Data security and service continuity

Nuance Dragon Medical Cloud Services

Nuance is committed to meeting the high security and service continuity demands of our healthcare clients.

Introduction

Nuance® Dragon® Medical One is a cloud-based speech recognition solution for documenting care in the EHR and beyond. It provides a consistent and personalized clinical documentation experience, allowing clinicians to use their voices to securely capture the patient story more naturally and efficiently—anywhere, anytime.

Dragon Medical embedded in the EHR or in mobile applications is a cloud-based speech recognition solution that allows partner solutions to provide a consistent and personalized clinical documentation experience.

PowerMic™ Mobile is a complementary, cloud-based solution that turns a smartphone into a high-quality microphone and field navigation tool for generating high-quality clinical documentation.

Our security practices, combined with a high-availability and redundant infrastructure, help ensure that your clinicians will experience fast, accurate, secure, and uninterrupted clinical speech recognition.

Designed for security, compliance, and resilience Dragon Medical One has been certified by the Health Information Trust Alliance (HITRUST®) as meeting the HITRUST Common Security Framework (CSF®), a set of industry-defined, risk- and compliance-based security standards and controls tailored for the health-care industry.[1]

Dragon Medical One's certified security practices helps ensure uninterrupted clinical speech recognition.

Nuance works with Microsoft® Azure™ to host Dragon Medical One, Dragon Medical Embedded and PowerMic Mobile. Microsoft Azure is the world's largest multi-terabit global network. It offers 24x7x365 high availability and guaranteed 99.9% uptime by operating through a network of secure, redundant data centers located within the continental United States. These Microsoft data centers are both SOC Type 1- and SOC Type 2-compliant.

Committed to a high security standard

The Microsoft Azure environment is also HITRUST CSF certified and contains several layers of security to keep data private and protected, including physical barriers, auditing and log management, encryption, identity and access management, and threat monitoring.

Microsoft Azure employs rigorous security standards and practices to ensure data privacy and security such as denial of service, intrusion detection, and routine penetration testing, and utilizes a red team approach to continually strengthen threat detection.

In addition to HITRUST CSF, Microsoft Azure supports compliance efforts related to more than 65 national, regional, and industry-specific requirements governing the collection and use of individuals' data, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- International Standards including ISO 27001, ISO 27017, and ISO 27018
- US Federal Risk and Authorization Management Program (FedRAMP)
- Security Organization Controls (SOC 1, SOC 2, and SOC 3)
- EU General Data Protection Regulation (GDPR)

Nuance maintains a business associate agreement (BAA) with Microsoft as required by HIPAA.

Secure access to Microsoft Azure data centers

- **Physical access.** Nuance employees do not have or need physical access to Microsoft data centers. Microsoft uses advanced secure physical access methods, including biometrics, to secure its Azure data centers.
- **Electronic access.** Nuance follows the HIPAA requirement of "minimum necessary" when granting electronic access to Nuance resources within Microsoft Azure.
- **Two-factor authentication/jump hosts.** When electronically accessing the data center, authorized personnel are required to use two-factor authentication for identity verification. Additionally, all production access is conducted via an intermediate jump host to provide an extra level of insulation that separates direct access to servers and prevents unau-thorized access.

Nuance security measures

Nuance security measures are designed to help protect customer and company data, including:

Engineered for security
We follow industry-standard frameworks such as the Microsoft Security Development Lifecycle (Microsoft SDL) and the Building Security in Maturity Model (BSIMM). Our secure software development lifecycle (SDLC) program provides secure design and implementation governance, potential identification and remediation of any security issues before new products are released, and rapid response by development teams should there be security issues discovered after release.

Additionally, Nuance utilizes a third-party service to conduct periodic penetration testing against Dragon Medical Cloud Services. Nuance also performs weekly internal and external scans to identify potential vulnerabilities.

Data transmission—encryption in transit
Nuance speech-enabled client applications stream audio in real time to Dragon Medical Cloud Services for speech recognition processing. All communication between client applications and Dragon Medical Cloud Services is transmitted via HTTPS utilizing TLS 1.3, with an AES 256-bit cipher algorithm. Audio is never stored locally on a client's device, and recognized text is encrypted and returned directly to the target application for persistent storage.

Data storage—encryption at rest
Nuance safeguards all customer data using encryption at rest. Dragon Medical Cloud Services use Azure Managed Disks with Storage Service Encryption (SSE) to store all customer text and audio. Customer metadata, such as licensing information, user accounts, etc., are stored in SQL Server databases utilizing Azure's Transparent Data Encryption. Both of these Azure services implement AES 256-bit encryption to ensure the highest level of protection for data at rest.

Data retention and usage
Audio files and text are used to provide the service purchased and to train and optimize the speech engine for individual user profiles and improve speech recognition accuracy for every user.

High availability and service continuity

In the event of a data center failure, we can quickly failover the Dragon Medical One environment to an alternate active data center. Data is kept synchronized between the two centers to maintain a low Recovery Point Objective (RPO) of 15 minutes in the event of a total failure at the production data center. The Maximum Allowable Outage (MAO) is 90 minutes.

Within each data center, the system architecture of Dragon Medical Cloud Services provides the following high-availability features:

- Fully redundant network infrastructure, including load balancers and switches
- Multiple clustered application servers
- High-availability network storage with fiber-optic connections
- Clustered database servers

Conclusion

At Nuance, we are fully committed to an ever-advancing, defense-in-depth security strategy and corresponding controls intended to ensure that the healthcare data you entrust to us is kept private and protected.

Our security practices, combined with a highly available and redundant infrastructure, are designed to provide your clinicians with the fast, secure, and uninterrupted service they expect—and your patients deserve.

LEARN MORE

To learn more about Nuance Dragon Medical One for clinical documentation, please call 1-877-805-5902 or visit nuance.com/healthcare. To learn more about the HITRUST CSF, visit hitrustalliance.net/hitrust-csf/.

Endnotes

1 HITRUST and HITRUST CSF are registered trademarks of HITRUST Alliance.