Nuance Healthcare Solutions
Healthcare Hosted Infrastructure Services

Data security and disaster recovery

Dragon® Medical One and
Dragon® Medical SpeechKit

NUANCE

Data security is extremely important to Nuance and we are dedicated to meeting the high data security and continuity demands of our healthcare clients.

Nuance has partnered with Microsoft® Azure™ as our cloud computing service for both Dragon® Medical One and the Dragon® Medical SpeechKit. Microsoft Azure meets a broad set of international and industry specific compliance standards. For more information on Microsoft Azure security, please see the Microsoft Trust Center.

All communication between client applications and Nuance speech services is via HTTPS utilizing TLS 1.2 with the 256-bit AES cipher algorithm. As part of our hosted services security practices, combined with our highly available and redundant infrastructure, it helps ensure that your clinicians will enjoy fast, secure and timely clinical speech support services.

Nuance cloud services stream audio in real-time to the secure server environment for speech recognition processing. Audio is never stored locally on the client and recognized text is returned directly to the target application that is responsible for any persistent storage.

Streaming and data storage

Nuance hosted services stream audio in real time to the secure server environment for speech recognition processing. Audio is never stored locally on the client and recognized text is returned directly to the target application that is responsible for any persistent storage.

Audio files and text are used to "train" and optimize the speech engine for individual user profiles and to improve speech recognition accuracy for every user. The audio and text that Nuance stores is largely anonymous, in that Nuance hosted services do not have direct access to the patient record and do not require any patient metadata. For example, if a physician dictates, "the patient has community-acquired pneumonia", there is no stored information that associates that information with an individual patient.

Our security is your security

It's important for your organization to understand the protection measures used to secure the Nuance hosted services infrastructure.

Qualys® SSL Labs rated "A"
We are constantly monitoring security standards and perform external audits to ensure that our data center meets the highest standards for secure data transmission. To that end, our hosting environment has received an "A" rating from Qualys SSL Labs server test for certificate (256-bit, trusted), protocol support (TLS 1.0, 1.1, and 1.2, secure renegotiation downgrade attack prevention, SSL 2 handshake compatibility), key exchange, and cipher strength.

Microsoft Azure Security Standards
As a leading cloud provider that serves multiple industries including healthcare, government and financial sectors, Microsoft has very rigorous security standards and practices. Microsoft provides denial of service, intrusion detection, and performs routine penetration testing. In addition, Microsoft utilizes a "red team" approach to continually strengthen threat detection. As a direct result of these security measures Microsoft data centers are SOC I Type 1 and SOC 2 Type 2 compliant.

N3 certification
In addition to, and because of the aforementioned security measures, the Nuance Healthcare Infrastructure is N3 certified, providing customers with access to Nuance Healthcare solutions, like, Nuance Dragon Medical One, through the NHS' national broadband network N3.

Shared responsibility
Because you're developing, or using, applications and platforms that leverage Nuance hosted services, the security responsibilities are shared by both you and Nuance, with both parties having HIPAA security and privacy policies and procedures in place. Nuance secures the underlying infrastructure and it is your responsibility to secure the environments that utilize or consume those services.

High availability
The Microsoft Azure cloud is designed to be highly available 24x7 and deliver consistent uptimes of 99.95 percent; it offers the following features:

– Fifteen (15) billion dollar investment in a worldwide footprint
– Four (4) regional data centers in the United Kingdom
– World's largest multi-terabit global network with extensive dark fiber footprint

From an installation perspective, the core hosted Nuance cluster 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 server
– Clustered and extensible speech server "farm"

Secure and robust cloud offering
Our security practices, combined with our highly available and redundant infrastructure, help ensure that your clinicians will enjoy fast, secure and uninterrupted clinical speech recognition.

Our association with Microsoft allows us to offer best in class security practices, combined with a highly available and redundant infrastructure, helping ensure that your clinicians will enjoy fast, secure and uninterrupted clinical speech.

Frequently asked questions

Our best in class security practices, combined with our highly available and redundant infrastructure, help ensure that your clinicians will enjoy fast, secure and uninterrupted clinical speech recognition.

Physical Security	
What are the primary physical security and business continuity features of your data center?	Microsoft Azure provides extensive electronic and physical security measures. Our data center configuration provides automatic failover in the event of server outage.
Who (including data center staff, other employees and vendors) has physical access to the host servers?	Only Microsoft staff are allowed access to the physical facility. No other staff is allowed access to the facility.
Network Security	
Are industry-standard firewalls deployed? Where are they deployed? How do you keep the software for the firewalls current? Is administrative access to firewalls and other perimeter devices allowed only through secure methods or direct serial port access?	Firewalls are deployed at the data center and provide firewall services both at the perimeter as well as between internal networks of different security levels. Administrative access is gained through SSH or on exception through serial port interfaces. Firewall software upgrades are performed at discretion of the Network Engineering team and follow Change Management processes in performing such upgrades.
What protocols and ports are allowed to traverse the network and firewall?	Any data considered PHI is encrypted when being transported using HTTPS communications.
Are formal incident-response procedures in place? Are they tested regularly?	There are Incident Management processes in place, which include specific procedures to classify the level and the handling of incidents. These processes are tested regularly across required teams across the Nuance healthcare organization.
Systems Security	
Are ongoing vulnerability assessments performed against the systems?	Microsoft Azure provides denial of service, intrusion detection and performs routine penetration testing.
Are file permissions set on a need-to-access basis only?	Production file access is restricted to the Nuance Data Center Operations team and the Support Services teams.
Are audit logs implemented on all systems that store or process critical information? Are root commands logged? What processes will be used to control access to devices and logs?	Platform applications log relevant information on data access within the platform. System logging is accomplished through Windows Event Logs, which requires logging of Security events and also maintains System and Application logging.
What change management procedures are in place?	Change Management processes are in place, which dictate the management approval levels and communications required for various types of changes.
What is the process for monitoring the integrity and availability of host servers?	System monitoring is in place and leverages internally developed tools as well as industry standard tools. Alerts generated by these tools are routed to pagers, which are covered 24x7 by Nuance Data Center Operations staff.
Have unnecessary services been disabled on host servers?	Yes, only necessary applications are installed and running on host systems.
Web Security	

What is the process for doing security Quality Assurance testing for applications?	The Nuance cloud platform has been subjected to static and dynamic inspection using HP Fortify with no significant issues reported.
Has a web code review for the explicit purpose of finding and remediating security vulnerabilities been done? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?	Applications are subjected to static and dynamic inspection using HP Fortify with no significant issues reported.
Have unnecessary HTTP modules or extensions been disabled on host servers?	Yes, only the needed IIS extensions are enabled during installation.
Does the account running HTTP service have OS administrator privileges?	IIS service account runs as Local Service account.
Staff Security	
What are the credentials of the systems administration staff?	User accounts are unique to individual Nuance Host Healthcare Infrastructure Services (HHIS) staff and application support members with the exception of particular application or service accounts.
Are hosting staff onsite available 24x7?	Nuance Hosted Health Infrastructure System (HHIS) and its Site Reliability Center (SRC) personnel provide 24x7 coverage in the event of an emergency.
Are user accounts for contract personnel created with expiration dates? How are user accounts closed after termination?	An account termination process is in place and generates automatic requests to operations personnel when termination has occurred to trigger the account removal process.
Application Security	
Is any data stored locally on the device or computer?	Neither audio nor recognized text is ever stored locally on the device or computer. Nuance streams audio in real time to the secure server environment for speech recognition processing. Persistence of the recognized text that is returned by the Nuance cloud is the responsibility of the target application.
Is the data encrypted during transmission?	Yes, both the audio and recognized text are encrypted during transmission using an encrypted HTTPS connection.

Nuance Healthcare Solutions
Healthcare Hosted Infrastructure Services

To learn more about how Nuance can help you improve financial performance, raise the quality of care, and increase clinician satisfaction, please contact us at 07887051154 or visit www.nuance.co.uk/healthcare.

www.nuance.co.uk/healthcare

@voice4health

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

NUANCE

NUAN–DI–001–01–DS–UK, October 2016