Data security and business continuity.

Nuance mPower Clinical Analytics

NUANCE

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

Introduction

Nuance® mPower™ Clinical Analytics offers powerful, customizable tools to help radiologists improve operational efficiency and patient outcomes while facilitating the transition to value-based care. This solution provides access to a single, user-friendly application that unlocks data, making it easier to monitor, understand, and improve clinical and operational performance.

Nuance mPower Clinical Analytics applies an interactive approach to data mining to unlock critical information from PowerScribe® 360 reports and other sources. It allows organizations to quickly enhance productivity and streamline the reimbursement process while improving clinical quality and patient safety.

To secure these robust application services, skilled analysts at our Security Operations Center use advanced technologies for threat monitoring, intrusion detection and prevention, advanced endpoint protection, and next-generation antivirus protection. This allows Nuance to effectively monitor, analyze, and rapidly respond to alerts and potential incidents detected within our environment.

Designed for security, compliance, and resilience

Nuance follows 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.

For mPower Clinical Analytics, static and dynamic code scans are performed on every release, and ongoing automated vulnerability scans are performed against the application and its environment. Additionally, periodic penetration testing is conducted on the production environment, while relevant application, system, and audit logs are actively monitored by Nuance Product Security.

Nuance works with Microsoft® Azure™ to host mPower Clinical Analytics. Microsoft Azure is the world's largest multi-terabit global network. It offers 24x7x365 high availability and guaranteed 99.95% uptime by operating through a network of 10 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, such as denial of service, intrusion detection, and routine penetration testing, to ensure data privacy and security, and utilizes a red team approach to continually strengthen threat detection. Additionally, Nuance maintains a business associate agreement (BAA) with Microsoft as required by the Health Insurance Portability and Accountability Act (HIPAA). For more information on Microsoft Azure security, please visit the Microsoft Trust Center.

Modern cloud architecture
mPower Clinical Analytics is built using a modern container-based cloud architecture. Hosted by Azure, the application infrastructure and platform services include platform-as-a-service products such as Azure Container Services' managed Kubernetes orchestration system and a fully managed Azure PostgreSQL database. For infrastructure-as-a-service, mPower Clinical Analytics uses Azure's Log Analytics, App Insights, Load Balancer, Availability Groups, regional and geographic redundant storage accounts, and DNS.

Each Nuance customer environment functions as a logically isolated cell within Azure that includes a distinct database and a full set of mPower services. These services operate as Docker containers and are hosted at a customer-specific subdomain (e.g., customer.nuancempower.com). The cluster is horizontally scalable across nodes in the Azure datacenter, with multiple replicas of services running on distinct nodes to optimize uptime. This architectural approach effectively provides customers with their own siloed application installation while cost-effectively distributing services across shared nodes for higher availability.

All cluster and cell deployments are fully automated and are managed via an audited control portal.

Data communication
Azure's Network Security Group allows only approved web traffic to reach the load balancer, with a minimum number of required services exposed from Kubernetes to the load balancer. This allows all non-essential services to remain protected through firewalls to maintain privacy.

Secure authentication and single sign-on (SSO)
mPower Clinical Analytics federated identity features are interoperable with SAML, OpenID Connect (OIDC), and WS-Federation protocols. As a result, the solution enables healthcare professionals to use federated identity management technology to verify their identity and gain authorized access to existing Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) services. This allows an organization to increase control over users' access to information, using existing password policies and security protocols (such as multi-factor authentication).

Data transmission—encryption in transit
All communication between client applications and mPower Clinical Analytics—including browser traffic and data uploaded from the mPower Accelerator—is transmitted via HTTPS using the TLS 1.2 cryptography protocol and its AES 256-bit cipher algorithm. All sensitive internal traffic is encrypted between services within the cluster. TLS versions are negotiated by the client and server. Nuance systems use TLS 1.2 yet maintain the ability to negotiate down to TLS 1.1 or TLS 1.0 when required by a customer. This allows Nuance mPower Clinical Analytics to provide users with fast, reliable, and secure services.

Data storage—encryption at rest
Nuance safeguards all customer data using encryption at rest. Nuance mPower Clinical Analytics uses Azure Storage endpoints that are encrypted at the Storage Account level.

Audit logging
Audit logs, application logs, and system logs are securely streamed into Azure OMS. Audit logging is used when PHI is viewed or management actions are taken. Nuance Global Security monitors relevant logs for cross-product patterns of access.

Data retention
As a retrospective analytics tool, mPower Clinical Analytics retains customer data for as long as the customer has an active mPower subscription. Upon termination of a subscription, the customer's cell and database are removed, and all backups are purged within 60 days.

Physical and personnel security
All Nuance employees undergo an initial background check and are required to complete annual security and compliance training that includes modules focused on HIPAA, data privacy, security awareness, malware protection, and password management. Physical access to production systems is restricted to required, trained personnel.

Disaster recovery and business continuity
In the unlikely event of a data center failure, Nuance can quickly restore the mPower Clinical Analytics environment using designated backups.

The Azure database backup takes full, differential, and transaction log backups, which are saved to geo-redundant storage (GRS) and retained for 35 days. This allows mPower Clinical Analytics to maintain a four-hour Recovery Point Objective (RPO).

Using mPower's fully automated cluster deployment capability, backups can be restored within a Microsoft Azure environment located in a different geographic region within the same day, providing a 24-hour Recovery Time Objective (RTO). Key configuration elements and backup use geo-redundant storage (GRS), which makes the data durable even in the case of a complete regional outage or a disaster.

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.

To learn more about Nuance mPower Clinical Analytics, please call 1-877-805-5902 or visit nuance.com/healthcare.

Nuance provides a more natural and insightful approach to clinical documentation, freeing clinicians to spend more time caring for their patients. Nuance healthcare solutions capture and communicate more than 300 million patient stories each year helping more than 500,000 clinicians in 10,000 healthcare organizations globally. Nuance's award-winning clinical speech recognition, medical transcription, CDI, coding, quality and diagnostic imaging solutions provide a more complete and accurate view of patient care, which drives meaningful clinical and financial outcomes.

About Nuance Communications, Inc.
Nuance Communications, Inc. is a leading provider of voice and language solutions for businesses and consumers around the world. Its technologies, applications and services make the user experience more compelling by transforming the way people interact with devices and systems. Every day, millions of users and thousands of businesses experience Nuance's proven applications. For more information, visit www.nuance.com/healthcare or call 1-877-805-5902. Connect with us through the healthcare blog, What's next, Twitter, LinkedIn and Facebook.

NUANCE