**Where are PureCloud recordings stored?**

PureCloud recordings are stored in your region.

**What can you do?**

can do a lot of things.

## What kind of encryption do we use?

Our public/private keypairs use RSA with key length of 3072. We will only ever only ever have one public key per one private key. We generate a symmetric media key per recording at the source of the recording (E.g. the Edge) to encrypt most of the data using AES256, and then encrypt the media key using our public key.

For more details: [Recording Encryption in the PureCloud Edge and Interaction Media Server](https://genesyslab-my.sharepoint.com/display/MediaGroup/Recording+Encryption+in+the+PureCloud+Edge+and+Interaction+Media+Server)

We also have an open source example of a local key manager. The key generation used in this app is pretty like what we do in the cloud: <https://github.com/MyPureCloud/local-key-manager>

## Where are the public/private keys stored?

Public key metadata can be stored with the recording itself, or in DynamoDb, or cached... or possibly other places. Since the public key is not sensitive, it does not matter very much.  The private key is stored in an s3 bucket with server-side encryption enabled. It is protected from insider attacks by very strict IAM access protection. Only the appropriate machines can access the bucket (no humans).

## What risk is mitigated by rotating keys?

We keep old keypairs in order to decrypt historical recordings, but only use the latest to encrypt new recordings.  Rotating keys is useful for reducing the total number of recordings encrypted by a single encryption key.  If a key (somehow) gets compromised, this means that only the subset of recordings encrypted by that key could potentially be decrypted.  We provide mechanisms that allow customers to define a schedule for us to automatically generate new keys.

## Recording Encryption Lifecycle:

See also: [API and Sequence Diagrams](https://genesyslab-my.sharepoint.com/display/PureCloud/API+and+Sequence+Diagrams)

Encryption service manage the keypairs and publishes the public half for the Edge (and other services) to use for encrypting recordings from the moment they are created.

After a conversation is complete, we have customer defined rules executed by recording service that decide whether or not to keep a recording. In the case where it should not be kept, it is deleted directly from the Edge. For on-premise Edges, this means that the deleted recordings never leave the site. Otherwise, we upload it to aws and store it in s3. In addition to our own encryption, we also use s3 server side encryption on this bucket. The recording remains this way for most of its life. We also have rules that can help customers to delete recordings on a schedule automatically, if they want.

When a recording has been requested for playback, we follow the flow in the diagrams here: [API and Sequence Diagrams](https://genesyslab-my.sharepoint.com/display/PureCloud/API+and+Sequence+Diagrams).  Playback service pulls off the keypairId from the recording and asks (over https) encryption service to unencrypt the data key for that particular recording. Playback and encryption service each have encrypted volumes, and their ELBs will only communicate to other services via https. Each data key is only used for one recording. Once Playback has the data key, it can decrypt the rest of the audio payload of that recording.

Once the file has been decrypted in the cloud, Playback service may do some transcoding on demand, and put the resulting file into an encrypted s3 bucket where it will live for a short time (approximately an hour). We generate a url for this s3 path which is returned to the client. The url will either be a cloudfront url with PureCloud authentication required or a signed s3 url. In both cases, the link itself also expires after a short time (a few minutes).

Encryption for digital (chat, email, etc.) recording is very similar, except that encryption takes place on an EC2 instance instead of on the Edge. Same as with the Edge, these services do not have access to the private keys and are only able to encrypt. They cannot decrypt.

## Key Generation and Management

The master keys used for recording encryption are a public/private key pair.  Using a public/private key pair allows the PureCloud Edge/Interaction Media Server to securely create recordings without necessitating communication with a key management server.  Only the public key is required to create encrypted recordings.  The private key of the pair is only required to decrypt the recording and is never present on the Edge.  Each recording gets a unique 256-bit symmetric Data Encryption Key (DEK).  However, as asymmetric cryptographic operations are relatively expensive, we don't directly encrypt the data encryption key of a recording with the public key.  Instead, we use an intermediary Key Encryption Key (KEK) to encrypt the Data Encryption Key.  The the Key Encryption Key is encrypted with the public key.  The Key Encryption Key is rotated at regular intervals (once per hour by default).  The encrypted DEK and KEK are included in the recording file as metadata in the unencrypted header.  This keeps the recording file as a self-contained unit without the need for separate out-of-band communication or storage to maintain the key.  The following steps describe this process in more detail:

1. The service that wants to perform an encrypted recording supplies the public key with the request to perform a recording.
2. The Edge media service creates a unique 256-bit symmetric Data Encryption Key (DEK).
3. It checks whether it already has a Key Encryption Key (KEK) for the supplied public key and the KEK is not too old (does not have to be rotated.)  If a new KEK is needed, it creates a 256-bit KEK and encrypts it with the public key using RSA-OAEP (PKCS#1v2).
4. It encrypts the DEK with the KEK and combines the encrypted DEK together with the encrypted KEK into a serialized package.  The EAX-AES cryptographic mode of operation is used for encryption of the DEK with the KEK.  This not only encrypts the DEK but allows authentication of the encrypted DEK and associated metadata.  This package thus contains everything that's needed to recover the DEK from the private key associated the public key provided in step #1.
5. This package containing the encrypted keys is stored in the plain-text (un-encrypted header of the recording file.
6. The recording is encrypted with the DEK
7. After the recording completes, the cryptographic context of that recording's DEK is securely wiped from memory.

The following diagram provides a simplified schematic representation of the recording encryption process and the relationship between the public key, DEK, and KEK:

Schematic representation of the recording encryption process

Figure 1: Schematic representation of the recording encryption process

While in memory, all cryptographic keys (other than the public key) that are involved in the encryption operations described above are only held in specialized container objects.  These key containers ensure that the key data are securely wiped from the process memory as soon as they are no longer needed.  This prevents leaking of cryptographic keys into the common process heap memory.  This guarantees that a memory dump of the process contains only the keys and cryptographic contexts that were operationally required at that point it time.

### How to engage the Genesys Privacy Office?

Global:

* Legal request via SFDC for any assistance related to compliance, customers, partners, prospect & vendors.
* For general questions, you can reach the Data Privacy Group at [dataprivacy@genesys.com](mailto:dataprivacy@genesys.com).

EMEA:

For any privacy and/or security contract reviews, a legal DSR must also be opened within SFDC.

### PureCloud Security and Privacy Support

* Assign SC to complete first review using existing tools:
* PureCloud Resource Centre (<https://help.mypurecloud.com/articles/about-security/> & <https://help.mypurecloud.com/articles/legal/>)
* Qvidian RFP tool (<https://genesys.seismic.com/Link/Content/DCSqrrqNAOckyV9kKcsHgTzg>)
* [https://genesyslab.sharepoint.com/_layouts/15/images/icdocx.pngFAQ-Security-Privacy.docx](https://genesyslab.sharepoint.com/sites/EMEACloudSC/SiteAssets/SitePages/ECCC%20Security%20%26%20Privacy/FAQ-Security-Privacy.docx). (Note: You are welcome to download and update this document with additional questions/content,  Please send your feedback to Shahzad Ahmad & Erich Cohen so we can keep on improving this document)
* If required, assigned SC will contact ECCC Program Management Team for additional support via [EMEACloudProgramManagement@genesys.com](mailto:EMEACloudProgramManagement@genesys.com)
* ECCC Team Program Management will assign ECCC Team member
* SC will assign ECCC Team member to the existing DSR as a Virtual Team member
* ECCC Team will contact Information Security & Compliance team as needed
* For any privacy and/or security contract reviews, a legal DSR must also be opened within SFDC

### Privacy Shield Framework

If you are in the European Economic Area (“EEA”) or Switzerland, Genesys and its controlled United States subsidiaries have certified to the EU-U.S. Privacy Shield and U.S.-Swiss Privacy Shield Frameworks for the transfer of Personal Information from the EEA or Switzerland to the United States, as described in our Privacy Shield Privacy Notice. To learn more about the EU-U.S. or U.S.-Swiss Privacy Shield Framework and to view our certification, please visit www.privacyshield.gov.

### What Customer Data does Genesys collect through the PureCloud services?

In general, PureCloud collects information that your organization already stores by connecting with services such as Active Directory and Customer Relationship Management (CRM) software. Additionally, you may choose to provide information to PureCloud, such as through importing your own information from third party websites, uploading files, screensharing, video or audio calls, or chat messages.

Genesys will only collect Customer Data when it is voluntarily made available to us by you or your organization.

### How may we use Personal Data collected through the PureCloud services?

We will use this information to provide PureCloud services to you. For example, we may allow you to share files you provide to use with other members of your organization. As another example, we may allow you to share your screen with other members of your organization.

We will also use this information to comply with your request for information. For example, if you request technical support assistance, we may ask who you are, which services you are using, and in what computer system environment you are using the services to respond to your request as efficiently and effectively as possible. If you are interested in signing up for one of our Webinars, the Customer Data you provide to us will enable us to tailor the Webinar more closely to your specific needs. In addition, from time to time, we may refer to your Customer Data to better understand your needs and how we can improve our products and services. We may use that information to contact you.

As between Genesys and You, You retain ownership of and all intellectual property rights in Customer Data and grant Us a non-exclusive, non-sublicenseable (except to parties working on Our behalf), non-transferable, royalty-free license to access, process, store, transmit, and otherwise make use of the Customer Data as necessary to provide the Services and to otherwise fulfill Our obligations under the Agreement.

You agree that the Customer Data may be transferred or stored outside the country where You and Your customers are in order to carry out the Services and Our other obligations under the Agreement.

You represent and warrant that You have obtained all consents necessary for Us to collect, access, process, store, transmit, and otherwise use Customer Data in accordance with the Agreement.

You shall comply with all requirements of integrity, quality, legality and all other similar aspects in respect of Customer Data. We may, but are not obligated to, review or monitor any Customer Data. We expressly disclaim any duty to review or determine the legality, accuracy or completeness of Customer Data.

We have developed and will maintain a privacy program designed to respect and protect Customer Data under our control. We will not rent or sell any Customer Data.

We may aggregate data and information related to the performance, operation and use of the Cloud Services to create statistical analyses, to perform benchmarking, to perform research and development and to perform other similar activities (“Service Improvements”). We will not incorporate Customer Data in Service Improvements in a form that could identify You or Your customers and we will use industry standard techniques to anonymize Customer Data prior to performing Service Improvements. We retain all intellectual property rights in Service Improvements and may make them publicly available.

### How may you direct or restrict the use of your information?

Certain features, such as screensharing and video chat, allow users to direct the use of their information. For example, when you initiate a screensharing session, you may choose what aspects of your screen to share, who can view those aspects of your screen, and when you want to stop sharing your screen. Your screen will not be shared with users that you do not choose, and aspects of your screen that you choose not to be shared at all will not be shared with any other users.

We will provide you with the opportunity to opt out of (1) any disclosure of your Personal Data to any third party that is not authorized to receive such data (e.g. our Agents); or (2) the use of that data for a purpose other than the purpose for which it was originally collected from, or subsequently authorized by you.

Some Personal Data is considered Sensitive Personal Data, such as any Personal Data that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information that concerns health or sex life, and information about criminal or administrative proceedings and sanctions. We will not disclose Sensitive Personal Data to a third party that is not our Agent or use Sensitive Personal Data for a purpose other than the purpose for which it was originally collected from, or subsequently authorized by, you unless we have received your affirmative and explicit consent to do so (opt-in).

For additional information regarding how you may restrict the use of your Personal Data please contact us at [DataPrivacy@genesys.com](mailto:DataPrivacy@genesys.com).

### What steps will we take before transferring your information to third parties?

PureCloud uses third-party data processors (Agents) around the world to provide certain services, such as a cloud processing, monitoring, and troubleshooting. During their services, the Agents may process Personal Data provided by Genesys, on its behalf and under its instruction. We will obtain assurances from our Agents that they will safeguard Personal Data in accordance with this Privacy Policy.

Such assurances may include:

Requiring our Agent to provide at least the same level of protection as is required under the Privacy Shield Framework;

The use of Model Clauses;

Requiring our Agent to comply with appropriate certain governmental data protection regulations, such as EU Directive 95/46/EC on the protection of individuals about the processing of personal data and on the free movement of such data, or findings of adequacy by the European Commission under Article 25(6) of Data Protection Directive; or,

Requiring our Agent to have their own Privacy Shield certification.

### How can you access, or correct information held about you?

Upon request, we will provide you with reasonable access to the Personal Data that we hold about you except where the burden or expense of providing this access would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated by the provision of such access.

We will take reasonable steps to enable you to correct, amend or delete Personal Data related to you in our possession and control that is inaccurate or incomplete.

### How will your information be protected?

Genesys is committed to protecting the Personal Data entrusted to us. We have implemented appropriate physical, electronic and administrative procedures to safeguard and secure this information from loss, misuse, unauthorized access or disclosure, alteration and destruction.

We will take special care to ensure the security of Sensitive Personal Data. We will use Personal Data only in a way that is compatible with and relevant to the purpose for which it was collected or authorized by you or for other compatible purposes.

To the extent necessary for those purposes, we will take reasonable steps to ensure that Personal Data is relevant to its intended use, accurate, complete, current and reliable for its intended use.

What information may be gathered from children?

The Sites are not intended or designed to attract children under the age of 13. Genesys does not collect personally identifiable data from any person it knows to be under the age of 13.

### What are cookies and how are they used?

Some pages within the Sites may use a technology called “cookies”. A cookie is a token that a server gives to your browser when you access an Internet website. Cookies can store many types of data. Cookies help provide additional functionality to the Sites or to help us analyze site usage more accurately. In all cases in which cookies are used, the cookie will not collect Personal Data except with your explicit permission.

### How will we ensure compliance with this policy?

We will conduct compliance audits of our privacy practices to verify compliance with this Privacy Policy.

Any Genesys employee that we determine has acted in violation of this Privacy Policy will be subject to disciplinary action up to and including termination of employment.

Any questions or concerns regarding our use or disclosure of Personal Data should be addressed to the Genesys legal department at the address given below.

We will investigate and attempt to resolve any complaints and disputes regarding the use and disclosure of Personal Data in accordance with the provisions of this Privacy Policy.

Please contact [DataPrivacy@genesys.com](mailto:DataPrivacy@genesys.com) with any questions or concerns.

### Changes to this Privacy Policy

Any changes we make to this Privacy Policy will be posted on this page. The date the Privacy Policy was last revised is identified at the bottom of the page. If we make material changes to how we treat the Personal Data that falls within the scope of our Privacy Policy, we will notify you by email to the email address specified in your account or through a notice in the PureCloud services.

You are responsible for ensuring we have an up-to-date, active and deliverable email address for you, and for periodically visiting the Site and this Privacy Policy to check for any changes.

Who should you contact if you have any questions concerning this Privacy Policy or the Sites?

We encourage you to contact us to inform us of any complaints or disputes you may have regarding the use of your Personal Data. We will investigate the matter and attempt to resolve the issue quickly.

Please contact us at [DataPrivacy@genesys.com](mailto:DataPrivacy@genesys.com) with any questions or concerns you may have about this Privacy Policy or our use of your Customer Data.

### How to view your security and compliance settings?

1. Click **Admin**.
2. Under Account Settings, click **Organization Settings**.
3. Click the**Settings** tab.
4. Under Security & Compliance, view your compliance settings.
   * The HIPAA setting enables compliance with the Health Insurance Portability and Accountability Act (HIPAA). If your organization requires a HIPAA compliant PureCloud organization, this toggle should be on. For more information, see [HIPAA compliance.](https://help.mypurecloud.com/?p=89254)
   * The PCI DSS setting enables compliance with the Payment Card Industry Data Security Standard (PCI DSS) for handling payment cardholder data. If your organization requires a PCI compliant PureCloud organization, this toggle should be on. For more information, see [PCI DSS compliance](https://help.mypurecloud.com/?p=133895).
5. To enable HIPAA or PCI DSS compliance, contact PureCloud Support.

### GDPR Definitions

The [General Data Protection Regulation](https://gdpr-info.eu/) (GDPR) is a European Union regulation. It articulates the rights of people about the protection of their personal data. It also defines the responsibilities of organizations that collect and process personal data. Generally, the GDPR applies to individuals in the European Union. It deals with the responsibilities for organizations directing business to those individuals. GDPR enforcement begins 25 May 2018. The GDPR “protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”. These fundamental rights include the right to access their personal data, rectify their personal data, and delete their personal data stored by an organization.

A customer is a "**data controller**". Our customers determine the purpose for which and the manner in which any personal data is processed.

Genesys acts as a "**data processor**". This means we process data on behalf of data controllers (our customers).

End-users are "**data subjects**". That's you and me (individuals) as consumers of a service.

For more details on these definitions, open this [link](https://gdpr-info.eu/art-4-gdpr/).

### GDPR Compliance Documentation

* PureEngage Cloud: <https://docs.genesys.com/Documentation/System/latest/SDG/GDPR>
* PureEngage Premise: <https://docs.genesys.com/Documentation/System/latest/SDG/GDPR-Premise>
* PureConnect: <https://my.inin.com/products/cic/Documents/Security_Precautions_TR.pdf> (Chapter 9)
* PureCloud: <https://help.mypurecloud.com/articles/how-is-genesys-purecloud-addressing-gdpr/>
* AltoCloud: <https://altocloud.atlassian.net/wiki/spaces/IN/pages/600768650/GDPR>

### Genesys Privacy Compliance Program Statement

As part of our GDPR compliance program, Genesys created a Privacy office with an appointment of a Global Chief Privacy Officer (Bill William Dummett) and EU based Data Protection Officer (Shahzad Ahmad) early 2017. Our EU & Swiss Privacy Shield certifications are approved and can be found on the following link (<https://www.privacyshield.gov/participant?id=a2zt0000000L0jFAAS&status=Active> ). International Processing across Genesys entities will be assured with the use of EU Standard Model Contract Clauses in the short term before we submit our Binding Cooperate Rules (BCRs) for an approval next year.   We have completed (Data Mapping), Data Privacy Impact Assessment (DPIA) and implementation of mandatory tools/processes for compliance.  This also includes the creation of product features/tools and/or processes to assure the compliance.  We will either provide you the tools or means to fulfill data subject requests or execute them on your behalf. We will be signing the data privacy agreement (DPA) with you in line with Article 28 of GDPR to cover all the details of our obligations as a processor or sub-processor. Please let us know if DPA contract template is required. Our privacy office will be happy to provide more detailed info or answers as/if required.

### Edge security overview

The Edge is a black box appliance with limited capabilities through local access.

You configure the Edge only through the following methods:

* PureCloud administrative user interface
* The Edge LCD (optional)
* The Edge USB Flash Drive (optional)

An Edge device pairs with only a single organization (yours) defined in PureCloud. No other organization defined within PureCloud can access or communicate with a paired Edge device.

An Edge provides no accessibility through other network-based connections, such as remote desktop protocol (RDP), telnet/SecureShell (SSH), web server, File Transfer Protocol (FTP) server, and so on.

The Edge uses hard drives in a RAID-1 configuration and an encrypted file system. Disassembly of the Edge device and removal of the hard drives exposes no customer information.

The advantage of the Edge is that there is no extraneous device maintenance required. All updates and configuration changes are performed through the PureCloud user interface.

### PureCloud Edge cryptography

PureCloud Edge provides the following encryption features:

* RSA certificates with key sizes that meet or exceed NIST and NSA Suite B guidelines
* Private Root Certificate Authorities that are never accessible online
* Ciphers that provide perfect forward secrecy through elliptical curve Diffie-Hellman ephemeral (ECDHE) key agreement
* Multiple independent certificate chains in the PKI to isolate functionality  
  For example, the chain that signs the Pairing certificates is not the chain that signs the Edge Proxy certificates. The following diagram illustrates these certificate chains:

### https://help.mypurecloud.com/wp-content/uploads/2016/03/pcedge-security01.png

### What is PCI DSS?

PCI DSS is a proprietary information security standard for organizations that handle payment card information. The PCI Standard is mandated by payment card brands and administered by the [Payment Card Industry Security Standards Council](https://www.pcisecuritystandards.org/). The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually.

### How has PureCloud’s PCI DSS compliance been validated?

PureCloud’s PCI DSS compliance has been validated by an external Qualified Security Assessor (QSA).

### What level and version of PCI DSS compliance is PureCloud?

PureCloud is Service Provider Level 1 compliant with PCI DSS version 3.2.

### Can I review the PureCloud Attestation of Compliance (AOC) for PCI DSS?

PureCloud may distribute the PCI DSS AOC to interested parties after they execute a non-disclosure agreement (NDA) with PureCloud.

To receive an NDA from PureCloud, contact your Customer Success Manager (CSM) or sales account executive.

### What features and deployment models are PCI DSS compliant?

[Secure Pause](https://help.mypurecloud.com/?p=53210) and [Secure Call Flows](https://help.mypurecloud.com/articles/secure-call-flows/) have been validated by an external Qualified Security Assessor as Level 1 PCI DSS-compliant.  Both Secure Pause and Secure Call Flows are certified for PCI Compliance with either local Edge devices or with virtual edges and PureCloud Voice in any deployment region.

[BYOC (Bring Your Own Carrier) Premises](https://help.mypurecloud.com/?p=152741) is PCI DSS compliant.

[BYOC Cloud](https://help.mypurecloud.com/?p=152702) has **not** yet been validated for PCI DSS compliance.

**Caution:** Using non-PCI DSS-compliant services to store, process, or transmit cardholder data is not covered under the terms of the PureCloud license.

### How can I sign up for PureCloud with PCI DSS compliance?

If you are an administrator, you can check the status of your organization’s PCI compliance by reviewing the PCI DSS compliance setting on the [Manage Organization page: Settings tab](https://help.mypurecloud.com/?p=56928). The PCI DSS compliance setting is sometimes referred to as the PCI DSS toggle.

If your organization requires a PCI-compliant PureCloud organization, please contact [PureCloud Customer Care](https://help.mypurecloud.com/?p=20798).

### What is different in PureCloud with the PCI DSS compliance setting enabled?

PureCloud provides PCI DSS-compliant organizations a similar user interface and user experience as non-PCI DSS-compliant organizations. PCI DSS-compliant organizations disable the logging of DTMF and media capture by the Edge.

**Note:**PureCloud provides the same high level of security to all organizations. PCI DSS-compliant organizations and non-PCI DSS-compliant organizations are equally secure.

### What are my responsibilities for using PureCloud in a PCI DSS-compliant manner?

You and PureCloud share responsibilities for operating PureCloud in a PCI DSS-compliant manner.

First, contact PureCloud to enable the PCI setting, which is found on the [Manage Organization page: Settings tab](https://help.mypurecloud.com/?p=56928).  This setting notifies PureCloud that you intend to use PureCloud for cardholder data transactions.

Next, determine how handle transactions involving cardholder data in PureCloud. You have two options:

* Use [Secure Pause](https://help.mypurecloud.com/?p=53210). When activated, Secure Pause temporarily stops recording to exclude sensitive information, such as entry of a credit card number. Before receiving cardholder data using PureCloud, an agent must always initiate Secure Pause to stop recording. After receiving cardholder data, to resume recording the agent must deactivate Secure Pause.
* Use [Secure Flow](https://help.mypurecloud.com/articles/secure-call-flows/). When activated, a secure flow temporarily prevents system recording or agent access to a caller’s entry of sensitive information, such as cardholder data. Before receiving cardholder data using PureCloud, an agent must [transfer a call to a Secure Flow](https://help.mypurecloud.com/articles/transfer-secure-call-flow-action/). After cardholder data has been received, the call may be transferred back to the agent.

If you are using an Edge, you must choose TLS v1.1 or TLS v1.2 for authentication.

More information about your responsibilities can be found at [PCI DSS customer responsibility matrix](https://help.mypurecloud.com/?p=113619).

### What is HIPAA?

The [Health Insurance Portability and Accountability Act (HIPAA)](http://www.hhs.gov/hipaa) is a United States federal law that was originally passed in 1996 and includes subsequent additions passed in the years since. Because HIPAA is a U.S. Federal Law, it only governs transactions or entities within the United States and is not an international law or standard.

HIPAA was designed to regulate both health insurance plans (Title I) and the privacy and security of health information (Title II), among other things. The Privacy Rule in Title II regulates the use and disclosure of protected health information (PHI). The Security Rule in Title II complements the Privacy Rule and lays out administrative, physical, and technical safeguards required for HIPAA compliance.

### What is a business associate and a BAA?

[Covered entities, which include health care providers, health plan providers, and health care clearinghouses](http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html), may engage PureCloud in the role of a business associate to help carry out their health care activities and functions. Business associates include entities that perform functions or activities on behalf of, or provide certain services to covered entities, such as creating, receiving, maintaining, and/or transmitting protected health information.

Generally, covered entities using the services of a business associate must have a written business associate agreement (BAA) with each business associate. A BAA should ensure that business associates will appropriately safeguard protected health information and should also clarify and limit the permissible uses and disclosures of protected health information by the business associate.

### Is PureCloud HIPAA-certified?

There is no HIPAA certification for a cloud services provider such as PureCloud. However, PureCloud has undergone an independent audit which verified our administrative, physical, and technical controls.

As a potential business associate to covered entities, PureCloud is required to implement the administrative, physical, and technical controls required for HIPAA compliance. For details about these controls, the PureCloud security program, network security and more, see [Security and compliance](https://help.mypurecloud.com/?p=31212).

### Is PureCloud HIPAA-compliant?

PureCloud features are HIPAA-compliant with the following exceptions:

* ACD emails
* SMS messages

**Caution:** Using non-HIPAA compliant services to transmit ePHI is not covered under the terms of the PureCloud BAA.

### Where does PureCloud support HIPAA compliance?

HIPAA compliance is available in the Amazon Web Services (AWS) US-East region.

### Does PureCloud have a business associate agreement with Amazon?

Yes. This agreement helps ensure that your customer data is fully protected.

### What is different in PureCloud with HIPAA compliance enabled?

PureCloud provides HIPAA-compliant organizations a similar user interface and user experience as non-HIPAA compliant organizations. However, some PureCloud features work differently for HIPAA-compliant organizations:

* In HIPAA-compliant organizations, PureCloud does not send email notifications to inform users of new voicemails, including personal and group ring voicemails. PureCloud users in HIPAA-compliance organizations will continue to receive in-app notifications for new voicemails, and can listen to voicemails by accessing their inbox.
* SMS messages are not HIPAA-compliant and should not be used to transmit ePHI.

**Note:**PureCloud provides the same high level of security to all organizations. HIPAA-compliant organizations and non-HIPAA compliant organizations are equally secure.

### How do I sign up for PureCloud with HIPAA compliance?

All HIPAA PureCloud organizations require a valid business associate agreement with PureCloud.  When a business associate agreement is signed by all parties, PureCloud will set a HIPAA toggle for your organization.

If you are an administrator, you can check the status your organization’s HIPAA compliance by reviewing the HIPAA setting toggle on the [Manage Organization page:Settings tab](https://help.mypurecloud.com/?p=56928).

## How do I set up a business associate agreement with PureCloud?

To receive a BAA from PureCloud, [contact us](http://www.genesys.com/about/contact-us).

### Can I enable HIPAA compliance on an existing PureCloud organization?

If you are an administrator, you can check the status your organization’s HIPAA compliance by reviewing the HIPAA setting toggle on the [Manage Organization page:Settings tab](https://help.mypurecloud.com/?p=56928). If you need to enable HIPAA compliance, [contact us](http://www.genesys.com/about/contact-us).

### Can I use non-compliant services with HIPAA compliance enabled?

Yes. However, using non-HIPAA compliant services to transmit electronic protected health information is not covered by the PureCloud BAA and may be a violation of HIPAA regulations. For more information, [contact us](http://www.genesys.com/about/contact-us).

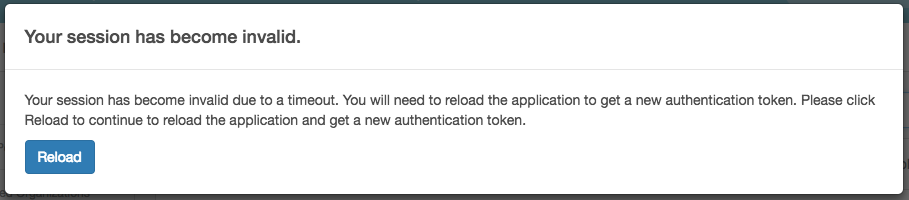
### Do I have any responsibilities for using PureCloud in a HIPAA-compliant manner?

PureCloud customers:

* Must enforce an inactivity timeout on user workstations to meet organizational policy.

The PureCloud API does have a HIPAA idle timeout. But applications, including the PureCloud user interface, can make requests on behalf of the user while the user is idle. These requests include fetching data to keep the application up to date or saving application logs. A request resets the HIPPA API timeout.

When Using the PureCloud web or desktop applications, if the user is idle longer than the API timeout, the user will see the following message prompting them to re-authenticate.



**Caution:**The only way to guarantee the inactivity timeout required by HIPPA is an operating system level lockout on the user workstation. PureCloud recommends a 15-minute inactivity timeout on user workstations.

* Should use Full Disk Encryption.

PureCloud may store a Session Token in local storage on client devices so that PureCloud sessions can survive browsers that are frequently closed and reopened.

### PureCloud Service Terms and Conditions for Security

This PureCloud Security Policy is incorporated by this reference into your PureCloud Service Terms and Conditions agreement with Us and describes the contractual requirements for information security and data protection provided by Us to You related to the provision of PureCloud Services that You have licensed from Us. This PureCloud Security Policy is applicable to the extent that We have access and control over Customer Data.

**1 SECURITY PROGRAM**

1.1 Security Standards. We have implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect Customer Data as appropriate to the nature and scope of the PureCloud Services provided.

1.2 Security Awareness and Training. We have developed and will maintain an information security and awareness program that is delivered to all employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass.

1.3 Policies and Procedures. We will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed annually and updated as necessary.

1.4 Change Management. We will utilize a change management process based on industry standards to ensure that all changes to Your environment are appropriately reviewed, tested, and approved.

1.5 Data Storage and Backup. We will create backups of critical Customer Data according to documented backup procedures. Customer Data will be stored and maintained solely on designated backup storage media within the Data Center(s). Backup data will not be stored on portable media. Customer Data stored on backup media will be protected from unauthorized access

1.6 Anti-Virus and Anti-Malware Protection. We will utilize industry standard anti-virus and anti-malware protection solutions to ensure that all non-Linux servers in Your Cloud Service environment are appropriately protected against malicious software such as trojan horses, viruses, and worms. We will use standard industry practice to ensure that the PureCloud Services as delivered to You does not include any program, routine, subroutine, or data (including malicious software or “malware,” viruses, worms, and Trojan Horses) that are designed to disrupt the proper operation of the PureCloud Services, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause the PureCloud Services to be destroyed, damaged or rendered inoperable. You acknowledge that the use of license keys will not be a breach of this section.

1.7 Vulnerability and Patch Management. We will maintain a vulnerability management program that ensures compliance with the standards of Our information security program.

1.8 Data Destruction. We and Our subcontractors will follow industry standard processes to destroy obsolete data and retired equipment that formerly held Customer Data.

1.9 Penetration Testing. On at least an annual basis, We will conduct a vulnerability assessment and penetration testing engagement with an independent qualified vendor. Issues identified during the engagement will be appropriately addressed within a reasonable time-frame commensurate with the identified risk level of the issue. A cleansed version of the executive summary of the test results will be made available to You upon written request and will be subject to non-disclosure and confidentiality agreements.

**2 NETWORK SECURITY**

2.1 Network Controls. We will employ effective network security controls based on industry standards to ensure that Customer Data is segmented and isolated from other customer environments within the Data Center. Controls include, but are not limited to:

(A) Firewall Services. We use firewall services to protect the PureCloud Services infrastructure. We maintain granular ingress and egress rules and changes must be approved through Our change management system.

(B) Intrusion Detection System. We have implemented intrusion detection systems across the PureCloud Services environments which may be either network based, host based or a combination of the two.

(C) No Wireless Networks. We will not use wireless networks within the Data Center environments.

(D) Data Connections between You and the PureCloud Services Environment. We use TLS, VPN and/or MPLS circuits to secure connections between browsers, client apps, and mobile apps to the PureCloud Services. Connections traversing an untrusted network (e.g. the Internet) will use TLS.

(E) Data Connections between PureCloud Services Environment and Third Parties. Transmission or exchange of Customer Data with You and any third parties authorized by You to receive the Customer Data will be conducted using secure methods (e.g. TLS, HTTPS, SFTP).

(F) Encrypted Recordings. We encrypt call recordings and chat sessions. We may elect to implement a unique password, known only to You, to protect the encryption keys used to secure the call recordings and chat sessions. You are responsible for keeping sensitive data out of the recordings via the PureCloud Services interface, such as using the pause functionality.

(G) Encryption Protection. We use industry standard methods to support encryption.

(H) Logging and Monitoring. We will log security events from the operating perspective for all servers providing the PureCloud Services to You. We will monitor and investigate events that may indicate a security incident or problem. Event records will be retained one year.

**3 USER ACCESS CONTROL**

3.1 Access Control. We will implement appropriate access controls to ensure only authorized Users have access to Customer Data within the PureCloud Services environment.

3.2 Your User Access. You are responsible for managing User access controls within the application. You define the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for its users. You are entirely responsible for any failure by itself, its agents, contractors or employees (including without limitation all its users) to maintain the security of all usernames, passwords and other account information under its control. Except in the event of a security lapse caused by Our gross negligence or willful action or inaction, You are entirely responsible for all use of the PureCloud Services through Your usernames and passwords whether or not authorized by You and all charges resulting from such use. You will immediately notify Us if You become aware of any unauthorized use of the PureCloud Services.

3.3 Our User Access. We will create individual User accounts for each of Our employees or contractors that have a business need to access Customer Data or Your systems within the PureCloud Services environment. The following guidelines will be followed regarding Our user account management:

(A) User accounts are requested and authorized by Our management.

(B) Strong password controls are systematically enforced.

(C) Connections are required to be made via secure VPN using strong passwords that expire every ninety (90) days.

(D) Session time-outs are systematically enforced.

(E) User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

**4 BUSINESS CONTINUITY AND DISASTER RECOVERY**

4.1 Disruption Protection. The PureCloud Services will be deployed and configured in a high-availability design and the PureCloud Services will be deployed across separate Data Centers to provide optimal availability of the PureCloud Services. The Data Center environment is physically separated from Our corporate network environment so that a disruption event involving the corporate environment does not impact the availability of the PureCloud Services.

4.2 Business Continuity. We will maintain a corporate business continuity plan designed to ensure that ongoing monitoring and support services will continue in the event of a disruption event involving the corporate environment.

4.3 Disaster Recovery. The PureCloud Services will be deployed in a high-availability, redundant design. For the PureEngage Cloud, PureConnect Cloud and Outbound Communication PureCloud Services, a disruption event at a single Data Center will trigger a system fail-over to the back-up Data Center to minimize disruption to the PureCloud Services. For these PureCloud Services, You are responsible for defining specific parameters regarding fail-over. With regard to the PureCloud Service, We employ an active-active-active configuration.

**5 SECURITY INCIDENT RESPONSE**

5.1 Security Incident Response Program. We will maintain a Security Incident response program based on industry standards designed to identify and respond to suspected and actual Security Incidents involving Customer Data. The program will be reviewed, tested and, if necessary, updated on at least an annual basis. “Security Incident” means a confirmed event resulting in the unauthorized use, deletion, modification, disclosure, or access to Customer Data.

5.2 Notification. In the event of a Security Incident or other security event requiring notification under applicable law, We will notify You within thirty-six (36) hours and will reasonably cooperate so that You can make any required notifications relating to such event, unless We are specifically requested by law enforcement or a court order not to do so.

5.3 Notification Details. We will provide the following details regarding any Security Incidents to You: (i) date that the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions We have already taken; (iv) corrective measures to be taken; and (v) evaluation of alternatives and next steps.

5.4 Ongoing Communications. We will continue providing appropriate status reports to You regarding the resolution of the Security Incident, continually work in good faith to correct the Security Incident and to prevent future such Security Incidents. We will cooperate, as reasonably requested by You, to further investigate and resolve the Security Incident.

**6 DATA CENTER PROTECTIONS**

6.1 Data Center. We contract with third-party providers for Data Center space. Data Center providers and related services are reviewed on an annual basis to ensure that they continue to meet Our needs and Yours. Each Data Center provider maintains certification based on its independent business models. Security and compliance certifications and/or attestation reports for the Data Center(s) relevant to Your PureCloud Services will be provided upon written request and may require additional non-disclosure agreements to be executed.

6.2 Physical Security. Each Data Center is housed within a secure and hardened facility with the following minimum physical security requirements: (a) secured and monitored points of entry; (b) surveillance cameras in facility; (c) on-site access validation with identity check; (d) access only to persons on an access list approved by Us; (e) on-site network operations center staffed 24x7x365.

6.3 Environmental Controls. Each Data Center is equipped to provide redundant external electrical power sources, redundant uninterruptible power supplies, backup generator power and redundant temperature and humidity controls.

**7 Use of the PureCloud Services**

7.1 You will not, and will not permit or authorize others to, use the PureCloud Services for any of the following: (i) to violate applicable Law; (ii) to transmit Malicious Code; (iii) to transmit 911 or any emergency services (or reconfigure to support or provide such use); (iv) to interfere with, unreasonably burden, or disrupt the integrity or performance of the PureCloud Services or third-party data contained therein; (v) to attempt to gain unauthorized access to systems or networks; or (vi) to provide the PureCloud Services to non-User third parties, including, by resale, license, lend or lease.

7.2 You will use commercially reasonable efforts to prevent and/or block any prohibited use by Users.

7.3 You will maintain any reasonable, appropriate administrative, physical, and technical level of security regarding its account ID, password, antivirus and firewall protections, and connectivity with the PureCloud Services.

7.4 You shall maintain strict security over all VoIP Services lines. You acknowledge that We do not provide You the ability to reach 911 or other emergency services and You agree to inform any individuals who may be present where the PureCloud Services are used, or who use the PureCloud Services, of the non-availability of 911 or other emergency dialing.

7.5 If the PureCloud Services will be used to transmit or process Personal Data, You will ensure that all Personal Data is captured and used solely via the use of available Security Features.

7.6 Recordings. As between Us and You, You acknowledge that use of Recordings is solely within Your discretion and control. Without limiting the foregoing: (i) You accept sole responsibility for determining the method and manner of performing recording such that it is compliant with all applicable Laws and for instructing the services accordingly; and (ii) You shall ensure that Recordings shall be made only for diagnostic, quality assurance, archival, and/or Support purposes, and in any event only for purposes required and/or in compliance with, all applicable Laws. You will ensure that (a) Recordings will not knowingly include any bank account number, credit card number, authentication code, Social Security number or Personal Data, except as allowed or required by all applicable Laws; or (v) Recordings are encrypted at all times. To the extent Recordings are encrypted or where encryption is electable by You as part of the PureCloud Services, You shall elect such encryption. You shall not modify, disable, or circumvent the Recording encryption feature within the PureCloud Services and shall otherwise ensure that it will use the PureCloud Services in compliance with the encryption feature.

**8. Industry-Specific Certifications.**

Our security and operational controls are based on industry standard practices and are certified to meet the guidelines indicated in the table below. Nevertheless, you are solely responsible for achieving and maintaining any industry-specific certifications required for your business:

| **Cloud Service** | **PCI** | **SOC2 TYPE II** | **ISO 27001** | **HIPAA** | **SIG FULL** | **SIG LITE** | **PRIVACY SHIELD** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PureCloud | Yes | Yes |  | Yes |  | Yes | Yes |

**9. Audits.**

Subject to Our reasonable confidentiality and information security policies, You or a qualified third party chosen by You, shall have the right, not more than once a year and upon thirty (30) days’ written notice, to perform a security assessment of Our compliance with the terms of this Schedule I, provided that You have demonstrated that You have a reasonable belief that We are not in compliance. During normal business hours, You or Your authorized representatives may inspect Our policies and practices implemented to comply with this Schedule I, which may include a site visit and a review of reasonable supporting documentation, if you agree that such right shall not include the right to on-site inspections or audits of Our third-party hosting facilities and equipment. No such assessment shall violate Our obligations of confidentiality to customers or reveal Our Intellectual Property. Any assessment performed pursuant to this Section shall not interfere with the normal conduct of Our business. We shall cooperate in a commercially reasonable manner with any such assessment and reserve the right to charge You for Our reasonable costs incurred in connection with any such assessment.

**10. PRIVACY**

We have developed and will maintain a privacy program designed to respect and protect Customer Data under our control, and this is located at https://help.mypurecloud.com/articles/purecloud-privacy-policy/.

**11. CUSTOMER DATA**

11.1 As between Genesys and You, You retain ownership of and all intellectual property rights in Customer Data and grant Us a non-exclusive, non-sublicenseable (except to parties working on Our behalf), non-transferable, royalty-free license to access, process, store, transmit, and otherwise make use of the Customer Data as necessary to provide the Services and to otherwise fulfil Our obligations under the Agreement.

11.2 You agree that the Customer Data may be transferred or stored outside the country where You and Your customers are located in order to carry out the Services and Our other obligations under the Agreement.

11.3 You represent and warrant that You have obtained all consents necessary for Us to collect, access, process, store, transmit, and otherwise use Customer Data in accordance with the Agreement.

You shall comply with all requirements of integrity, quality, legality and all other similar aspects in respect of Customer Data. We may, but are not obligated to, review or monitor any Customer Data. We expressly disclaim any duty to review or determine the legality, accuracy or completeness of Customer Data.

11.4 We have developed and will maintain a privacy program designed to respect and protect Customer Data under our control. We will not rent or sell any Customer Data.

11.5 We may aggregate data and information related to the performance, operation and use of the Cloud Services to create statistical analyses, to perform benchmarking, to perform research and development and to perform other similar activities (“Service Improvements”). We will not incorporate Customer Data in Service Improvements in a form that could identify You or Your customers and we will use industry standard techniques to anonymize Customer Data prior to performing Service Improvements. We retain all intellectual property rights in Service Improvements and may make them publicly available.