# FUSION NARRATE®
# SECURITY BRIEF

OCTOBER 13, 2025

# CONTENTS

# EXECUTIVE OVERVIEW

Fusion Narrate® powered by nVoq™ provides cloud-based speech recognition, enabling providers to accurately and efficiently capture the patient narrative for seamless inclusion in the patient record. The Fusion Narrate suite also includes the add-on modules:

**Fusion Narrate AI Assist**: Integrates AI into dictation and workflow automation tasks

**Fusion Narrate CAPD™**: Analyzes dictated text for clinical documentation improvement (CDI)

**Text Extract**: Leverages OCR and AI to extract typed or handwritten text content from an image or PDF

**Fusion Narrate ACI™**: Generates draft reports using ambient speech technology

**Fusion Narrate Text™**: On-premise solution which allows providers to send dictation to transcription

**Fusion Narrate Hub™**: On-premise solution which provides bidirectional integration with the LIS or RIS via HL7® to streamline result documentation workflow

This document provides information on the security features of the full Fusion Narrate product suite. It is intended to help customers understand how the platform can support their organizations' compliance with the Health Insurance Portability and Accountability Act and implementing regulations ("HIPAA") and the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA").

We understand that performance and robust security must go together. The Fusion Narrate platform delivers a secure solution with configurable options that instill confidence and allow customers to tailor features to their internal compliance program.

This document first provides a general system overview, followed by a summary of the flow of PHI within the platform. Finally, we summarize the following security areas:

- Data Encryption
- User Accounts and Password Management
- Fusion Narrate Client Software Security
- Mobile Applications
- Data Storage and Retention
- Data Center and Hosting Security
- System Auditing
- Shortcuts
- Virtual Desktop Infrastructure (VDI)
- System Maintenance
- Technical Support

The Fusion Narrate cloud-based speech recognition solution is delivered through a partnership between Dolbey and Company, Inc. (Dolbey) and nVoq. Dolbey and its resellers provide Technical Support for the full application suite, while nVoq manages the speech recognition servers in a secure cloud hosting platform. The Fusion Narrate Technical Support team is available during the implementation process to address and help configure security settings per the customer's requirements.

# ADDITIONAL DOCUMENTS

*Fusion Narrate ACI Security Brief*

This document is specific for the Fusion Narrate ACI (Ambient Clinical Intelligence) workflow and functionality. It serves as an add-on to this Security Brief.

*Fusion Narrate Security Brief with Transcription*

This version of the Security Brief also includes architecture and security information for the Fusion Narrate Text premise-based solution for back-end transcription.

*Fusion Narrate Text Requirements (Job Player)*

This document provides the hardware and software requirements for the on-premise components required for the Fusion Narrate Text transcription system.

*Fusion Narrate Hub Requirements*

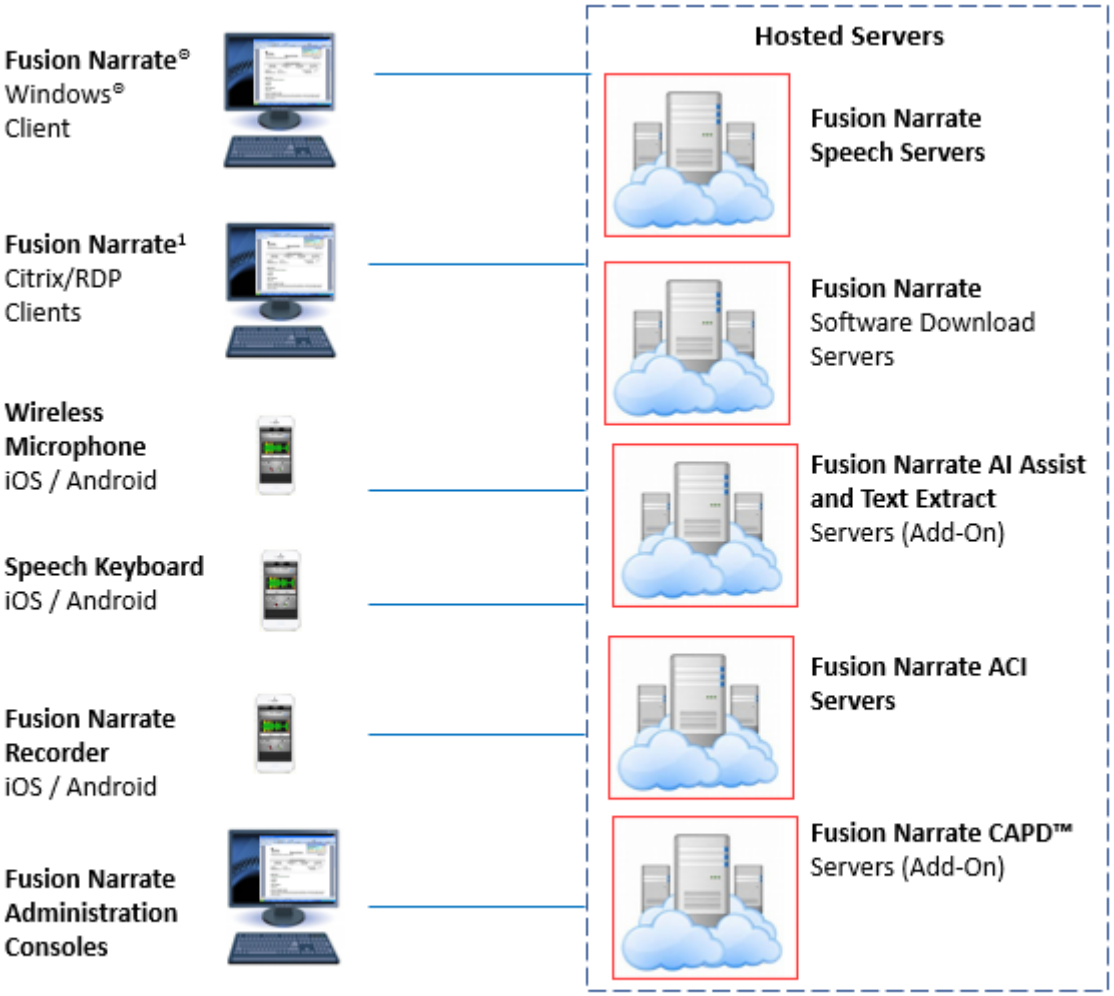
This document provides the hardware and software requirements for the on-premise components required for Fusion Narrate Hub. Fusion Narrate Hub optimizes workflow for pathology by integrating inbound and outbound HL7® interfaces with the LIS system.

*Fusion Narrate Hub Pathology Interface Specifications*

This document details the HL7® message structure for receiving LIS order information and sending outbound results.

## SYSTEM ARCHITECTURE

The following diagram provides an overview of the system architecture for the entire suite of products comprising the Fusion Narrate platform. Note that some components depicted below may not be in scope for a given project.




[1] Fusion Narrate installed on the Citrix or RDP Server
All in-transmit data is at TLS 1.2, Port 443

Additional information regarding the above components and the requirements can be found in the online Fusion Narrate Help Center.

# PHI WITHIN THE FUSION NARRATE PLATFORM

The starting point for any security assessment is understanding what data is collected, whether it contains any Protected Health Information (PHI), and the flow of PHI throughout the system.

### Fusion Narrate Client Application

Except for Fusion Narrate Hub, the Fusion Narrate client application does not interface with or provide access to patient record data that may reside in customer's other applications (e.g., EHR, LIS, RIS). Rather, the Fusion Narrate client software receives input directly from the provider, summarized below. In some specialized workflows, the Fusion Narrate client may be configured to interface with an external application to retrieve current patient or study information through automation shortcuts. The Fusion Narrate CAPD client does interface with patient record data from customer's other applications but does not store such data, as described below.

*Front-End Speech Recognition*: Generally, the dictation received for front-end speech recognition does not contain any PHI. Providers use the Fusion Narrate tool for front-end speech recognition within another application (e.g., EHR, LIS, RIS) that already includes the patient identifying information; thus, providers generally do not dictate a patient name or an identifying number when documenting the patient encounter or results because it is unnecessary and inefficient. This audio is streamed to the Fusion Narrate cloud-based speech recognition servers. The Fusion Narrate client application does not write or store audio on the client device and does not provide user access to historical audio recordings or recognized text.

*Fusion Narrate CAPD*: The optional Fusion Narrate CAPD module analyzes the text of the patient record for clinical document improvement (CDI) and notifies the provider of any recommendations. The analyzed text includes a combination of the speech recognized text from the provider's input, as well as any other text that Fusion Narrate is able to read from the current application (e.g., EHR, LIS, RIS). This text, which may contain PHI, is sent to the Fusion Narrate CAPD cloud servers for analysis but is not stored on the Fusion Narrate CAPD servers or the client device.

*Application Logging*: The Fusion Narrate client writes log data to the Windows® App Data folder which typically resides on the device on which the Fusion Narrate client runs. By default, the logging level is set to a low level to meet the minimum requirements of technical support. A higher logging level may be enabled temporarily for troubleshooting an issue; at these levels there is a greater possibility that PHI could be included in the log file. Logs may also be submitted upon request to the Fusion Narrate speech recognition servers to enable support staff to diagnose an issue. Historical log data is automatically purged off the client device after a configurable file size is reached.

### Fusion Narrate Speech Recognition Servers

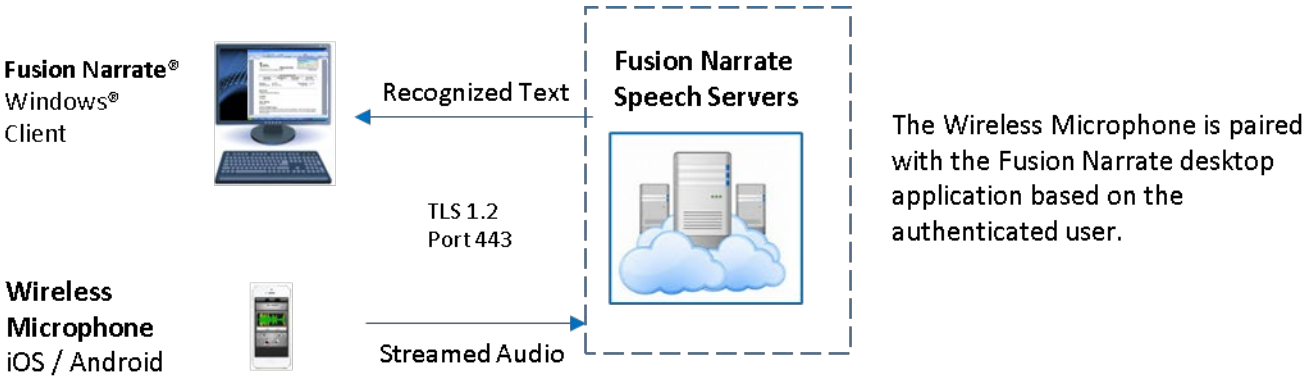
The Fusion Narrate speech recognition servers store the following types of data which are accessible from the Administration Console:

- Audio and recognized text for each dictation, which may contain PHI if dictated.
- Client log data which can be uploaded to the servers from the Fusion Narrate client upon request for technical support purposes.

The Fusion Narrate Administration Console is used to perform a variety of management functions including generating reports and managing users, shortcuts (i.e., voice commands), custom vocabulary, and groups. This tool also provides an Administrator the option to download the audio and the recognized text to their client device for technical support purposes. This can only be done on a per dictation basis. Since it is possible that this data contains PHI, this function should only be performed if the client device employs an appropriate third-party encryption solution.

### Wireless Microphone

This is a mobile application for iOS and Android that can be used as a microphone for the Fusion Narrate application. It can be used in place of a microphone attached to the workstation. Audio for front-end speech recognition is streamed from the device to the speech recognition servers and is not written or stored to the device. The speech recognized text is streamed to a connected Fusion Narrate desktop client authenticated with the same user. The application does not provide access to any PHI, including audio or speech recognized text.




### Speech Keyboard

This is a mobile application for iOS and Android that can be used in place of the built-in operating systems' keyboard. It allows the provider to use secure speech recognition to quickly insert text into other mobile applications. Similar to that of the Fusion Narrate workstation client application, this mobile application streams dictated audio to the speech recognition servers which return the recognized text. Audio is not written or stored to the device. The application does not provide access to any PHI, including historical audio or speech recognized text. The speech keyboard does not access the existing text from the target application with the exception of capturing what is needed to determine proper spacing and capitalization. Characters typed with the keyboard are neither stored nor transmitted to the servers.

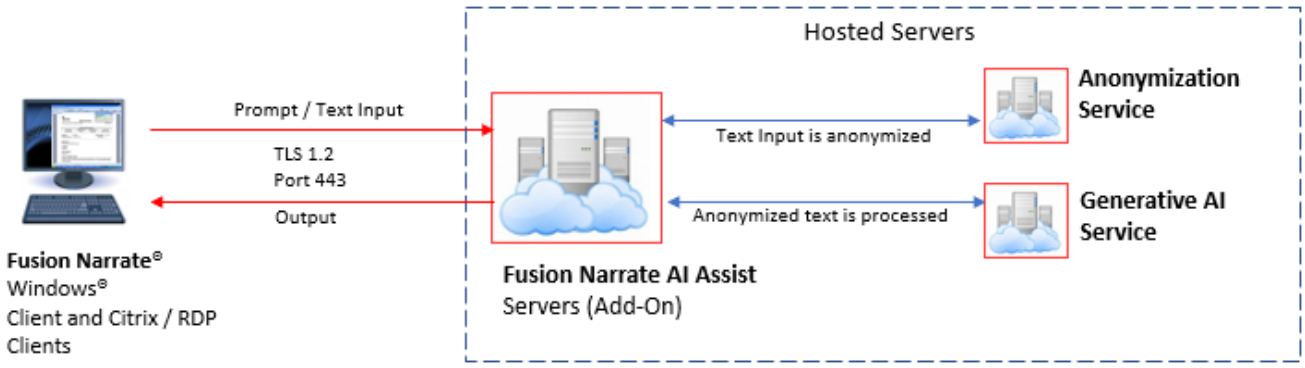
### Fusion Narrate CAPD Servers

The Fusion Narrate CAPD servers receive text from the Fusion Narrate client application, process the text, and return recommendations for documentation improvements. The text received may contain PHI, but the received text is not written or stored to the Fusion Narrate CAPD servers.

## Fusion Narrate AI Assist

AI Assist is an optional add-on component for the Fusion Narrate application. It allows organizations to integrate generative AI into their workflow. AI Assist is a shortcut type that offers broad flexibility and capabilities for text analysis, summarization, transformation, and generation.

The input to AI Assist is a combination of a prompt (i.e., what is being requested) and text such as the current patient note or selected text. This input is transmitted to the Fusion Narrate AI Assist server components where the input is first anonymized and processed through the Anonymization Service. This output is then processed by a generative AI model. Neither the input nor the output is stored in the Anonymization or Generative AI Services. The data is always encrypted during transit. The following depicts the data flow.




The anonymized input and output may be stored on the Fusion Narrate AI Assist servers to provide fine tuning of the generative AI models for a user's future requests.

AI Assist output is not reviewed by a human. This tool is not a substitute for the user's independent professional medical judgment. All output generated by AI Assist must be independently reviewed for accuracy and appropriateness by the healthcare professional before using or relying on the AI-generated output for any purpose. The tool must not be used to support time-critical decision making or in emergency situations.

AI Assist Dictation

AI Assist Dictation is a specific use case of Fusion Narrate AI Assist. This functionality allows a user to easily submit recent dictation through a generative AI LLM for further processing for purposes of adding punctuation, correcting grammar, adding formatting, and merging with a template.

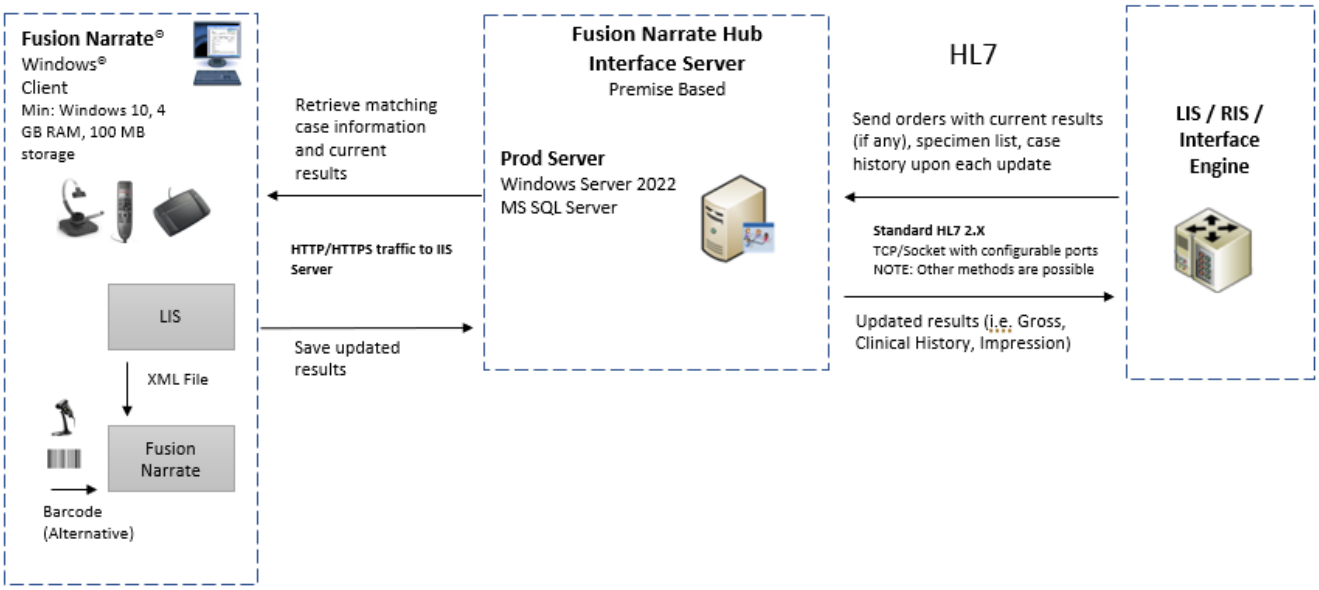
## Text Extract

Text Extract is an optional add-on tool that allows users to convert text contained within images and PDFs to text that can be pasted into a text area. Once initiated, the user is provided a screen capture / snip it selection tool to select the desired area. The captured area is submitted to the Fusion Narrate Text Extract server to convert the image data to text. The resulting text is pasted to the clipboard for the user to insert into the desired text area;

however, the specific workflow can be customized. Image data is only processed. Neither the image data nor the converted text is stored within the system.

### Fusion Narrate Hub

Fusion Narrate Hub is an extension of the Fusion Narrate client application that allows interaction with an LIS or RIS system through HL7® interfaces facilitated by an on-premise Fusion Narrate Hub server.




Order and patient demographics, as well as results, are stored on the premise-based Fusion Narrate Hub Interface server in a SQL Server® database. Additionally, the order number is typically stored with the dictation record on the Fusion Narrate Speech servers for audit purposes.

See the documents titled *Fusion Narrate Hub Requirements* and *Fusion Narrate Hub Pathology Interface Specifications* for more information.

# DATA ENCRYPTION

### Data in Transit

All data transmitted between the client and mobile applications, the Fusion Narrate speech recognition servers, and the Fusion Narrate CAPD servers uses TLS 1.2 with FIPS approved AES encryption. Only strong ciphers TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 are allowed.

### Data at Rest

All data at rest on the Fusion Narrate speech recognition servers, the Fusion Narrate CAPD servers, and the Fusion AI Assist servers, including log files, is encrypted with FIPS approved AES 256-bit encryption. This includes data stored in the AWS Aurora database and AWS S3 storage. Cryptographic keys are managed and rotated using AWS Key Management Service.

On the client device, all data stored by the Fusion Narrate client application is encrypted using AES 256-bit encryption with Microsoft® .NET encryption libraries. This is for log files, dictations and associated demographics which are stored temporarily if the optional Fusion Narrate Text solution is used.

# USER ACCOUNTS AND PASSWORD MANAGEMENT

User Accounts for both access to the Fusion Narrate client applications and the Administration Console are managed in the Administration Console. Users can be manually created or imported.

### User Types / Roles

*Client User*

This user type provides access to use the Fusion Narrate client and mobile applications and does not provide access to the Administration Console. This role represents most users as it is rare for a provider to require or be given an Administrator role.

Client users do not have access to any historical dictations or recognized text for front-end speech recognition.

*Administrator User*

This user type provides access to the Administration Console and administration features within the Fusion Narrate client. An Administrator user can be defined with one of the following three roles:

- *Read-only*: Full read access to the Administration Console.
- *Customer Administrator*: Full read/write access to the Administration Console. This role is required to manage users.

Users with the Read-only or Customer Administrator roles have access to historical dictation and recognized texts up to the configured retention period. Most Fusion Narrate customers do not require any users with these roles as Technical Support will manage administrative tasks for the customer.

- *Shortcut Designer:* Full read/write access to organization and individual user shortcuts for management purposes.

### Microsoft® Active Directory (AD) Integration

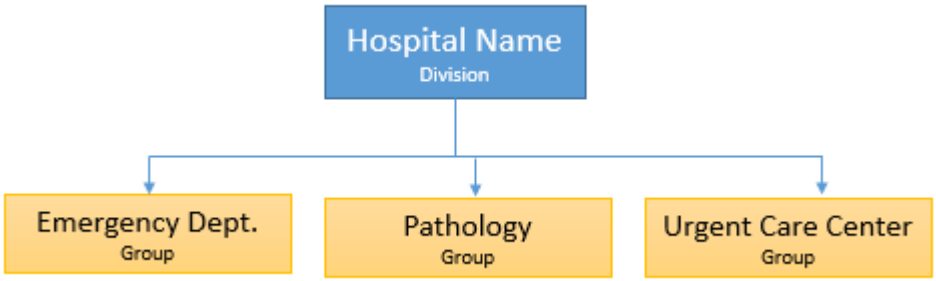
The Fusion Narrate client application supports Microsoft® AD authentication. However, AD cannot be used to control privileges and roles within the Fusion Narrate client or Administration Console.

### User Account Deletion

An Administrator can also disable or delete user accounts in the Administration Console in accordance with the customer's policies. If a user is deleted, then all associated dictated audio and text data is permanently deleted.

### Hierarchy

A customer's User Accounts can be organized into groups. Administrator access can be restricted to specified groups. For example, a customer could organize its users into multiple groups representing different departments or locations, such as the following:




### Password Settings

The Fusion Narrate client applications require username and password to sign-in. There are several options for 3rd party authenticators and single sign-on where the following password policies do not apply. See the *Authentication and Single Sign-On* section for more information.

The system provides the following configurable Client User password policies:

*Strength Settings*:

- Strong: Requires at least 8 characters and must contain lowercase, uppercase, a number and a symbol.
- Medium: Requires at least 7 characters and must contain a letter and number.
- Weak: Requires at least 1 character.

*Require Password Change on Initial Login:* A user's initial password must be set by an Administrator.

*Password History:* Prevents the user from using a previous password, with a configurable history count.

*Auto Lockout*: Automatic account lockout after a configurable number of failed attempts. When an account is locked it is unavailable for 15 minutes or until the password is reset. If the user attempts to login again without resetting the password during the 15-minute lockout period, the timer is reset, and another 15-minute lockout begins.

*Password Expiration*: Configurable number of days before requiring users to change a password.

Administrator Users are required to have a minimum of medium for password strength, history count of 5, lockout of 5 attempts, and max password age of 90 days.

Passwords are encrypted with a one-way hash using SHA-256 and salt using SHA1PRNG secure random number generation algorithm with 1000 iterations. This is done in accordance with OWASP guidelines. Existing passwords are not visible to any users or an Administrator.

Administrators can reset passwords if required. Users can self-reset passwords with a link that is sent to their configured email address.

### Inactivity Timeout

The system provides a configurable number of minutes before the Fusion Narrate client application will auto logout the user from the application. Inactivity is defined by no mouse, keyboard, or recording activity.

Administration Console sessions automatically log out after 30 minutes of no interaction.

### Multi-Factor Authentication

Multi-factor authentication (MFA) together with username and password is supported for the Administration Console. MFA utilizes Duo but is compatible with other authentications as well. MFA is not supported for the Fusion Narrate client or mobile applications.

## FUSION NARRATE CLIENT APPLICATION SECURITY

The Fusion Narrate client is a Windows® desktop application. It is developed using the Microsoft® .NET Framework. All security-related features and changes are reviewed by the product management team and tested by the QA team. Top OWASP desktop application security risks are understood and used as a guideline by the team throughout the development cycle.

### Windows® Security

The Fusion Narrate client application is compatible with anti-virus and anti-malware software packages. Please see the online Help documentation for recommendations on exclusion settings to ensure optimal performance.

It is the customer's responsibility to apply operating system security patches which include Microsoft® .NET Framework updates.

### Software Distribution and Updates

Fusion Narrate client binaries and MSIs are digitally signed with a certificate issued by DigiCert EV Code Signing CA (SHA2). The software is an XCopy based installation and does not require write access to any system areas of the operating system or elevated privileges to operate.

The client application can be installed via web link (app.fusionnarrate.com), MSI, or XCopy. Neither the web link nor XCopy installation methods required local admin privileges. All installation methods provide an option for automatic software updates after the initial installation via the Fusion Narrate Download Server. Major updates are typically released every 4 to 8 months and minor updates are typically released every 4 to 6 weeks. Customers on manual updates are notified via email and application notifications when major updates are available.

### Authentication and Single Sign-on

The Fusion Narrate client application supports a variety of authentication methods. These do not apply to Fusion Narrate mobile applications, which only support Standard Authentication. The Fusion Narrate Recorder mobile application supports facial recognition as an alternative authentication after initial Standard Authentication.

*Standard Authentication:* Users are prompted for a Fusion Narrate username and password, and the password is maintained and stored on the Fusion Narrate server platform. See the *Password Settings* section for more information.

*Windows® Trusted Security*: This is the most common method of single sign-on where the Fusion Narrate client will automatically authenticate using the Windows® logged-in credentials. In this model, users do not need to enter credentials into the Fusion Narrate application.

*3rd Party:* Users can sign-in to Fusion Narrate with industry standard authenticators using OpenID Connect over OAuth 2.0. Standard options are Microsoft® (Microsoft® Azure AD), Google (e.g., a Gmail account), and Okta (organization identity management service). All options require that the user's Fusion Narrate username matches the 3rd party authenticator or a configured preferred username for Fusion Narrate. Once authenticated with this method, Fusion Narrate will continue to sign-in with this method for the current Windows® user until the authentication token expires.

*LDAP Security:* The Fusion Narrate client can prompt and validate credentials against an LDAP / Active Directory server. In this model, users must enter credentials into the Fusion Narrate application.

*User Sync:* The Fusion Narrate client automatically syncs user credentials with another application (e.g., EHR, LIS, RIS). In this model, users do not need to enter credentials into the Fusion Narrate application. This requires setup work in the other application.

Windows® Trusted Security, LDAP, and User Sync authentication required a site-specific API Key to be assigned and installed. More details can be found in the Fusion Narrate online Help.

The Administration Console and mobile applications only support Standard Authentication.

Users can log into the Fusion Narrate clients from multiple devices at the same time. However, the system protects against unexpected single user usage by only allowing up to three simultaneous dictations.

## MOBILE APPLICATIONS

There are three types of mobile applications designed for use with Fusion Narrate: Wireless Microphone, Speech Keyboard, and Fusion Narrate ACI Recorder. These applications have the following official names and can be installed from the Apple® App Store or Google Play Store.

- Wireless Microphone
  - IOS: “nVoq Wireless Microphone”
  - Android: “nVoq Wireless Microphone”
- Speech Keyboard
  - iOS: “Fusion Narrate Keyboard”
  - Android: “nVoq.Mobile Voice”
- Fusion Narrate ACI Recorder
  - iOS: “Fusion Narrate Recorder”
  - Android: “Fusion Narrate Recorder”

The mobile applications require Standard Authentication (username and password) to utilize. They are developed in compliance with OWASP Mobile Application Verification Standard L1. The Wireless Microphone and Speech Keyboard do not provide access to any sensitive or patient information.

There are no known incompatibilities with deploying via Mobile Device Management (MDM) platforms, but these solutions are not directly tested or supported. When installed, users are prompted to allow for the minimum device access privileges needed, such as microphone access.

## DATA STORAGE AND RETENTION

The Fusion Narrate application is designed as a tool to enable insertion of the patient narrative into a customer’s application (e.g., EHR, LIS, RIS); it is not intended to function as a record repository. This section describes the categories and configurable retention settings for data stored on the Fusion Narrate speech recognition servers. *To avoid the unnecessary retention of data, it is recommended that customers configure the system to purge audio and speech recognized text frequently, at intervals no greater than 30 days.* Data that is beyond the configured retention period is automatically deleted nightly.

It is possible to set the retention period to 0 days if only front-end speech recognition is in scope. Setting the retention to 0 days means audio and text is never stored on the server. While this configuration is supported, it is not recommended since it significantly impedes the ability for Technical Support to troubleshoot reported speech recognition issues and it does not allow for sentence model training of a user’s speech profile.

### Front-End Speech Audio and Recognized Text

Audio received from the client devices is processed on the speech servers and the recognized text is returned. The system does not associate a dictation to any particular patient or visit. This dictation and the recognized text is available to Administrators from the Administration Console up until the configured retention period.

In addition, audio and recognized text may be periodically collected, de-identified, and pulled into a system-wide aggregated audio and text corpus. All user demographics associated with this data are removed. This de-identified data set is used to train acoustic profiles and language models for continual improvement to speech recognition accuracy. Customers may opt-out of contributing de-identified data to the aggregated corpus.

### Language Modeling Data

The Fusion Narrate platform delivers highly accurate speech recognition without any training. For most users this is sufficient. However, the system also provides the ability to tune the language models for the various topics with text data to improve speech recognition accuracy. This is called sentence modeling. Sentence modeling data can be gathered in two ways.

- *Review and Correct*: This is the process of reviewing recognized texts in the Administration Console, correcting any recognition errors, and saving the corrected texts as part of the data used to improve a user's language model. These texts are stored on the speech servers and are retained until the associated user's account is deleted. If users dictate PHI, it is standard practice to exclude it from any saved text for sentence modeling for added security and since this content is not helpful to the learning process. This process can be performed by a Customer Administrator, Technical Support, or as part of the Accuracy Optimization Service (AOS) add-on.

- Importing: Representative texts can be imported for an individual or group of users. It is recommended that customers redact any PHI from any imported text prior to submission. Sentence Modeling data is retained on the speech servers until manually deleted or until the associated groups or individual accounts are deleted. This import process can be performed using the Administration Console.

### Administration Data

The deletion of administration data, such as users and organizations, results in a soft delete. In other words, the user and organization information are no longer visible in the Administration Console, but their configuration and associated transaction data are still in the database. This is primarily for billing and reporting purposes.

### Backups

All data has the possibility of existing one year after purging from primary storage as it is aged out of system backups. Backups are stored on AWS S3 and encrypted.

### Data Access

All server data storage (database and AWS S3) is located behind firewalls and is not publicly accessible. Data can only be accessed through authenticated use of the platform's web APIs which are used by the various client applications.

## DATA CENTER AND HOSTING SECURITY

### Fusion Narrate Data Center

**United States**

The Fusion Narrate speech recognition platform servers and storage are managed within AWS and are built with full redundancy across two AWS regions (Oregon and Virginia) with access managed through the AWS Global Accelerator and AWS Load Balancer. The Fusion Narrate Download, Fusion Narrate CAPD, Fusion Narrate ACI, and Fusion Narrate AI Assist servers are managed in the United States within the AWS Ohio Region across multiple availability zones using the AWS Load Balancer. These servers are managed and supported by the vendor operation teams, exclusively within the United States.

**Canada**

The Fusion Narrate speech recognition platform servers and storage are managed within AWS and are built with full redundancy across multiple availability zones in the AWS Canada Central region using the AWS Load Balancer. The Fusion Narrate Download, Fusion Narrate ACI, and Fusion Narrate AI Assist servers that are managed in the United States also serve Canada. A separate installation of the Fusion Narrate CAPD servers is hosted in Canada. These servers are managed and supported by vendor operation teams that exist in a combination of the United States and Canada.

**Security Measures in Both United States and Canada**

The following security measures protect the cloud environment:

- Required MFA authentication for vendor personnel to access the servers.
- Monthly patching of servers.
- Intrusion detection systems, threat protection systems, and penetration testing.
- Traffic restricted to required ports and protocols.
- Web application firewalls to filter and sanitize application requests.
- DDoS protection with AWS Shield.
- Industry standard best practices such as network segmentation, anti-virus, and network perimeter firewalls.
- Threats monitored at the network level and alerts automatically sent to the operations team.
- Separated production, test, and development environments.
- Internal and external quarterly vulnerability scans.
- Annual independent 3rd party evaluations of external security posture through penetration testing.

**Additional Information**

In addition to the above security measures that are employed, see AWS Compliance documentation for more information.

### Backups and Recovery

Full system backups are performed nightly with additional periodic incremental backups.

The Recovery Point Objective (RPO) is 24 hours. Since audio and text data are only stored on the platform for troubleshooting and speech profile training purposes, loss of data has no impact to users.

The Recovery Time Objective (RTO) is 8 hours.

### Hosted Server Platform

An annual 3rd party SOC 2 Type 2 audit is performed against the speech recognition platform covering the areas of Security, Availability, Confidentiality, and Privacy with enhanced reporting for related aspects of HIPAA in accordance with the AICPA's AT-C315 Attestation and the Trust Service Criteria for Security. This audit also covers the security controls for the Personal Information Protection and Electronic Documents Act (PIPEDA) for Canada. An attestation letter from the auditor is available upon request.

3rd party testing is conducted against the server platform web APIs using automated scanning tools paired with expert knowledge to conduct a manual security analysis. Attempts are made to exploit and gain unauthorized access to data through misconfigurations and vulnerabilities in three phases: Black Box, Gray Box, and White Box. This testing includes numerous attacks including OWASP leading application layer threats.

3rd party penetration testing is performed at least annually.

Application endpoints (healthcare.nvoq.com and app.fusionnarrate.com) are rated A+ per SSL Labs automated analysis tools.

Static Application Software Testing (SAST) tools are employed to potential security issues and, additionally, Dynamic Application Software Testing (DAST) is employed regularly (typically monthly).

Note that this audit does not include the Fusion Narrate Download Servers, Fusion Narrate CAPD Servers, Fusion Narrate ACI Servers, or the Fusion Narrate AI Assist Servers. Work is underway to prepare for a SOC 2 Type 2 audit of these environments. Note that these servers are hosted in a secure AWS environment that undergoes regular SOC 2 Type 2 audits. See AWS SOC FAQs for more information.

# SYSTEM AUDITING

System audit logging is performed on both the client application workstation and the speech servers.

### Fusion Narrate Client Application

The client logs record many application events which include:

- Log in, failed log in attempts, and log out
- Starting and ending a dictation
- Shortcut edits and execution
- Setting changes

Additionally, these logs capture the current user's settings and some client device and microphone information.

### Fusion Narrate Speech Servers

Interactions with the speech servers from client applications are also logged. The following events are available for viewing from the Administration Console:

- Starting and ending a dictation
- Shortcut execution
- Log in and log out events
- Last activity timestamp
- Workstation and Fusion Narrate version used

Security audit queries can be performed to gather the following events upon request.

- Changes to organizations and users
- Anyone who accesses a page that includes audio recordings and/or recognized text, for example, the Review and Correct web page
- Account password changes

### Fusion Narrate CAPD Servers

The Fusion Narrate CAPD servers store user information about each text that is processed, including username, date time stamp, and any notifications that were presented to the user.

### Fusion Narrate AI Assist Servers

The Fusion Narrate AI Assist servers store user information about each request that is processed, including the username, date time stamp, and provided prompt.

## SHORTCUTS

In addition to speech recognition, a core feature of the Fusion Narrate client application is to provide users the ability to automate redundant tasks such as inserting text and templates, clicking buttons, and pressing keystrokes. Fusion Narrate also provides more advanced shortcuts using scripting and browser automations. Typically, anything that a user can manually do in an application can be performed using the Fusion Narrate application with an assigned voice command, microphone button, or function key.

Administrators can create and manage shortcuts for the entire organization. Shortcuts can be created at the organizational and individual user level. Client Users can only create shortcuts at the individual user level but can make use of organizational shortcuts.

The Fusion Narrate client does not place restrictions on what a user can do with a shortcut. It is up to each customer to set guidelines for what they allow users to automate. Administrators can place restrictions on users regarding the types of shortcuts they can create and edit. For example, users may be restricted from creating scripting type shortcuts.

Each time a shortcut is performed, the action is recorded for auditing purposes. Administrators can run reports to review the shortcuts a user is performing. Fusion Narrate does not have knowledge as to what a button or keystroke may do in an application and thus the result of shortcut actions is not logged, nor can it be determined whether a shortcut performed the desired action.

## VIRTUAL DESKTOP INFRASTRUCTURE (VDI)

The Fusion Narrate client application can be installed on client workstations as well as on Microsoft® RDS, VMware Horizon, and Citrix servers. In most cases the Fusion Narrate client is installed on the workstations to provide users the best performance and most flexible use of the product.

Ordinarily, when both the Fusion Narrate client and the target application (e.g., EHR, LIS, RIS) run on the workstation, Fusion Narrate automatically provides Direct Editor mode integration with many text editors. This mode provides improved cursor context, faster insertion of text, advanced voice commands, and field navigation.

When the target application runs on an RDS or Citrix server, it is required to install the *Fusion Narrate Virtual Direct Server* service on the RDS or Citrix server to provide this same level of integration. This component is a lightweight application that runs as a service on the server. It does not have a user interface, it does not handle audio, and it does not communicate to the Internet. Its purpose is to communicate with the Fusion Narrate client over an established RDS or Citrix virtual channel to provide speech recognition integration with the current text field.

## SYSTEM MAINTENANCE

Periodically, software updates are applied to the server platforms. This could be in the form of product updates, security updates, and general operating system updates. Since the system is designed with a fully redundant architecture, these updates typically do not require downtime for end users. This ensures 99.9% uptime.

If desired, administrators can subscribe to system update and maintenance notifications at status.nvoq.com. This site also provides historical uptime reports and root cause analysis for any unexpected platform outages.

## TECHNICAL SUPPORT

We strive to deliver the best Technical Support of any speech recognition system in the industry. This is demonstrated in our consistently high KLAS® scores and positive customer comments. Technical Support is delivered in many forms: installation, training, configuration assistance, shortcut creation, and issue resolution. It can be accessed in a variety of ways:

- Email
- Telephone
- In App Contact Us Form
- Online Help with Contact Us Form

For the United States system, all Technical Support representatives are in the United States. For the Canada system, all first tier Technical Support representatives are in Canada, with second tier Technical Support located in the United States.

It is sometimes necessary to utilize desktop sharing tools such as Microsoft® Teams to train users and troubleshoot Fusion Narrate client issues. This is scheduled on an as needed basis with the approval of the customer.