nVoq AI: Data Security and Privacy Explained

nVoq AI
Transforming Clinical Documentation

Many of the AI features used in nVoq's products are developed by and proprietary to nVoq. Some AI capabilities also leverage strategic partnerships with providers like OpenAI. These interactions occur exclusively through secure APIs with zero-retention policies, ensuring that data is processed temporarily and never stored or used for model training.

Regardless of the development method, here's what stays constant:

- ✓ **No Protected Health Information (PHI) is used to train our AI models**
- ✓ **Data is never stored or used to improve third-party models**
- ✓ **All generative AI features are opt-in and fully under your control**

AI Technologies Used in nVoq Products and Platforms

MACHINE LEARNING ALGORITHMS

nVoq uses neural networks for core speech recognition. These models are trained on a combination of publicly available open-domain datasets and nVoq's own curated datasets. No data used for training includes Protected Health Information (PHI).

NATURAL LANGUAGE PROCESSING (NLP)

nVoq uses a combination of commercial, open-source, and proprietary models to support its text processing capabilities. Any data shared with third parties is protected by a Business Associate Agreement (BAA), which prohibits the retention or use of data for model training purposes. All models—whether open-source or proprietary—are hosted securely in nVoq's AWS environment and managed under audited security and privacy standards.

ROBOTIC PROCESS AUTOMATION (RPA)

nVoq is developing a clinician-guided automation tool designed to assist with populating Electronic Health Records (EHRs) using a "human-in-the-loop" approach. Unlike traditional RPA tools that operate in the background, nVoq's solution interacts directly with the user interface through local operating system APIs, providing full transparency to clinicians.

GENERATIVE AI (LLMS)

When using generative AI features powered by large language models (LLMs), nVoq connects to trusted partners like OpenAI through zero-retention API calls, ensuring no customer data is stored or used for training generalized models. For customers who opt to train models on their own data, only de-identified data is used. The resulting models are fully siloed—accessible exclusively to that customer and not shared across tenants.

PREDICTIVE ANALYTICS- Not currently in use within nVoq's platform.
DECISION SUPPORT- Not a component of nVoq's AI capabilities currently.

Use of Specialized Language Models (SLMs)

nVoq uses Specialized Language Models (SLMs), for speech recognition, trained only on data that has been thoroughly validated to exclude PHI. All training data is either:

- Reviewed by medical transcriptionists to confirm that it contains no PHI, or
- Processed through redundant PHI removal tools

nVoq does not use any data containing PHI to train its AI models. As a result, SLMs are free of patient-identifiable information.

nVoq AI: Data Security and Privacy Explained

Handling of Customer Confidential Data (CCD)

nVoq's AI tools may use proprietary LLMs, SLMs, or secure third-party services such as OpenAI. Any CCD that could contain PHI is:

- Isolated in tenant-specific environments
- Inaccessible to other customers
- Not accessible by third-party vendors for model training or product improvement

For added protection, your clinicians' prompts (inputs), responses (outputs), embeddings, and training data:

- Are not visible to other clients
- Are not shared with third parties
- Are not used to improve third-party models

Data Domiciling by Region

- U.S. data remains within the United States.
- Canadian data remains within Canada.

This supports compliance with data residency regulations and organizational policies.

Personal Data Processed

nVoq's AI features may use a subset of personally identifiable data from your nVoq instance. This includes:

- Names of patients, clinicians, caregivers, and family members
- Clinical data associated with the patient and their case

The data processed is determined by what is spoken by the clinician or included in a transcribed discussion.

Purpose and Use of Personal Data

All generative AI features use personally identifiable data solely to deliver the specific feature to the client.

- Data is not shared with other clients or vendors
- Vendor agreements prohibit data persistence or training use

Data Retention Policy for Vendors

All vendors supporting generative AI features follow a Zero Data Retention (ZDR) policy:

- Data is deleted immediately after a query response is delivered
- No data is stored post-response

Protection Against Data Leakage Between Clients

Generative AI features are deployed within a client's isolated instance.

- No other nVoq client can access that data
- All interactions remain private to the client environment

Opt-In Functionality for Generative AI

- Generative AI features are on-demand
- Clients can choose to use—or not use—them at any time
- Opt-out is as simple as discontinuing feature use

Feature-Specific AI Practices

CLINICAL NOTE AUDIT TOOLS

These tools combine nVoq's core models with customer-defined rules to identify potential documentation gaps. All rules are secured within nVoq's multi-tenant architecture, providing isolation and protection.

INTELLIGENT FORMATTING

This capability uses large language models (LLMs) to format dictated text into clear, structured documentation. Its limited, well-defined scope reduces common AI risks such as hallucination or bias.