nVoq and HIPAA

About nVoq

- www.sayit.nvoq.com
- 4775 Walnut Street, Suite 104
  Boulder, CO 80301
- Providing true cloud-based speech recognition solutions for healthcare, customer care and other industries.

SayIt:

There are three access points to the SayIt 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 SayIt 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 should contain PHI. Data sent via the API or SDK is designed to be transmitted securely (see below).
3. The SayIt Administrative Console. SayIt 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 SayIt is handled as follows:

1. Data is designed to be transmitted to and from SayIt servers using industry standard SSL/TLS encryption. SayIt uses a minimum of 128-bit encryption — the same level of security employed by major financial institutions.
2. SayIt transcription data is encrypted with AES-256 before being written to a database. Each SayIt tenant has its own independent database. In the United States, SayIt is hosted by nVoq within US-based data centers and is backed up at another US location for disaster recovery purposes. All SayIt backup data is encrypted with AES-256. Any SayIt service provided to customers outside of the US would be subject to similar local data security laws and requirements.
3. SayIt production systems and associated nVoq policies and procedures are audited for PCI-DSS Level 1 compliance, which currently supports standards that comply with HIPAA and the HITECH Act. PCI-DSS is a data security standard developed by the Payment Card Industry. It contains 12 sections laying out the criteria, policies and procedures for IT systems which come into contact with personal financial information, such as account numbers, social security numbers, addresses, and the like. A PCI-DSS Certificate of Compliance is available to customers on request.

As part of PCI-DSS certification, we engage 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 come into contact with PHI when supporting customer implementations. All employees have Self-Encrypting Drives (SEDs) in their laptops and workstations. SEDs use AES 256-bit hardware encryption. Remote management and drive locking is provided by the Wave Cloud SED management platform. In the event that an employee laptop is lost or stolen, the data on the laptop's drive is designed to be inaccessible.

nVoq work which involves PHI is handled as follows:

1. PHI redacted information is used to build language models to support dictation. Customers are requested to redact PHI before sending transcripts to be used in language modeling.
2. Language models are uploaded (securely) through the Administrative Console.
3. Customers who wish to send transcripts (redacted or otherwise) are required to use a HIPAA compliant service such as Box or Hightail.
4. For nVoq personnel who work with data that may contain PHI on their computers must have an encrypted hard drives designed to protect the data, strong passwords and the data must be scrubbed of PHI as soon as practical and deleted after use.