIPAA Subaccounts. If only select Subaccounts are designated as HIPAA Subaccounts at the signing of a BAA, then the customer will need to request that any later-created Subaccounts be designated as HIPAA Subaccounts. Similarly, if any new Projects are created after the signing of a BAA, the customer will need to request that the new Project created be designated as a HIPAA Project. Customers can contact their Twilio Account Representative or contact Support to enable HIPAA eligibility for new Projects.

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.

Changes to Twilio Experience from HIPAA Accounts

When a Project or a Subaccount is designated as HIPAA, there are minor changes to the customer's experience on Twilio.

- The Twilio Console experience for any Projects or Subaccounts with HIPAA designation will have an automatic logoff triggered by 15 minutes of inactivity. This is because the Twilio Console can contain the customer's PHI.
- Any Projects or Subaccounts with HIPAA designation will be exempted from certain content moderation that Twilio typically conducts. However, HIPAA customers still remain subject to review of content if carrier and/or consumer complaints are received, or other risk indicators, such as high error rates are present.

Additionally, any product-specific changes that occur as a result of HIPAA Accounts are listed under each product's respective section throughout this document.

Customer Requirements for All Twilio 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.

Support Tickets

Customers may not put PHI in any Support tickets submitted through Twilio's Support Center (via Console), through Email, or through Chat with any one of our Support Agents. Customers should use Call SIDs or Message SIDs (or other Twilio-specific IDs) rather than phone numbers when troubleshooting with Twilio Support Agents.

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 – 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

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. Depending on the customer use case, Studio may expose PHI to users of Twilio's Console and through the Studio REST API. 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. Note that Studio still cannot be used in conjunction with non-HIPAA-eligible products.

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 can be created and managed through Twilio Console or via Serverless API, which allows for Functions to be created and managed programmatically via a REST API.

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.

Sync
Twilio Sync is a state synchronization service, offering two-way real-time communication between browsers, mobile devices, and the cloud. Sync is leveraged internally by Twilio to support certain products, as well as being available as an API that customers can leverage to manage communication across multiple channels.

Special Considerations for HIPAA

Assets

Assets can be used to upload and host static files that support web, voice, and messaging applications. There are two types of Assets: Public and Private. Public Assets are made available over the public internet, so it should not be used to store PHI or any other sensitive information. In order to build a HIPAA compliant workflow, customers should only use Private Assets to store any PHI.

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 TwiML stored on TwiML Bins. TwiML Bins (without PHI) can still be used to develop HIPAA compliant workflows.

Customer Requirements for Individual Twilio Products

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.

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. TLS and 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

Call Recordings and Storage
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 workflows 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 and MMS traffic to/from US area codes are considered HIPAA eligible at this time.

Required for HIPAA

MMS
MMS enables exchange of attachments and picture messages between mobile phones over the carrier network without requiring a separate mobile app. Customers can send multimedia messages (MMS) with the existing Programmable SMS APIs by adding a media URL to the message request. By default, Twilio's Media 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 MMS, customers are required to enforce HTTP basic auth on Media URLs using the account's AccountSid and Authentication token. This can be done in your Twilio Console under Messaging -> Settings -> General.

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.

Message Redaction
Message Redaction offers two types of redactions - message body redaction and phone number redaction. Message Body Redaction ensures that Twilio never retains message bodies that contain sensitive information. Phone Number Redaction will obfuscate the last four digits of the non-Twilio phone number in the message request. When processing PHI through SMS workflows, we highly recommend that customers subject to HIPAA turn on both features to protect the privacy of patients. Customers can configure this capability for their accounts through the Twilio Console.

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.

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 and Facebook Messenger cannot be used in conjunction with Programmable SMS for workflows requiring HIPAA compliance at this time.

Programmable Chat

Note: Twilio has announced our intent to sunset the Programmable Chat API on July 25, 2022 to focus on the next generation of chat, the Twilio Conversations API. Conversations API is HIPAA eligible, and information on how to migrate can be found on our website.

Twilio's Programmable Chat makes it easy for customers to add chat features into web and native mobile applications without building or scaling a real-time chat backend. Unless specifically referenced below, all Programmable Chat capabilities listed under HIPAA Eligible Products and Services are eligible. Features that require special considerations for HIPAA are outlined below, as well as features that are commonly used with Chat that are not yet HIPAA eligible.

Required for HIPAA

Private Channels
Channels are the heart of all chat activity within a Service. Channel Members send Messages to the Channel, which are then distributed to other Members of the Channel. For building HIPAA-compliant workflows where Members may exchange PHI, only private channels (not public) may be used.

Special Considerations for HIPAA

Integration with Third Party Applications
REST APIs and webhooks enable customers to link Twilio chat with external services like Salesforce or connect to chat apps like Slack and HipChat. It is the customer's responsibility to ensure that the third party services or applications are used in a HIPAA compliant manner.

Not Eligible for HIPAA

This section outlines features that are commonly used in conjunction with Twilio's Programmable Chat APIs 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.

Autopilot (also referred to as Chat Bots):
Integration with Autopilot for bot-enabled Chat workflows are not HIPAA eligible at this time. Customers may choose to integrate Twilio's Chat 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.

Twilio Conversations

Twilio Conversations lets customers manage and orchestrate end-user conversations across multiple channels. For HIPAA eligible use cases, the channels that can be exposed to PHI are limited to SMS and Chat (i.e., WhatsApp cannot be used at this time). 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.

Required for HIPAA

All configurations required for each HIPAA-eligible channel used in Conversations are applicable when used in conjunction with Conversations. Please refer to each channel's respective sections in this document (SMS and Chat) for requirements on building for HIPAA compliance.

Special Considerations for HIPAA

All special considerations for each HIPAA-eligible channel used in Conversations are applicable when used in conjunction with Conversations. Please refer to each channel's respective sections in this document (SMS and Chat) for requirements on building for HIPAA compliance.

Not Eligible for HIPAA

All non-eligible features for each HIPAA-eligible channel used in Conversations are applicable when used in conjunction with Conversations. Please refer to each channel's respective sections in this document (SMS and Chat) for requirements on building for HIPAA compliance. This section outlines features that are commonly used in conjunction with Twilio Conversations 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.

WhatsApp: Twilio's API for WhatsApp enables developers to quickly build, scale, and operate messages for WhatsApp users through Twilio's scalable infrastructure. WhatsApp APIs are not HIPAA eligible at this time as WhatsApp (Facebook) does not offer a BAA.

Autopilot (also referred to as Chat Bots): Integration with Autopilot for bot-enabled Conversations workflows are not HIPAA eligible at this time. Customers may choose to integrate Twilio's Conversations 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.

Twilio Frontline

Twilio Frontline enables customer sales teams to securely connect with their end customers everywhere. Frontline is a pre-built application with customizable workflows that integrates with any CRM or customer database, and is available for both iOS and Android devices. For HIPAA eligible use cases, the channels that can be exposed to PHI are limited to SMS, MMS, Chat via Twilio Conversations, and Voice (i.e., WhatsApp cannot be used at this time).

Required for HIPAA

All configurations required for each HIPAA-eligible channel used in Frontline are applicable when used in conjunction with Frontline. Please refer to each channel's respective sections in this document (SMS, MMS, and Chat via Conversations, and Voice) for requirements on building for HIPAA compliance.

Validate Callbacks from Twilio
A callback is a function that will be executed only after the current function has finished executing. You subscribe to a callback by configuring a url which will process an incoming request and respond back in a certain format. For HIPAA-compliance workflows, you must verify that Twilio is the service that sent a callback before responding to that request. More information about callback security can be found here.

On October 5, 2021, Twilio Frontline introduced V2 of its callbacks. For HIPAA-compliance workflows, only V2 of callbacks may be used. Please refer here for more information on V2 callbacks.

Special Considerations for HIPAA

All special considerations for each HIPAA-eligible channel used in Frontline are applicable when used in conjunction with Frontline. Please refer to each channel's respective sections in this document (SMS, MMS, and Chat via Conversations, and Voice) for requirements on building for HIPAA compliance.

App Security
Twilio Frontline works with your existing Identity Provider to authenticate users and enable single sign-on (SSO). It is the customer's responsibility to ensure that their access controls and other user security policies are compliant with HIPAA.

Not Eligible for HIPAA

All non-eligible features for each HIPAA-eligible channel used in Frontline are applicable when used in conjunction with Frontline. Please refer to each channel's respective sections in this document (SMS, MMS, and Chat via Conversations, and Voice) for requirements on building for HIPAA compliance.

WhatsApp: Twilio's API for WhatsApp enables developers to quickly build, scale, and operate messages for WhatsApp users through Twilio's scalable infrastructure. WhatsApp APIs are not HIPAA eligible at this time as WhatsApp (Facebook) does not offer a BAA.

Verify

Twilio Verify lets customers build multi-channel user verification, two-factor authentication, and passwordless login into their applications. For HIPAA eligible use cases, the channels that can be used for HIPAA workflows are limited to SMS and Voice with traffic only to/from US area codes. Note that Email channel is not HIPAA eligible at this time.

Required for HIPAA

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

Not Eligible for HIPAA

This section outlines features that are commonly used in conjunction with Twilio's Verify 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.

Email Channel: Verify allows you to integrate email verification via Twilio Sendgrid. Use of this channel in Verify is not HIPAA eligible at this time.

Lookup

Twilio's Lookup API provides a way to retrieve additional information about a phone number. Lookup instantly delivers a region-specific number formatting and validation, carrier information, and caller ID name so the right medium can be utilized by a customer or business message to ensure the intended communication can be delivered appropriately (i.e., not delivering a text message to a landline number that cannot receive it).

Required for HIPAA

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

Not Eligible for HIPAA

This section outlines features that are commonly used in conjunction with Twilio's Lookup API 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.

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.

Event Streams (Beta)

Event Streams allows you to tap into a unified stream of every interaction sent or received on Twilio through a single API. Event Streams evolves event delivery at Twilio beyond a single-producer-to-single-consumer model, giving developers flexibility to stream events to multiple sinks. Event Streams is currently available as a Beta release. Beta products are not covered by a Twilio SLA. Learn more about Beta product support.

Required for HIPAA

No specific configuration requirements are necessary for use of the Event Streams API. Please be sure to refer back to Security Requirements for All Products at the beginning of this document.

Special Considerations for HIPAA

Event Sinks are the destinations to which events selected in a subscription will be delivered. It is the responsibility of the customer to ensure that the designated Sinks are configured in a HIPAA compliant manner. For example, AWS Kinesis, a supported Sink Resource Type, is HIPAA eligible but requires that customers follow Amazon's Architecting for HIPAA Security and Compliance on AWS.

Not Eligible for HIPAA

Event Types generated from non-HIPAA-eligible products are not HIPAA eligible. It is the responsibility of the customer to ensure that no PHI data is processed through non-HIPAA-eligible products.

Twilio for Salesforce (Beta)

Twilio for Salesforce is a managed package for Salesforce that brings programmable communications to your Salesforce environment. Using Twilio for Salesforce, you can send automated, customized SMS messages from Salesforce and/or message one-on-one with Contacts in Salesforce. Twilio for Salesforce is currently available as a Beta release. Beta products are not covered by a Twilio SLA. Learn more about Beta product support.

Required for HIPAA

Customers using Twilio for Salesforce for HIPAA-compliance workflows must execute a Business Associate Agreement (BAA) with Salesforce, in addition to the BAA with Twilio.

Twilio Flex

Twilio Flex is a programmable cloud contact center platform that gives your company complete control over how, when, and what you deploy. Twilio's customer engagement platform powers over a half million agents today and helps businesses deploy tailored cloud contact centers while freeing them from the limitations of SaaS solutions or on-premise devices.

Required for HIPAA

Changes to Flex Insights
This section lists several changes necessary to Flex Insights for workflows that are subject to HIPAA. There are two types of changes - Twilio-configured and Customer-configured. When a Flex Account SID is designated as a HIPAA Account per the Twilio BAA, Twilio will automatically enforce some changes to various aspects of Flex Insights - these changes will be marked as Twilio-configured. The other configuration changes are required for the customer to implement - these are marked as Customer-configured. It is the responsibility of the customer to ensure that any Flex workflows subject to HIPAA are developed on Account SIDs that are designated as HIPAA Accounts and to ensure that all of the Customer-configured changes are implemented.

Twilio-configured
Twilio will redact any TaskRouter Attributes that could contain PII (per definition of the Attribute field) from ingressing into Flex Historical Insights. The redacted fields are customer Names, Phone, and Email, and External_id. The updated list of preserved attributes available after redaction is listed in our documentation.

Above means that conversations are not linked to a single customer by default. Each conversation behaves as it was from a different customer.

Twilio will disable the visual waveform feature (blue, green, red, orange bars) on Conversations Screen (Player). This means that users will not be able to see when an agent or a customer is speaking while playing back recordings.

Twilio will disable speech essentials metrics (agent talk, customer talk, crosstalk, silence, individual silence findings, and any other metrics built on top of these metrics).

Customer-configured
It is the customer's responsibility to ensure that no data that could be construed as PHI is entered into the preserved Attribute fields for Flex Insights, including any of the custom attributes that are available to be configured. Note that individual Attributes may not be PHI by themselves, but a combination of multiple preserved data points in Flex Insights could be deemed PHI.

It is the customer's responsibility to ensure that no PHI data is entered into Comments and Assessments by Agents / Supervisors.

Enforce HTTP Auth for Recordings
As indicated in the Programmable Voice section above, customers are required to Enforce HTTP Auth on Media URLs using the account's AccountSid and Authentication token. This information can be found in the voice settings page in the console. Your recording URLs are visible to any services that consume TaskRouter events (e.g., third party applications via add-

ons), and securing the endpoints is a good practice. Ensure that your infrastructure does not require this endpoint to be unsecured.

Secure Playback of Media from Custom Storage
Flex Insights allows customers to configure playback of call recordings that are configured to be stored on the customer's custom storage (vs. Twilio's recording storage). For building a HIPAA-compliant workflow in Flex, customers are required to follow the configurations on Secure Playback of Media from Custom Storage.

Custom Media Attached to Conversations
Flex Insights enables customers to drill down from Historical Reporting directly to calls and chat transcripts. Customers can attach a list of custom media URLs that can point to additional media or other resources related to a conversation or its segments. For building a HIPAA-compliant workflow, it is the responsibility of the customer to ensure that the customer media URLs are properly secured and do not expose sensitive content to unauthorized users.

Session Log-off
Flex does not currently have support for a session timeout. In the case that PHI will be exposed and accessible through the Flex Agent UI, it is the responsibility of the customer to implement a timeout for users accessing the Flex application. This could be done through a variety of different methods; for example, implementing an enforced desktop/laptop log-out, or enforcing a VPN connection (that times out with inactivity) for Flex login would ensure that PHI does not remain exposed and/or unattended for an unreasonable length of time.

Flex UI Configuration
Flex UI's configuration allows you to control the way the overall app loads, as well as the behavior of individual Flex UI Components. For building a HIPAA-compliant workflow, it is the responsibility of the customer to ensure that there is no PHI in any Properties of Configuration Objects. Details on Configuration Objects and Properties can be found here.

Access to PHI through Flex UI
In the case that PHI will be exposed and accessible through the Flex UI, it is the responsibility of the customer to ensure that only those that are authorized to access PHI have access to Flex. In some scenarios, PHI may be available to be downloaded by an Agent to their workstation from Flex UI. It is the responsibility of the customer to ensure that those with access have proper training on HIPAA prior to being given access.

Special Considerations for HIPAA

Flex Plugins
Flex Plugins enable customization of the Flex UI. It is the responsibility of the customer to ensure that any Plugin is developed and used in a HIPAA compliant manner, which includes not putting any PHI into error messages that may be collected by Flex (or any other third party services) for troubleshooting purposes. Twilio cannot guarantee that any Plugins developed by a third-party, regardless of whether or not they are an official partner of Twilio, are HIPAA compliant. Plugins developed by Twilio Professional Services have also not been developed with HIPAA considerations at this point; it is the responsibility of the customer to ensure that any Plugins used are developed and used in a HIPAA compliant manner.

Integrations
It is the responsibility of the customer to ensure that any integrations between Flex and third party applications, regardless of the party that developed the integration, are built in a HIPAA compliant manner. It is the responsibility of the customer to obtain a BAA with the third party vendor if PHI will be transmitted.

Not Eligible for HIPAA

WhatsApp and Facebook Messenger: Twilio's APIs for WhatsApp and Facebook Messenger enable developers to quickly build, scale, and operate messages for WhatsApp or Facebook Messenger users through Twilio's scalable infrastructure. For Twilio, WhatsApp and Facebook Messenger are not HIPAA eligible at this time as Meta does not offer a BAA.

SendGrid Email: Flex integration with Twilio SendGrid Email API is available only as a private beta offering. This integration is not eligible for HIPAA and cannot be used in Flex workflows that are subject to HIPAA.

Customer Requirements for All Twilio Segment Products

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

Twilio Segment allows customers to personalize end user engagement by collecting, processing, aggregating, and activating your first-party customer data. Segment simplifies the process of collecting user data when they interact with any of your interfaces and sending, often in real-time, to your marketing, product, analytics tools, and data warehouses. “Interfaces” is Segment’s generic word for any digital properties you own: your website, mobile apps, and processes that run on a server or OTT device.

Designation of Workspaces as HIPAA Project(s)

Customers looking to build HIPAA compliant workflows with Segment will need to purchase the Segment Healthcare package and specify which of their Segment Workspace(s) are designated as HIPAA Projects requiring HIPAA eligibility (per the BAA). Any future Workspace(s) created will NOT automatically be designated as HIPAA Projects. Instead, the customer will need to request that the new Workspace(s) created be designated as HIPAA eligible by contacting their Segment Account Representative or Segment Support. Customers should ensure their Workspace is enabled as a HIPAA Project by checking the Workspace Setting screen before submitting any PHI.

Changes to Segment Experience When Workspace ID(s) designated as HIPAA Project(s)

When Workspace ID(s) are designated as HIPAA Project(s), there are minor changes to the customer’s experience on Segment. The Segment Console experience for any Workspace ID(s) identified as HIPAA Project(s) will have an automatic logoff triggered by 15 minutes of inactivity. This is because the Segment Console can contain the customer’s PHI. Additionally, any product-specific changes that occur as a result of Workspace IDs enabled as HIPAA Project(s) are listed under each product’s respective section throughout this document.

Support Tickets

Customers may not put any sensitive data including PHI in any support tickets submitted through Segment’s Contact Support (via the application), through Email, through Zendesk or through live chat with any one of our support Agents. Customers should use anonymous ids or any other id or secured link available to help direct the support agent while troubleshooting.

Customer Requirements for Individual Twilio Segment Products

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

Connections

Connections is Segment's core product offering: you can collect event data from your Sources (mobile apps, websites, and servers) with one API, then pull in contextual data from cloud apps like your CRM, payment systems, and internal databases to build a unified picture of your customers and forward them to Destinations business tools and apps (like Google Analytics, Mixpanel, Customer.io,etc).

Required for HIPAA

Schema Controls
Schema controls help customers in controlling specific events flowing into a Destination. To comply with minimum necessary requirements of HIPAA, customers should define schema controls and pass only those events that are absolutely required by the Destination to perform their job and in accordance with applicable law.

Destination Filters
Destination filters help customers in controlling and filtering event properties, traits and fields flowing into a Destination. Customers building HIPAA compliant workflows must set up Destination filters and pass only those events properties, traits and fields that are absolutely required by the Destination to perform their job and in accordance with applicable law.

Special Considerations for HIPAA

Destinations and Storage Destination
When sending data from Segment to any Destination from the catalog, Customers must ensure that any Destination that will receive and process PHI is HIPAA compliant, including entering into a separate BAA with any third party vendor; otherwise customers must use Destination filters to remove any PHI from flowing into a Destination.

Functions
Functions let you create your own Sources and Destinations directly within your Workspace to bring new types of data into Segment and send data to new tools with just a few lines of JavaScript and no additional infrastructure. It is the customer's responsibility to ensure workflows and use cases built using Functions are HIPAA compliant.

Reverse ETL

Reverse ETL (Extract, Transform, Load) extracts data from your data warehouse and sends it downstream to supported third-party Destinations.

Required for HIPAA

Data Mapping
Mappings enable you to map the data you extract from your Warehouse to the fields in your Destination. Customers building HIPAA compliant workflows must set up Data Mapping and pass only those fields that are absolutely required by the Destination to perform their job and in accordance with applicable law.

Special Considerations for HIPAA

Destinations
When sending data from Segment to any Destination from the catalog, customers must ensure that any Destination that will receive and process PHI is HIPAA compliant, including entering into a BAA with any third party vendor; otherwise, customers must use Data Mapping to remove any PHI from flowing into a Destination.

Segment Unify (formerly known as Profiles)

Segment Unify (formerly known as Profiles) enables customers to view the complete Pprofile of their end -users, including their event history, traits, and identifiers. Segment Unify includes the following functionality: Identity Resolution, Profiles Explorer, Profiles Sync, and Profiles API.

Required for HIPAA

Profile Explorer

Profile Explorer allows customers to view all user data, including their event history, traits, and identifiers. Customers building HIPAA compliant workflows are encouraged to leverage the Privacy Portal to correctly classify PHI data. This will ensure PHI data is automatically masked for users with non-granted access based on defined policy control.

Special Considerations for HIPAA

Profiles Sync

Profiles Sync allows customers to connect identity-resolved end user profiles to your data Warehouse. When sending profile data from Segment to any Destination or Warehouse using Profile Sync, customers must ensure that the data Warehouse is HIPAA compliant, including entering into a BAA with any third party vendor, and obtain necessary consents required for the disclosure of such Customer Data.

Profile API

Profile API provides a single API to read user-level and account-level Customer Data. Profile API allows customers to query the entire user or account object, including the external_ids, traits, and events that make up a user's Profile. When building HIPAA compliant workflows using Profile API, it is the customer's responsibility to understand the role of any third party application / API being used in conjunction with Profile API, enter into a BAA with any third party vendor as necessary, and obtain necessary consents required for the use and disclosure of such Customer Data.

.

Protocols

Segment's Protocols help customers automate and scale data quality best practices by defining a well thought-out Tracking Plan that includes defining, detecting, validating data quality violations and enforcing controls.

Required for HIPAA

Tracking Plan

For customers using Protocols to build HIPAA compliant workflows, customers are required to build a Tracking Plan that enforces strict controls to block non-conforming and non-relevant data and events. If configured to forward non-relevant data and events to a quarantined source, customers should regularly monitor, analyze, review and action such data and events.

Privacy Portal

Special considerations for HIPAA

Privacy Portal

Segment's Privacy Portal helps customers by automatically detecting and maintaining a dynamic inventory of data that they can monitor and enforce their data privacy policies on them. Customers building HIPAA compliant workflows are encouraged to preload PHI data matchers, beyond the default provided, and classify and set any needed policy controls on them. This will ensure PHI data is appropriately blocked from entering Segment and/or automatically masked for users with non-granted access based on defined policy control.

It is also recommended to regularly monitor and classify the newly detected data in the Privacy Inbox. However, the classification (and its associated policies) will only apply to the data on a forward-looking basis; it is the responsibility of the customer to ensure that any PHI that is already in Segment is handled in a compliant manner.

User Deletion and Suppression

In keeping with user privacy and consent, it is the responsibility of the customer to ensure that no data belonging to non-consenting users is sent to Segment. To ensure no data for non-consenting users is accidentally sent to Segment (and subsequently forwarded to Destinations) or to delete and suppress previously sent data, customers are recommended to programmatically or via UI to mark the users for suppression.

Engage Foundations

Powered by real-time data, Engage Foundations is a customizable personalization platform with which you can build, enrich, and activate Audiences.

Engage uses Segment Identity Resolution to take event data from across devices and channels and intelligently merge it into complete user- or account-level profiles. User profiles can be further enriched using Computed traits.

Twilio never shares or sells user data. Engage inherits Segment's holistic approach to security and privacy, using HIPAA compliant standard encryption to safeguard data stores both at rest and in transit.

Required for HIPAA

Engage Destinations
Customers must ensure that any Destination that will receive PHI from Engage is HIPAA compliant (including having a BAA with the Destination vendor, if a third party application); otherwise customers must filter or block any PHI in Engage from flowing into a Destination.

Computed and SQL traits
When using Computed and SQL traits, customers are required to only retrieve PHI data that is necessary for building profiles and audiences.

Not eligible for HIPAA

This section outlines features that are commonly used in conjunction with Engage that may not yet be HIPAA eligible. This does not constitute a comprehensive list of Engage or 3rd party products and services that are not yet HIPAA eligible.

Engage Premier: With Engage Premier, you can build on top of these Audiences, helping you connect with and market to your customers through email and SMS campaigns. Engage Premier is not HIPAA eligible at this time.

Campaigns: With Engage, you can build and analyze performance of email and sms marketing campaigns within Journeys. Building and sending email and SMS campaigns for multi-channel customer engagement using Engage is not currently HIPAA eligible.

Thanks for reading

If you would like to learn more about what Twilio can do for your business, please contact the Twilio sales team or give us a call at 844 814 4627.

Change log

4/27/2023	Added Changes to Segment Experience When Workspace ID(s) designated as HIPAA Project(s)
3/31/2023	Added Reverse ETL, Profiles Sync, and clarification on customer requirements for Segment Unify (formerly known as Profiles)
11/13/2022	Added Twilio Segment
7/13/2022	Added Twilio Flex
3/31/2022	Added Information on Changes to Twilio Experience from HIPAA Accounts; Added Voice Channel to Twilio Frontline
12/17/2021	Added Twilio Frontline and Twilio for Salesforce
9/30/2021	Added MMS; Notice of intent to sunset Programmable Chat
7/9/2021	Added Event Streams
5/28/2021	Added Verify Push as HIPAA Eligible Product
3/3/2021	Removed requirements for HIPAA-eligible Phone Numbers; Added distinction between Private and Public Assets; Added MMS Debugger event
10/23/2020	Added Verify and Lookup
8/21/2020	Added Sync, Programmable Chat, and Twilio Conversations; Added clarification on HIPAA Designated Projects and Subaccounts
6/22/2020	Change to Inbound MMS configurations
5/13/2020	Added Studio and Functions under Runtime Tools, Message Redaction for SMS
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

Millions of software developers use Twilio's platform and communication APIs to help businesses build more meaningful relationships with their customers.