nVoq and HIPAA

OVERVIEW

About nVoq

- www.nvoq.com
- 1790 38th Street, Suite 105
  Boulder, CO 80301
- Providing true cloud-based speech recognition solutions purposefully built for home health and hospice markets

nVoq Platform and Services:

There are three access points to the nVoq service:

1. The end-user client used for dictations, workflow shortcuts, and automations- Only dictations should contain Personal Health Information (PHI). Data sent to and received from nVoq is designed to be transmitted securely (see below).
2. The SDK/API used by other programs and services (primarily for dictations and automations)- Only dictations or sentence modeling submitted or received via the API or SDK may contain PHI. Data sent via the API or SDK is designed to be transmitted securely (see below).
3. The nVoq Administrative Console- nVoq administrators are subject to access privileges, i.e., they can only see data for which they affirmatively have (access) privileges. All data sent to and from the Administrative Console is designed to be transmitted securely.

Data Security for nVoq is handled as follows:

1. Data is transmitted to and from nVoq servers using industry standard SSL/TLS encryption. nVoq uses a minimum of 128-bit encryption — the same level of security employed by major financial institutions.
2. nVoq transcription data is encrypted with AES-256 before being written to a database. Each nVoq tenant has its own independent database. In the United States, nVoq is hosted on the AWS cloud within multiple US-based availability zones for redundancy and the data is replicated to another US-based AWS region for disaster recovery purposes. Any nVoq service provided to customers in Canada are subject to local data security laws and requirements.
3. nVoq systems and associated nVoq policies and procedures are audited for SOC2 Type 2 compliance, with enhanced reporting for HIPAA in the US and PIPEDA in Canada. System and Organization Controls (SOC) 2 is a comprehensive reporting framework developed by the American Institute of Certified Public Accountants (AICPA) in which independent, third-party auditors (i.e., CPA's) for an assessment and subsequent testing of controls relating to the 5 Trust Services Criteria (TSC), of which nVoq is audited for Security, Availability, Confidentiality and Privacy. The SOC2 report is available to customers and prospects on request and upon completion of a non-disclosure agreement.
4. nVoq engages an independent third party to conduct regular penetration tests of our production systems. Penetration test results and a logical network topology diagram of production systems are both available to customers under non-disclosure agreement on request.

NVOQ PERSONNEL AND PHI:
nVoq personnel may work with PHI on their nVoq issued laptop, while supporting nVoq customers and the nVoq platform. All employees have AES 256-bit, Full Disk Encryption (FDE) on their laptops and workstations. If an employee laptop is lost or stolen, the data on the laptop's drive is rendered inaccessible. Encryption management and drive locking is provided by Microsoft Bitlocker, Apple FileVault, or other similar industry recognized tools.

nVoq work which involves PHI is handled as follows:

1. Customers shall redact PHI before sending transcripts to be used in language modeling.
2. Language modeling materials are uploaded (securely) through the Administrative Console. Customers who wish to send transcripts (redacted or otherwise) are required to use a HIPAA compliant service such as Box.
3. nVoq personnel who work with data that may contain PHI on their computers must have encrypted hard drives designed to protect the data, strong passwords and the data must be deleted after use.

02/27/2023