

nVoq Platform Data Persistence

FAQs

Can nVoq dictation data be persisted?

The answer is Yes, and it is completely configurable by customer need. Each customer's tenant database within the nVoq production platform will default to save dictation data, but this can be changed as required. Therefore, customers can choose to save end user dictation audio and transcribed text for up to a full year or decide to not persist data at all. Also, persistence intervals for tenant data can be updated at any time. *nVoq would recommend persisting data for all new users for at least 1 year, to improve dictation accuracy and troubleshoot end user concerns.*

Why would I want my data persisted?

By persisting the audio and text for a speaker on the nVoq platform, additional steps can be taken to improve dictation accuracy for the speaker. Specifically, a Review and Correct function can be applied to the end user's account, if requested. This feature improves dictation accuracy by correcting transcription errors and applying the de-identified corrections to the speaker's voice profile. The de-identified corrections can also be crowd sourced by the nVoq system and applied to dictation topics to further improve dictation accuracy for speakers using that topic.

Who has access to my data?

Access to customer data is closely controlled and highly configurable. By deciding who has administrative access to their tenant, each customer controls who has access to their end user data. By default, the nVoq System Administration team will have access to persisted data in your tenant for data administration purposes, but they can be instructed to not view your data, as required.

How is my data secured?

Data is transmitted to and from nVoq servers using industry standard SSL/TLS encryption. nVoq uses a minimum of 128-bit encryption for any data in motion and 256-bit encryption for any data at rest. This is the same level of security employed by major financial institutions, and compliant with HIPAA and HITECH requirements.

Each nVoq tenant has its own independent database. In the United States, nVoq systems are hosted within US-based data centers and are backed up to other US facilities for disaster recovery purposes. All nVoq backup data is also encrypted with AES-256. Any nVoq service provided to customers outside of the US is subject to similar local data security laws and requirements.

Is the nVoq platform HIPAA compliant?

Yes, the nVoq platform conforms to standards that comply with HIPAA and the HITECH Act. nVoq production systems and associated nVoq policies and procedures are annually assessed for PCI-DSS Level 1 compliance. PCI-DSS standards comply and/or exceed both HIPAA and HITECH Act requirements.

PCI-DSS is a data security standard developed by the Payment Card Industry, which contains detailed criteria, policies, and procedures for secure IT systems to follow. Both a PCI-DSS Certificate of Compliance as well as an nVoq Business Associate Agreement (BAA) are available upon request.

Where is nVoq platform data stored?

nVoq platform data is stored in the country of origin. Therefore, for US based customers, the data is stored on US-based servers and backup facilities. For Canadian customers, the data is stored on Canadian servers and backup facilities. All nVoq platform data stays within the borders of the respective country of origin, throughout its lifetime.

Can I self-host the nVoq platform?

No, we do not generally offer SayIt in a self-hosted configuration for end-customer deployment.