Security Brief

There are three access points to the nVoq service:

1. **The end-user client used for dictations, workflow shortcuts, and automations**.
   Only dictations could possibly contain Personally Identifiable Information (PII) or Personal Health Information (PHI). Data sent to and received from nVoq is designed to be transmitted securely (see below).
2. **The API used by other programs and services, for dictations and automations**.
   Only dictations or sentence modeling submitted or received via the API could contain PII or PHI. Data sent via the API 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 designed to be 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 by nVoq within US-based data centers and is backed up at another US location for disaster recovery purposes. All nVoq backup data is encrypted with AES-256. Any nVoq service provided to customers outside of the US would be subject to similar local data security laws and requirements.
3. nVoq US production systems and associated nVoq policies and procedures are assessed for PCI DSS Level 1 compliance, which currently supports standards that comply with HIPAA and the HITECH Act. nVoq's policies and procedures as applied and performed in the US are also applied to the Canadian system.

   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 on request under a non-disclosure agreement.

Data Removal

Deleting administration data such as users and organizations via the API or Administrative application results in a soft delete. In other words, the user and organization information is no longer visible in the application, but their configuration and associated transaction data are still in the database. This is primarily for billing and reporting purposes. Text and audio are always fully removed according to the group rules for the user in question, whether or not that user has been deleted. All data has the possibility of existing one year after it is purged from primary storage as it is aged out of system backups.

nVoq work which involves PII or PHI is handled as follows:

1. PII or PHI de-identified information is used to build language models to support dictation. Customers are requested to de-identify PII or 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 (de-identified or otherwise) are required to use a HIPAA compliant service such as Box.
4. nVoq personnel who work with data that may contain PII or PHI on their computers must have an encrypted hard drive designed to protect the data, strong passwords, and the data must be scrubbed of PHI as soon as practical and deleted after use.

nVoq personnel and PHI:

nVoq personnel may come into contact with PHI when supporting customer implementations. All employees have AES 256-bit, Full Disk Encryption (FDE) on their laptops and workstations. In the event that an employee laptop is lost or stolen, the data on the laptop's drive is designed to be inaccessible. Encryption management and drive locking is provided by Microsoft Bitlocker or Apple FileVault.

Payment Card Industry Data Security Standard (PCI DSS):

nVoq has obtained **Level 1 PCI compliance**. We were validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Our solution also follows the guidelines for compliance with the industry specific requirements of HIPAA.

On an annual basis, nVoq's US systems and operations are assessed for compliance with the twelve requirements of PCI DSS.

Those twelve requirements cover a spectrum of six general areas:

I. Build and Maintain a Secure Network

Requirement 1 – Install and maintain a firewall configuration to protect cardholder data.

Intrusion Detection Systems, Threat Protection Systems, and Web Application Firewalls keep data protected at all times. Non-production resources are never mixed with production resources.

***Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameter*s.**

All system administration passwords and vendor default passwords are changed at installation and on a regular basis. Additionally, these updated passwords are stored in an encrypted key database system with limited, private key-based access.

II. Protect Cardholder Data

***Requirement 3 – Protect stored cardholder data*.**

All transaction text data at rest is encrypted with AES-256 and retained on-shore only. Data is stored for a limited time and purged regularly. As well, nVoq customers also have the control to turn off data retention completely. Data is stored in an unstructured format. Each nVoq tenant data set is stored in a separate database.

***Requirement 4 – Encrypt transmission of cardholder data across open, public network*s.**

All nVoq Internet communication utilizes TLS encryption over HTTPS or WSS. nVoq transcription text at the client is session-based, with no text data stored between sessions.

III. Maintain a Vulnerability Management Program

***Requirement 5 – Use and regularly update anti-virus software or programs*.**

Anti-virus keeps data and systems protected at all times. Servers and workstations are updated and scanned regularly to insure known risks are mitigated.

***Requirement 6 – Develop and maintain secure systems and applications*.**

nVoq software developers are required to attend secure coding training based on the OWASP recognized vulnerability list. Additionally, the nVoq software development process requires the application of security best practices, including those from OWASP, in the development and/or modification of application code.

IV. Implement Strong Access Control Measures

Requirement 7 – Restrict access to cardholder data by business need to know.

The nVoq solution does not require the collection or creation of private data. However, system usage could include this information. As such it is critical that system and data access is limited only to those with a need to inspect and analyze this data. Within nVoq this is limited to critical members of our support team and members of the DevOps team.

***Requirement 8 – Assign a unique ID to each person with computer access*.**

nVoq users and system administrators use unique user identification to access nVoq dictation and automation functionality as well as user administration. Shared and generic system accounts are not allowed in the usage and ongoing maintenance of nVoq and the supporting systems.

Requirement 9 – Restrict physical access to cardholder data.

nVoq's primary infrastructure is housed in PCI compliant data centers. The data centers themselves are secured with a variety of measures to prevent unauthorized access. Only select individuals have access to the physical devices which support nVoq infrastructure.

V. Regularly Monitor and Test Networks

Requirement 10 – Track and monitor all access to network resourses and cardholder data.

Application events and properties for Users and Administrators are logged and maintained for authorized auditing purposes. System Infrastructure and Networking components have access activity, event, and security logging and are monitored regularly.

***Requirement 11 – Regularly test security systems and processes*.**

nVoq regularly tests and audits the security of our systems and processes. As an example, 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 on request under a non-disclosure agreement.

VI. Maintain an Information Security Policy

***Requirement 12 – Maintain a policy that addresses information security for employees and contractors*.**

The nVoq application has strong role-based password protection for Users, Administrators, and Infrastructure Administration with controls for items such as login failure threshold, expiration, complexity, and history. These passwords are encrypted with a salted one-way hash for additional protection. nVoq maintains an internal information security policy that all employees and contractors must adhere to.

Statement on Standards for Attestation Engagements No 18 (i.e., SSAE18), Reporting on Controls at a Service Organization.

nVoq has also achieved certification from an external auditor for compliance with the SSAE 18 SOC 2 framework. Annually, nVoq undergoes an SSAE18 Service Organization Controls 2 Type II assessment related to the following Trust Service Principles:

I. Security
II. Availability
III. Confidentiality
IV. Privacy