Updated: 04.19.2024.

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 eligible 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 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 highlighted 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 that Twilio may update this document 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 Services without at least 180 days' notice to our customers. Any notice of deprecation or removal will be posted as an update to this document. Any capitalized term used but not defined in this document will have the meaning provided in the BAA and in the applicable product documentation available at https://www.twilio.com/docs and https://www.segment.com/docs.

Designation of HIPAA Projects

Customers looking to build HIPAA eligible workflows on Twilio will need to purchase a Twilio Editions package that contains the product offering HIPAA Accounts in order to designate their accounts, Projects and subaccounts as HIPAA Project(s). Customers that enter into a BAA with Twilio will need to specify which of their accounts, Projects, or subaccounts are designated as HIPAA Projects. Customers may use any Twilio products and services under their designated HIPAA Projects, but workflows that may contain PHI can only be built using HIPAA Eligible Products and Services. Designated HIPAA Projects cannot be used to process, store, or transmit PHI using Twilio products and services that are not explicitly designated as HIPAA Eligible Services.

If an account or 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 Projects. Any subaccounts that existed prior to the signing of the BAA, unless specified in the BAA, will not automatically be designated as HIPAA Projects. If only select subaccounts are designated as HIPAA Projects at the signing of a BAA, then the customer will need to request that any later-created subaccounts be designated as HIPAA Projects. 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 accounts, Projects and subaccounts. For information regarding Twilio Segment, please refer to the Twilio Segment Section of this document.

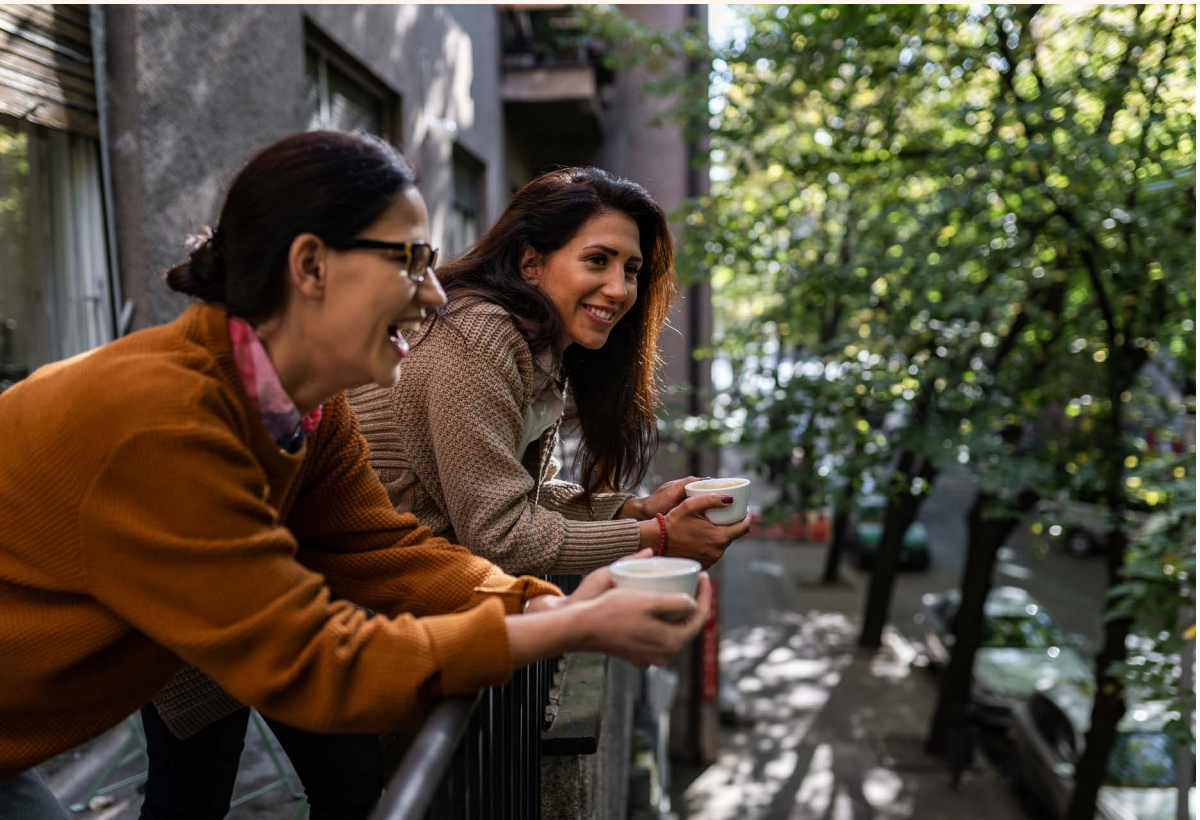
Changes to Twilio Experience from HIPAA Projects

When an account, Project or a subaccount is designated as a HIPAA Project, there are minor changes to the customer's experience using Twilio's products and services.

- The Twilio Console experience for any account, 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 account, Projects or subaccounts designated as a HIPAA Project will be exempt from certain content moderation that Twilio typically conducts. However, 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, enabling the designation of a HIPAA Project may result in product-specific changes, the specifics of which are listed under each product's respective section throughout this document.

CustomerAI for all HIPAA eligible services (Twilio and Twilio Segment products)



Twilio may introduce Services, features or functionalities that utilize artificial intelligence or machine learning technology (AI/ML Feature(s)). At this time, any Services made available by Twilio that incorporate AI/ML Features are not considered HIPAA Eligible Services and should not be used for HIPAA eligible workflows. Twilio's current AI/ML Features are listed below (list not exhaustive):

- Voice Intelligence (Twilio)
- Verify Fraud Guard (Twilio)
- Unified Profiles (Twilio)
- Agent Copilot (Twilio)
- Generative Audiences (Twilio Segment)
- Predictions (Twilio Segment)
- Suggestive Predictive Audiences (Twilio Segment)
- Engage Product Recommendations (Twilio Segment)

Please note that the above product names are subject to change.

Customer requirements for all Twilio products

This section outlines the set of required and recommended best practices for building a HIPAA eligible 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 or using Twilio's APIs. This section identifies the requirements for building HIPAA eligible 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 eligible workflows are required to use HTTPS for making requests to Twilio and for configuring Twilio's requests made to the customer. Note: Twilio cannot currently handle self signed certificates.

Signed webhook requests
Customers building HIPAA eligible workflows are required to ensure that the requests to your web application are 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 Support agents. Customers should use call SIDs or message SIDs (or other Twilio-specific IDs) rather than phone numbers when troubleshooting with Twilio Support.

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 have access. Customers building HIPAA eligible workflows are encouraged to use either tier 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 eligible 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 connected 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 eligible 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 eligible 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 HIPAA Eligible Services are used when developing a workflow with PHI.

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 employees with access to the Twilio Console have the right access credentials and training for handling PHI. Note that Studio cannot be used in conjunction with non-HIPAA Eligible Services.

Functions
Twilio Functions is a serverless environment which empowers developers to quickly and easily create production-grade, event-driven 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 eligible 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 customer 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 to build HIPAA eligible workflows, 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 eligible workflows.

Customer requirements for individual Twilio products

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

Programmable Video

Note: On December 5, 2023 Twilio announced our intent to End of Life Programmable Video effective as of December 5, 2024. As of March 26, 2024, Twilio announced the extension of Twilio Programmable Video End of Life to **December 5, 2026**. Since Twilio will end of life (EOL) this product, it will also no longer be available as a HIPAA Eligible Service as of December 5, 2026. As an alternative, Twilio will be partnering with Zoom to provide its Video SDK as a solution for your video needs. Information on how to migrate to Zoom's Video SDK can be found in the migration guide. Additional information on the Programmable Video EOL is available in Twilio's Help Center here.

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 Services are HIPAA eligible.

Required for HIPAA

HTTP Auth for accessing media recordings
For building a HIPAA eligible workflow using media recordings, customers are required to enforce HTTP basic auth using Twilio account SID 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 one 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 secure 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 eligible 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 with the third party 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 Programmable Voice and SIP that are not yet HIPAA eligible. Only Programmable Voice traffic to and 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 eligible workflow using recordings, customers are required to enforce HTTP basic auth to access media using the account SID and authentication token. This information can be found in the Programmable Voice settings page in the Twilio Console.

Basic SIP security

When exposing a SIP application to the internet, customers should secure their applications against unauthorized access. For building a HIPAA eligible 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 a customer's existing VoIP infrastructure and their TwiML application built using Programmable Voice. When connecting the existing VoIP infrastructure with 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 internet: Transport Layer Security (TLS) and Secure Real-time Protocol (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 eligible workflows, Secure Trunking must be used to enable SRTP to encrypt media and 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 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 eligible 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 a customer retrieves it, ensuring that the recording can only be accessed by the holder of the corresponding private key.

Recording Transcription
Recording Transcription offered directly through Twilio's API is may be used to build HIPAA eligible workflows. However, any transcription services available via the Twilio Marketplace are not HIPAA eligible.

Media Streams
When using Twilio 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 the third party complies with HIPAA and a BAA is obtained from the third party.

Virtual Agent (with Google Dialogflow)
Customers using Virtual Agent (with Google Dialogflow) for HIPAA eligible workflows must execute a BAA with Google, in addition to a BAA with Twilio.

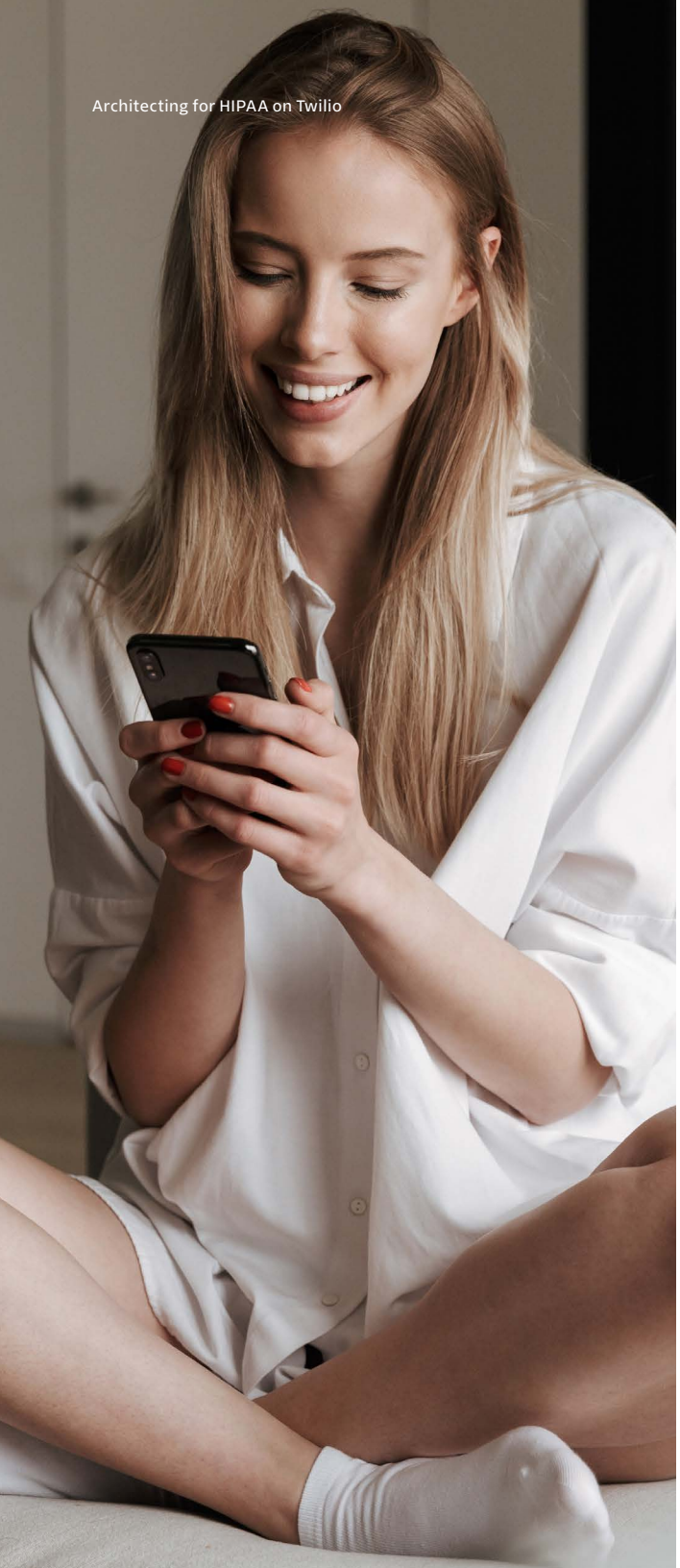
Not eligible for HIPAA

This section outlines features that are commonly used in conjunction with Twilio's Programmable Voice and SIP products that are not HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not 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 is not HIPAA eligible at this time. IVR workflows without Autopilot may be used to build HIPAA eligible workflows.

Voice Intelligence: Voice Intelligence turns customer calls into actionable data insights with AI/ML Features to identify and extract important signals from unstructured voice calls at scale. Voice Intelligence is not a HIPAA Eligible Service at this time.



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 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 eligible workflow using MMS, customers are required to enforce HTTP basic auth on Media URLs using the account SID and authentication token. This can be done in your Twilio Console under Messaging -> Settings -> General.

Special considerations for HIPAA

Messaging Geographic Permissions
Twilio provides customers 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 redaction capabilities: message body redaction and phone number redaction. Enabling Message Body Redaction will prevent the entire message body from being otherwise available in the console, APIs, or Twilio internal support systems after messages are transmitted. Enabling 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 Message Redaction features to protect the privacy of their End Users. Customers can configure these capabilities 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 HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not 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 (also known as SMS Bots): Integration with Autopilot for bot-enabled SMS workflows is not available as a HIPAA Eligible Service 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 customers 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.

Message Tagging: Message Tagging enables customers to attach custom attributes as key value pairs to messages at the point of sending. This feature is built into Twilio's Programmable SMS API and customers can assign any freeform text metadata in JSON key value pairs to messages. Message Tagging enables customers to tag and categorize their SMS, MMS, or Whatsapp campaigns for simplified and enhanced reporting, analysis, and optimization. It is the customer's responsibility to ensure that no data that could be construed as PHI is entered into the custom attributes fields for Message Tagging, including any of the custom attributes that are available to be configured. Message Tagging is not HIPAA eligible 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 a HIPAA Eligible Service, 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 HIPAA eligible.

Required for HIPAA

Private Channels
Channels are the heart of all chat activity within Twilio's products and services. Channel Members send Messages to the Channel, which are then distributed to other Members of the Channel. For building HIPAA eligible 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 HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not 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 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 HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not 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 chatbot): 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 eligible 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 eligible 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 HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not HIPAA eligible.

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

Verify Fraud Guard: Verify Fraud Guard uses automatic SMS fraud detection to block suspicious messages from being sent from your Verify Service. Verify Fraud Guard 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 HIPAA eligible. This does not constitute a comprehensive list of Twilio's products and services that are not 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 customers 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 eligible workflows must execute a BAA with Salesforce, in addition to their 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 Project, 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 Projects 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 if 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 SID and authentication token. This information can be found in the voice settings page in the Twilio 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 eligible 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 eligible 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 customers to control the way the overall app loads, as well as the behavior of individual Flex UI Components. For building a HIPAA eligible 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, but is not limited to, 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 and 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 and should not be used in Flex workflows that are subject to HIPAA.

SendGrid Email: Email in Flex provides native capability of supporting email as a channel in Flex using Twilio SendGrid as the primary mail service provider. It allows agents in contact centers to send and receive messages. Email is available as both an inbound (customer-initiated) and outbound (agent-initiated) channel. Email in Flex is not eligible for HIPAA and should not be used in Flex workflows that are subject to HIPAA.

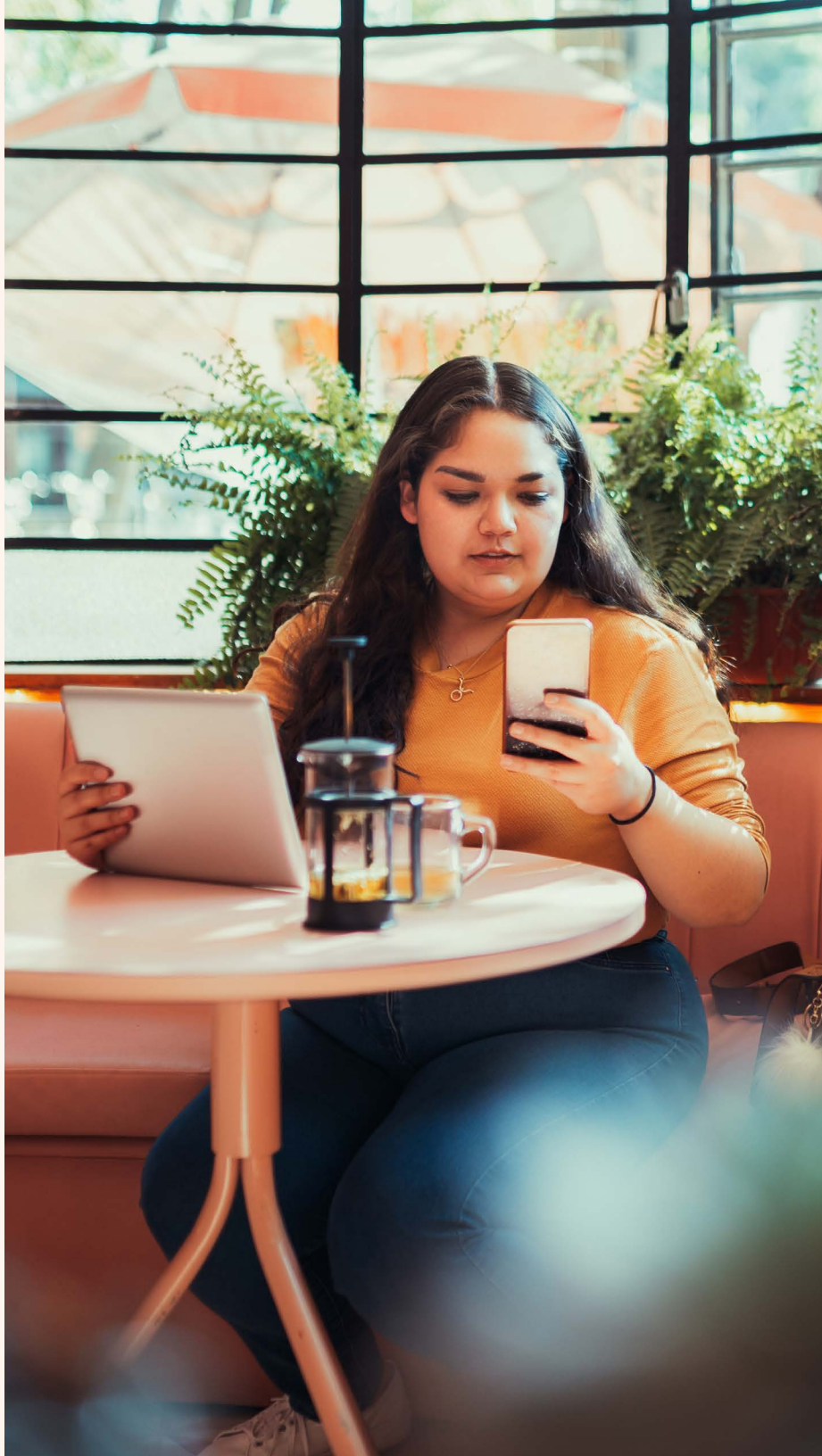
Flex Webchat: Flex Webchat is a chat widget that customers can embed on their websites. The widget helps your customers chat with an agent without leaving your webpage. Flex Webchat is natively integrated with Flex UI and built on Flex Conversations. Flex Webchat is not eligible for HIPAA and should not be used in workflows that are subject to HIPAA.

Unified Profiles: Unified Profiles in Flex provides your agents with real-time customer data from multiple enterprise systems within Flex to provide personalized support based on each customer's history. Unified Profiles in Flex is not eligible for HIPAA and should not be used in Flex workflows that are subject to HIPAA

Agent Copilot: Agent Copilot in Flex provides your agents with post-work automated summaries, disposition codes, and customer sentiment. By automatically generating this information through AI/ML Features, Agent Copilot reduces agents' workload and speeds up their workflows while providing insights based on customer data and interactions. Agent Copilot in Flex is not eligible for HIPAA and should not 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 eligible workflow on Twilio Segment, regardless of which Twilio 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 eligible workflows with Twilio Segment will need to purchase the Segment Healthcare package and specify which of their Twilio Segment Workspace(s) are designated as HIPAA Projects requiring HIPAA eligibility. 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 a HIPAA Project by contacting their Twilio Segment Account Representative or Twilio 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 Twilio 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 Twilio Segment. The Twilio 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 Twilio Segment Console can contain 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 Twilio 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 eligible workflow on Twilio Segment.

Connections

Connections is Twilio 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 the 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 control and filter event properties, traits and fields flowing into a Destination. Customers building HIPAA eligible t 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
When sending data from Twilio 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, or Data Encryption, to encrypt any PHI 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 Twilio 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

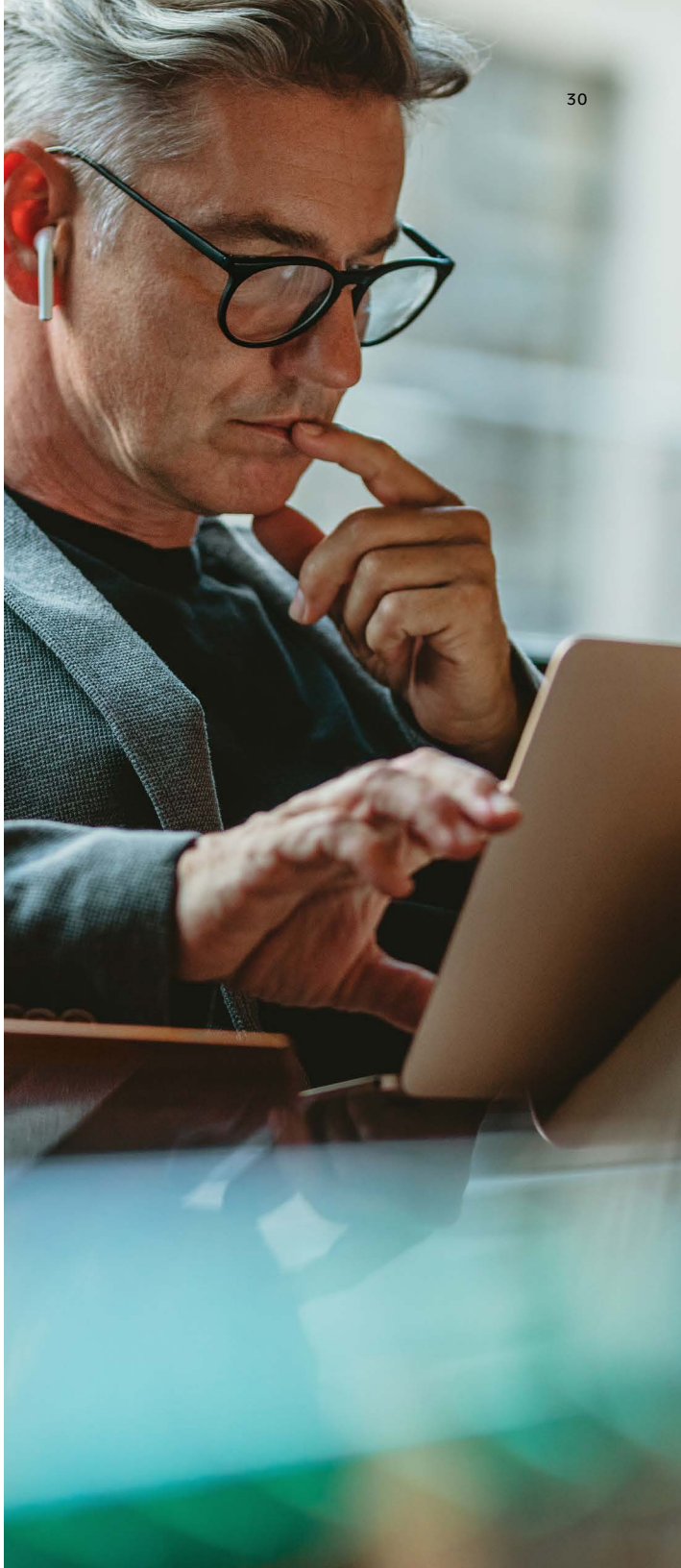
Data mapping

Mappings enable you to map the data you extract from your Warehouse to the fields in your Destination. Customers building HIPAA eligible 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 Twilio 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.



Unify (formerly known as Profiles)

Unify (formerly known as Profiles) enables customers to view the complete Profile 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 eligible 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 eligible 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.

Not eligible for HIPAA

This section outlines features that are commonly used in conjunction with Unify that are not HIPAA eligible. This does not constitute a comprehensive list of Unify or third party products and services that are not HIPAA eligible.

Predictions: With Unify, you can use Twilio Segment's AI/ML Features to predict the likelihood that users will perform any event tracked in Twilio Segment. Twilio Segment saves Predictions or Predictive traits to user profiles, letting you build Audiences, trigger Journeys, and send data to downstream destinations. Predictions is not HIPAA eligible at this time and should not be used in HIPAA eligible workflows.

Protocols

Twilio 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 eligible 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

Twilio 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 eligible 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 Twilio 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 Twilio Segment. To ensure no data for non-consenting users is accidentally sent to Twilio 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 Twilio 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 are not HIPAA eligible. This does not constitute a comprehensive list of Engage or third party products and services that are not 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.

Suggested predictive audiences: Suggested Predictive Audiences is an out-of-the-box Audience template driven by AI/ML Features that can help you improve customer engagement, drive higher conversion rates, and reduce ad spend. Suggested Predictive Audiences is not HIPAA eligible at this time and should not be used in HIPAA eligible workflows.

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.

Generative Audiences: Generative Audiences uses AI/ML Features to create Engage Audiences with natural language prompts. Generative Audiences is not HIPAA eligible at this time and should not be used in HIPAA eligible workflows.

Engage Product Recommendations:
Engage Product Recommendations uses AI/ML Features to build personalized recommendations for marketing teams to add to existing websites, Destinations, email marketing systems, and Audiences. Engage Product Recommendations is not HIPAA eligible at this time and should not be used in HIPAA eligible workflows.

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

April 19, 2024	End of Life notice for Programmable Voice; Added clarification to Virtual Agent (with Google Dialogflow) for Programmable Voice; Added clarification that Verify Fraud Guard and Voice Intelligence are not HIPAA Eligible Services; Added clarification that AI/ML Features are not HIPAA Eligible Services; Added clarification in Twilio Flex that Email in Flex, Flex Webchat, Unified Profiles, Agent Copilot are not HIPAA Eligible Services; Added clarification in Twilio Segment that Predictions, Suggested Predictive Audiences, Generative Audiences, and Engage Product Recommendations are not HIPAA Eligible Services.
September 1, 2023	Added information regarding data encryption for Cloud Mode Destinations for Twilio Segment and Message Tagging for Programmable Voice
April 24, 2023	Added Changes to Segment Experience When Workspace ID(s) designated as HIPAA Project(s)
March 28, 2023	Added Reverse ETL, Profiles Sync and clarification on customer requirements for Segment Unify (formerly known as Profiles)
November 13, 2022	Added Twilio Segment
July 13, 2022	Added Twilio Flex
March 31, 2022	Added Information on Changes to Twilio Experience from HIPAA Accounts; Added Voice Channel to Twilio Frontline
December 17, 2021	Added Twilio Frontline and Twilio for Salesforce
September 30, 2021	Added MMS; Notice of intent to sunset Programmable Chat
July 9, 2021	Added Event Streams
May 28, 2021	Added Verify Push as HIPAA Eligible Product
March 3, 2021	Removed requirements for HIPAA-eligible Phone Numbers; Added distinction between Private and Public Assets; Added MMS Debugger event
October 23, 2020	Added Verify and Lookup
August 21, 2020	Added Sync, Programmable Chat, and Twilio Conversations Added clarification on HIPAA Designated Projects and Subaccounts
June 22, 2020	Change to Inbound MMS configurations
May 13, 2020	Added Studio and Functions under Runtime Tools, Message Redaction for SMS
March 20, 2020	Added Programmable Voice / SIP and Programmable SMS
March 10, 2020	Added clarification on customer requirements for Programmable Video
February 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.