Healthcare Solutions
Nuance Dragon Medical
Cloud Services for Australia

White Paper

Data security and service continuity

Nuance Dragon Medical Cloud Services for Australia.

NUANCE®

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 Electronic Medical Record (EMR) and beyond. It provides a consistent and personalised 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 EMR or in mobile applications is a cloud-based speech recognition solution that allows partner solutions to provide a consistent and personalised clinical documentation experience.

PowerMic Mobile is a complementary, cloud-based solution that turns a smartphone into a high-caliber 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

Nuance works with Microsoft Azure to host Dragon Medical One, Dragon Medical Embedded and PowerMic Mobile. Microsoft Azure provides a cloud computing platform over the world's largest multi-terabit global network. Azure services are highly available, 24x7x365, with uptime guarantees of at least 99.9%. Dragon Medical One, Dragon Medical Embedded and PowerMic Mobile are operating through a network of two geographically-distributed locations across the country. The Microsoft data centers are both SOC Type 1- and SOC Type 2-compliant.

Committed to a high security standard

The Microsoft Azure environment is an ASD-certified cloud service* 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 utilises a red team approach to continually strengthen threat detection. Complete details of Microsoft Azure in Australia are available at https://azure.microsoft.com/en-au/.

Microsoft Azure supports compliance efforts related to a broad set of international and industry-specific requirements governing the collection and use of individuals' data, including:

- Privacy Act 1988, which includes a set of thirteen Australian Privacy Principles (APPs)
- EU General Data Protection Regulation (GDPR)

*https://www.cyber.gov.au/irap/asd-certified-cloud-services

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 to secure its Azure data centers.
- **Two-factor authentication/jump hosts.** When electronically accessing the data center, authorised personnel are required to use two-factor authentication for identity verification. Additionally, access to our production environment is conducted through an intermediate jump host to help prevent unauthorised 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 to help ensure our software applications are architected and developed free from security problems while providing security testing, structure, and guidance to product developers.

Nuance utilises third-party services to protect Nuance cloud services from virus or malware infection and conducts regular penetration testing. Nuance also performs weekly internal and external scans to identify potential vulnerabilities. Any discovered vulnerabilities are resolved with the highest priority.

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 utilising TLS 1.2, with an AES 256-bit cipher algorithm. Audio is never stored locally on a client's device, and recognised 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 utilising 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 optimise the speech engine for individual user profiles and improve speech recognition accuracy for every user. Dragon Medical One and Dragon Medical Embedded do not require any patient metadata and do not associate specific information with any individual patient.

High availability and service continuity

Dragon Medical One services are deployed in an active/active configuration, with continuous data replication between two Azure data centers. In the unlikely event of a data center failure, operations are rerouted to the alternate data center to maintain a Recovery Point Objective (RPO) with a Recovery Time Objective (RTO) of 15 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
- Clustered speech server farm

Nuance provides a more natural and insightful approach to clinical documentation, freeing clinicians to spend more time caring for their patients.

Conclusion

At Nuance, we are fully committed to an ever-advancing, defence-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.

To learn more about Nuance Dragon Medical One for clinical documentation, please call 02 9434 2300 or visit nuance.com/en-au/healthcare.

nuance.com/en-au/healthcare

@voice4health

About Nuance Communications, Inc.

Nuance Communications (NASDAQ: NUAN) is the pioneer and leader in conversational AI innovations that bring intelligence to everyday work and life. The company delivers solutions that understand, analyse, and respond to people – amplifying human intelligence to increase productivity and security. With decades of domain and AI expertise, Nuance works with thousands of organisations globally across healthcare, financial services, telecommunications, government, and retail – to empower a smarter, more connected world. For more information, please visit nuance.com/en-au/healthcare.