# Data security and service continuity.

Nuance UK cloud services.

## Nuance UK Cloud services

Nuance offers Dragon® Medical One (DMO), PowerMicTM Mobile (PMM), Dragon Medical Embedded (DME) and eScription UK as Nuance UK cloud services.

Data security and service availability are extremely important to Nuance, and we are dedicated to meeting comprehensive data security standards while providing high availability for our cloud services.

## Premium secure cloud providers

Nuance has partnered with Microsoft Azure UK to host DMO, PMM, and DME out of the Azure regions UK South and UK West.
Nuance is hosting eScription UK out of a data centre in Slough. The secondary data centre is located in the Azure region UK South.
The Microsoft Azure cloud is designed to be highly available 24x7 and delivers consistent uptimes of 99.95%. Details of Microsoft Azure in the UK are available here https://azure.microsoft.com/en-gb/.
Microsoft Azure meets a broad set of international and industry-specific compliance standards. Details of all certifications per region can be found at: https://azure.microsoft.com/en-gb/overview/trusted-cloud/.

## Nuance security measures

In addition to the core secure services offered by Microsoft Azure, Nuance has implemented numerous additional security measures to protect customer data.

### Engineered for security

Nuance employs software development and engineering security best practices. We develop according to Secure Software Development Lifecycle and utilise Veracode for static code analysis to scan for vulnerabilities. Each release is scanned prior to production release and all critical and high issues are resolved before production rollout.

### Data transmission—encryption in transit

Nuance speech-enabled client applications stream audio in real time to Nuance cloud services for speech recognition processing. All communication between client applications and Nuance cloud services is transmitted via HTTPS utilising TLS 1.1 or TLS 1.2, with an AES 256-bit cipher algorithm.

Security standards and transmission protocols are constantly evolving in response to new security threats. To that end, we monitor security standards and perform external audits to ensure that our data centres meets the highest standards for secure data transmission. Our Nuance cloud services hosting environments routinely receive an “A+” rating from Qualys SSL Labs, which performs a deep analysis on our TLS endpoints. Among other things, the test checks the strength of our certificates, supported protocols (TLS 1.1, 1.2), supported ciphers, and vulnerabilities in our configuration.

NUANCE

**Data storage—encryption at rest**
Nuance safeguards all customer data that resides in Nuance or Nuance Azure data centres using encryption at rest.
At the Nuance Azure data centres Nuance cloud services leverage Azure Managed Disks with Storage Service Encryption (SSE) to persist 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.
In all UK data centres AES 256-bit encryption is implemented to ensure the highest level of protection for data at rest.

**Data retention and usage**
Audio files and text are stored in the Nuance data centres to "train" and optimise the speech engine for individual user profiles, and to improve speech recognition accuracy for every user. The audio and text that Nuance stores in its data centre is largely anonymous.
DMO and DME 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.
For eScription metadata is securely transmitted from the EHR via an HL7 feed and securely stored with the transcription job.

**Data centre security**
In addition to the core Azure data centre security, Nuance employs many industry best practices to further safeguard customer data and bolster the overall security of Nuance cloud services.

– Physical access. Physical access to the data centres is secured using many advanced security techniques, including advanced biometrics. For Microsoft Azure data centres Nuance employees do not have or need physical access to the data centre.
– Electronic access. Nuance follows the requirement of "minimum necessary" when granting electronic access to the data centre for support purposes. All requests for electronic access are subject to VP-level approval. A list of all Nuance employees with access is submitted annually to NHS Digital as part of Nuance's IG Toolkit re-certification.
– Two-factor authentication/jump hosts. When accessing the data centre, all Nuance employees are required to use two-factor authentication. In addition, all production access is via an intermediate "jump host," which provides an extra level of insulation.
– Anti-virus and malware protection. Nuance has deployed Trend Micro anti-virus to proactively protect the Nuance cloud services from virus or malware infection.
– Intrusion detection and protection system (IDPS). Nuance leverages Trend Micro's IDS solution, which examines every packet that is transmitted to the data center for potential irregularities.
– Penetration testing. Nuance utilises a third-party service to conduct annual penetration testing against the hosted Nuance cloud services. Vulnerabilities that are discovered are resolved with the highest priority.
– Patches and updates. In addition to penetration testing, Nuance operations personnel perform monthly scans of the Nuance hosted services using Nexpose to identify potential vulnerabilities and their related remedies. Based on the severity of the vulnerability, the vendor patch is tested and deployed to production.
– Security monitoring. To provide an integrated comprehensive view into the security status of Nuance cloud services, Nuance leverages Azure Operations Management Suite (OMS) and other tools. This provides a "single pane of glass" that gives real-time insight into all security aspects of our operations.

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 recognition

**High availability and service continuity**
Nuance has partnered with Microsoft Azure UK to host DMO, PMM, and DME out of the Azure regions UK South and UK West. Nuance is hosting eScription UK out of a data centre in Slough. The secondary data centre is located in the Azure region UK South.

The services are deployed in an active/stand-by configuration, with the primary data centre taking live traffic, and all relevant data is replicated to the secondary data centre continuously. In the unlikely event of a data centre failure, all traffic will be rerouted to the secondary data centre. The potential for data loss in the event of an outage, Recovery Point Objective (RPO), is 15 minutes or less.

Within each data center, the system architecture of Nuance cloud services provides the following high-availability features:

– Fully redundant network infrastructure, including load balancers and switches
– Multiple clustered application server
– 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 infrastruc-ture, ensure that your physicians will enjoy fast, secure, and uninterrupted clinical speech recognition.

| **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? | We use Network Security Groups (NSGs) that provide our firewall functionality. Firewalls are deployed at the data centres. They provide firewall services 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. |
| What protocols and ports can traverse the network and firewall? | All speech-enabled applications transmit and receive data over HTTPS port 443 utilising TLS 1.1/1.2 with a 256-bit AES encryption. |
| Are formal incident-response procedures in place? Are they tested regularly? | Incident management processes are in place which include specific procedures to classify the level and the handling of incidents. These processes are tested regularly among required teams across the Nuance healthcare organisation. |
| Does Nuance UK hosted cloud services have access to the NHS Broadband Network (N3)? | Yes, Nuance Communications UK Ltd has attained IGSoC and Nuance UK hosted cloud services may securely connect via N3 into NHS organisations including hospitals and clinics. The IG ToolKit assessment and approval can be viewed here. This assessment process must be carried out and renewed on an annual basis. Attainment of IGSoC means that Nuance Communication UK Ltd has met all the requirements of Information Governance Management required by IGSoC: Confidentiality and Data Protection Assurance, and Information Security Assurance. |

| | |
|---|---|
| **Systems Security** | |
| Are file permissions set on a need-to-access basis only? | Production file access is restricted to the Nuance data centre operations and 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 maintains system and application logging. |
| What change management procedures are in place? | Change management processes are in place that dictate the management approval levels and communications required for various changes. |
| What is the process for monitoring the integrity and availability of host servers | System monitoring is in place and leverages internally developed tools and industry-standard tools. Alerts generated by these tools are routed to pagers, which are covered 24x7 by Nuance data centre operations staff. |
| Have unnecessary services been disabled on host servers? | Yes, only necessary applications are installed and running on host servers. |
| **Web Security** | |
| Have unnecessary HTTP modules or extensions been disabled on host servers? | Our webservers are hardened and have the minimum number of modules enabled. |
| Does the account running HTTP service have OS administrator privileges? | Nuance does not have administrative privileges. |
| **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, except for specific application or service accounts. |
| Are on-site hosting staff available 24x7? | Nuance Hosted Health Infrastructure Services (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. To trigger the account removal process, it generates automatic requests to operations personnel when termination has occurred. |
| Is the data encrypted during transmission over public network connections? | All communication between client applications and Nuance cloud services is transmitted via HTTPS utilising TLS 1.1 or TLS 1.2, with an AES 256-bit cipher algorithm. |
| **Application Security** | |
| Is the data encrypted during transmis sion over public network connections? | All communication between client applications and Nuance cloud services is transmitted via HTTPS utilising TLS 1.1 or TLS 1.2, with an AES 256-bit cipher algorithm. |

**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.co.uk



NUAN–DI–001–01–WP–UK, March 2018