SPEECH RECOGNITION
SOLUTIONS



Earning your trust through data security

Our platforms and security infrastructure are designed to protect **YOUR** data and eliminate unnecessary disruptions to **YOUR** business. The combination of the best security technologies combined with regular scanning and testing, and audits performed annually on our security program and HIPAA compliance enables us **to protect both YOU and YOUR data**. At nVoq, here is what we do to protect **YOUR** data…

Independent Audits Ensure Integrity, Privacy & Availability

The nVoq platform undergoes regular rigorous independent audits in accordance with the AICPA's SOC2 Type 2 standard to confirm compliance and safeguarding of client data.

To ensure that the necessary security protocols are in place and function properly, nVoq undergoes a SOC2 Type 2 assessment annually, based on these four Trust Service Principles…

1. **Security**
2. **Availability**
3. **Confidentiality**
4. **Privacy**

nVoq is both HIPAA compliant in the US and PIPEDA compliant for its platforms in Canada. Conrad McCarty serves as nVoq's Security & Privacy Officer in both the U.S. and Canada.

nVoq goes above and beyond to ensure the safety, security, and privacy of your data.

High Availability and Redundancy

To ensure you have high availability and redundancy, nVoq operates its speech recognition platform in a secure, hosted environment to ensure the security of **YOUR** data, uptime and performance. Redundant data centers and multiple independent Internet service providers ensure availability. Redundant hardware is in place throughout the network infrastructure to ensure network traffic delivery. We protect the environment from hardware failure by utilizing load balancing and clustering technologies.



Earning your trust through data security

Monitoring and Backup

nVoq utilizes advanced monitoring technologies on all levels of our applications and infrastructure. This includes a status page published to the internet for customer access regarding system status and even notification. This information is also available via text or email subscription 24/7 to ensure real-time alerting and response to any issues.

nVoq relies on a multi-tiered, redundant backup strategy to help ensure recovery of archived data. Backup procedures include daily snapshots of all critical client data to multiple media types and geographically diverse locations. We test backups regularly to ensure recovery reliability. We encrypt and securely transport offsite data backups to alternate locations.

Foundational Security Technology

Your confidence in our ability to manage and protect **YOUR** sensitive patient data is important to us. We protect our client data with powerful underlying technology tools including:

- Encryption for data in Motion and at Rest
- Strong Encryption Technologies
- MFA employed strategically on our platform
- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)
- Web Application Firewalls (WAF)
- Dark Web Monitoring
- Virus and Malware Detection & Removal
- Network Firewalls
- Penetration Testing
- Vulnerability Scanning
- Dynamic Application Security Testing (DAST)
- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)

Clients access our platform environment via encrypted TLS sessions. We encrypt sensitive customer data both during transmission and at rest using the same industry standard protocols used by modern financial institutions.

SPEECH RECOGNITION
SOLUTIONS



Earning your trust through data security

To ensure you have high availability and redundancy, nVoq operates its speech recognition platform in a secure, hosted environment to ensure the security of **YOUR** data, uptime and performance. Redundant data centers and multiple independent Internet service providers ensure availability. Redundant hardware is in place throughout the network infrastructure to ensure network traffic delivery. We protect the environment from hardware failure by utilizing load balancing and clustering technologies.

Availability & Disaster Recovery Protocols

The nVoq platform is designed to allow upgrades and updates without service interruptions to maximize availability to our customers and their users. We maintain, review, and test our disaster recovery plan to be well-prepared for potential disasters. At a high level, we have plans in place to coordinate key personnel, restore critical infrastructure systems, data, application functions, and conduct post-failover validation. These plans are tested regularly. Not only do we review the results of disaster recovery testing activities, but we also update and refine our plans as needed to improve our level of preparedness.

Security Designed into Our Platform

nVoq believes that protecting your critical data is worth the extra effort and so we have designed security into our platform. As just a few examples, you can require your company administrators to utilize multi-factor authentication for system log-ins, all relevant account administration activities are logged and retained, data persistence is configurable by your company administrators, strong passwords are required for all administrators. We have a program to proactively apply important patches and to rapidly patch publicly disclosed vulnerabilities. All nVoq client software access requires a unique username and password.

For more information on our compliance efforts or for answers to your security questions, please reach out to:

Compliance@nVoq.com