FUSION NARRATE® SECURITY BRIEF

DECEMBER 2022

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 Fusion Narrate CAPD™ module for clinical documentation improvement (CDI) as well as the Fusion Narrate Text™ premise-based solution for back-end transcription. This document provides information on the security features of the 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").

Dolbey understands that performance and robust security must go hand-in-hand. 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.

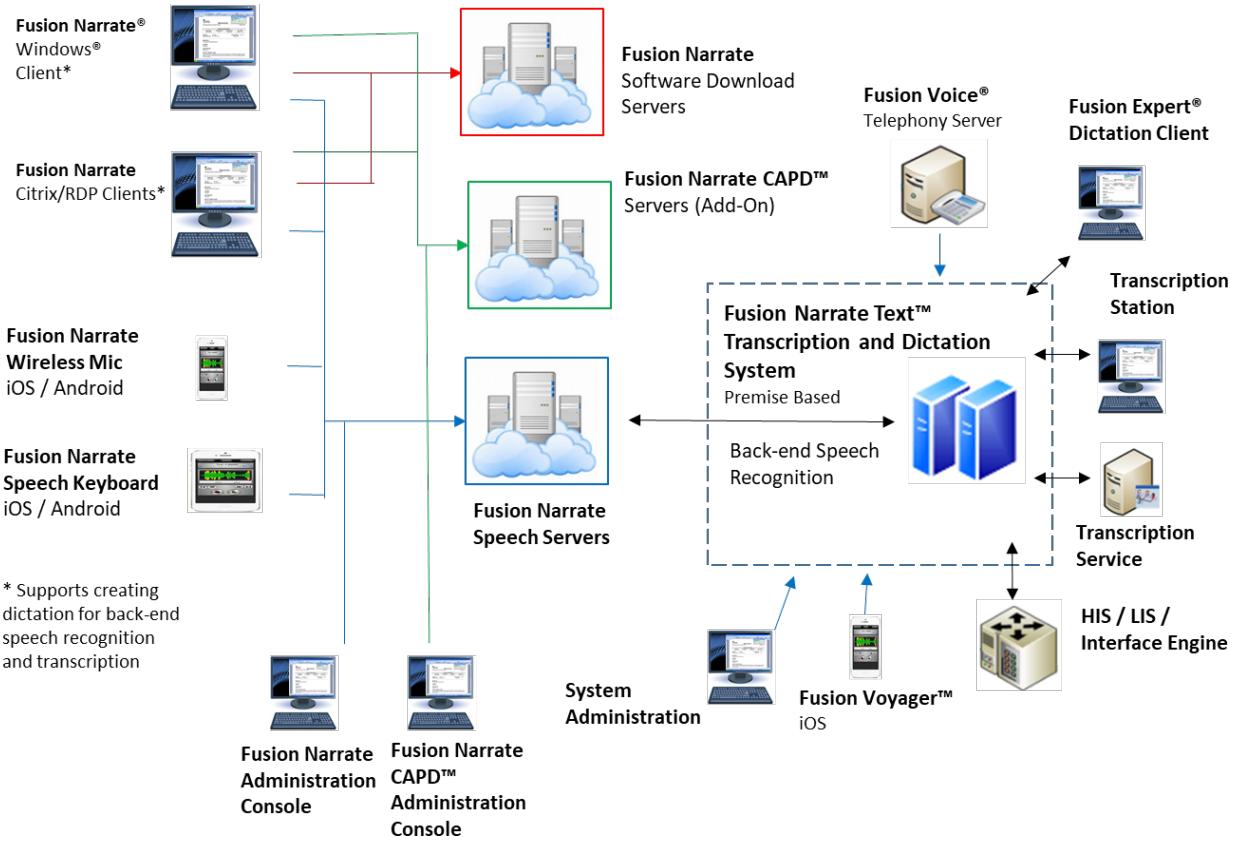
This document first provides a general system overview, followed by a summary of the flow of PHI within the platform. Finally, we summarize the following security features:

- Data Encryption
- User Accounts and Password Management
- Client Software Security
- Data Storage and Retention
- Data Center Security and Backups
- System Auditing

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

SYSTEM ARCHITECTURE

The following diagram provides an overview of the system architecture for the entire suite of products comprising the Fusion Narrate platform.



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

The Fusion Narrate Text system is an add-on premise-based transcription software solution that incorporates back-end speech recognition, dictation workflow, output distribution and a host of other features. Security topics for this system are covered in separate documentation available upon request.

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.

In order to minimize capture and retention of PHI with in the Fusion Narrate platform, Dolbey recommends that customers train their users to avoid dictating PHI into the system whenever possible.

Fusion Narrate Client

In standard use cases, the Fusion Narrate client does not interface with or provide access to patient record data that may reside in customer's other applications, such as an EHR. 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. 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 audio file 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 (such as an EHR or LIS) that already includes the patient identifying information; the provider does not need to dictate a patient name or identifying number when documenting the patient encounter or results. This audio is streamed to the Fusion Narrate cloud-based speech recognition servers. The Fusion Narrate client application does not store audio on the client device and does not provide user access to past audio recordings stored on the speech servers. The Fusion Narrate client also analyzes text areas of the screen to build a speech grammar of the identified words for advanced select and say commands (i.e. 'SELECT headache'). These grammars together with the spoken audio commands are submitted to the speech servers for recognition. It is possible that these grammar files may contain fragments of PHI. Advanced select and say can be disabled upon request.

Back-End Speech Recognition: The optional Fusion Narrate Text premise-based transcription module allows users to dictate a report for transcription. The captured dictation is sent to the Fusion Narrate cloud-based speech recognition servers as an audio file, processed through back-end speech recognition, and then transmitted to the Fusion Narrate Text system located on the customer's network for a transcriptionist to review and correct as necessary. Customers using the Fusion Narrate Text module may configure the Fusion Narrate client to prompt the provider for a patient identifier such as an MRN that can help automate the lookup process for the transcriptionists. Additionally, when dictating for back-end transcription, providers sometimes dictate patient identifying information so that the transcriptionists can confirm the patient information. Dictation audio files for the Fusion Narrate Text module are temporarily stored on the client device until transmitted to the cloud-based speech recognition servers, and are then removed from the client device. Optionally, the system can be configured to retain a configurable number of days of dictations locally, allowing for an administrator to recover and resubmit a dictation if needed. Also, the Fusion Narrate client can be configured to allow the user to see a list of their past dictations on the server and to listen to them.

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 such as the EHR. 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 where no PHI is logged. A higher logging level may be enabled temporarily for troubleshooting an issue; at these levels, it is possible 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
- Advanced select and say speech grammars
- Client log data which can be uploaded to the servers from the Fusion Narrate client upon request for technical support purposes, which may contain PHI if higher level logging is enabled
- Language modeling data that can be imported for sentence modeling
- Demographic data provided by a user when creating a standard dictation for submission to transcription, which may contain PHI depending on how the Fusion Narrate Text client is configured

The Administration Console is also used to perform a variety of management functions including managing users, shortcuts (i.e. voice commands), custom vocabulary, groups, and reporting tools.

Fusion Narrate Wireless Microphone

This is a smart phone 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 stored on the device.

Fusion Narrate Speech Keyboard

This is a smart phone application for iOS and Android that can be used in place of the built-in operating systems' keyboard. It allows the provider to use speech recognition to quickly insert text into other mobile applications. Similar to that of the Fusion Narrate workstation client, this mobile application streams dictated audio to the speech recognition servers which return the recognized text. Audio is not stored on the device. 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 are separate from the Fusion Narrate speech recognition servers and run on a different cloud hosting platform. The Fusion Narrate CAPD servers receive text from the Fusion Narrate client, process the text, and return back recommendations for documentation improvements. The text received may contain PHI, but the received text is not stored on the Fusion Narrate CAPD servers.

On occasion it may be necessary for Dolbey technical support to enable detailed logging on the Fusion Narrate CAPD servers to diagnose an issue. These detailed logs would contain the text received from the client, and thus could contain PHI. This information is only retained on the Fusion Narrate CAPD servers for the necessary time to troubleshoot and resolve an issue.

Fusion Narrate Text Premise Based System

The Fusion Narrate Text system is a premise-based transcription system that receives back-end speech recognized dictations from the Fusion Narrate speech recognition servers. The Fusion Narrate Text system stores the audio dictations and associated recognized text, the transcribed reports, and any associated identifying information which the provider is prompted to provide per the customer's configuration. PHI may be included in this data. Security topics for this system are covered in separate documentation available upon request.

DATA ENCRYPTION

Data in Transit

All data transmitted between the client applications, the Fusion Narrate speech recognition servers, and the Fusion Narrate CAPD servers uses TLS 1.2 with 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 and the Fusion Narrate CAPD servers, including log files, is encrypted with AES 256-bit encryption. Encryption within the Fusion Narrate Text premise-based system is covered in separate documentation available upon request.

On the client device, all data stored by the Fusion Narrate client application is encrypted using AES 256-bit encryption, including 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.

User Account Types

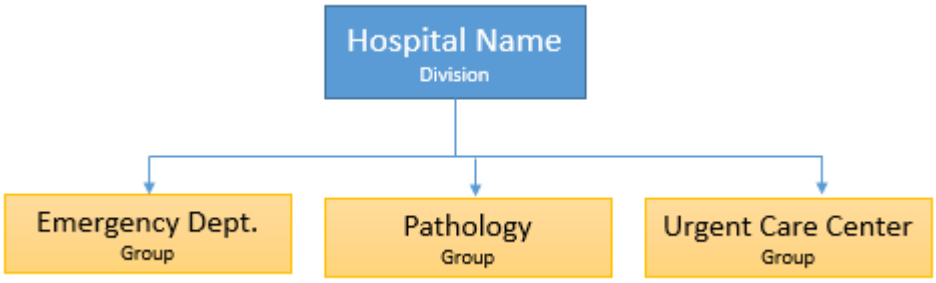
Client User: Provides access to use the Fusion Narrate clients and not the Administration Console

Administrator: Provides access to the Administration Console and optionally the Fusion Narrate clients. Administrators can be defined as one of the following roles:

- *Read-only*: Full read access to the Administration Console.
- *Shortcut Designer:* Full read/write access to organization and user personal shortcuts for management purposes.
- *Customer Administrator*: Full read/write access to the Administration Console.

Hierarchy

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



Password Settings

The system provides the following configurable 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

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.

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

Client Inactivity Timeout: Configurable number of minutes before the client will auto logout the user.

All passwords are encrypted during transmission and at rest. User passwords are not visible to Administrators.

Administrators can reset passwords if required. Administrators can also disable or delete user accounts in accordance with the customer's policies.

Passwords are stored in hashed format.

MFA

Multi-factor authentication is not supported for the Fusion Narrate client. Multi-factor authentication is supported for the browser-based Administration Console.

Fusion Narrate Text Premise Based System

Usernames and passwords for the Fusion Narrate Text system are maintained in the premise-based SQL Server database. This system also includes standard application security settings such as password expiration, strength, auto lockout, inactivity, and password history settings.

CLIENT SOFTWARE SECURITY

All client software access requires a unique user name and password.

The customer can elect to use third party anti-virus and anti-malware software packages in conjunction with the client applications. Please see the online help documentation for recommendations on exclusion settings to ensure optimal performance.

Fusion Narrate client executables are digitally signed with a VeriSign security certificate. The software is an XCopy based installation and does not require write access to any system areas of the operating system or elevated privileges in order to install or operate.

Single Sign-on

The Fusion Narrate client supports several methods of single sign-on (SSO).

Windows Trusted Security: This is the most common method whereas 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.

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, such as an EHR or LIS system. In this model, users do not need to enter credentials into the Fusion Narrate application.

All models of single sign-on required a site-specific API key to be assigned and installed.

More details can be found in the Fusion Narrate online help.

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 (such as an EHR or LIS); 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, Dolbey recommends that customers configure the system to purge audio and speech recognized text frequently, at intervals no greater than 30 days.*

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. This audio and the recognized text is available to administrators from the Administration Console for a

configurable period of time, after which it is purged. In addition, audio and recognized text is periodically collected, anonymized, and pulled into a system-wide aggregated audio and text corpus. This anonymized data set is used to train acoustic profiles and language models for continual improvement to speech recognition accuracy. Customers may opt-out of contributing anonymized data to the aggregated corpus, but this may result in smaller improvements over time.

Back-End Dictation Audio and Recognized Text

Dictation recorded for back-end transcription, and the associated recognized text, is available to administrators from the Administration Console. Additionally, any demographic data such as MRN that the provider may have been prompted for is stored with the dictation record on the speech servers. By default, this information is hidden in the Administration Console, but could be configured to be visible. The audio and text can be configured to purge at the same intervals as the speech audio and recognized text described above. The final transcribed text (i.e. the corrected text) is sent back to the speech servers and added to the dictator's sentence model data to provide for a continuous improvement feedback loop. As with front-end speech recognition, this audio and text is anonymized and included in the audio and text corpus; this is the recommended approach as it helps improve speech recognition accuracy over time. Upon request, audio and recognized text records can be configured to purge immediately after being pulled into the premise-based Fusion Narrate Text transcription system. The demographic data associated with the records can be configured to purge at the same intervals as the audio and recognized text, or more frequently if desired.

Language Modeling Data

The system provides the ability to tune the language models for the various topics with text data in order to improve speech recognition accuracy. This can be performed in two different ways from within the Administration Console: Accuracy Optimization Services (AOS) and Sentence Modeling.

- AOS is an optional 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, then the audio and associated texts could contain PHI; however, Dolbey recommends that users avoid dictating PHI whenever possible.

- Sentence Modeling data is automatically collected from front-end speech recognition dictations that are corrected in the Administration Console and from back-end speech recognition dictations where the corrected text is received from the Fusion Narrate Text system after transcription. Optionally, representative texts can be imported for an individual or group of users using the Administration Console. Dolbey recommends 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.

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 it is purged from primary storage as it is aged out of system backups.

DATA CENTER SECURITY

Fusion Narrate Data Center

The Fusion Narrate speech recognition servers are managed within AWS in the United States and in Canada for the Canadian Fusion Narrate install. The speech recognition software solution is managed and supported by the nVoq engineering team, exclusively within the United States. The following security measures protect the cloud environment:

- Required two-factor authentication for nVoq 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.
- 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.

Annual SOC 2 Type 2 examinations are conducted, covering the areas of Security, Availability, Confidentiality, and Privacy with enhanced reporting for related aspects of HIPAA.

The system employs a load balanced n+1 horizontally scalable web architecture with a hot standby data center at a different geographic location. Production data is replicated in real-time to the hot standby data center. Full nightly backups are performed with copies stored in multiple secure locations.

Fusion Narrate CAPD Data Center

The Fusion Narrate CAPD servers are housed in a secure data center located in the United States, and are backed up at another US location for disaster recovery purposes. These servers are managed within AWS. The following security measures protect the cloud environment:

- Required two-factor authentication for Dolbey 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.
- 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.

The Fusion Narrate CAPD solution leverages AWS's secure cloud platform. A third-party security review was completed with all risks addressed. Third-party penetration testing of the Fusion Narrate CAPD production system is performed monthly. This testing includes numerous remote and local attacks as well OWASP leading application layer threats.

The system is designed with auto failure such that if the primary servers are unreachable, clients are automatically directed to the secondary servers. Backups are retained for 1 year.

SYSTEM AUDITING

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

Fusion Narrate Client

The client logs record many application events which include:

- Log in, failed log in attempts, log out
- Inactivity timeouts
- Starting and ending a dictation
- Shortcut 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
- Last activity timestamp

nVoq also can run Security Audit Queries on the following events which covers Administration Console and client activities.

- Log in and failed log in attempts
- Changes to organizations and users
- Anyone who accesses a page that includes audio recordings and/or transcripts, for example, the Review and Correct page
- Account password changes

Fusion Narrate CAPD Servers

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